Министерство науки и высшего образования РФ

ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

А.А. Конев, А.Ю. Якимук

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебно-методическое пособие
для студентов направлений подготовки
10.00.00 Информационная безопасность

Томск, 2022

УДК 004.056
ББК 32.973.26-018.2
К 64

Конев А.А., Якимук А.Ю.
К 64 Управление информационной безопасностью: учебно-методическое пособие. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 124 с.

Настоящее учебно-методическое пособие содержит описания лабораторных, практических и самостоятельных работ по дисциплине «Управление информационной безопасностью» для направлений подготовки, входящих в укрупненную группу специальностей и направлений 10.00.00 Информационная безопасность.

УДК 004.056
ББК 32.973.26-018.2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью преподавания дисциплины является овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

Задачи изучения дисциплины – получение студентами:

– знаний о структуре и принципах построения политики информационной безопасности организации;

– умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации;

– знаний об основных методах контроля обеспечения информационной безопасности в организации.

ЛАБОРАТОРНАЯ РАБОТА №1
Анализ рисков информационной безопасности на основе построения модели информационных потоков

1 Цель работы

Целью данной лабораторной работы является практическое изучение анализа рисков информационной системы на основе программного продукта ГРИФ 2006 из состава Digital Security Office.

2 Краткие теоретические сведения

Система ГРИФ 2006 предоставляет возможность проводить анализ рисков информационной системы при помощи анализа модели информационных потоков, а также, анализируя модель угроз и уязвимостей - в зависимости от того, какими исходными данными располагает пользователь, а также от того, какие данные интересуют пользователя на выходе.

При работе с ***моделью информационных потоков*** в систему вносится полная информация обо всех ресурсах с ценной информацией, пользователях, имеющих доступ к этим ресурсам, видах и правах доступа. Заносятся данные обо всех средствах защиты каждого ресурса, сетевые взаимосвязи ресурсов, а также характеристики политики безопасности компании. В результате получается полная модель информационной системы с точки зрения информационной безопасности 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.

Основные понятия и допущения модели:

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

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

Отдел - структурное подразделение организации.

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.

Средства защиты рабочего места группы пользователей - средства защиты клиентского места пользователя, т.е. 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. Т.е. объект, к которому осуществляется доступ. Исходя из допущений данной модели, вся информация является ценной, т.к. оценить риск неценной информации не представляется возможным.

Средства защиты - средства защиты ресурса, на котором расположена (или обрабатывается) информация и средства защиты самой информации, т.е. применяемые к конкретному виду информации, а не ко всему ресурсу.

Эффективность средства защиты - количественная характеристика средства защиты, определяющая степень его влияния на информационную систему, т.е. насколько сильно средство влияет на защищенность информации и рабочего места группы пользователей. Определяется на основе экспертных оценок.

Базовая вероятность (конфиденциальности и целостности) - вероятность реализации угрозы (конфиденциальности или целостности) без применения средств защиты, т.е. максимальная вероятность реализации угрозы. Вероятность реализации угрозы (конфиденциальности или целостности) без применения средств защиты, т.е. максимальная вероятность реализации угрозы.

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.

Сетевое устройство - устройство, с помощью которого осуществляется связь между ресурсами сети. Например, коммутатор, маршрутизатор, концентратор, модем, точка доступа.

Контрмера - действие, которое необходимо выполнить для закрытия уязвимости.

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

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

3 Ход работы

3.1 Модель информационных потоков

Запустите ярлык «ГРИФ 2006» на рабочем столе. Для входа в систему под именем пользователя «user» используйте пароль «user».

В окне «Алгоритм анализа рисков» (рис. 1) выберите пункт «Анализ модели информационных потоков», создайте новый проект.

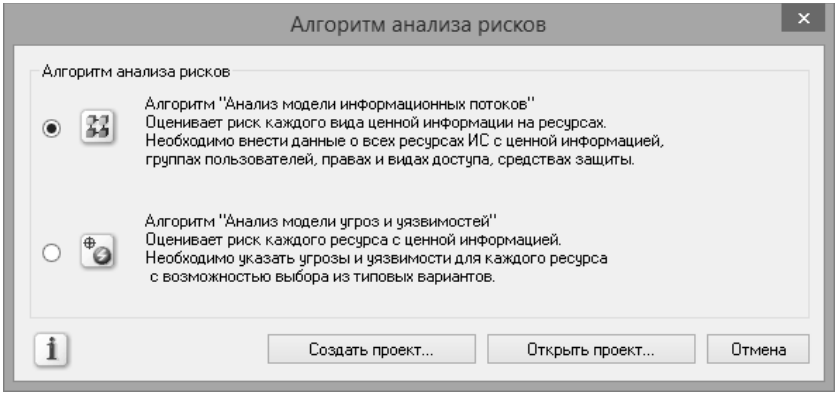


Рис. 1. Создание проекта

Шаг 1. На первом этапе работы с программой пользователь вносит все объекты своей информационной системы: отделы, ресурсы (специфичными объектами данной модели являются сетевые группы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

Шаг 2. Далее пользователю необходимо проставить связи, т.е. 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.

Шаг 3. На завершающем этапе пользователь отвечает на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

3.2 Модель информационной системы

Для начала работы необходимо иметь описание системы. Информационная система Компании состоит из одного отдела – бухгалтерии. Имеются сервер и рабочая станция, которые физически связаны между собой. На сервере хранятся два вида информации: бухгалтерский отчет и база клиентов; на рабочей станции. база данных наименований товаров с описанием. В компании есть три сотрудника: финансовый директор, главный бухгалтер, бухгалтер. К бухгалтерскому учету на сервере локальный доступ имеет главный бухгалтер, к базе клиентов удаленный доступ имеют бухгалтер (с рабочей станции через коммутатор) и финансовый директор. При чем финансовый директор имеет удаленный доступ через Интернет. К базе данных наименований товаров с описанием на рабочей станции локальный доступ имеет бухгалтер.

Для описания информационной системы существуют такие виды объектов, как отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы (рис. 2).

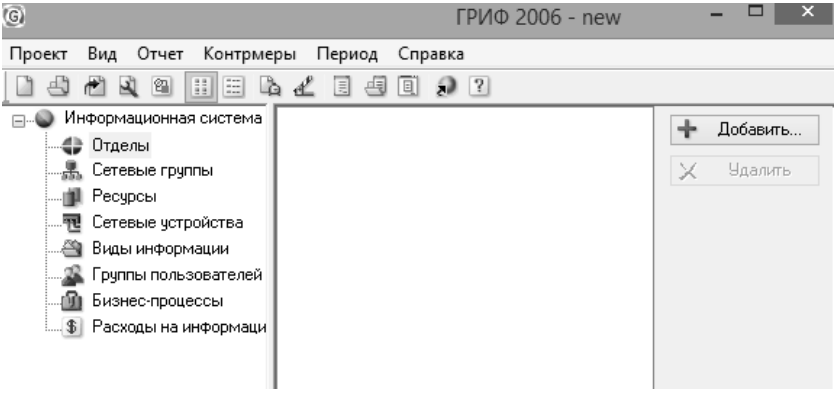


Рис. 2. Основное окно программы

Внесем входные данные. Так как, информационная система Компании состоит из одного отдела – бухгалтерии. В отделе имеется одна сетевая группа. Добавьте отдел «Бухгалтерия» и одноименную сетевую группу (рис.3).

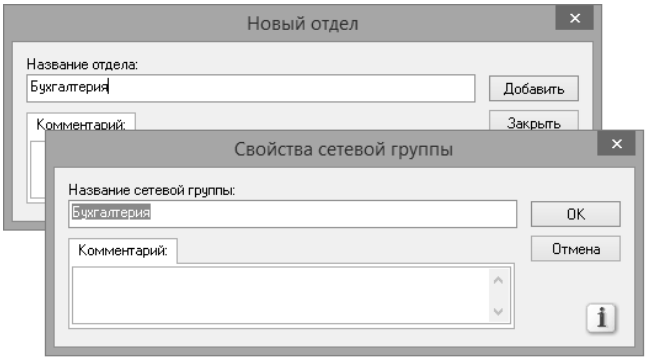


Рис. 3. Добавление нового отдела и сетевой группы

Информационная система содержит два ресурса: сервер и рабочую станцию, которые физически связаны между собой (находятся в одной сетевой группе).

Добавьте ресурсы «Сервер» и «Рабочая станция», указав тип ресурса (сервер, рабочая станция, мобильный компьютер, твердая копия, веб-сервер), сетевую группу и отдел, к которым принадлежит ресурс (рис. 4).

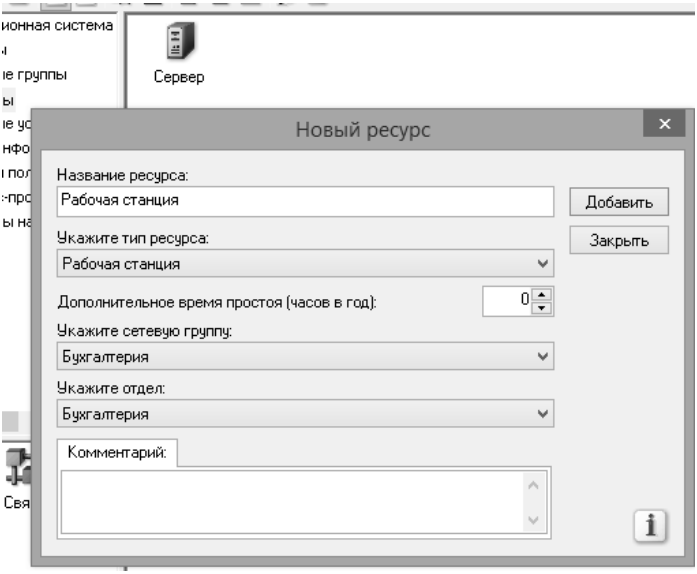


Рис. 4. Добавление нового сетевого ресурса

На сервере хранятся два вида информации: бухгалтерский отчет и база клиентов; на рабочей станции – база данных наименований товаров с описанием. Добавьте эти три вида информации аналогичным образом.

Рассмотрим трех сотрудников, каждый из которых отнесем к отдельной группе пользователей. Создайте группы пользователей: главный бухгалтер, бухгалтер и финансовый директор (рис. 5). При чем для финансового директора укажите класс группы пользователей «Авторизованные пользователи из Интернет» (так как у него должен быть удаленный доступ к базе клиентов компании), а для бухгалтеров – «Пользователи».

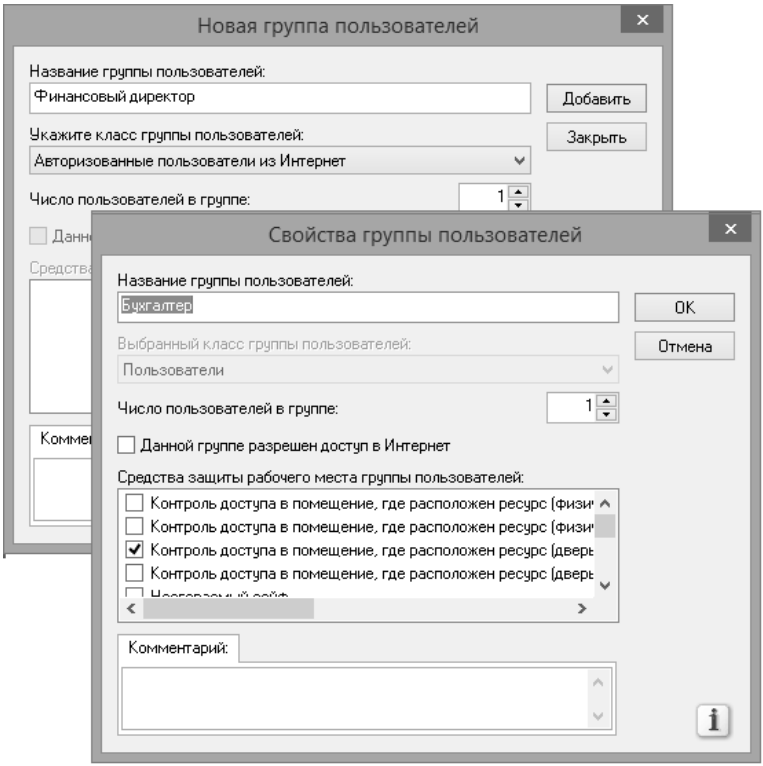


Рис. 5. Добавление новой группы пользователей

В зависимости от выбора класса будут предложены средства защиты рабочего места группы пользователей. Средства защиты клиентского места групп авторизованных Интернет-пользователей (здесь

- финансовый директор) оценить невозможно, т.к. неизвестно, откуда будут осуществлять доступ пользователи этой группы.

Для клиентского места бухгалтера укажите следующие средства защиты: контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение); средства антивирусной защиты (антивирусный монитор); отсутствие возможности подключения внешних носителей; персональный межсетевой экран; система криптозащиты электронной почты. То же самое проделайте и для клиентского места главного бухгалтера, отметьте разрешение доступа в Интернет.

К информации «бухгалтерский учет» на сервере локальный доступ имеет группа пользователей «главный бухгалтер».

К информации «база клиентов» на сервере удаленный доступ имеют группы пользователей «бухгалтер» (с рабочей станции через коммутатор) и «финансовый директор» (через глобальную сеть Интернет, как уже было указано).

К информации «база данных наименований товаров с описанием» на рабочей станции локальный доступ имеет группа пользователей «бухгалтер».

Соответственно, для полного описания информационной системы необходимо добавить сетевое устройство типа «коммутатор».

3.3 Связи

После добавления всех объектов в информационную систему, пользователю необходимо проставить связи, т.е. 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.

В левом нижнем поле основного окна выберите «Связи».

Для добавления к ресурсу «Сервер» двух видов информации (как указано выше) «Бухгалтерский отчет» и «База клиентов» необходимо в вкладке «Виды информации» кнопкой «Добавить» вызвать окно добавления вида информации, в котором в выпадающем меню выбрать требуемые пункты.

После выбора вида информации станет доступно поле «Ущерб по угрозам». Установите ущерб по угрозе «Конфиденциальность» - 100 у.е. в год, по угрозе «Целостность» - 100 у.е. в год, по угрозе «Доступность» - 1 у.е. в час для обоих видов информации (рис. 6).

В случае, если единицы измерения ущерба по угрозам отличны от у.е., откройте справку, найдите каким образом выбрать другие единицы измерения.

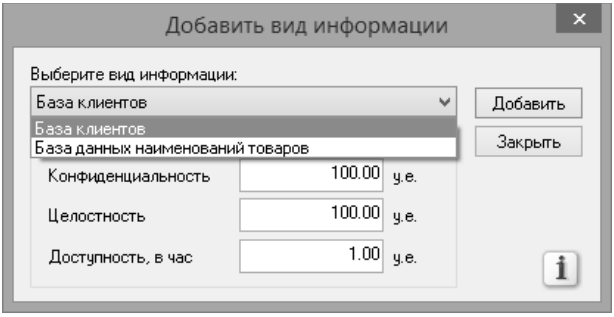


Рис. 6. Добавление вида информации к ресурсу

Проделайте аналогичные действия для ресурса «Рабочая станция» (вид информации – «База данных наименований товаров»; ущерб по угрозам в точности такой же, как и у других видов).

Перейдите на вкладку «Группы пользователей»

Укажите группы пользователей и их права на конкретный вид информации в соответствии с табл. 1.

Табл. 1 - 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	удаленный	чтение	есть	1
Финансовый директор / база клиентов	удаленный	чтение, запись	есть	1
Бухгалтер / база данных наименований товаров	локальный	чтение, запись, удаление	нет	1

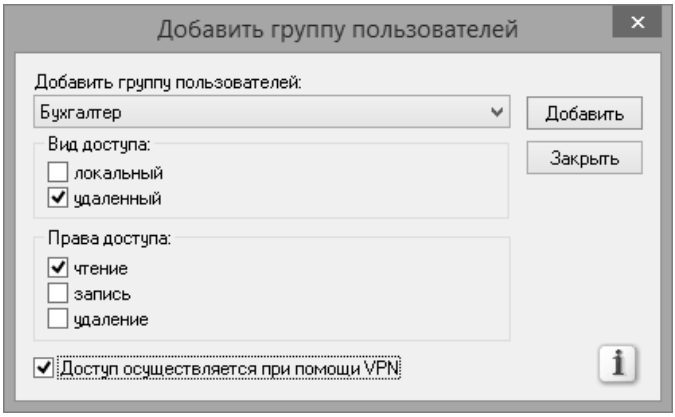


Рис. 7. Добавление группы пользователей и их права на конкретный вид информации

Во вкладке «Каналы связи» укажите, что группа пользователей «бухгалтер» имеет доступ к ресурсу «Сервер» через сетевое устройство «Коммутатор».

Чтобы указать средства защиты ресурса, перейдите на вкладку «Средства защиты», нажмите кнопку «Изменить» (рис. 8) и укажите для ресурса «Сервер» следующие пункты: контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение); отсутствие возможности подключения внешних носителей; межсетевой экран; обманная система; система антивирусной защиты на сервере; аппаратная система контроля целостности. Для ресурса «Рабочая станция» задайте средства защиты из шаблона (необходимо задать: контроль доступа в помещение, где расположен ресурс (дверь с замком, видеонаблюдение); средства антивирусной защиты (антивирусный монитор); отсутствие возможности подключения внешних носителей; персональный межсетевой экран; система криптозащиты электронной почты). Для этого в окне выбора шаблона выберите группу пользователей «Бухгалтер» (рис. 9).

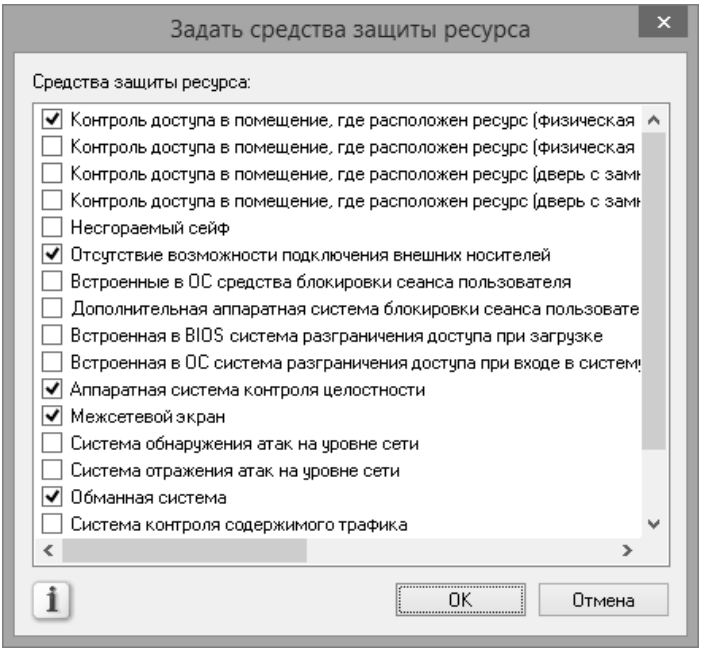


Рис. 8. Задание средства защиты ресурса

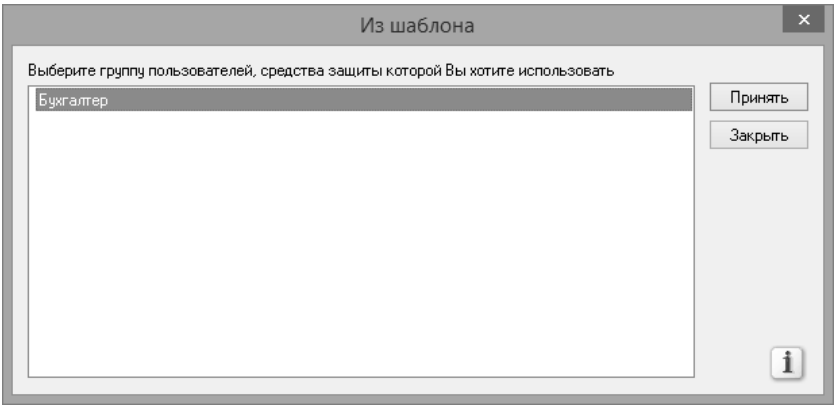


Рис. 9. Выбор средства защиты из шаблона

В последней вкладке необходимо указать средства защиты для каждого вида информации. Для вида информации «Бухгалтерский учет»

отметьте все средства защиты, кроме «Дополнительная программно-аппаратная система контроля доступа» (рис. 10).

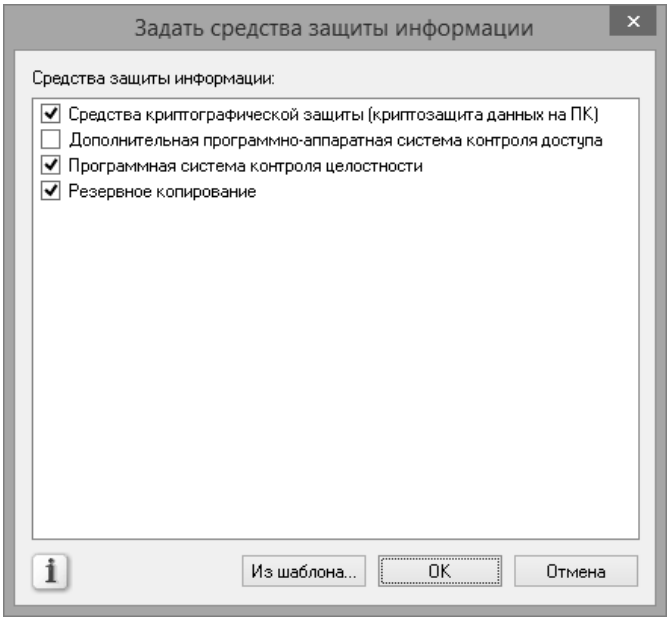


Рис. 10. Выбор средства защиты информации

Для вида информации «База клиентов» средств защиты информации нет.

Для вида информации «База данных наименований товаров» укажите пункты «Резервное копирование» и «программная система контроля целостности».

3.4 Политика безопасности

Так как модель «Информационных потоков» не может учесть организационные меры, связанные с поведением сотрудников организации, существует раздел «Политика безопасности» (рис. 11).

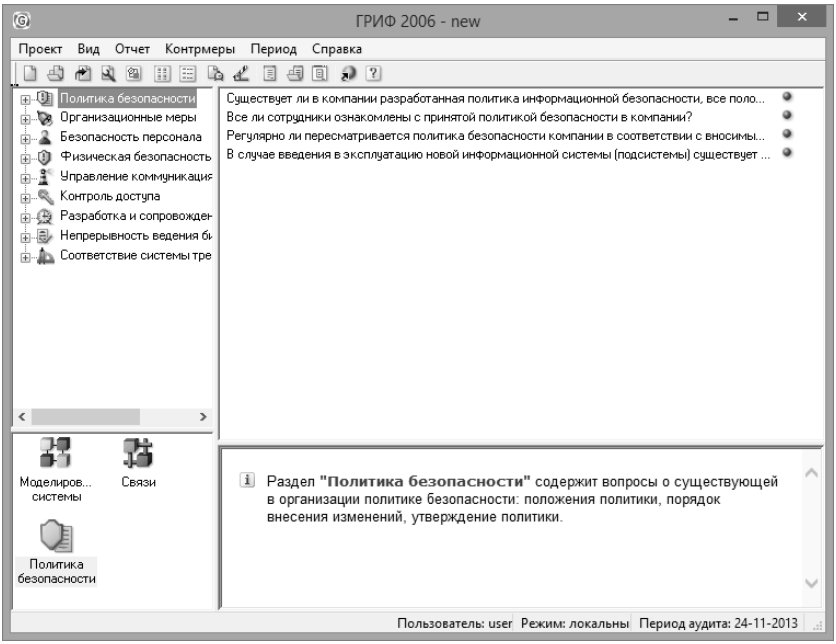


Рис. 11. Раздел «Политика безопасности»

В нем пользователю необходимо ответить на ряд вопросов. Ответы на вопросы влияют на веса средств защиты и изменяют риск реализации информационной безопасности.

3.5 Контрмеры

После выполнения всех этапов, на выходе пользователь получает полную сформированную модель информационной системы с точки зрения информационной безопасности, что позволяет перейти к программному анализу введенных данных для комплексной оценки рисков, а также внедрению контрмер.

Для перехода в окно управления рисками, в главном меню выберите пункт «Контрмеры» и из выпадающего списка нажмите «Управление рисками» (рис. 12).

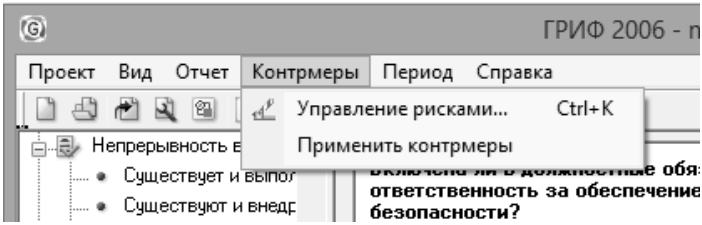


Рис. 12. Меню «Контрмеры»

После чего появится окно «Управление рисками», в нем содержится информация по каждому ресурсу системы, средствах защиты каждого ресурса отдельно, а также сведенья о пользователях (рис. 13).

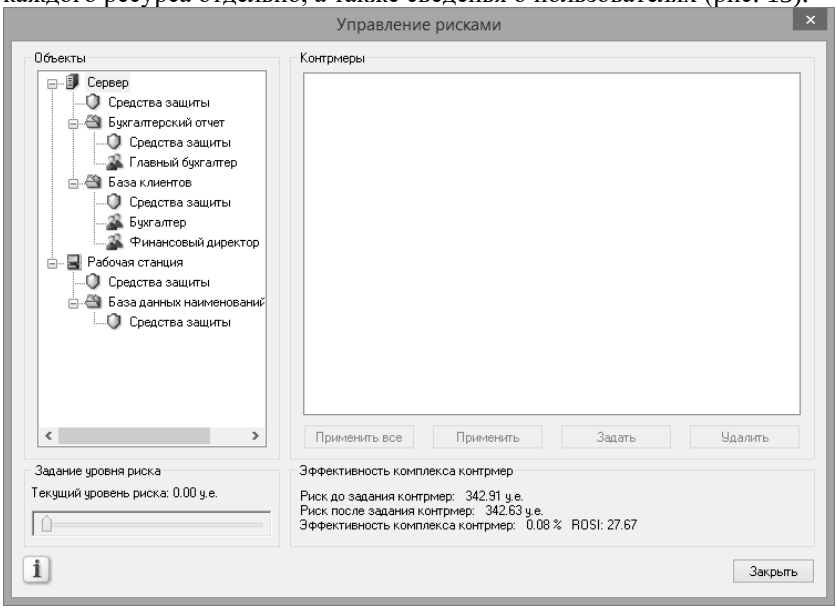


Рис. 13. «Управление рисками»

В нижней части окна расположены регулятор уровня риска «Задание уровня риска» (по умолчанию он установлен в 0) и информация об эффективности контрмер для всей системы.

Регулятор уровня риска позволяет отфильтровать объекты системы по значимости, например, по умолчанию он установлен в 0.00 у.е., это означает что в поле «Объекты» буду показаны все объекты, уровень риска которых превышает данный порог.

Передвинув регулятор вправо, определите какой уровень риска не превышает ресурс «Рабочая станция».

В поле «Эффективность комплекса контрмер» показан суммарный риск всей системы.

Для внедрения контрмер выберите интересующий вас ресурс, в рамках ресурса будет показано, какие средства защиты не используются для защиты ресурса, какой вид информации использует данный ресурс и какие средства защиты еще не применены к данному виду информации, а также какая группа пользователей работает с данной информацией.

Выберите одно из предложенных средств защиты, нажмите кнопку «Задать», откроется окно «Новая контрмера» (рис. 14)

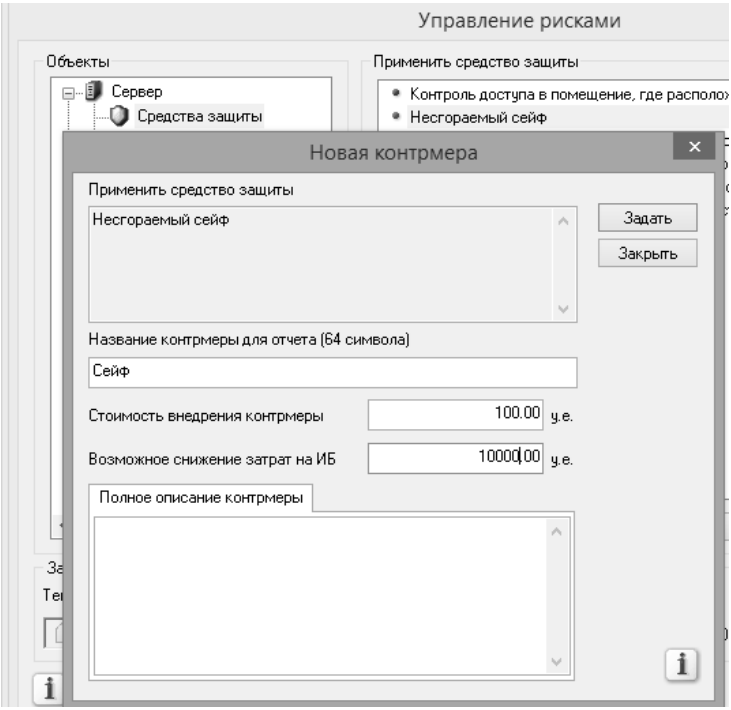


Рис. 14. Задание контрмеры

Заполните необходимы поля в соответствии с рисунком 14, нажмите «Задать», контрмера будет учитываться при расчете риска в окне «Эффективность комплекса контрмер» (рис. 15). Примите еще несколько контрмер.

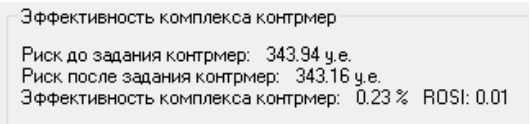


Рис. 15. Риск после задания контрмеры

Внедрение контрмеры, напрямую снижает уровень риска реализации угроз, чем больше будет применено контрмер к системе, тем ниже будет показатель риска.

Заданные контрмеры подсвечиваются оранжевым кругом, после применения контрмеры, она пропадет из списка, а риск информационной системы обновится.

Вы можете принять все контрмеры, или только некоторые, исходя из необходимости и возможности их внедрения в рассматриваемую вами конкретную систему.

3.6 Отчет

Результатом работы системы ГРИФ является отчет, содержащий расчеты затрат компании на ИБ, на контрмеры, вероятности реализации рисков в общем и по отделам и другую информацию, представленную в виде обобщающих диаграмм, графиков и таблиц.

Создайте отчет, для чего в главном меню системы гриф выберите пункт «Отчет» и нажмите «Создать отчет…».

Появится окно конфигурации отчета, в нем пользователь выбирает, какая информация будет выведена в отчете и в каком виде (рис. 16). Ознакомьтесь с содержанием отчета.

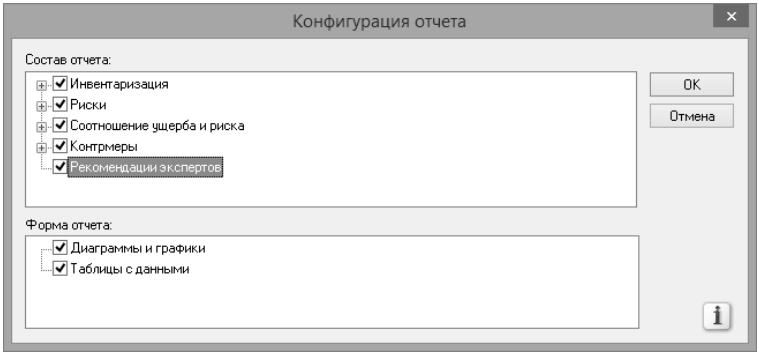


Рис. 16. Конфигурация отчета

4 Задание на лабораторную работу

Постройте модель информационной системы, соответствующую описанию, предложенному в вариантах заданий по лабораторной работе №1. установите логические связи, ответьте на вопросы из раздела «Политика безопасности» по собственному представлению, ознакомьтесь с предложенными контрмерами (примите необходимые), сформируйте отчет.

5 Контрольные вопросы

1) Что представляет собой система ГРИФ и для чего она предназначена?
2) Что понимается под характеристиками группы пользователей?
3) Что такое эффективность средства защиты?
4) Приведите примеры ресурсов, используемых при построении модели информационных потоков в ГРИФ.
5) Что понимается под базовым временем простоя ресурсов?
6) С какой целью создан раздел контрмер?
7) Опишите пошагово работу с моделью информационных потоков.
8) Почему для класса группы авторизованных Интернет-пользователей система ГРИФ не предлагает никакие средства защиты рабочего места?
9) По каким угрозам оценивается ущерб в изученной системе?
10) Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?

ЛАБОРАТОРНАЯ РАБОТА №2
Анализ рисков на основе модели угроз и уязвимостей

1 Цель работы

Целью работы является осуществление анализа рисков на основе модели угроз и уязвимостей с использованием программного комплекса РискМенеджер. Необходимо оценить риски информационной системы, созданной в предыдущей лабораторной работе.

2 Краткие теоретические сведения

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

Основные понятия и допущения модели:

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

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (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 информационной системе, 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.

3 Ход работы

3.1 Модель угроз и уязвимостей

Создание модели угроз и уязвимостей осуществляется по следующему алгоритму:

Шаг 1. На первом этапе работы с продуктом пользователь вносит объекты своей информационной системы: отделы, ресурсы (специфичными объектами для данной модели: угрозы информационной системы, уязвимости, через которые реализуются угрозы).

Шаг 2. Далее пользователю необходимо проставить связи, т.е. определить к каким отделам относятся ресурсы, какие угрозы действуют на ресурс и через какие уязвимости они реализуются.

При построении модели информационной системы для пользователя главной задачей на первом этапе является внесение всех объектов, ресурсов, а также угроз и уязвимостей.

Разделы информационной системы выглядят следующим образом (рис. 1).

Рис. 1. Разделы информационной системы

Добавление объектов происходит аналогично методу «Информационных потоков», выделите нужный объект, кликнув по нему правой кнопкой мыши, в появившемся контекстном меню нажмите «Добавить…» (рис. 2).

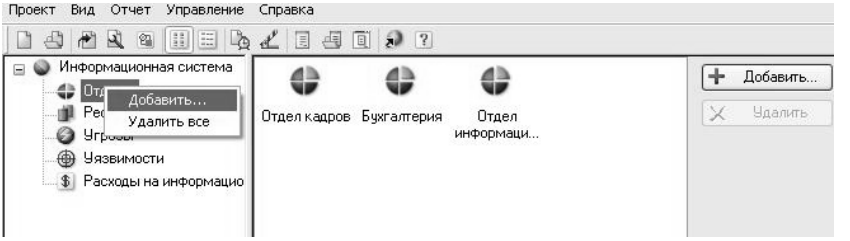


Рис. 2. Добавление отдела

В появившемся окне введите название отдела (рис. 3).

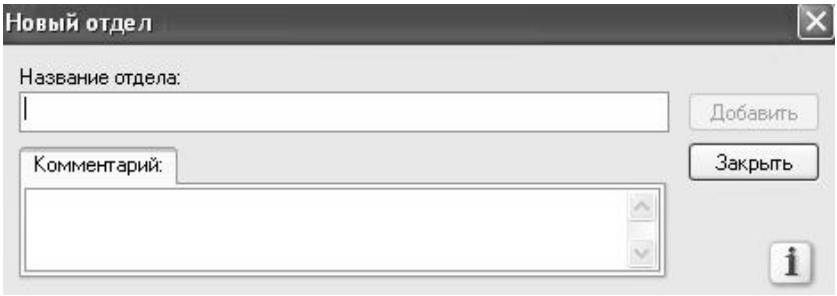


Рис. 3. Окно «Новый отдел»

Для добавления ресурса, необходимо указать тип ресурса (сервер, рабочая станция, мобильный компьютер, твердая копия, веб-сервер), указать отдел, к которому относится данный ресурс, а также указать критичность ресурса (как сильно реализация угрозы на ресурс повлияет на работу информационной системы) (рис. 4).

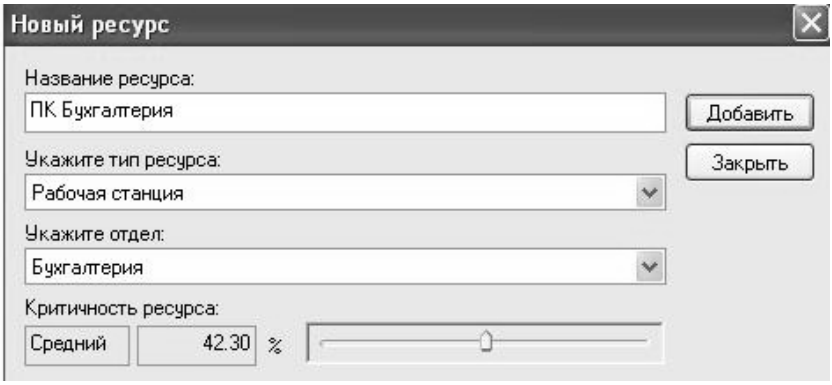


Рис. 4. Добавление нового ресурса

После добавления всех отделов и всех ресурсов системы, необходимо добавить все возможные угрозы. Окно добавления угроз показано ниже (рис. 5).

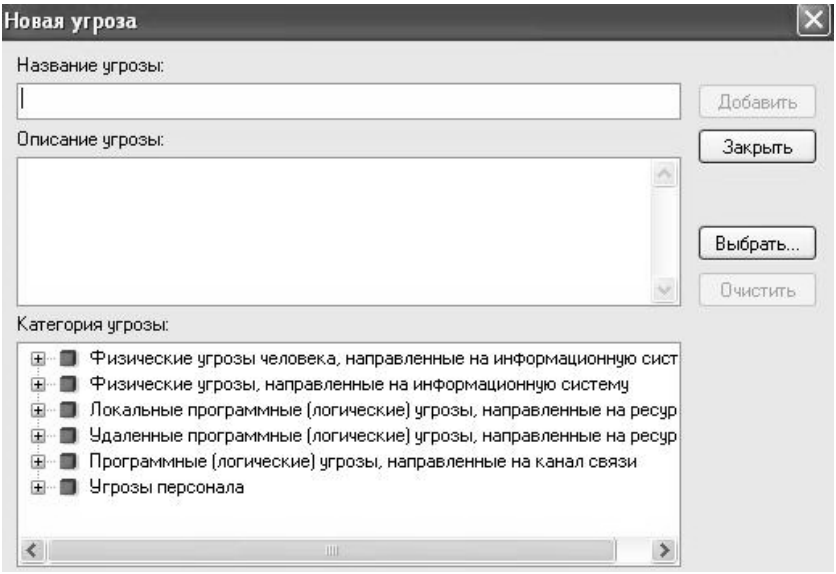


Рис. 5. Окно добавление угроз

Как видно из рисунка выше система «ГРИФ» делит угрозы на шесть категорий:

- физические угрозы человека (потенциального нарушителя);
- физические угрозы (вызванные форс-мажорными обстоятельствами);
- локальные программные угрозы, направленные на ресурс (без использования каналов связи);
- удаленные программные угрозы, направленные на ресурс (с использованием каналов связи);
- программные угрозы, направленные на канал связи (кабельная система, коммуникационное оборудование, ПО);
- угрозы персонала (вызванные действиями сотрудников компании).

Добавить угрозу можно двумя способами, первый это выбрать из списка, нажав кнопку «Выбрать…» (рис. 6).

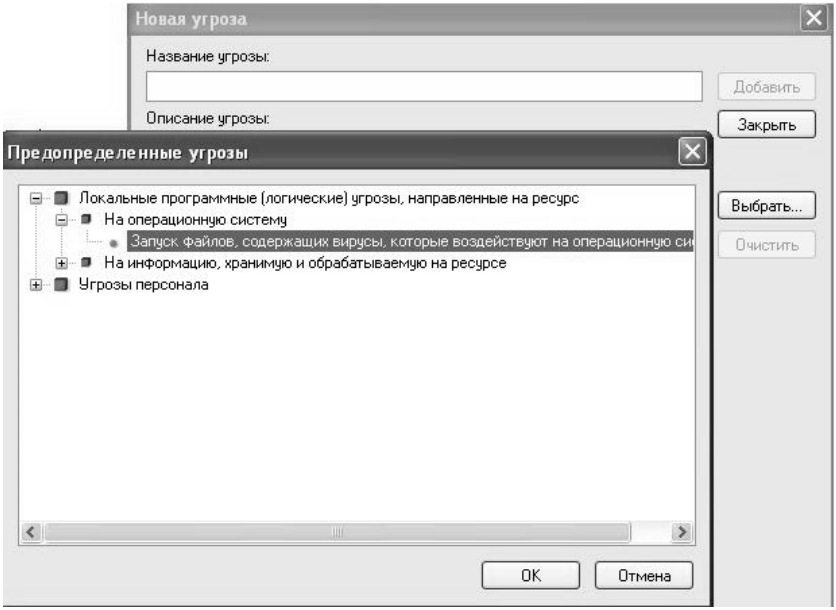


Рис. 6. Предопределенные угрозы

Нажав кнопку «ОК», будет показано описание угрозы, останется только ввести название (рис. 7).

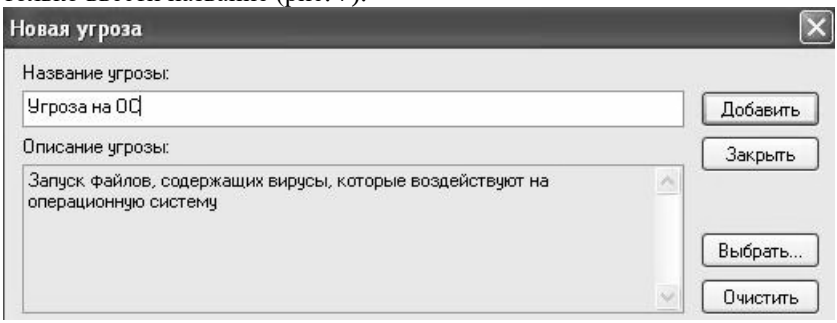


Рис. 7. Добавление угрозы

Второй способ, это задать нужные угрозы самому (не из списка), для этого нужно ввести название угрозы, описание угрозы (не обязательно) и обязательно указать к какой категории относится данная угроза (рис. 8).

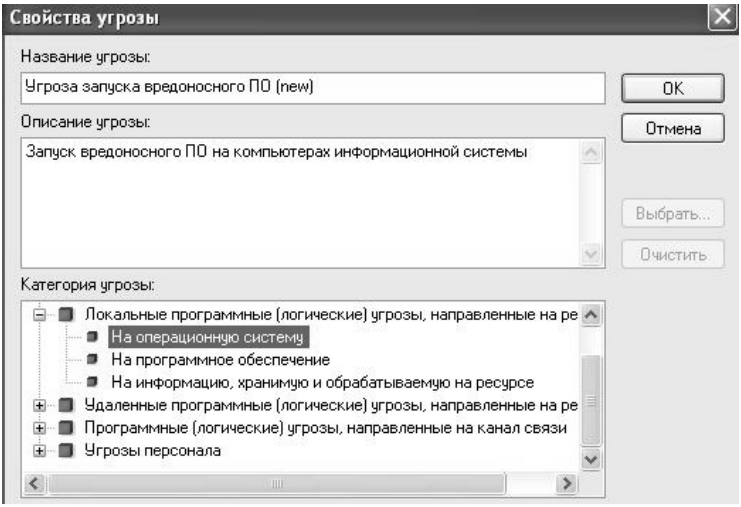


Рис. 8. Добавление новой угрозы

После добавления всех угроз можно перейти к добавлению уязвимостей, окно добавления уязвимостей показано ниже (рис. 9).

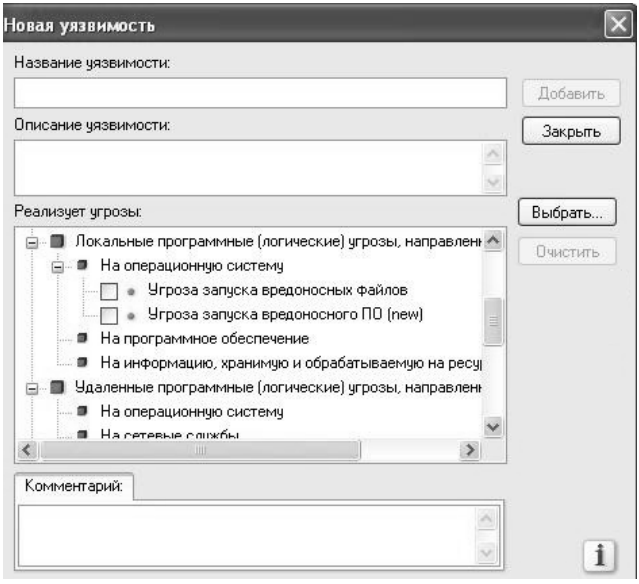


Рис. 9. Окно добавления уязвимостей

Чтобы добавить уязвимость, её необходимо связать с угрозой, например, назовем уязвимость «Отсутствие антивирусного ПО (new)» и свяжем её с угрозой «Угроза запуска вредоносного ПО (new)» поставив галочку на против данной угрозы (рис. 10).

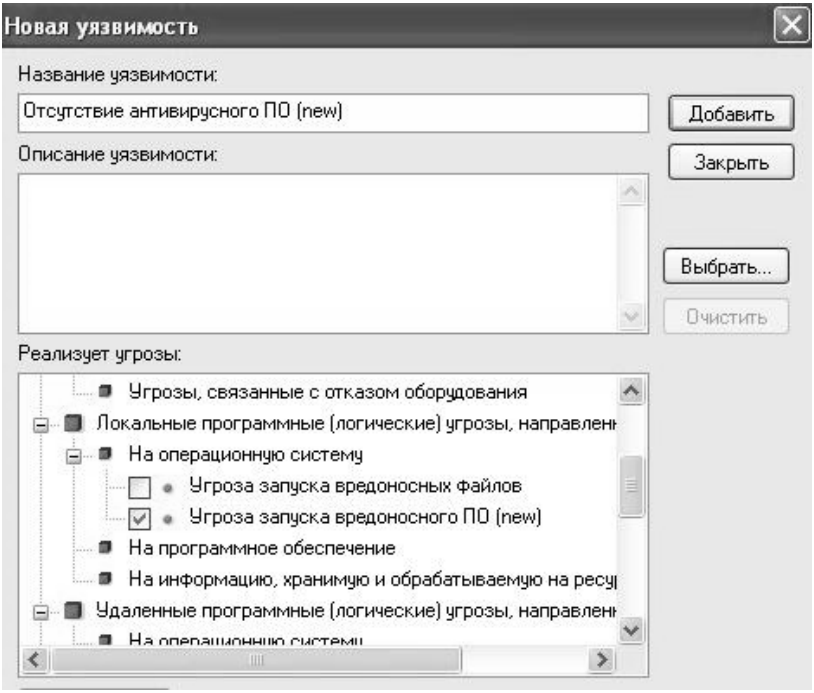


Рис. 10. Связь угрозы и уязвимости

3.2 Связи

Далее пользователю необходимо проставить связи, то есть, указать какие угрозы действуют на ресурс и через какие уязвимости они реализуются (рис. 11).

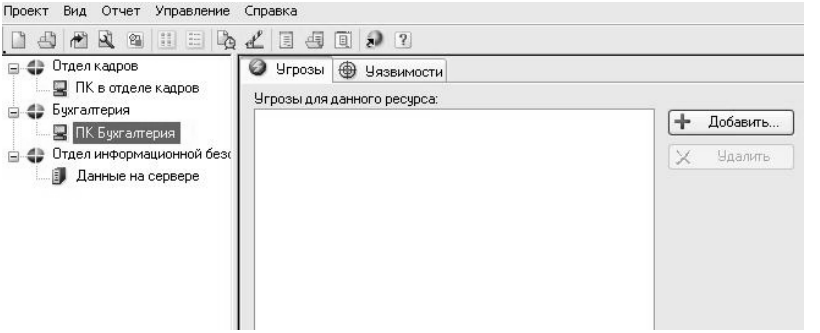


Рис. 11. Угрозы и уязвимости, направленные на ресурс

Для добавления связи ресурс-угроза, нажмите кнопку «Добавить…» в правой части окна (рис. 11).

Появится окно добавления угроз, в нем будут показаны категории и все угрозы, которые пользователь добавлял на предыдущем этапе (построение информационной системы), после выбора одной из угроз нажмите кнопку «Добавить…», после чего необходимо указать уязвимости, вытекающие из этой угрозы и задать два параметра (рис. 12):

- «Вероятность угрозы через данную уязвимость в течение года»;
- «Критичность реализации угрозы».

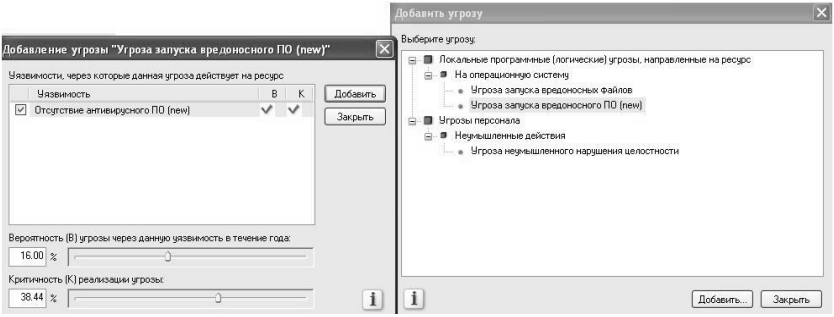


Рис. 12. Окно добавления угроз

Важно отметить, что для угроз, созданных пользователем, вероятность в течение года и критичность реализации по умолчанию равны 0%, для предопределенных угроз это значение устанавливает система гриф (отличное от 0), при надобности пользователь может его изменить.

3.3 Управление рисками и контрмеры

Когда пользователь построил полную информационную систему, указал все угрозы на ресурсы, можно переходить к управлению рисками и применению контрмер. Для этого в главном меню нажмите на пункт «Управление» и в выпадающем списке выберите пункт «Управление рисками…» (рис. 13).

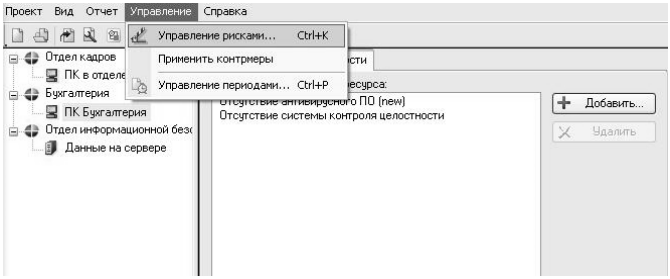


Рис. 13. Меню «Управление»

Появится окно, изображенное на рисунке ниже (рис. 14). На нем изображена иерархическая структура информационной системы, на верху иерархии расположены все ресурсы организации, и перечень угроз, относящихся к ним.

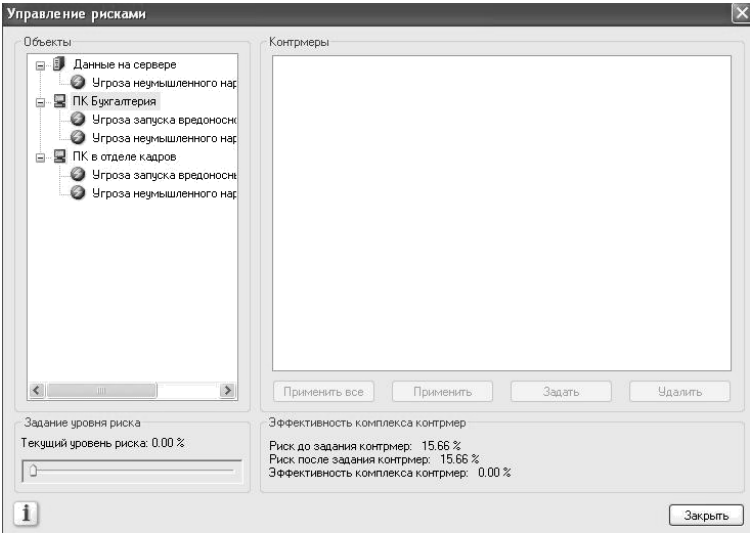


Рис. 14. Окно «Управление рисками»

В нижней части окна показана эффективность комплекса контрмер, риск до внедрения контрмер и после внедрения. Также есть регулятор текущего уровня риска (рис. 15).

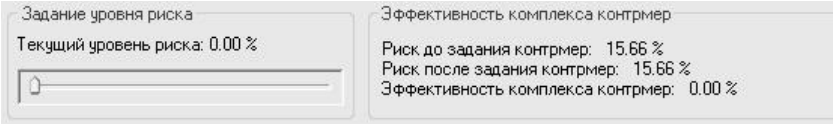


Рис. 15. Уровень риска

При выделении угрозы, в правой части окна появится список уязвимостей, которые необходимо устранить, для этого выделите любую уязвимость из списка и нажмите кнопку «Задать», появится окно (рис. 16).

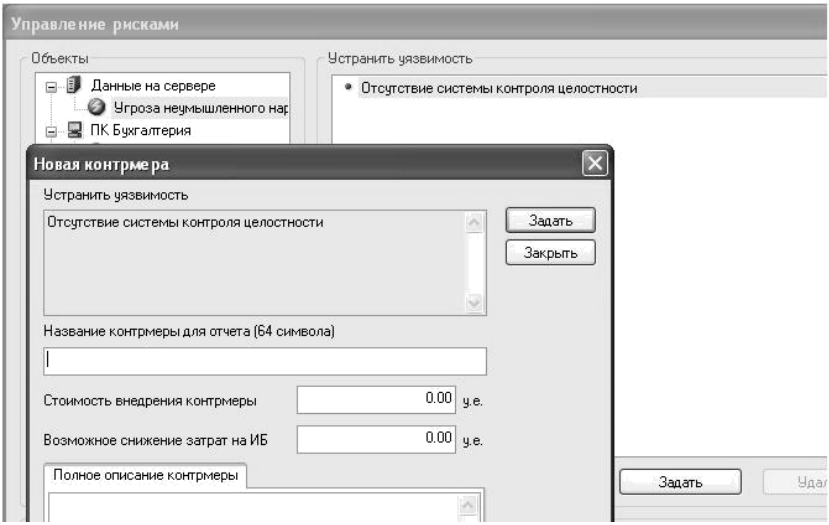


Рис. 16. Задание контрмеры

После того как пользователь задал контрмеру, риск на информационную систему снизится, величина снижения риска зависит от вероятности угрозы через данную уязвимость в течение года и от критичности реализации угрозы.

Таким образом, пользователь может задавать различные контрмеры для различных уязвимостей, тем самым снижая риск реализации угрозы.

3.4 Отчет

Для создания отчета, в главном меню нажмите на пункт «Отчет» и в выпадающем списке выберите «Создать отчет…» (рис. 17).

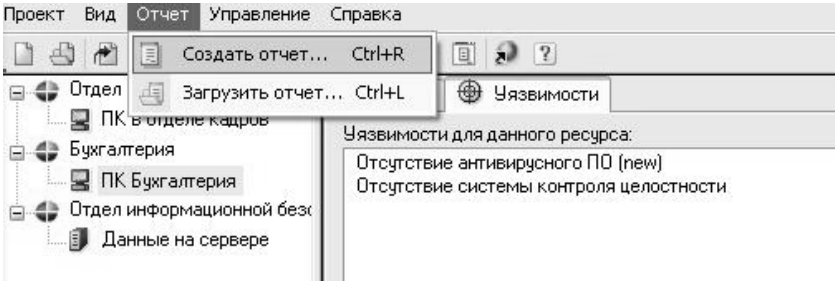


Рис. 17. Меню «Отчет»

После чего откроется окно настройки отчета (рис. 18).

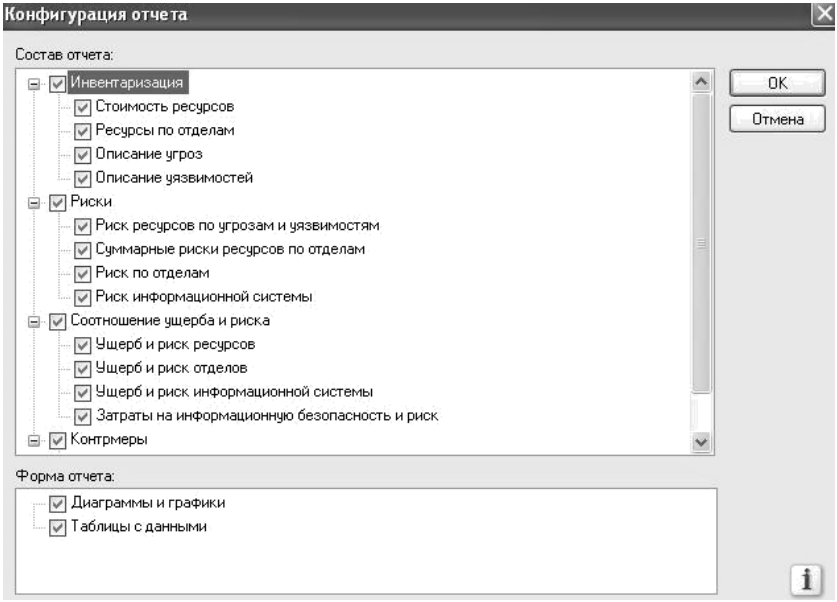


Рис. 18. Окно «Конфигурация отчета»

Выберите необходимые пункты, поставив галочку напротив, и нажмите кнопку «ОК».

Отчет разбит на четыре раздела:

- «Инвентаризация»;
- «Информационные риски»;
- «Соотношение ущерба и риска»;
- «Контрмеры».

Раздел «Инвентаризация» содержит в себе информацию, о стоимости ресурса, описания угроз, описания уязвимостей. То есть общую информацию о системе (рис. 19).

Имя	Описание
Угроза неумышленного нарушения целостности	Неумышленное нарушение целостности (модификация) информации
Угроза запуска вредоносных файлов	Запуск файлов, содержащих вирусы, которые воздействуют на операционную систему
Угроза запуска вредоносного ПО (new)	Запуск вредоносного ПО на компьютерах информационной системы

Имя	Описание
Отсутствие системы контроля целостности	Отсутствие системы контроля целостности
Отсутствие антивирусного ПО (new)	
Отсутствие антивирусного ПО	Не установлено антивирусное ПО

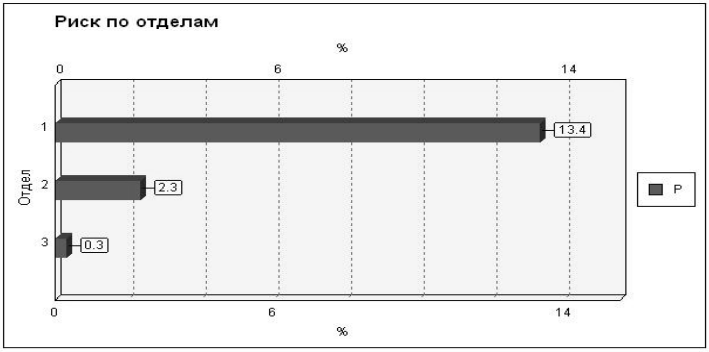
Рис. 19. Описание угроз и уязвимостей

Раздел «Информационные риски» показывает риск ресурсов, по угрозам и уязвимостям, а также суммарные риски ресурсов по отделам (рис. 20).

Отдел кадров

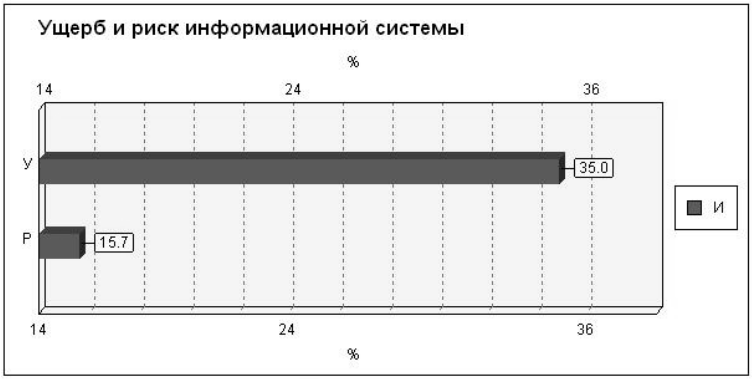
ПК в отделе кадров

Угроза	Уязвимость	Риск, ур.
Угроза неумышленного нарушения целостности	Отсутствие системы контроля целостности	Низкий
Угроза запуска вредоносных файлов	Отсутствие антивирусного ПО	Низкий



№	Отдел	Риск, ур.
1	Отдел кадров	Низкий
2	Бухгалтерия	Низкий
3	Отдел информационной безопасности	Низкий

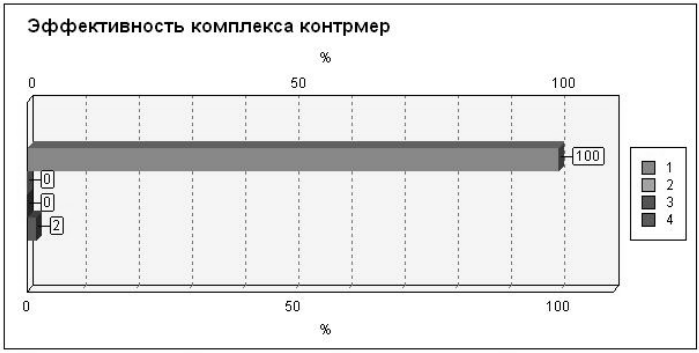
Рис. 20. Риск ресурсов и риск по отделам



	Итого, ур.
Ущерб	Средний
Риск	Средний

Рис. 21. Ущерб и риск информационной системы

В разделе «Соотношение ущерба и риска» находится информация о соотношении ущерба и риска отделов, ресурсов и всей информационной системе в целом (рис. 21).



№	Ресурс	Значение риска до всех контрмер, %	Значение риска после всех контрмер, %	Эффективность комплекса контрмер, %
1	Данные на сервере	0.32	0.00	100.00
2	ПК Бухгалтерия	2.34	2.34	0.00
3	ПК в отделе кадров	13.36	13.36	0.00
4	Информационная система	15.66	15.39	1.73

Рис. 22. Эффективность комплекса контрмер

Последний раздел «Контрмеры» содержит информацию об эффективности контрмер (рис. 22).

Задание: оценить риски информационной системы Вашей организации.

4 Задание на лабораторную работу

Для варианта системы, рассмотренного в лабораторных работах №№ 1-2 определите критичность для каждого из ресурсов. Укажите возможные угрозы безопасности (кроме базовых создайте несколько дополнительных). Аналогично укажите уязвимости. Для всех добавленных угроз и уязвимостей проставьте связи, указав на какие ресурсы действуют угрозы и через какие уязвимости реализуются. Задайте вероятности угроз и критичность их реализации. Для имеющихся угроз примените контрмеры, указав все необходимые параметры. Создайте отчет.

5 Контрольные вопросы

1) Опишите пошагово работу с моделью угроз и уязвимостей.
2) Что такое угроза?
3) Что понимается под уязвимостью?
4) На какие категории система ГРИФ делит угрозы?
5) Как происходит добавление уязвимости?
6) Перечислите факторы, значимые для использования уязвимости.
7) Какие параметры можно указать при создании угрозы?
8) Чему по умолчанию равны вероятность в течение года и критичность реализации для только что созданной угрозы?
9) Каким образом можно снизить риск реализации угрозы?
10) Какие разделы содержит в себе отчет? Охарактеризуйте каждый.

ЛАБОРАТОРНАЯ РАБОТА №3
Анализ рисков на основе международного стандарта ISO 17799

1 Цель работы

Целью работы является осуществление анализа рисков на основе системы разработки и управления политикой безопасности информационной системы компании на основе международного стандарта ISO 17799 КОНДОР, являющейся частью программного комплекса DigitalSecurity.

2 Краткие теоретические сведения

КОНДОР – мощная система разработки и управления политикой безопасности информационной системы компании на основе международного стандарта ISO 17799 «Управление информационной безопасностью. Практические правила». Требования стандарта ISO 17799 обеспечивают комплексный подход к обеспечению информационной безопасности. Система выполняет следующие задачи:

– определяет слабые места в политике безопасности информационной системы;

– анализирует риск невыполнения каждого положения политики безопасности и ранжирует их по степени критичности, что позволяет определить приоритет планируемых действий;

– позволяет эффективно управлять рисками, возникающими в связи с невыполнением положений политики безопасности.

3 Ход работы

3.1 Создание нового проекта аудита

При первом запуске КОНДОР вам потребуется ввести имя пользователя и пароль. Для начала работы с системой создайте новый проект аудита (рис. 1) – проект той информационной системы, которую необходимо проанализировать.

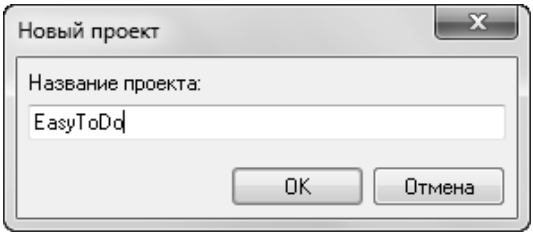


Рис. 1. Создание нового проекта

Рабочее поле программы состоит из четырех частей (рис. 2):

1) Окно навигации. Отображает периоды аудита.

2) Окно разделов с вопросами. Позволяет осуществлять переход между вопросами.

При выборе раздела в рабочем поле отображается перечень вопросов данного раздела. Напротив, каждого вопроса находится иконка, которая показывает состояние вопроса. Синяя иконка означает, что на вопрос не дан ответ, желтая – ответ дан, а серая показывает, что вопрос неприменим к информационной системе.

3) Окно рабочего поля. Позволяет работать с вопросами.

4) Окно подсказки. Отображает справочную информацию по выбранному разделу.

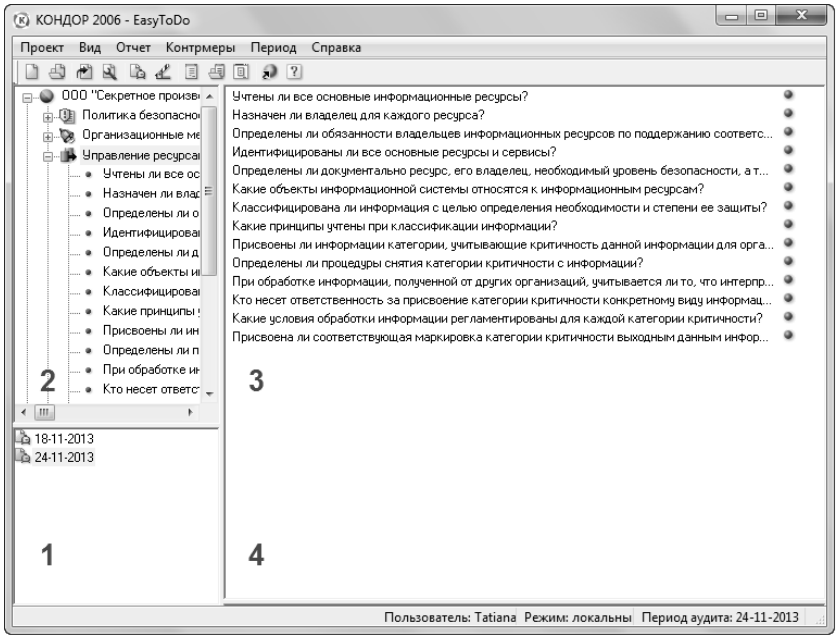


Рис. 2. Рабочее поле программы

3.2 Анализ информационной системы на соответствие требованиям стандарта ISO 17799

Система КОНДОР 2006 состоит из положений стандарта ISO 17799, сформулированных в виде вопросов, отвечая на которые, можно получить полную картину – какие положения выполняются в системе, а

какие нет. Каждый раздел соответствует разделу стандарта. Для получения наиболее верных результатов аудита необходимо ответить на все вопросы и указать вопросы, неприменимые к информационной системе.

Для перехода к вопросу два раза щелкните по нему левой кнопкой мыши в окне разделов с вопросами. Вы сможете увидеть поле для работы с вопросами (рис. 3). Для управления вопросами используйте кнопки (табл. 1).

Табл. 1. Управление вопросами

Следующий	Позволяет перейти к следующему вопросу.
Предыдущий	Позволяет перейти к предыдущему вопросу.
Изменить...	Позволяет ответить или изменить ответ на данный вопрос. При нажатии на эту кнопку появляется окно «Ответ на вопрос».
	Позволяет вводить комментарий. При нажатии на эту кнопку появляется окно «Задать комментарий».

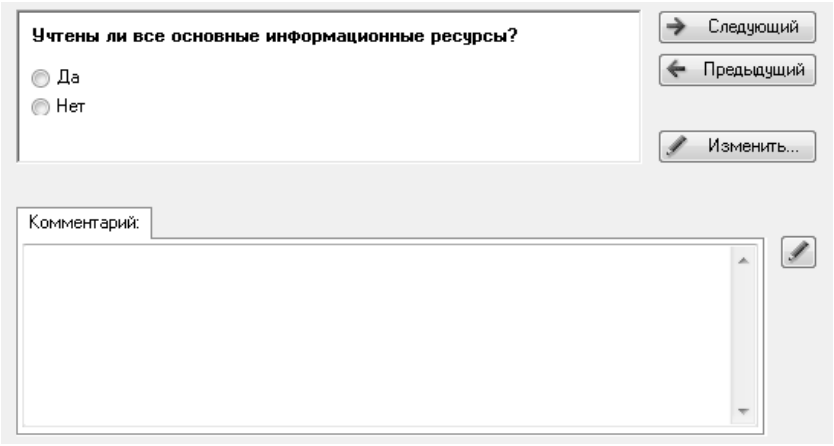


Рис. 3. Поле для работы с вопросами

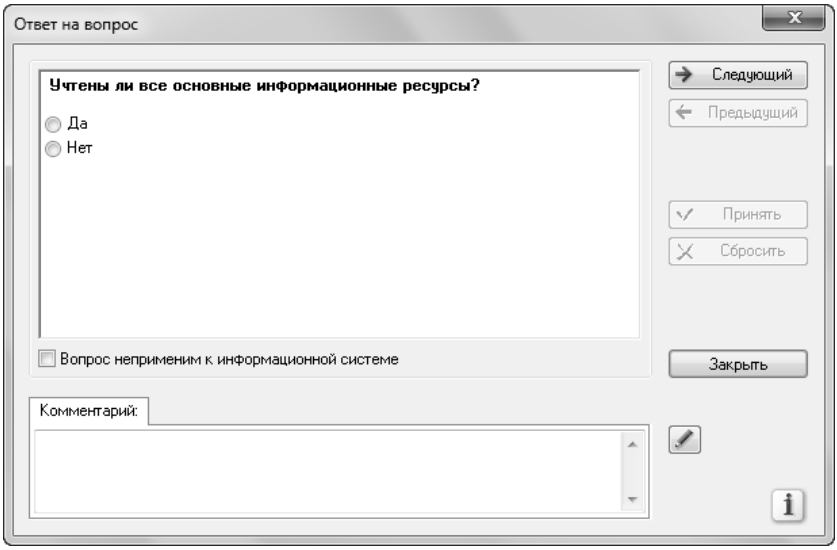


Рис. 4. Окно «Ответ на вопрос»

В окне «Ответ на вопрос» (рис. 4) воспользуйтесь следующими кнопками (табл. 2).

Табл. 2. Ответы на вопросы

Следующий	Позволяет перейти к следующему вопросу раздела.
Предыдущий	Позволяет перейти к предыдущему вопросу раздела.
Принять	Позволяет принять ответ на вопрос.
Сбросить	Позволяет сбросить ответ на вопрос.
Закрыть	Позволяет закрыть окно "Ответ на вопрос".
	Позволяет вводить комментарий. При нажатии на эту кнопку появляется окно «Задать комментарий».

Примером исходных данных для работы с системой могут быть результаты предпроектного исследования или его части (табл. 3). Каждая часть может быть легко соотнесена с одним (или несколькими) разделами стандарта ISO 17799 и программы КОНДОР соответственно.

Табл. 3. Описание системы

Информация по текущему состоянию информационной безопасности в организации	Раздел
Политика безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная генеральным директором организации Политика информационной безопасности. Пересмотр положений ПБ проводится в случае серьезных инцидентов или обнаружения новых уязвимостей.	Политика безопасности
Прием персонала на работу Для минимизации рисков, связанных с приемом на работу ненадежных людей, при найме персонала выполняется: - идентификация личности по паспорту; - проверка подлинности документов, удостоверяющих личность; - проверка рекомендаций и данных из резюме. Не обязательными для подтверждения являются ученые степени и профессиональные навыки.	Безопасность персонала
Политика использования сетевых служб Для уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым сервисам, не компрометируют их безопасность, создана политика использования сетевых служб, содержащая: - положение, определяющее сети и сетевые услуги, к которым разрешен доступ; - положение, описывающее процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ; - положение, определяющее мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.	Контроль доступа
Требования безопасности и методы защиты оставленного без присмотра оборудования Все пользователи и подрядчики ознакомлены с требованиями безопасности и методами защиты оставленного без присмотра оборудования: - завершать активные сеансы по окончании работы, если отсутствует механизм блокировки, например, хранитель экрана, защищенный паролем; - защищать PC или терминалы от неавторизованного использования посредством замка или эквивалентного средства контроля, например, защита доступа с помощью пароля, когда оборудование не используется. Пользователи не ознакомлены с требованием отключаться от сервера, когда сеанс закончен (то есть не только выключать PC или терминал).	Контроль доступа

Продолжение табл. 3

Информация по текущему состоянию информационной безопасности в организации	Раздел
Активы, ответственность за обеспечение безопасности активов Каждый актив организации идентифицирован и классифицирован с точки зрения безопасности. Результаты инвентаризации оформляются в сводной таблице: с указанием инвентарного номера и владельца актива. Фактическое местоположение актива не указывается. Для каждого материального и информационного актива и процесса, связанного с информационной безопасностью, назначен ответственный администратор (владелец) из числа руководителей. Все детали обязанностей и степени ответственности каждого владельца ресурса, несущего ответственность за обеспечение его безопасности, четко определены и закреплены документально. Не все уровни полномочий ответственных лиц закреплены документально. Документально не закреплен список прав доступа для каждого ресурса. Владелец ресурса может передавать свои полномочия по обеспечению безопасности какому-либо сотруднику или поставщикам услуг. При этом ответственность за обеспечение безопасности актива передается тому, кому переданы обязанности.	Управление ресурсами Организационные меры
Политика использования криптографических средств защиты информации Чтобы максимизировать преимущества и минимизировать риски, связанные с использованием криптографических средств, а также избежать неадекватного или неправильного их использования, в организации разработана политика использования криптографических средств защиты информации. При этом определены: а) методика использования криптографических средств в организации, включая общие принципы, в соответствии с которыми следует защищать служебную информацию; б) принципы управления ключами, включая методы восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей; в) роли и обязанности должностных лиц за: - реализацию политики; - управление ключами; г) перечень мероприятий, которые должны обеспечивать эффективность внедрения методов криптозащиты в организации; е) требования законодательства и ограничения Не определен порядок определения адекватного уровня криптографической защиты.	Разработка и сопровождение систем

Продолжение табл. 3

Информация по текущему состоянию информационной безопасности в организации	Раздел
Порядок обращения с лицензионным ПО В организации разработаны типовые процедуры приобретения лицензионного ПО: выбор ПО, проверка его на качество, покупка ПО, регистрация в журнале инвентаризации. Лицензии, сертификаты и финансовые документы не всегда сохраняются до конца срока использования ПО.	Соответствие системы требованиям
Процедуры обращения с информацией и ее хранения Процедуры обращения с информацией и ее хранения, определенные в организации: - обработка и маркирование всех носителей информации; - ограничение доступа с целью идентификации неавторизованного персонала; - обеспечение формализованной регистрации авторизованных получателей, данных; - обеспечение уверенности в том, что данные ввода являются полными, процесс обработки завершается должным образом и имеется подтверждение вывода данных; - хранение носителей информации в соответствии с требованиями изготовителей; - сведение рассылки данных к минимуму; - четкая маркировка всех копий данных, предлагаемых вниманию авторизованного получателя; - регулярный пересмотр списков рассылки и списков авторизованных получателей. Не обеспечивается защита информации, находящейся в буфере данных и ожидающей вывода в соответствии с важностью этой информации.	Управление коммуникациями и процессами
Расположение объектов по территории Все средства обработки информации организации физически изолированы от средств обработки информации сторонних организаций. Справочники и внутренние телефонные книги, идентифицирующие местоположения средств обработки важной информации, хранятся в сейфе и не доступны посторонним лицам. Огнеопасные и взрывчатые материалы хранятся на безопасном расстоянии от охраняемых зон. Резервное оборудование и резервные носители данных располагаются в основном здании.	Физическая безопасность

Продолжение табл. 3

Информация по текущему состоянию информационной безопасности в организации	Раздел
Управление непрерывностью бизнеса Особое внимание уделяется оценке зависимости бизнеса от внешних факторов и существующих контрактов. Проводится обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление. Все согласованные процедуры по обеспечению непрерывности ведения бизнеса требуют документации. Тестирование планов обеспечения непрерывности бизнеса требует установки определенной периодичности.	Непрерывность ведения бизнеса

Таким образом, можно ответить на соответствующие вопросы разделов (табл. 4).

Табл. 4. Вопросы разделов

Раздел	Вопросы раздела
Политика безопасности	**Существует ли в компании разработанная политика информационной безопасности, все положения которой на практике внедрены в информационную систему?** ◉ Да ○ Нет **Утверждена ли существующая политика информационной безопасности руководством организации?** ◉ Да ○ Нет **В каких случаях пересматриваются положения политики безопасности в организации?** ☑ После серьезных инцидентов в области информационной безопасности ☑ После обнаружения новых уязвимостей ☐ После изменений в организационной или технической инфраструктуре организации
Организационные меры	**Определены ли ответственность и обязанности по защите отдельных ресурсов и выполнению конкретных действий по обеспечению безопасности?** ◉ Да ○ Нет

Продолжение табл. 4

Раздел	Вопросы раздела
	Если происходит полная или частичная передача обязанностей по обеспечению безопасности с владельца ресурса на какого-либо сотрудника или поставщика данного ресурса, то на ком остается ответственность за безопасность данного ресурса? ○ На владельце ресурса ◉ На том, кому переданы обязанности по обеспечению безопасности **Четко ли определены зоны ответственности каждого владельца ресурса, несущего ответственность за обеспечение его безопасности?** ◉ Да ○ Нет **Что включает в себя определение зоны ответственности за обеспечение безопасности ресурса?** ☑ Четко определены и описаны все ресурсы, входящие в зону ответственности, а также все действия по обеспечению безопасности в данной зоне ☑ Для каждого ресурса (или процесса) назначен ответственный сотрудник из числа руководителей. Все его обязанности и степень ответственности закреплены документально ☐ Четко определены и задокументированы уровни полномочий каждого ответственного лица ☐ Для каждого ресурса определен и закреплен документально список прав доступа (матрица доступа)
Управление ресурсами	**Учтены ли все основные информационные ресурсы?** ◉ Да ○ Нет **Идентифицированы ли все основные ресурсы и сервисы?** ◉ Да ○ Нет **Определены ли документально ресурс, его владелец, необходимый уровень безопасности, а также местоположение ресурса?** ○ Да ◉ Нет **Классифицирована ли информация с целью определения необходимости и степени ее защиты?** ◉ Да ○ Нет

Продолжение табл. 4

Раздел	Вопросы раздела
Безопасность персонала	**Какие проверки персонала осуществляются при приеме на работу?** ☑ Проверяются рекомендации и данные из резюме ☐ Обязательное подтверждение ученых степеней и профессиональных навыков ☑ Проводится необходимая идентификация личности (паспорт и т.п.)
Физическая безопасность	**Изолированы ли средства обработки данных организации от средств обработки данных сторонних организаций?** ◉ Да ○ Нет **Доступны ли случайным лицам каталоги и внутренние телефонные книги, которые могут дать информацию о нахождении критичных ресурсов?** ○ Да ◉ Нет **Расположены ли огнеопасные и взрывчатые материалы на безопасном расстоянии от охраняемых зон?** ◉ Да ○ Нет **Располагаются ли резервные носители информации и резервное оборудование в отдельном месте, на безопасном расстоянии?** ○ Да ◉ Нет
Контроль доступа	**С какими правилами защиты оборудования, оставленного без присмотра, ознакомлены пользователи?** ☑ Необходимо завершать активную сессию перед уходом, если невозможно использование специальных блокирующих механизмов, например, парольная блокировка экрана ☐ Обязательно завершать соединение с сервером по окончании работы с ним, а не просто выключать терминал или компьютер ☑ Неиспользуемые рабочие станции и терминалы должны быть защищены от неавторизованного доступа при помощи блокировки клавиатуры или парольной защиты

Продолжение табл. 4

Раздел	Вопросы раздела
Управление коммуникациями и процессами	**Какие процедуры обращения с информацией и ее хранения определены в организации?** ☑ Учет и маркировка всех носителей ☑ Ограничение доступа неавторизованных пользователей ☑ Ведение регистрации всех авторизованных лиц, получающих доступ к данным ☑ Обеспечение контроля полноты входных данных, корректной обработки и соответствия информации на выходе ☐ Обеспечение защиты буферных данных соответственно уровню их критичности ☑ Хранение носителей данных в соответствии с указаниями поставщика ☑ Предоставление доступа к данным минимальному числу лиц ☑ Регулярная проверка перечней пользователей, имеющих право доступа к данным
Разработка и сопровождение систем	**Существует ли политика использования систем криптографической защиты информации (СКЗИ)?** ◉ Да ○ Нет **Что учитывается при разработке политики использования СКЗИ?** ☑ Управленческий подход к использованию СКЗИ внутри организации (например, какие именно классы информации должны быть защищены) ☑ Распределение обязанностей: кто и за что несет ответственность ☑ Внедрение политики ☑ Управление ключами ☐ Порядок определения адекватного уровня криптографической защиты ☑ Стандарты, которые могут быть внедрены и адаптированы в организации (какие решения для каких бизнес-процессов подходят) **Существует ли в организации политика управления ключами, включая методы для восстановления зашифрованной информации в случае утери, компрометации или уничтожения ключей?** ◉ Да ○ Нет
Непрерывность ведения бизнеса	**Уделяется ли внимание оценке зависимости бизнеса от внешних связей?** ◉ Да ○ Нет

Продолжение табл. 4

Раздел	Вопросы раздела
	Документируются ли все согласованные процедуры по обеспечению непрерывности ведения бизнеса? ○ Да ◉ Нет **Определена ли периодичность тестирования и обновления планов по обеспечению непрерывности ведения бизнеса?** ○ Да ◉ Нет
Соответствие системы требованиям	**Разработаны ли в компании типовые процедуры приобретения программного обеспечения?** ◉ Да ○ Нет **Обеспечена ли возможность доказательства того, что установленное программное обеспечение лицензионное (лицензии, сертификаты, финансовые документы и т.д.)?** ○ Да ◉ Нет

3.3 Расходы на информационную безопасность

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

Изменим значения расходов на информационную безопасность, выбрав соответствующий раздел во втором окне рабочего поля (рис. 2):

Разовые затраты на приобретение систем защиты информации. Другими словами, это стоимость лицензии программного обеспечения. Кроме того, необходимо также учесть в данном пункте затраты на аппаратное обеспечение – стоимость одного или нескольких компьютеров, на которых развернуты компоненты системы защиты. Также необходимо учесть затраты на покупку или создание средств технической защиты. Помимо этого, часто система защиты использует дополнительное программное и аппаратное обеспечение, стоимость которого также необходимо учитывать. К такому обеспечению можно отнести базы данных, браузеры, системы настройки оборудования,

системы резервирования, сетевые кабели, тройники, системы бесперебойного питания и т.д.

Установите значение равным 1 000 000 руб.

В крупных компаниях, имеющих распределенную корпоративную сеть, не стоит забывать о ***затратах на внедрение систем защиты информации*** (включая этап предварительного аудита).

Установите значение равным 400 000 руб.

Ежегодные затраты на поддержку и обучение (если она не включена в стоимость системы защиты). Сюда же можно отнести и командировочные расходы IT-специалистов на поездки в удаленные офисы и настройку удаленных компонентов системы обеспечения информационной безопасности.

Установите значение равным 500 000 руб.

Ежегодные затраты на управление средствами защиты информации, которые включают зарплату администраторов безопасности и персонала, связанного с системой обнаружения атак, а также затраты на модернизацию программно-аппаратного обеспечения. К этой статье расходов относится оплата услуг аутсорсинговых компаний.

Установите значение равным 800 000 руб.

Прочие ежегодные затраты на обеспечение информационной безопасности.

Оставьте значение равным 0 руб.

Изменение затрат после внедрения контрмер – изменение затрат на информационную безопасность после принятия контрмер. Это значение равно разности стоимости внедрения контрмеры и возможного снижения затрат на ИБ. Данное поле заполняется автоматически после установления стоимости внедрения контрмер и возможного снижения затрат на ИБ.

Значения затрат отображаются в одном окне и удобны для анализа (рис. 5).

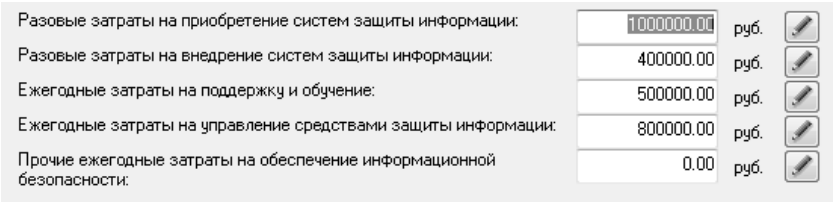


Рис. 5. Расходы на информационную безопасность

Свойства проекта. Для изменений свойств проекта выберете в меню пункт «Проект ⟶ Свойства проекта».

Данные о проекте. В закладке «Идентификация» введите данные о текущем проекте (рис. 6).

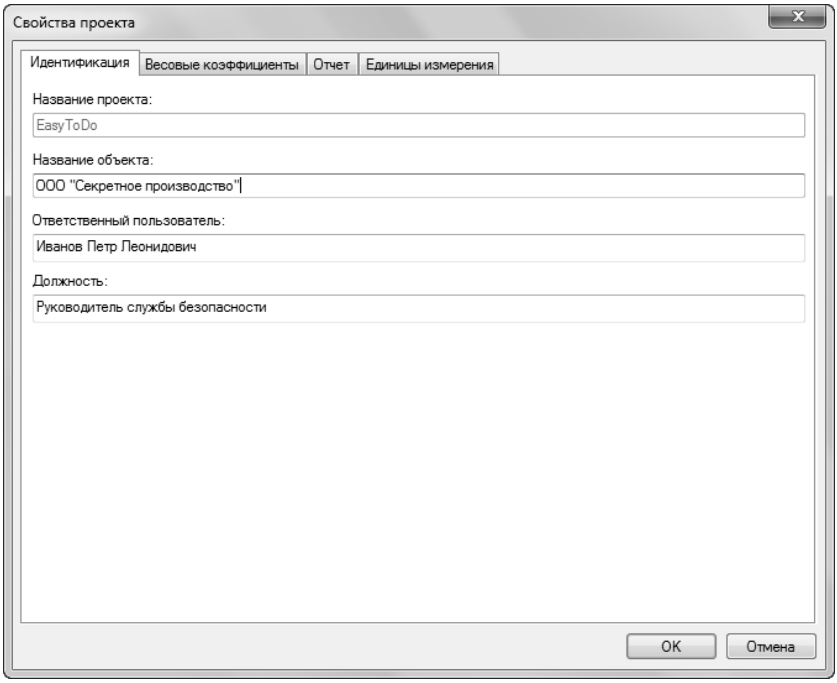


Рис. 6. Свойства проекта, идентификация

Весовые коэффициенты. Каждое требование стандарта имеет определенное весовое значение, которое характеризует степень критичности данного положения для поддержания необходимого уровня защищенности. Веса, заданные в системе по умолчанию, разработаны экспертами Digital Security. Учитывая, что универсальные значения весов не могут учесть все особенности различных компаний, в программе предусмотрена возможность изменения весов при работе с положениями стандарта.

Для просмотра весовых коэффициентов требований, заданных по умолчанию, а также для установки новых требований перейдите «Свойства проекта ⟶ Весовые коэффициенты» (рис. 7). Требования

также разделены по разделам, рядом с каждым требованием стоит номер раздела стандарта ISO 17799.

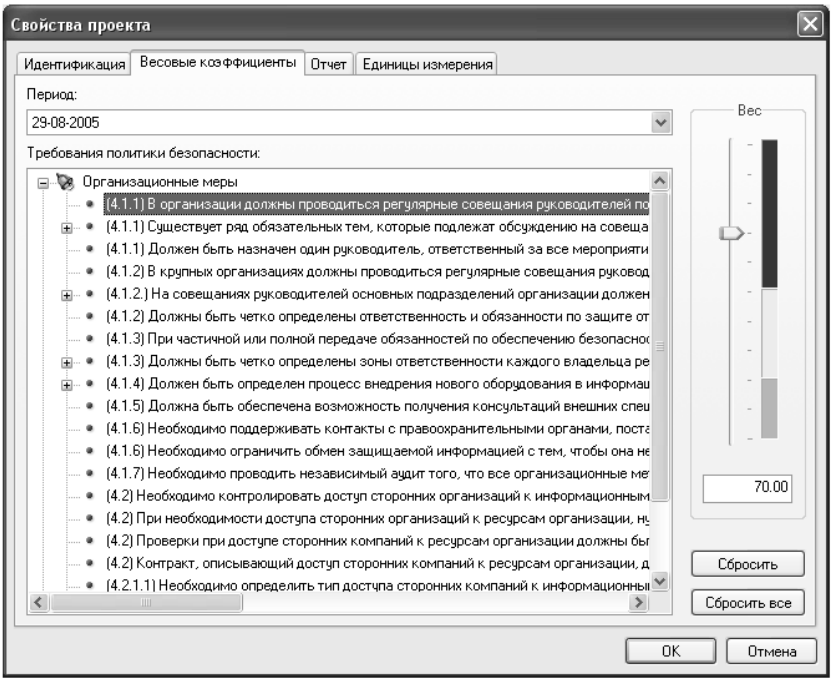


Рис. 7. Свойства проекта, весовые коэффициенты

Для изменения весов перетащите курсор слева на необходимый уровень или введите значение в окне. Кнопки «Сбросить» и «Сбросить все» позволяют установить значения веса требования или всех требований соответственно по умолчанию.

В списке требований также отражено состояние каждого требования. Если вес требования изменен, то индикатор будет желтого цвета, если нет – синего.

3.4 Содержание отчета

Отчет (рис. 8). закладка, позволяющая настраивать параметры создаваемых отчетов:

– выполненные требования. перечень требований стандарта, выполненных в организации;

– невыполненные требования. перечень требований стандарта, невыполненных в организации;

– контрмеры. контрмеры, заданные в информационной системе;

– рекомендации экспертов. комментарии специалистов к требованиям стандарта.

Окно «Форма отчета» позволяет выбрать форму отчета: с содержанием диаграмм и графиков или нет.

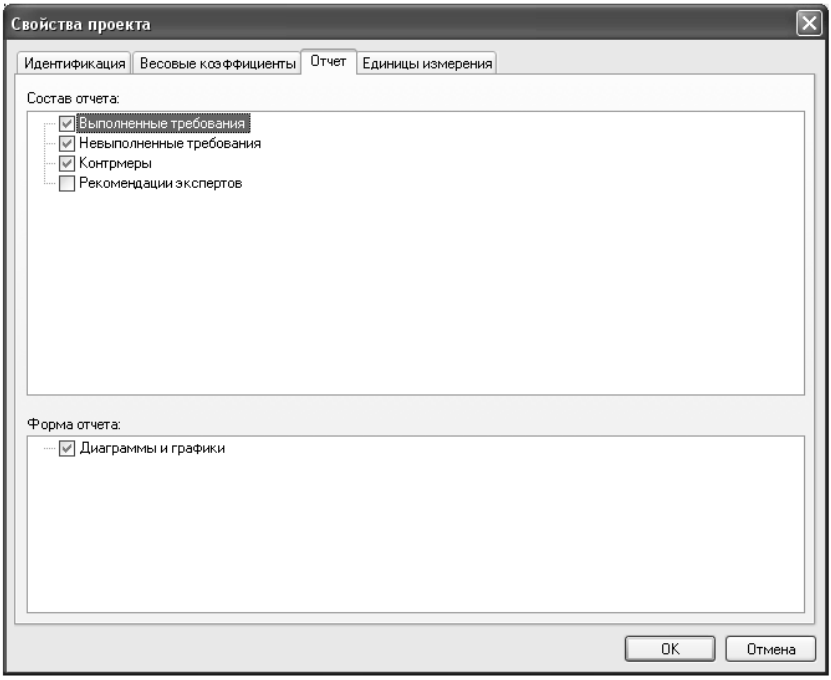


Рис. 8. Свойства проекта, отчет

Оставьте значения, установленные по умолчанию.

Единицы измерения. Перейдите на закладку «Единицы измерения» (рис. 9) и выберите «Российские рубли».

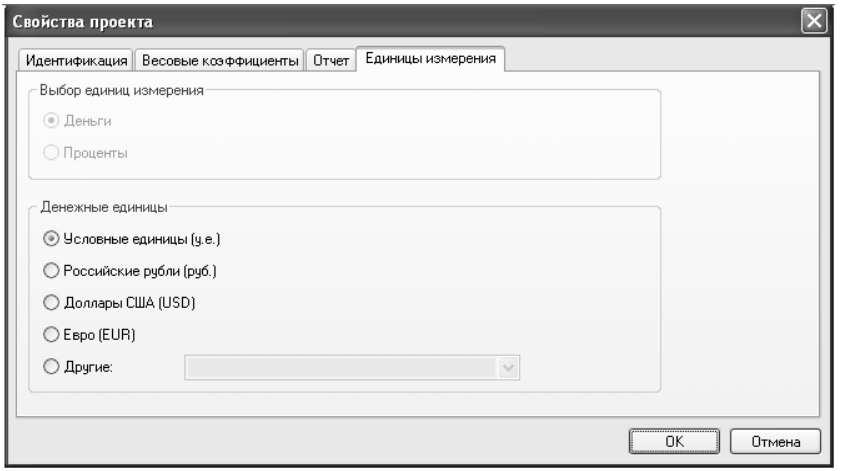


Рис. 9. Свойства проекта, единицы измерения

3.5 Управление рисками

После того, как даны все ответы, для анализа дальнейших действий в системе КОНДОР 2006 предусмотрен модуль управления рисками. В нем отражаются все невыполненные в компании положения политики безопасности (рис. 10).

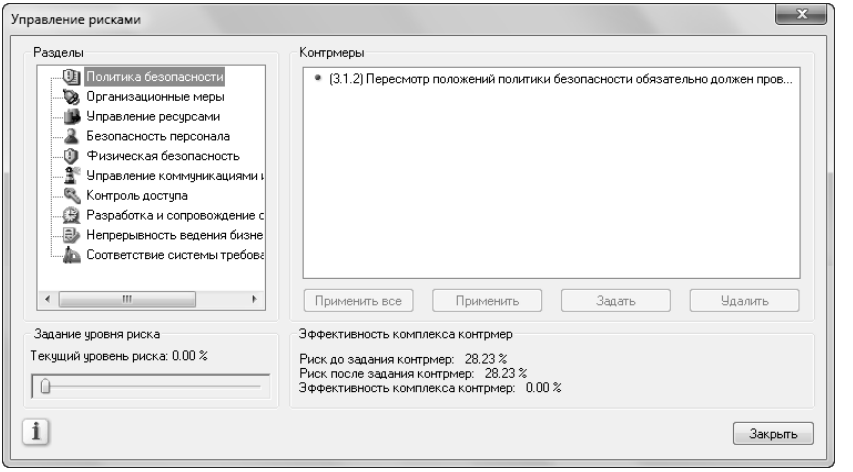


Рис. 10. Управление рисками

Причем можно задать пороговое значение весов, чтобы отображались только критичные для пользователя положения стандарта, которые не выполнены (рис. 11). Задайте уровень риска равным 50%.

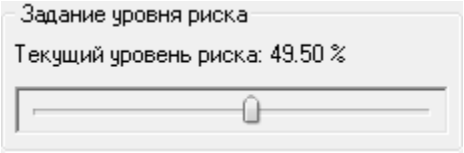


Рис. 11. Задание порога весов

Для задания контрмеры:

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

2) Нажмите кнопку «Задать» или клавишу {Enter}.

В окне «Новая контрмера» введите необходимые данные (рис. 12).

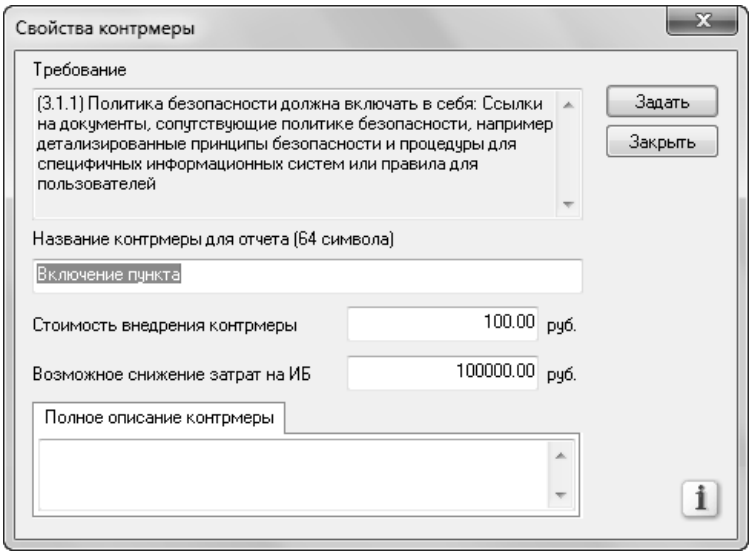


Рис. 12. Задание контрмеры

Для закрытия рассматриваемых уязвимостей и снижения риска нарушения информационной безопасности примените следующие контрмеры (рисунки 13 - 20).

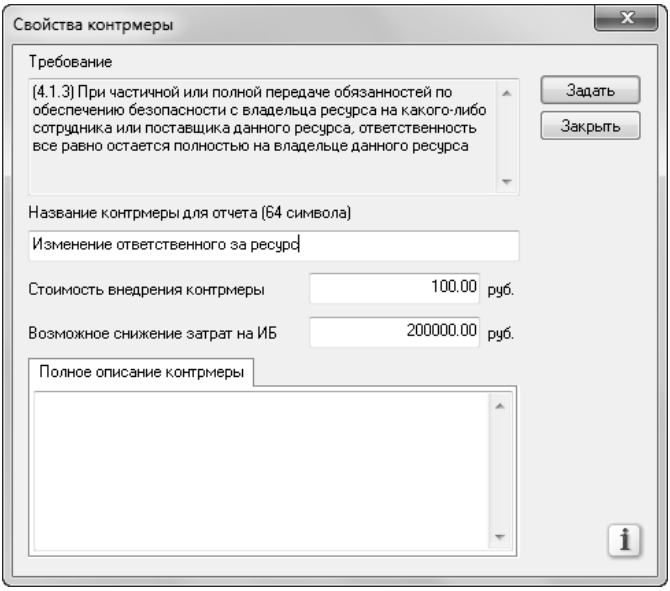


Рис. 13. Контрмера «Изменение ответственного»

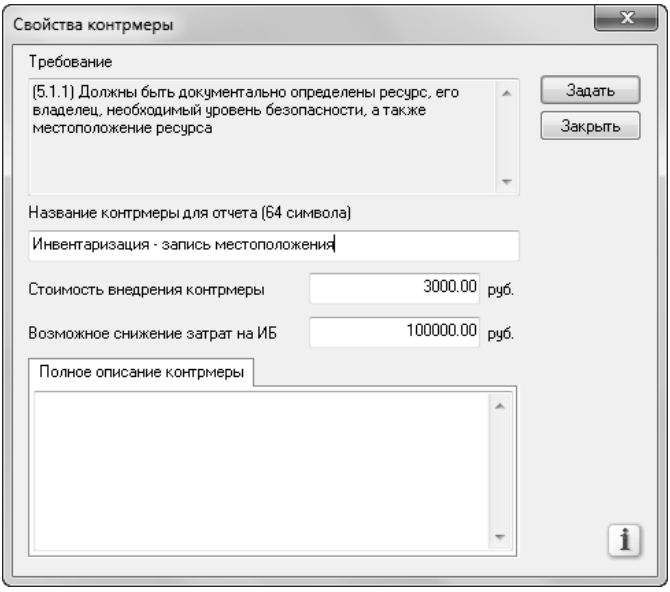


Рис. 14. Контрмера «Инвентаризация. местоположение»

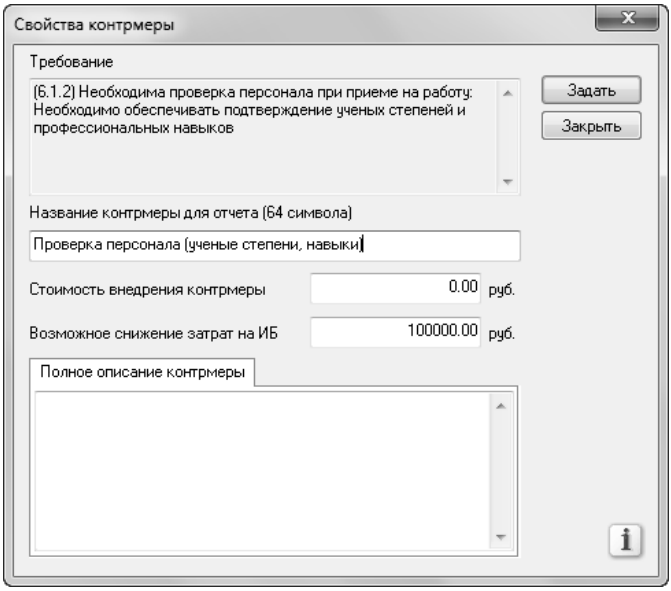


Рис. 15. Контрмера «Проверка персонала»

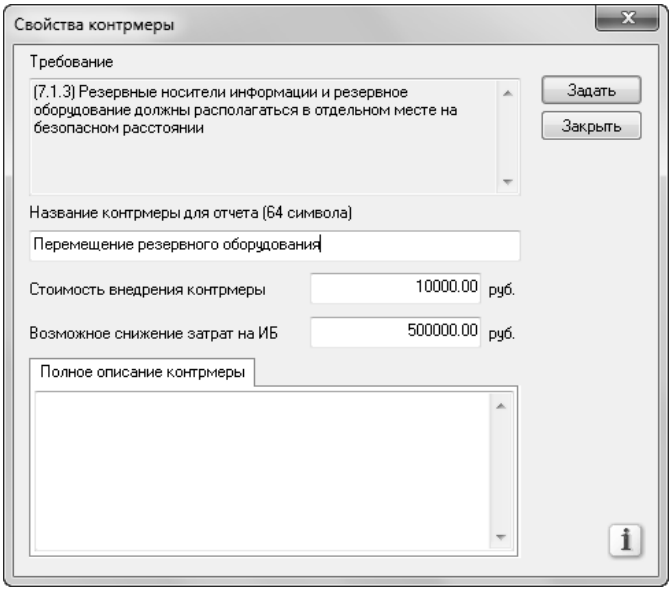


Рис. 16. Контрмера «Перемещение резервного оборудования»

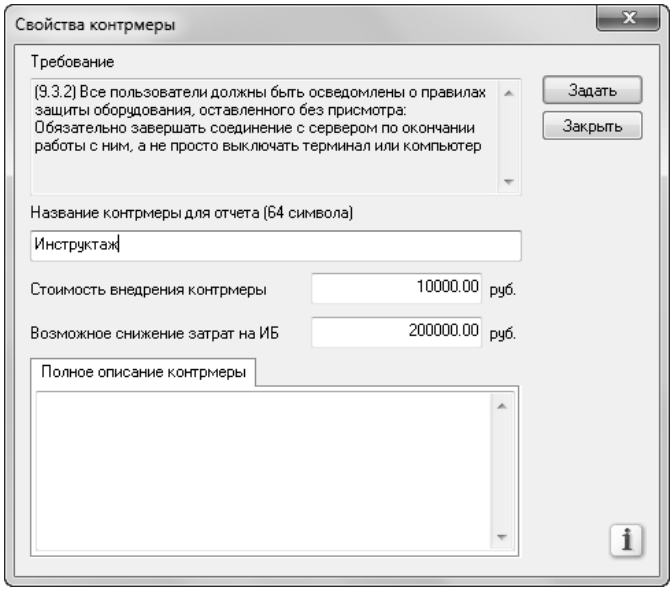


Рис. 17. Контрмера «Инструктаж»

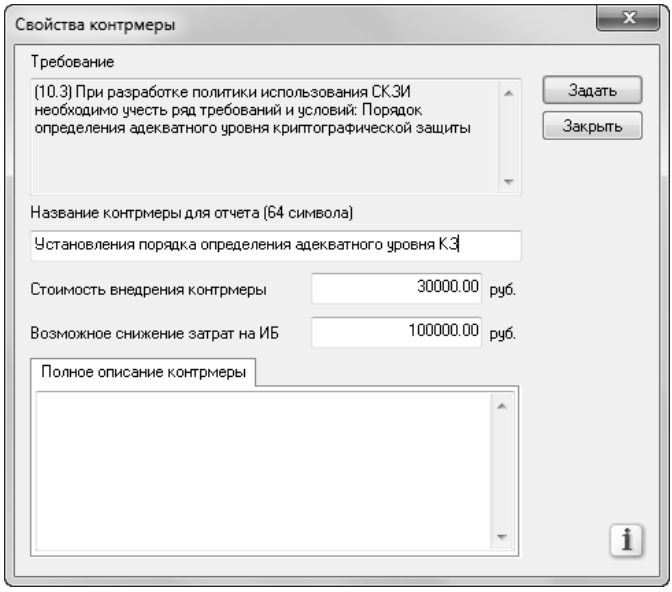


Рис. 18. Контрмера «Установление порядка определения уровня КЗ»

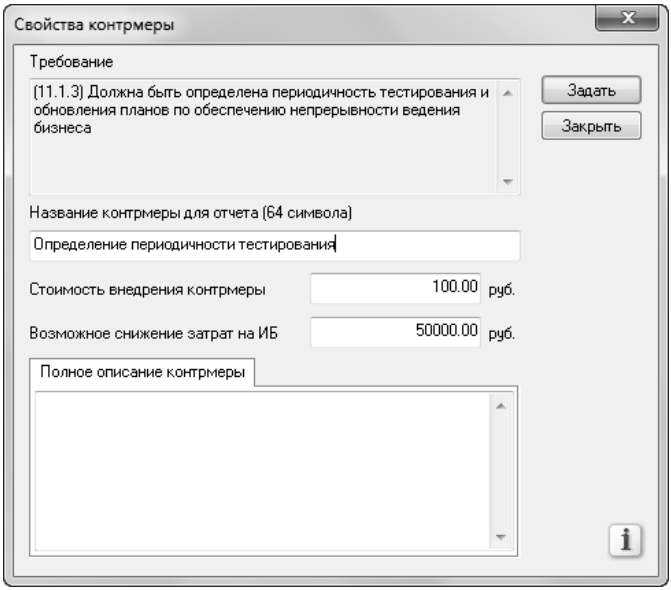


Рис. 19. Контрмера «Определение периодичности тестирования»

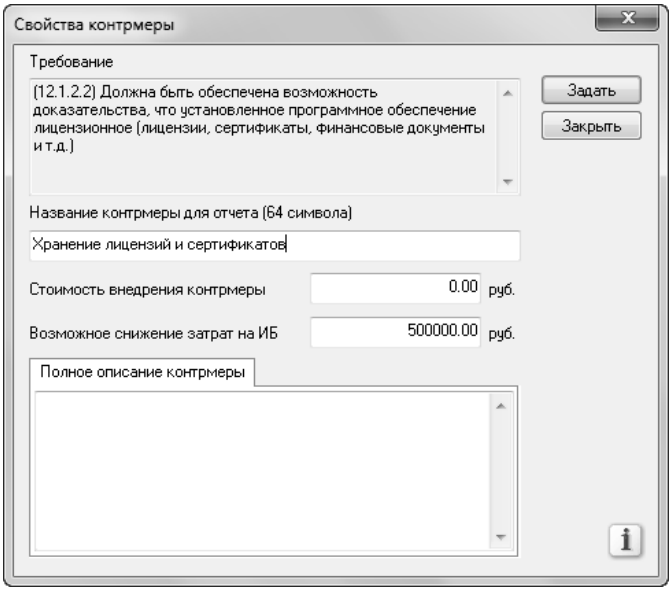


Рис. 20. Контрмера «Хранение лицензий и свидетельств»

После задания контрмеры к невыполненному положению можно увидеть соотношение стоимости данной контрмеры и величины, на которую изменилось значение риска от невыполненных требований (рис. 21). Убедитесь, что после задания контрмер риск будет снижен до приемлемого уровня. 10%.

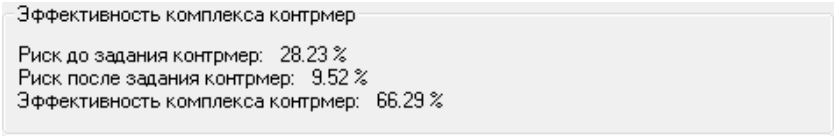


Рис. 21. Эффективность комплекса контрмер

Таким образом, КОНДОР позволяет расставить приоритеты и заранее оценить эффективность планируемых мероприятий при разработке или работе с уже существующей политикой информационной безопасности.

3.6 Управление периодами

Очевидно, что в зависимости от временного периода степень выполнения требований стандарта может меняться, поэтому аудит необходимо проводить периодически через определенные руководством компании промежутки времени. Таким образом, проект. временной интервал, содержащий несколько периодов, в котором анализируются изменения, произошедшие в компании за истекшие периоды.

Создать новый период аудита можно нажатием поля контекстного меню «Управление периодами» в первой части рабочего поля программы (рис. 1). Период. дата, на момент которой все введенные пользователем данные актуальны для информационной системы организации.

Возможны следующие действия при работе с периодами: выбор периода для редактирования, создание периода, изменение периода, удаление периода, сброс ответов за период (рис. 22).

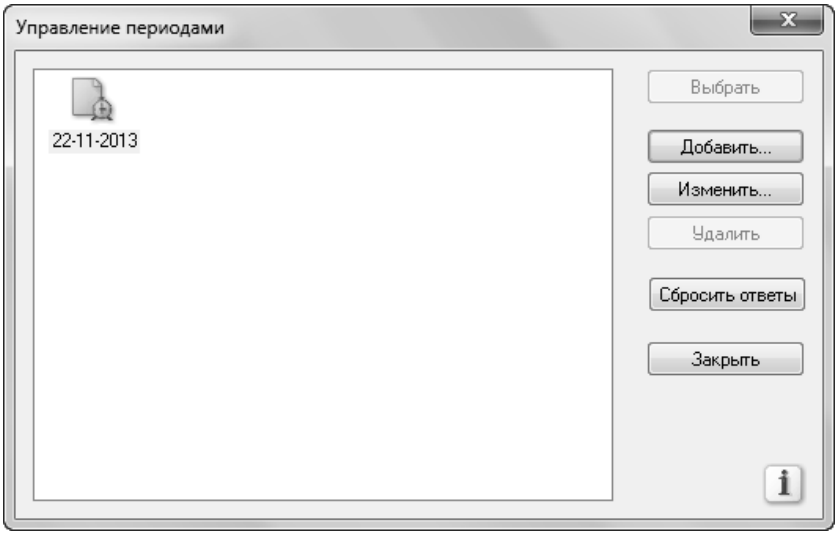


Рис. 22. Редактирование периодов аудита

3.7 Создание отчета

Выберите в меню программы раздел «Отчет ⟶ Создать отчет». Система позволяет сформировать и сохранить два типа отчета.

1) Отчет по периоду, который содержит:

– количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита;

– уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита;

– затраты на контрмеры в целом по системе для выбранного периода аудита;

– количество выполненных и невыполненных требований по каждому разделу стандарта;

– текст выполненных требований по каждому разделу;

– текст невыполненных требований по каждому разделу, отсортированных по уровню риска;

– введенные контрмеры для каждого невыполненного требования стандарта;

– комментарии эксперта по невыполненным требованиям.

2) Отчет по проекту, который содержит:

– изменения количества выполненных требований в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита;

– изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита;

– изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита.

С примером отчета, подготовленного к печати можно ознакомиться в приложении Б.

4 Задание на лабораторную работу

1) Изучите характеристики информационной системы для своего варианта (приложение В).

2) Ответьте на вопросы разделов, опираясь на имеющуюся информацию. Вопросы, явно незатронутые в тексте характеристики, считать не применимыми к информационной системе (ответа не требуют).

3) Установите расходы на информационную безопасность согласно варианту (табл. 5).

4) Измените весовые коэффициенты согласно варианту (табл. 6).

5) Установите контрмеры для невыполненных требований, пороговое значение которых больше 50%.

6) Сравните риск до применения контрмер и после. Стал ли риск приемлемым (не превышал 10%).

7) Оцените эффективность комплекса мер.

8) Создайте и сохраните отчет по периоду.

Табл. 5. Расходы на информационную систему, варианты

Расходы на информационную безопасность	
Вариант № 1	Затраты на внедрение систем ЗИ: 1 000 000 руб. Ежегодные затраты на поддержку и обучение: 600 000 руб. Ежегодные затраты на управление средствами защиты информации: 700 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 300 000 руб.
Вариант № 2	Затраты на внедрение систем ЗИ: 800 000 руб. Ежегодные затраты на поддержку и обучение: 250 000 руб. Ежегодные затраты на управление средствами защиты информации: 600 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 300 000 руб.

Продолжение табл. 5

Вариант № 3	Затраты на внедрение систем ЗИ: 900 000 руб. Ежегодные затраты на поддержку и обучение: 300 000 руб. Ежегодные затраты на управление средствами защиты информации: 650 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 250 000 руб.
Вариант № 4	Затраты на внедрение систем ЗИ: 600 000 руб. Ежегодные затраты на поддержку и обучение: 650 000 руб. Ежегодные затраты на управление средствами защиты информации: 700 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 200 000 руб.
Вариант № 5	Затраты на внедрение систем ЗИ: 500 000 руб. Ежегодные затраты на поддержку и обучение: 800 000 руб. Ежегодные затраты на управление средствами защиты информации: 500 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 200 000 руб.
Вариант № 6	Затраты на внедрение систем ЗИ: 700 000 руб. Ежегодные затраты на поддержку и обучение: 700 000 руб. Ежегодные затраты на управление средствами защиты информации: 400 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 50 000 руб.
Вариант № 7	Затраты на внедрение систем ЗИ: 400 000 руб. Ежегодные затраты на поддержку и обучение: 600 000 руб. Ежегодные затраты на управление средствами защиты информации: 500 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 100 000 руб.
Вариант № 8	Затраты на внедрение систем ЗИ: 800 000 руб. Ежегодные затраты на поддержку и обучение: 200 000 руб. Ежегодные затраты на управление средствами защиты информации: 500 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 150 000 руб.
Вариант № 9	Затраты на внедрение систем ЗИ: 850 000 руб. Ежегодные затраты на поддержку и обучение: 400 000 руб. Ежегодные затраты на управление средствами защиты информации: 450 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 50 000 руб.
Вариант № 10	Затраты на внедрение систем ЗИ: 650 000 руб. Ежегодные затраты на поддержку и обучение: 300 000 руб. Ежегодные затраты на управление средствами защиты информации: 500 000 руб. Прочие ежегодные затраты на обеспечение информационной безопасности: 100 000 руб.

Табл. 6. Весовые коэффициенты, варианты

Весовые коэффициенты	
Вариант № 1	Для раздела «Политика безопасности» поднимите весовые коэффициенты на 10 значений.
Вариант № 2	Для раздела «Организационные меры» поднимите весовые коэффициенты на 10 значений.
Вариант № 3	Для раздела «Управление ресурсами» опустите весовые коэффициенты на 15 значений.
Вариант № 4	Для раздела «Безопасность персонала» поднимите весовые коэффициенты на 10 значений.
Вариант № 5	Для раздела «Управление ресурсами» опустите весовые коэффициенты на 10 значений.
Вариант № 6	Для раздела «Безопасность персонала» опустите весовые коэффициенты на 5 значений.
Вариант № 7	Для раздела «Организационные меры» поднимите весовые коэффициенты на 5 значений.
Вариант № 8	Для раздела «Политика безопасности» опустите весовые коэффициенты на 15 значений.
Вариант № 9	Для раздела «Управление ресурсами» поднимите весовые коэффициенты на 5 значений.
Вариант № 10	Для раздела «Политика безопасности» опустите весовые коэффициенты на 10 значений.

5 Контрольные вопросы

1) Что представляет собой система КОНДОР и для чего она предназначена?
2) Какие задачи позволяет выполнять данная система?
3) Что понимается под расходами на информационную безопасность?
4) Для чего применяются весовые коэффициенты? Как их изменить?
5) Какие параметры можно включить в состав отчета по проекту?
6) Каким образом в системе КОНДОР задается контрмера для невыполненных требований?
7) Какие данные можно указать при задании контрмер?
8) Что такое «Управление периодами» и какие возможности оно предоставляет?
9) Какие типы отчетов позволяет создать система?
10) Каким образом можно реализовать, чтобы для пользователя отображались только критичные положения стандарта, которые не выполнены?

ПРАКТИЧЕСКАЯ РАБОТА №1
Формальное описание структуры информационной системы

1 Цель работы

Цель работы – получить навыки комплексного построения модели объекта защиты в виде формального описания процесса, связанного с обработкой защищаемой информации.

Задачи:

1. Выбор информационного процесса, в котором происходит обработка защищаемой информации.
2. Построение модели «чёрного ящика» данного процесса в нотации IDEF0.
3. Декомпозиция модели на три-четыре этапа в нотации IDEF0.
4. Корректировка модели «чёрного ящика» после декомпозиции на основе уточнённых данных.

Ответ на задание необходимо предоставить в виде файла в формате Word или PDF. В файле должны быть представлены основные результаты работы – модель «чёрного ящика» процесса и её декомпозиция, выполненные в нотации IDEF0.

Критерии оценки:

1. Выполнение задач на базовом уровне (в целом соблюдаются правила нотации IDEF0, этапы декомпозиции соответствуют выбранному варианту) оценивается в **4 балл**.
2. Выполнение задач на продвинутом уровне (соблюдаются правила нотации IDEF0, этапы декомпозиции и элементы т.е. стрелки, соответствуют выбранному варианту) и соблюдаются сроки сдачи работы оценивается в **6 балла**.

Итого за выполнение работы можно получить 6 балла.

Основные принципы функционального моделирования (IDEF0)

IDEF0 — методология функционального моделирования (англ. function modeling) и графическая нотация, предназначенная для формализации и описания бизнес-процессов.

1. Функциональный блок графически изображается в виде прямоугольника и олицетворяет собой некоторую конкретную функцию (действие) в рамках рассматриваемого процесса. Стрелки обозначают объекты различных типов

2. Верхняя сторона блока имеет значение «Управление» и входящие сверху в блок стрелки являются законодательными актами, регламентами, инструкциями, алгоритмами, фиксированными параметрами системы и др.

3. Левая сторона имеет значение «Вход», а правая сторона имеет значение «Выход» и все горизонтальные стрелки являются информацией (или носителем информации) в какой-либо форме представления – документы, файлы и базы данных, сетевые пакеты, количество ресурсов, сумма денег и т.п.

4. Нижняя сторона имеет значение «Механизм» (Mechanism) и входящие снизу в блок стрелки являются исполнителями – сотрудники организации, клиенты, автоматизированные системы, СУБД и т.п.

Более подробную информацию о данной нотации можно получить в рекомендациях Р 50.1.028-2001 "Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования".

Пример модели процесса

Тема **– Оплата покупки через контактный банковский терминал**.

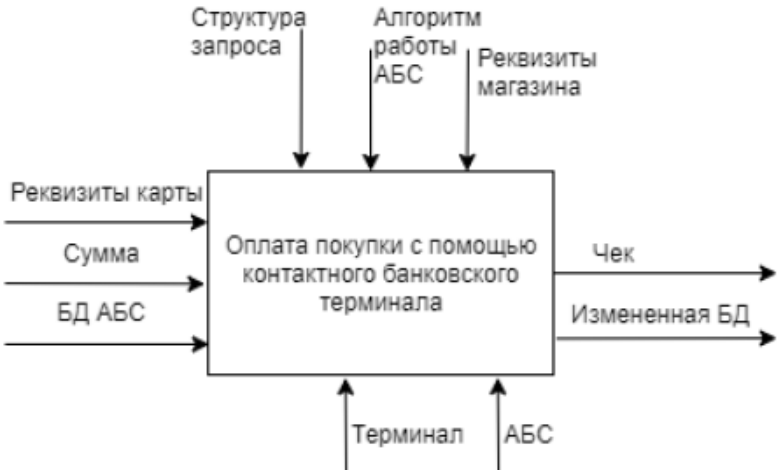


Рисунок 1 – Модель «чёрного ящика» процесса в нотации IDEF0

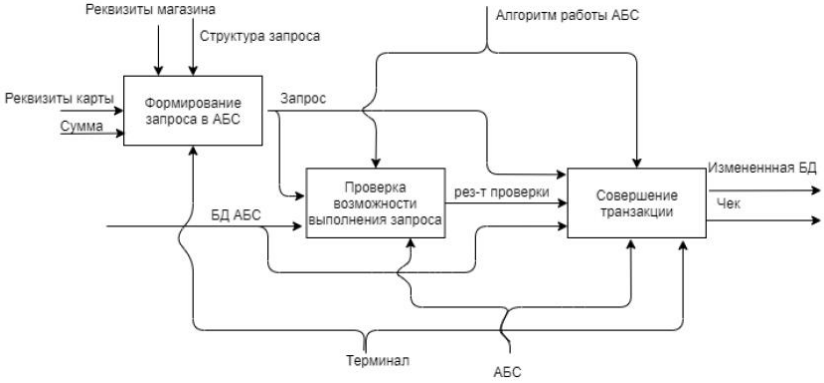


Рисунок 2 – Декомпозиция процесса в нотации IDEF0

ПРАКТИЧЕСКАЯ РАБОТА №2
Составление модели угроз информационной системе. Формирование требований к системе защиты информации

1 Цель работы

Цель работы – получить навыки комплексного моделирования угроз, учитывающего угрозы, направленные на информационную систему и обрабатываемую ей информацию, а также проектирование мер защиты от данных угроз.

Задачи:

1. На основе декомпозиции модели процесса, обрабатывающего защищаемую информацию, выделить перечень защищаемых элементов (все стрелки в декомпозиции) и классифицировать их на три типа – информационные элементы, исполнители, управление.

2. Привести по одному примеру угроз конфиденциальности, целостности и доступности для каждого информационного элемента (каждой горизонтальной стрелки) декомпозиции. Для каждой угрозы привести по одному примеру организационной и технической мер защиты.

3. Привести по одному примеру угроз конфиденциальности и целостности для каждого механизма реализации процесса (каждой стрелки снизу). Для каждой угрозы привести по одному примеру организационной и технической мер защиты.

4. Привести по одному примеру угроз конфиденциальности и целостности для каждого элемента управления процессом (каждой стрелки снизу). Для каждой угрозы привести по одному примеру организационной и технической мер защиты. Ответ на задание необходимо предоставить в виде файла в формате Word или PDF. В

файле должны быть представлены примеры угроз, направленных на различные элементы рассматриваемого процесса.

Критерии оценки:

1. Выполнение задач на базовом уровне (не менее 50% угроз для каждого типа элементов указаны корректно) оценивается в 2 балл.

2. Выполнение задач на продвинутом уровне (не менее 80% угроз для каждого типа элементов указаны корректно) оценивается в 3 балла.

3. Сдача работы в установленный срок 1 балл. Итого за выполнение лабораторной работы можно получить 4 балла.

Примеры угроз для различных типов стрелок.

Все → (горизонтальные стрелки) – это информация либо носители информации. Примеры угроз, направленных на информационные элементы: разглашение или перехват информации ограниченного доступа; несанкционированный доступ к документам; подделка документов; дезинформация; отказ в обслуживании и т.п.

Все ↑ (вертикальные стрелки снизу) – это исполнители. Примеры угроз, направленных на автоматизированные системы и людские ресурсы: несанкционированное отключение системы или её модуля; сбор информации о системе (её местонахождение, настройки и др.); повышение привилегий за счёт входа под чужой учётной записью; шантаж или подкуп сотрудника и т.п.

Все ↓ (вертикальные стрелки сверху) – это управление. Примеры угроз, направленных на управляющие, регламентирующие и нормативные данные, которыми руководствуются исполнители: внесение недекларированных возможностей в программное обеспечение; разработка нормативных документов, не соответствующих

законодательству; нарушение правил работы с конфиденциальной информацией и т.п.

Пример моделирования угроз

Тема – Оплата покупки через контактный банковский терминал.

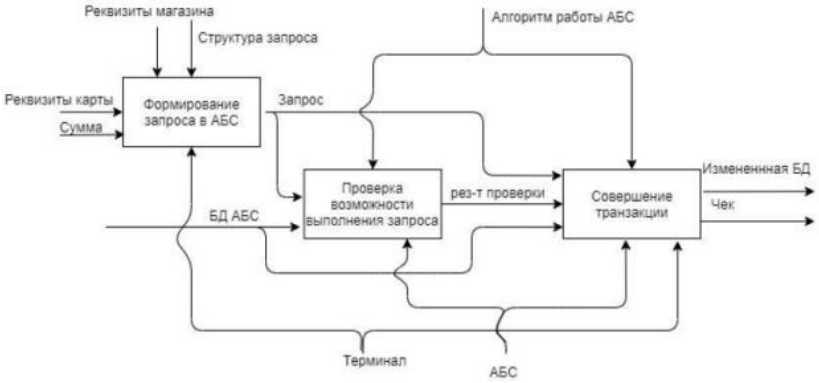


Рисунок 1 – Декомпозиция процесса в нотации IDEF0

ПРАКТИЧЕСКАЯ РАБОТА №3
Формирование требований к политике информационной безопасности. Формирование регламента действий при возникновении нештатных ситуаций.

1 Цель работы

Разработка предложения по совершенствованию системы управления информационной безопасностью. Осуществлять рациональный выбор средств обеспечения информационной безопасности с учетом предъявляемых к ним требований качества обслуживания и качества функционирования.

Сформировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа. Проводить технико-экономические обоснования и выбор оптимального решения задач, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности.

Входные данные:

- прайс лист средств защиты информации;
- перечень минимальных требований по защите информации;
- список выявленных уязвимостей в СЗИ.

2 Ход работы

Задачи команды защиты:

- изучение прайс-листа;
- выбор средств защиты и организационных мер;

Задачи команда аудита:

- проверка выбранных командой защиты средств, наличия у них сертификатов соответствия;
- оценка общей рентабельности и адекватности выбора средств.

Командой защиты составлена адекватная система защиты информации, которая удовлетворяет нормативным требованиям, и, по возможности, имеет минимальное количество уязвимостей.

Команда аудита проверила выбранные средства, опираясь на составленный ранее план, оценила общую рентабельность и адекватность выбора средств.

Команда защиты составляет таблицу следующего вида:

Уязвимость	Требование	Средство защиты/Организационная мера	Стоимость

В конце, Команда Защиты, подводит итог - общую стоимость средств, не выходящую за рамки бюджета.

План проверки Командой Аудита – заполненная таблица из первого этапа, проверка выполнения каждого требования. Каждое средство проверяется на наличие сертификатов соответствия, лицензий от регуляторов (ФСТЭК, ФСБ и пр.).

Общая рентабельность и адекватность внедрения средства защиты оценивается исходя из общего бюджета объекта, бюджета Команды Защиты и стоимости самого средства. Так же проверяется количество уязвимостей, закрываемых данным средством, совместимость с другими средствами, сравнение средства с его аналогами по стоимости и возможностям.

Приложение А
(Справочное)
Описание рассматриваемой системы

Вариант 1

Информационная система компании состоит из трех отделов: информационно-вычислительного центра, экономического отдела и бухгалтерии. Имеются два вида ресурсов: сервер и два компьютера. В компании одна сетевая группа. Компьютер экономического отдела, компьютер бухгалтерии и сервер объединены в сеть посредством сетевого коммутатора. На сервере хранится информация о ценовых предложениях для клиентов. Бухгалтерская информация хранится на компьютере бухгалтерии, информация о з/п хранится на компьютере экономического отдела. В системе всего три группы пользователей: системный администратор, экономисты, бухгалтеры. Выделены такие бизнес-процессы: внедрение изменений (для обработки информации о ценовых предложениях), подготовка и подписание договоров, начисление з/п. Системный администратор имеет доступ в Интернет и локальный доступ к информации о ценовых предложениях для клиентов со всеми правами доступа, экономисты имеют локальный доступ к информации о з/п с правами доступа «чтение» и «запись» и удаленный доступ с правом чтения к информации о ценовых предложениях для клиентов, бухгалтеры имеют локальный доступ к бухгалтерской информации с правом чтения и записи. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 2

Информационная система компании состоит из двух отделов: абонентского отдела и отдела связи. Имеются три вида ресурсов: сервер, компьютер, CD-диск. В компании одна сетевая группа. 3 компьютера и сервер связаны между собой маршрутизатором. На сервере хранится база данных абонентов, на компьютере в отделе связи – данные об услугах. Информация по эксплуатации и ремонту оборудования хранится на CD-диске. В системе для рассмотрения есть следующие пользователей: секретарь, инженер и техник. В компании осуществляется обслуживание клиентов, предоставляются услуги абонентам и производится контроль над оборудованием. При этом, секретарь имеет локальный доступ у себя на компьютере к данным об услугах с правом чтения, а инженер удаленный доступ через маршрутизатор к базе данных абонентов на сервере с правом чтения и удаления. Техник имеет локальный доступ к

информации по эксплуатации и ремонту оборудования с правом чтения. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 3

Информационная система компании состоит из трех отделов: отдел продаж, бухгалтерия и отдел по приему товара. В компании одна сетевая группа, которая состоит из 2 компьютеров и сервера, которые связаны между собой коммутатором. На сервере хранится информация о себестоимости продукции и бухгалтерская информация, на компьютере в отделе по приему товара – информация о ценовых предложениях. В системе есть такие пользователи, как менеджер, бухгалтер и секретарь. В компании осуществляется обслуживание клиентов, закупка товаров и начисление з/п. При этом, менеджер имеет локальный доступ к информации о себестоимости продукции с правами чтения и записи, бухгалтер имеет удаленный доступ к бухгалтерской информации с правами записи, чтения и удаления, а секретарь имеет локальный доступ к информации о ценовых предложениях с правом одного чтения. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 4

Информационная система компании состоит из трех отделов: конструкторский отдел, отдел кадров, научно-исследовательский отдел. В компании одна сетевая группа, которая состоит из 3 компьютеров и сервера. На сервере хранится информация о новых проектах, на компьютере отдела кадров – штатное расписание, на компьютере НИО – информация о новых информационных технологиях. В системе есть такие пользователи, как инженер-конструктор, начальник отдела кадров и программист. В компании осуществляется разработка конструкций, прием новых сотрудников и создание новых технологий. При этом, инженер-конструктор имеет удаленный доступ к информации о новых проектах (через коммутатор) с правами чтения, записи и удаления, начальник отдела кадров – локальный доступ к штатному расписанию с правами чтения и записи, а программист – локальный доступ к информации о новых информационных технологиях с правами чтения и записи. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 5

Информационная система компании состоит из трех отделов: отдел снабжения, отдел рекламы, профсоюз. В компании одна сетевая группа, которая состоит из 3 компьютеров и сервера (соединены маршрутизатором). На сервере хранится информация о заявках, на компьютере в отделе снабжения – данные о продукции, на компьютере профсоюза – информация о работниках. В системе есть такие пользователи, как менеджер, администратор, начальник профсоюза. В компании осуществляется закупка товара, создание рекламных лозунгов, работа с сотрудниками. При этом, менеджер имеет локальный доступ к информации о заявках с правами чтения и записи, администратор – локальный доступ к данным о продукции с правами чтения и записи, начальник профсоюза – локальный доступ к информации о работниках с правами чтения и удаления. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 6

Информационная система компании состоит из трех отделов: информационно-вычислительного центра, экономического отдела и бухгалтерии. Имеются два вида ресурсов: сервер и два компьютера. В компании одна сетевая группа. Компьютер экономического отдела, компьютер бухгалтерии и сервер объединены в сеть посредством сетевого коммутатора. На сервере хранится информация о ценовых предложениях для клиентов. Бухгалтерская информация хранится на компьютере бухгалтерии, информация о з/п хранится на компьютере экономического отдела. В системе всего три группы пользователей: системный администратор, экономисты, бухгалтеры. Выделены такие бизнес-процессы: внедрение изменений (для обработки информации о ценовых предложениях), подготовка и подписание договоров, начисление з/п. Системный администратор имеет доступ в Интернет и локальный доступ к информации о ценовых предложениях для клиентов со всеми правами доступа, экономисты имеют локальный доступ к информации о з/п с правами доступа «чтение» и «запись» и удаленный доступ с правом чтения к информации о ценовых предложениях для клиентов, бухгалтеры имеют локальный доступ к бухгалтерской информации с правом чтения и записи. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 7

Информационная система компании состоит из двух отделов: абонентского отдела и отдела связи. Имеются три вида ресурсов: сервер, компьютер, CD-диск. В компании одна сетевая группа. 3 компьютера и сервер связаны между собой маршрутизатором. На сервере хранится база данных абонентов, на компьютере в отделе связи – данные об услугах. Информация по эксплуатации и ремонту оборудования хранится на CD-диске. В системе для рассмотрения есть следующие пользователей: секретарь, инженер и техник. В компании осуществляется обслуживание клиентов, предоставляются услуги абонентам и производится контроль над оборудованием. При этом, секретарь имеет локальный доступ у себя на компьютере к данным об услугах с правом чтения, а инженер удаленный доступ через маршрутизатор к базе данных абонентов на сервере с правом чтения и удаления. Техник имеет локальный доступ к информации по эксплуатации и ремонту оборудования с правом чтения. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 8

Информационная система компании состоит из трех отделов: отдел продаж, бухгалтерия и отдел по приему товара. В компании одна сетевая группа, которая состоит из 2 компьютеров и сервера, которые связаны между собой коммутатором. На сервере хранится информация о себестоимости продукции и бухгалтерская информация, на компьютере в отделе по приему товара – информация о ценовых предложениях. В системе есть такие пользователи, как менеджер, бухгалтер и секретарь. В компании осуществляется обслуживание клиентов, закупка товаров и начисление з/п. При этом, менеджер имеет локальный доступ к информации о себестоимости продукции с правами чтения и записи, бухгалтер имеет удаленный доступ к бухгалтерской информации с правами записи, чтения и удаления, а секретарь имеет локальный доступ к информации о ценовых предложениях с правом одного чтения. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 9

Информационная система компании состоит из трех отделов: конструкторский отдел, отдел кадров, научно-исследовательский отдел. В компании одна сетевая группа, которая состоит из 3 компьютеров и

сервера. На сервере хранится информация о новых проектах, на компьютере отдела кадров – штатное расписание, на компьютере НИО. информация о новых информационных технологиях. В системе есть такие пользователи, как инженер-конструктор, начальник отдела кадров и программист. В компании осуществляется разработка конструкций, прием новых сотрудников и создание новых технологий. При этом, инженер-конструктор имеет удаленный доступ к информации о новых проектах (через коммутатор) с правами чтения, записи и удаления, начальник отдела кадров – локальный доступ к штатному расписанию с правами чтения и записи, а программист – локальный доступ к информации о новых информационных технологиях с правами чтения и записи. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Вариант 10

Информационная система компании состоит из трех отделов: отдел снабжения, отдел рекламы, профсоюз. В компании одна сетевая группа, которая состоит из 3 компьютеров и сервера (соединены маршрутизатором). На сервере хранится информация о заявках, на компьютере в отделе снабжения – данные о продукции, на компьютере профсоюза – информация о работниках. В системе есть такие пользователи, как менеджер, администратор, начальник профсоюза. В компании осуществляется закупка товара, создание рекламных лозунгов, работа с сотрудниками. При этом, менеджер имеет локальный доступ к информации о заявках с правами чтения и записи, администратор. локальный доступ к данным о продукции с правами чтения и записи, начальник профсоюза – локальный доступ к информации о работниках с правами чтения и удаления. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

Приложение Б
(Справочное)
Пример отчета о результатах анализа информационной системы

Отчет
о результатах анализа информационной системы

Объект:	ООО "Секретное производство"
Ответственный:	Иванов Петр Леонидович
Должность:	Руководитель службы безопасности
Дата:	27.11.2013

Отчет

Условные обозначения

Р - риск;
НТ - невыполненные требования.

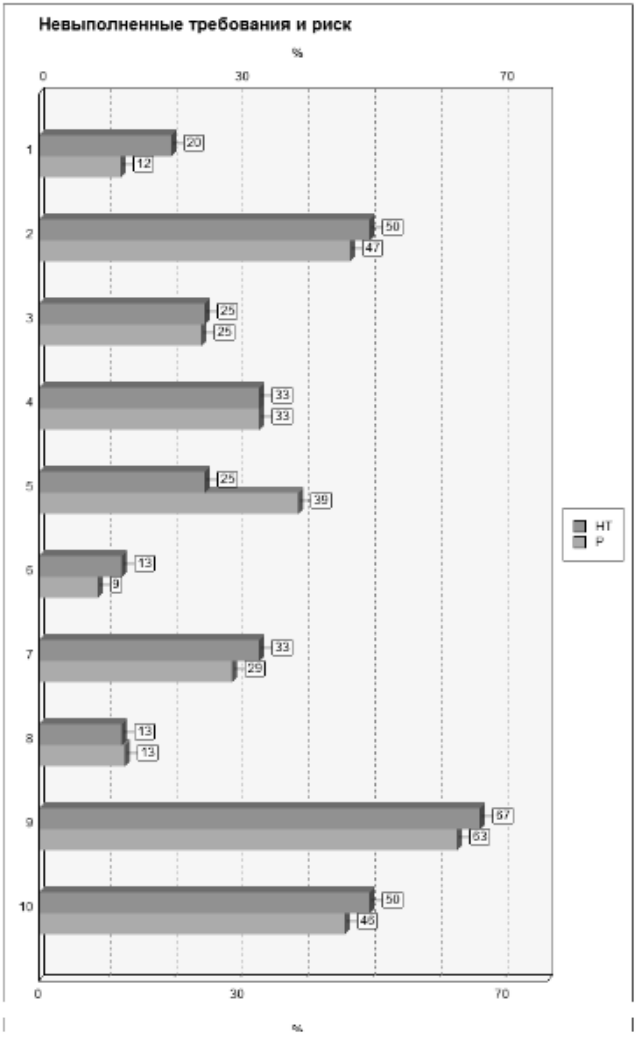
Период: 24.11.2013

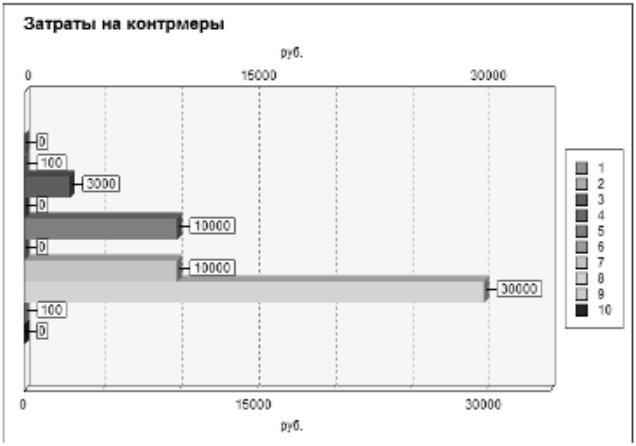
1. Сводные данные

1.1. Сводные данные по системе

Показатель	Значение
Не отвечено вопросов	398
Всего требований	46
Выполнено	33
Не выполнено	13
Уровень риска, %	28.23
Затраты на контрмеры, руб.	53200.00

1.2. Сводные данные по разделам


Невыполненные требования и риск
%
0
30
70
1
20
12
2
50
47
3
25
25
4
33
33
5
25
39
6
13
9
7
33
29
8
13
13
9
67
63
10
50
46
НТ
Р
%



№	Раздел	Всего требований	Выполнено	Не выполнено	Уровень риска, %	Затраты на контрмеры, руб.
1	Политика безопасности	5	4	1	12.33	0.00
2	Организационные меры	6	3	3	46.94	100.00
3	Управление ресурсами	4	3	1	24.66	3000.00
4	Безопасность персонала	3	2	1	33.33	0.00
5	Физическая безопасность	4	3	1	39.13	10000.00
6	Управление коммуникациями и процесами	8	7	1	8.82	0.00
7	Контроль доступа	3	2	1	29.17	10000.00
8	Разработка и сопровождение систем	8	7	1	12.96	30000.00
9	Непрерывность ведения бизнеса	3	1	2	63.16	100.00
10	Соответствие системы требованиям	2	1	1	46.15	0.00

2. Политика безопасности

2.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	12
Всего требований	5
Выполнено	4
Не выполнено	1
Уровень риска, %	12.33
Затраты на контрмеры, руб.	0.00

2.2 Выполненные требования

1. (3.1) В информационной системе должна существовать политика безопасности

2. (3.1.1) Политика безопасности должна утверждаться руководством организации

3. (3.1.2) Пересмотр положений политики безопасности обязательно должен проводиться в результате следующих случаев

- Серьезных инцидентов в области информационной безопасности
- Обнаружения новых уязвимостей

2.3 Невыполненные требования

2.3.1 Высокий уровень риска

-

2.3.2 Средний уровень риска

1. (3.1.2) Пересмотр положений политики безопасности обязательно должен проводиться в результате следующих случаев

- Изменений в организационной или технической инфраструктуре организации

Контрмера	Стоимость, руб.	Эффективность по системе, %
-	-	-

2.3.3. Низкий уровень риска

-

3. Организационные меры

3.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	18
Всего требований	6
Выполнено	3
Не выполнено	3
Уровень риска, %	46.94
Затраты на контрмеры, руб.	100.00

3.2 Выполненные требования

1. (4.1.2) Должны быть четко определены ответственность и обязанности по защите отдельных ресурсов и выполнению конкретных действий по обеспечению безопасности

2. (4.1.3) Должны быть четко определены зоны ответственности каждого владельца ресурса, несущего ответственность за обеспечение его безопасности

- Должны быть четко определены и описаны все ресурсы, входящие в зону ответственности, а также все действия по обеспечению безопасности в данной зоне
- Для каждого ресурса (или процесса) должен быть назначен ответственный сотрудник из числа руководителей. Все его обязанности и степень ответственности должны быть закреплены документально

3.3 Невыполненные требования

3.3.1 Высокий уровень риска

1. (4.1.3) При частичной или полной передаче обязанностей по обеспечению безопасности с владельца ресурса на какого-либо сотрудника или поставщика данного ресурса, ответственность все равно остается полностью на владельце данного ресурса

Контрмера	Стоимость, руб.	Эффективность по системе, %
Изменение ответственного за ресурс	100.00	8.00

2. (4.1.3) Должны быть четко определены зоны ответственности каждого владельца ресурса, несущего ответственность за обеспечение его безопасности

- Должны быть четко определены и задокументированы уровни полномочий каждого ответственного лица

Контрмера	Стоимость, руб.	Эффективность по системе, %
-	-	-

- Для каждого ресурса должен быть определен и закреплен документально список прав доступа (матрица доступа)

Контрмера	Стоимость, руб.	Эффективность по системе, %
-	-	-

3.3.2 Средний уровень риска

-

3.3.3. Низкий уровень риска

-

4. Управление ресурсами

4.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	10
Всего требований	4
Выполнено	3
Не выполнено	1
Уровень риска, %	24.66
Затраты на контрмеры, руб.	3000.00

4.2 Выполненные требования

1. (5.1) Должны быть учтены все основные информационные ресурсы

2. (5.1.1) Должны быть идентифицированы все основные ресурсы и сервисы

3. (5.2) Важно классифицировать информацию, чтобы определить необходимость и степень ее защиты

4.3 Невыполненные требования

4.3.1 Высокий уровень риска

1. (5.1.1) Должны быть документально определены ресурс, его владелец, необходимый уровень безопасности, а также местоположение ресурса

Контрмера	Стоимость, руб.	Эффективность по системе, %
Инвентаризация - запись местоположения	3000.00	10.29

-

4.3.2 Средний уровень риска

-

4.3.3. Низкий уровень риска

-

5. Безопасность персонала

5.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	19
Всего требований	3
Выполнено	2
Не выполнено	1
Уровень риска, %	33.33
Затраты на контрмеры, руб.	0.00

5.2 Выполненные требования

1. (6.1.2) Необходима проверка персонала при приеме на работу

- Должны проверяться рекомендации и данные из резюме
- Необходимо проводить идентификацию личности (паспорт и т.п.)

5.3 Невыполненные требования

5.3.1 Высокий уровень риска

1. (6.1.2) Необходима проверка персонала при приеме на работу

- Необходимо обеспечивать подтверждение ученых степеней и профессиональных навыков

Контрмера	Стоимость, руб.	Эффективность по системе, %
	0.00	8.00

5.3.2 Средний уровень риска

-

5.3.3. Низкий уровень риска

-

6. Физическая безопасность

6.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	43
Всего требований	4
Выполнено	3
Не выполнено	1
Уровень риска, %	39.13
Затраты на контрмеры, руб.	10000.00

6.2 Выполненные требования

1. (7.1.3) Средства обработки данных организации должны быть физически изолированы от средств обработки данных сторонних организаций

2. (7.1.3) Каталоги и внутренние телефонные книги, которые могут дать информацию о нахождении критичных ресуросв, должны быть недоступны случайным лицам

3. (7.1.3) Огнеопасные и взрывчатые материалы должны быть расположены на безопасном расстоянии от охраняемых зон

6.3 Невыполненные требования

6.3.1 Высокий уровень риска

1. (7.1.3) Резервные носители информации и резервное оборудование должны располагаться в отдельном месте на безопасном расстоянии

Контрмера	Стоимость, руб.	Эффективность по системе, %
Перемещение резервного оборудования	10000.00	10.29

-

6.3.2 Средний уровень риска

-

6.3.3. Низкий уровень риска

-

7. Управление коммуникациями и процессами

7.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	92

Показатель	Значение
Всего требований	8
Выполнено	7
Не выполнено	1
Уровень риска, %	8.82
Затраты на контрмеры, руб.	0.00

7.2 Выполненные требования

1. (8.6.3) Необходимо определить процедуры обращения с информацией и ее хранения

- Учет и маркировка всех носителей
- Ограничение доступа неавторизованных пользователей
- Ведение регистрации всех авторизованных лиц, получающих доступ к данным
- Обеспечение контроля полноты входных данных, корректной обработки и соответствия информации на выходе
- Хранение носителей данных в соответствии с указаниями поставщика
- Предоставление доступа к данным минимальному числу лиц
- Регулярная проверка перечней пользователей, имеющих право доступа к данным

7.3 Невыполненные требования

7.3.1 Высокий уровень риска

-

7.3.2 Средний уровень риска

1. (8.6.3) Необходимо определить процедуры обращения с информацией и ее хранения

- Обеспечение защиты буферных данных соответственно уровню их критичности

Контрмера	Стоимость, руб.	Эффективность по системе, %
-	-	-

7.3.3. Низкий уровень риска

-

8. Контроль доступа

8.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	91
Всего требований	3
Выполнено	2
Не выполнено	1
Уровень риска, %	29.17
Затраты на контрмеры, руб.	10000.00

8.2 Выполненные требования

1. (9.3.2) Все пользователи должны быть осведомлены о правилах защиты оборудования, оставленного без присмотра

- Необходимо завершать активную сессию перед уходом, если невозможно использование специальных блокирующих механизмов, например, парольная блокировка экрана
- Неиспользуемые рабочие станции и терминалы должны быть защищены от неавторизованного доступа при помощи блокировки клавиатуры или парольной защиты

8.3 Невыполненные требования

8.3.1 Высокий уровень риска

1. (9.3.2) Все пользователи должны быть осведомлены о правилах защиты оборудования, оставленного без присмотра

- Обязательно завершать соединение с сервером по окончании работы с ним, а не просто выключать терминал или компьютер

Контрмера	Стоимость, руб.	Эффективность по системе, %
Инструктаж	10000.00	8.00

8.3.2 Средний уровень риска

-

8.3.3. Низкий уровень риска

-

9. Разработка и сопровождение систем

9.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	56
Всего требований	8
Выполнено	7
Не выполнено	1
Уровень риска, %	12.96
Затраты на контрмеры, руб.	30000.00

9.2 Выполненные требования

1. (10.3) Должна существовать политика использования систем криптографической защиты информации (СКЗИ)

2. (10.3) При разработке политики использования СКЗИ необходимо учесть ряд требований и условий

- Управленческий подход к использованию СКЗИ внутри организации (например, какие именно классы информации должны быть защищены)
- Распределение обязанностей: кто и за что несет ответственность
- Внедрение политики
- Управление ключами
- Стандарты, которые могут быть внедрены и адаптированы в организации (какие решения для каких бизнес-процессов подходят)
- Политика управления ключами, включая методы для восстановления зашифрованной информации в случае утери, компрометации или уничтожения ключей

9.3 Невыполненные требования

9.3.1 Высокий уровень риска

1. (10.3) При разработке политики использования СКЗИ необходимо учесть ряд требований и условий

- Порядок определения адекватного уровня криптографической защиты

Контрмера	Стоимость, руб.	Эффективность по системе, %
Установления порядка определения адекватного уровня КЗ	30000.00	8.00

9.3.2 Средний уровень риска

-

9.3.3. Низкий уровень риска

-

10. Непрерывность ведения бизнеса

10.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	23
Всего требований	3
Выполнено	1
Не выполнено	2
Уровень риска, %	63.16
Затраты на контрмеры, руб.	100.00

10.2 Выполненные требования

1. (11.1.3) Особое внимание должно уделяться оценке зависимости бизнеса от внешних связей

10.3 Невыполненные требования

10.3.1 Высокий уровень риска

1. (11.1.3) Все согласованные процедуры по обеспечению непрерывности ведения бизнеса должны быть документированы

Контрмера	Стоимость, руб.	Эффективность по системе, %
-	-	-

2. (11.1.3) Должна быть определена периодичность тестирования и обновления планов по обеспечению непрерывности ведения бизнеса

Контрмера	Стоимость, руб.	Эффективность по системе, %
Определение периодичности тестирования	100.00	6.86

-

10.3.2 Средний уровень риска

-

10.3.3. Низкий уровень риска

-

11. Соответствие системы требованиям

11.1 Сводные данные по разделу

Показатель	Значение
Не отвечено вопросов	34
Всего требований	2
Выполнено	1
Не выполнено	1
Уровень риска, %	46.15
Затраты на контрмеры, руб.	0.00

11.2 Выполненные требования

1. (12.1.2.2) Должны быть разработаны типовые процедуры приобретения программного обеспечения

11.3 Невыполненные требования

11.3.1 Высокий уровень риска

1. (12.1.2.2) Должна быть обеспечена возможность доказательства, что установленное программное обеспечение лицензионное (лицензии, сертификаты, финансовые документы и т.д.)

Контрмера	Стоимость, руб.	Эффективность по системе, %
Хранение лицензий и сертификатов	0.00	6.86

-

11.3.2 Средний уровень риска

-

11.3.3. Низкий уровень риска

-

Приложение В
(Справочное)
Характеристики информационных систем

Табл. Б.1. Описание системы, вариант №1

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная Советом директоров организации Политика информационной безопасности. В ПБ не учтены требования по обеспечению непрерывности бизнеса. Данная Политика доведена до сведения всех сотрудников организации в доступной и понятной форме. Для гарантии качественного выполнения требований Политики безопасности на практике 1 раз в год проводится аудит.
Правила управления криптографической защитой В организации установлены правила управления криптографической защитой: – ограничения импорта и/или экспорта аппаратных и программных средств для выполнения криптографических функций; – ограничения импорта и/или экспорта аппаратных и программных средств, которые разработаны таким образом, что имеют, как дополнение, криптографические функции. Данные правила не включают обязательные или дискреционные методы доступа со стороны государства к информации, зашифрованной с помощью аппаратных или программных средств для обеспечения конфиденциальности ее содержания.
Структура планов обеспечения непрерывности В структуре планов обеспечения непрерывности бизнеса предусматривается следующее: – условия реализации планов, которые определяют порядок действий должностных лиц, которому необходимо следовать (как оценивать ситуацию, кто должен принимать участие, и т.д.) перед введением в действие каждого пункта плана; – процедуры на случай чрезвычайных ситуаций, которые должны быть предприняты после инцидента, подвергающего опасности бизнес-операции и/или человеческую жизнь; – меры по управлению связями с общественностью и эффективное взаимодействие с соответствующими государственными органами, например, с милицией, пожарной охраной и местными органами власти; – – процедуры перехода на аварийный режим работы, которые описывают необходимые действия по переносу важных бизнес-операций или сервисов-поддержки в альтернативное временное место размещения и по восстановлению бизнес-процессов в требуемые периоды времени; – процедуры возобновления работы, которые описывают необходимые действия для возвращения к нормальному режиму ведения бизнеса; – график поддержки плана, который определяет сроки и методы тестирования, а также описание процесса поддержки плана;

Продолжение табл. Б.1

Не включены мероприятия по обучению персонала, которые направлены на понимание процессов обеспечения непрерывности бизнеса сотрудниками, и поддержание постоя иной эффективности этих процессов.
Правила обеспечения безопасности при выборе и использовании паролей Политика безопасности обязывает всех пользователей информационной системы соблюдать определенные правила обеспечения безопасности при выборе и использовании паролей. Поэтому все пользователи осведомлены о необходимости: а) сохранения конфиденциальности паролей; б) запрещения записи паролей на бумаге, если только не обеспечено безопасное их хранение; в) изменения паролей всякий раз, при наличии любого признака возможной компрометации системы или пароля; г) выбора качественных паролей с минимальной длиной в шесть знаков, которые: – легко запоминаются; – не подвержены легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, например, имен, номеров телефонов, дат рождения и т.д.; – не содержат последовательных идентичных символов и не состоят из полностью числовых или полностью буквенных групп; д) изменения паролей через равные интервалы времени или после определенного числа доступов и исключения повторного или цикличного использования старых паролей (пароли для привилегированных учетных записей следует менять чаще, чем обычные пароли); е) изменения временных паролей при первой регистрации в системе; ж) з) исключения коллективного использования индивидуальных паролей. Отсутствует запрет включения паролей в автоматизированный процесс регистрации, например, с использованием хранимых макрокоманд или функциональных клавиш. Пользователям, нуждающимся в доступе к многочисленным услугам или бизнес-приложениям не рекомендуют использовать один качественный пароля для всех сервисов, обеспечивающих разумный уровень защиты хранимого пароля.
Требования к эксплуатации новых версий и обновлений ПО Для снижения риска перегрузки систем проводиться анализ предполагаемой ее нагрузки. Требования к эксплуатации новых версий и обновлений ПО документально оформляются и тестируются перед их приемкой и использованием. Проверка также определяет, не окажут ли вносимые изменения влияния на необходимую производительность компьютеров. Документально оформленные требования и критерии для принятия новых систем: – оценка выполнения требований к мощности и производительности компьютера; – определение процедур восстановления после сбоев и повторного запуска, а также формирование планов обеспечения непрерывной работы; – подготовка и тестирование типовых операционных процессов на соответствие определенным стандартам;

Продолжение табл. Б.1

– наличие необходимого набора средств контроля информационной безопасности; – разработка эффективных руководств по процедурам; – обязательная проверка отсутствия неблагоприятного влияния новых систем на существующие, особенно во время максимальных нагрузок, например, в конце месяца; – организация профессиональной подготовки персонала к эксплуатации и использованию новых систем. Не всегда соблюдается требование обеспечения непрерывности бизнеса. Не производится контроль проведения анализа влияния, оказываемого новой системой на общую информационную безопасность организации.
Проверка корректности данных вывода Чтобы обеспечивать уверенность в том, что обработка информации внутри системы выполнена правильно, данные, выводимые из прикладной системы, проверяются на корректность. Подтверждение корректности данных вывода включает: – проверки на правдоподобие с целью определения, являются ли выходные данные приемлемыми; – проверки контрольных счетчиков на предмет удостоверения, что все данные были обработаны; – процедуры по выполнению тестов на подтверждение выводимых данных; – определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных. Не производятся проверки того, достаточной ли информацией был обеспечен получатель результатов вывода или последующей системы обработки для определения корректности, законченности, точности и классификации информации.
Аутсорсинг, контракт Бухгалтерия организации передана на аутсорсинг. Составлен контракт, в котором учтено: – достижение договоренностей, обеспечивающих уверенность в том, что все стороны, включая субподрядчиков, осведомлены о своих обязанностях, касающихся безопасности; – как будут обеспечиваться и тестироваться параметры целостности и конфиденциальности бизнес-активов организации; – типы физических и логических методов по управлению информационной безопасностью, используемых при предоставлении необходимого доступа к чувствительной служебной информации организации сторонним пользователям; – обеспечение доступности сервисов в случае бедствия; – право на проведение аудита. Контракт не включает в себя: – определение, как будут обеспечиваться юридический требования, в частности закон о защите информации; – уровень физической безопасности, который должен обеспечиваться для оборудования аутсорсинговой организации.

Продолжение табл. Б.1

Учет активов организации Каждый актив организации идентифицирован и классифицирован с точки зрения безопасности. Результаты инвентаризации оформляются в сводной таблице: с указанием инвентарного номера и его фактического местоположения. Владелец актива не указывается.

Табл. Б.2. Описание системы, вариант №2

Содержание политики информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная генеральным директором организации Политика информационной безопасности. В политике содержится: – определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации; – изложение целей и принципов информационной безопасности, сформулированных руководством; – требования в отношении обучения руководящего состава вопросам безопасности; – ответственность за нарушения политики безопасности; – ссылки на документы, дополняющие политику информационной безопасности. ПБ не содержит инструкций предупреждения и обнаружения вредоносного ПО.
Задача сотрудников по обеспечению ИБ Задача обеспечения ИБ включена в должностные инструкции всех сотрудников, причем как общие обязанности по внедрению или соблюдению политики безопасности, так и специфические особенности по защите определенных активов или действий, касающихся безопасности. Существуют формализованные процедуры, устанавливающие дисциплинарную ответственность сотрудников, нарушивших политику и процедуры безопасности организации. К их числу относятся написание объяснительных записок, лишение премий, наложение штрафов и т.п., вплоть до увольнения с занесением в трудовую книжку. Соглашение о конфиденциальности не является частью трудового договора, но является рекомендуемым к подписанию.
Техническое обслуживание оборудования Для обеспечения непрерывной работоспособности и целостности оборудования проводится техническое обслуживание. При этом соблюдены требования: – оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком; – необходимо, чтобы техническое обслуживание и ремонт оборудования проводились только авторизованным персоналом; – следует хранить записи обо всех случаях предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного технического обслуживания;

Продолжение табл. Б.2

– необходимо принимать соответствующие меры безопасности при отправке оборудования для технического обслуживания за пределы организации. Кроме этого должны соблюдаться все требования, устанавливаемые использующимися правилами страхования. Оборудование, информацию или программное обеспечение можно выносить из помещений организации только на основании соответствующего разрешения. Оборудование следует регистрировать при выносе и при вносе, а также делать отметку, когда оно возвращено. При передаче третьей стороне носителей данных, содержащих важную информацию, иногда используются стандартные функции удаления.
Аутентификация сообщений Для обнаружения неавторизованных изменений или повреждений содержания переданного электронного сообщения особой важности (при электронных переводах денежных средств, пересылке спецификаций, контрактов, коммерческих предложений и пр.) используется аутентификация сообщений, реализованная в программном алгоритме (аппаратным путем). Для защиты содержания сообщения от неправомочного его раскрытия используются криптографические методы. Специальной политики использования СКЗИ в организации нет.
Аутсорсинг, контракт Бухгалтерия организации передана на аутсорсинг. Для управления ИБ составлен контракт, в котором учтено: – выполнение требований законодательства в отношении защиты данных; – достижение договоренностей, обеспечивающих уверенность в том, что все стороны, включая субподрядчиков, осведомлены о своих обязанностях, касающихся безопасности; – уровни физической безопасности, которые должны быть обеспечены в отношении оборудования, используемого в рамках аутсорсинга; – право на проведение аудита. В тексте контракта нет информации: – о том, как будут обеспечиваться и тестироваться параметры целостности и конфиденциальности бизнес-активов организации; – о типах физических и логических методов по управлению ИБ, используемых при предоставлении необходимого доступа к критичной служебной информации организации сторонним пользователям; – о принципах поддержания доступности сервисов в случае инцидента в области ИБ.
Требования к авторизации Предоставление и использование привилегий при применении средств многопользовательской информационной системы осуществляется только при условии выполнения требований безопасности посредством формализованного процесса авторизации. При этом применяются следующие меры: – идентификация привилегий в отношении каждого системного продукта, например, операционной системы, системы управления базами данных и каждого бизнес-приложения, а также категорий сотрудников, которым эти привилегии должны быть предоставлены;

Продолжение табл. Б.2

– привилегии предоставляются только тем сотрудникам, которым это необходимо для работы и только на время ее выполнения, например, предоставляя минимальные возможности по работе с системой для выполнения требуемых функций, только когда в этом возникает потребность; – обеспечивается процесс авторизации и регистрации всех предоставленных привилегий. Привилегии не предоставляются до завершения процесса авторизации; – используются различные идентификаторы пользователей при работе в обычном режиме и с использованием привилегий. В организации не проводится политика разработки и использования стандартных системных утилит (скриптов) для исключения необходимости в предоставлении дополнительных привилегий пользователям.
Ответственность персонала за активы Для каждого материального и информационного актива и процесса, связанного с информационной безопасностью, назначен ответственный администратор (владелец) из числа руководителей. Все детали обязанностей и ответственности четко определены и зафиксированы документально. Не все ресурсы определены документально с указанием их владельцев, необходимого уровня безопасности и местоположения.
Информационные ресурсы В организации назначено должностное лицо, отвечающее за защиту данных путем соответствующего разъяснения менеджерам, пользователям и поставщикам услуг об их индивидуальной ответственности, а также обязательности выполнения соответствующих мероприятий по обеспечению информационной безопасности. Владельцы данных обязаны информировать это должностное лицо о любых предложениях о способах хранения персональной информации в структуре файла данных, а также знать применяемые нормы законодательства в отношении защиты личных данных. Несмотря на информированность сотрудников и временных пользователей о том, что они имеют права доступа к информационным ресурсам только в случаях, которые санкционированы и закреплены документально, периодически информационные ресурсы организации подвергаются нецелевому использованию (не для производственных целей, а для личных целей сотрудников). В случае выявления нарушения блокируется доступ к информационным ресурсам.
Планы обеспечения непрерывности бизнеса В структуре планов обеспечения непрерывности бизнеса предусматривается следующее: – условия реализации планов, которые определяют порядок действий должностных лиц, которому необходимо следовать (как оценивать ситуацию, кто должен принимать участие, и т.д.) перед введением в действие каждого пункта плана; – процедуры на случай чрезвычайных ситуаций, которые должны быть предприняты после инцидента, подвергающего опасности бизнес-операции и/или человеческую жизнь;

Продолжение табл. Б.2

– меры по управлению связями с общественностью и эффективное взаимодействие с соответствующими государственными органами, например, с милицией, пожарной охраной и местными органами власти; – график поддержки плана, который определяет сроки и методы тестирования, а также описание процесса поддержки плана; – мероприятия по обучению персонала, которые направлены на понимание процессов обеспечения непрерывности бизнеса сотрудниками, и поддержание постоя иной эффективности этих процессов; – обязанности должностных лиц, ответственных за выполнение каждого пункта плана. – Не определены: – процедуры перехода на аварийный режим работы, которые описывают необходимые действия по переносу важных бизнес-операций или сервисов-поддержки в альтернативное временное место размещения и по восстановлению бизнес-процессов в требуемые периоды времени; процедуры возобновления работы, которые описывают необходимые действия для возвращения к нормальному режиму ведения бизнеса.
Меры предотвращения и обнаружения внедрения вредоносного программного обеспечения Для обеспечения защиты целостности программного обеспечения и массивов информации в организации принимаются меры предотвращения и обнаружения внедрения вредоносного программного обеспечения: – существует документированная политика, требующая соблюдения лицензионных соглашений и устанавливающая запрет на использование неавторизованного программного обеспечения; – существует документированная политика защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей, через внешние сети или из любой другой среды; – установлено и регулярно обновляется (не реже раза в неделю) антивирусное программное обеспечение для обнаружения и сканирования компьютеров и носителей информации, запускаемое в случае необходимости в качестве превентивной меры или рутинной процедуры; – проводятся регулярные инвентаризации программного обеспечения и данных систем, поддерживающих критические бизнес-процессы; – существуют управленческие процедуры и обязанности, связанные с защитой от вирусов; – проводится обучение пользователей применению этих процедур, вопросам оповещения и восстановления после вирусных атак; – разработан механизм восстановления после вирусных атак, включая все необходимые мероприятия по резервированию и восстановлению данных и программного обеспечения; – проводится контроль всей информации, касающейся вредоносного программного обеспечения, обеспечение точности и информативности предупредительных сообщений. Не соблюдаемые меры:

Продолжение табл. Б.2

– проверка всех файлов на носителях информации сомнительного или неавторизованного происхождения, или файлов, полученных из общедоступных сетей, на наличие вирусов перед работой с этими файлами; проверка любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования.

Табл. Б.3. Описание системы, вариант №3

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная Советом директоров организации Политика информационной безопасности. Назначенное должностное лицо отвечает за реализацию Политики и ее пересмотр в случае выявления существенных инцидентов нарушения информационной безопасности или появления новых уязвимостей, но не реже, чем раз в три месяца. Пересмотр включает в себя проверку эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности.
Доступ третьих лиц к ресурсам организации Для поддержания безопасности ресурсов организации доступ третьих сторон согласовывается, оформляется контракт, включающий процедуру определения прав и условий доступа других участников. Обязательно производится оценка риска, позволяющая определить последствия для безопасности и установить требования к мероприятиям по управлению информационной безопасностью. Для этого анализируется – тип требуемого доступа (физический/логический); – ценность информации; – причины для доступа; – мероприятия по управлению информационной безопасностью, используемые третьей стороной. Подписываемый контракт не учитывает возможность доступа других участников и условия их доступа. В контракте не всегда четко фиксируются сами процедуры проверки.
Контроль в отношении паролей Контроль в отношении паролей пользователей предусматривает: – подписание пользователями документа о необходимости соблюдения полной конфиденциальности личных паролей, а в отношении групповых паролей — соблюдения конфиденциальности в пределах рабочей группы; – в случаях, когда от пользователей требуется управление собственными паролями, предоставляется временный пароля, который пользователя принуждают сменить при первой регистрации в системе. Временные пароли используются в тех случаях, когда пользователи забывают свой личный пароль, и выдаются только после идентификации пользователя; – обеспечение безопасного способа выдачи временных паролей пользователям. Запрещено использование незащищенных (открытый текст)

Продолжение табл. Б.3

– сообщений электронной почты или сообщений по электронной почте от третьей стороны. Пользователь обязан подтверждать получение временного пароля. Сотрудникам не выполняют требования запрета хранения паролей в компьютерной системе в незащищенной форме.
Информационные ресурсы Активы организации, отнесенные к информационным ресурсам: – информационные активы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки (обслуживания), планы по обеспечению непрерывности функционирования информационного обеспечения, процедуры действий при сбоях, архивированная информация; – активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты. Не отнесены к информационным ресурсам: – физические активы: компьютерное оборудование (процессоры, мониторы, переносные компьютеры, модемы), оборудование связи (маршрутизаторы, частные автоматические телефонные станции с выходом в сеть общего пользования, факсы, автоответчики), магнитные носители (ленты и диски), другое техническое оборудование (электропитание, кондиционеры), мебель, помещения; – услуги: вычислительные услуги и услуги связи, основные коммунальные услуги, например, отопление, освещение, электроэнергия, кондиционирование.
Структура планов обеспечения непрерывности бизнеса В структуре планов обеспечения непрерывности бизнеса предусматривается следующее: – условия реализации планов, которые определяют порядок действий должностных лиц, которому необходимо следовать (как оценивать ситуацию, кто должен принимать участие, и т.д.) перед введением в действие каждого пункта плана; – процедуры на случай чрезвычайных ситуаций, которые должны быть предприняты после инцидента, подвергающего опасности бизнес-операции и/или человеческую жизнь; – обязанности должностных лиц, ответственных за выполнение каждого пункта плана. В ситуациях, несущих угрозы бизнесу и/или жизни не используются меры по управлению связями с общественностью и эффективное взаимодействие с соответствующими государственными органами, например, с милицией, пожарной охраной и местными органами власти.
Защита кабельных сетей Для защиты силовых и телекоммуникационных кабельных сетей, по которым передаются данные, от перехвата информации или повреждения: а) силовые и телекоммуникационные линии, связывающие средства обработки информации, проходят под землей; б) сетевой кабель защищен от неавторизованных подключений или повреждения, посредством использования специального кожуха;

Продолжение табл. Б.3

в) для исключения помех силовые кабели отделены от коммуникационных; Для чувствительных или критических систем: – используются оптико-волоконные линии связи; – кроссовые помещения и шкафы запираются и опечатываются, регулярно осуществляется контроль целостности; – проводятся проверки на подключение неавторизованных устройств к кабельной сети. Линии связи не закрыты защитными коробами. Не используются дублирующие маршруты прокладки кабеля.
Контроль искажений, данных при обработке С целью обнаружения искажений внутри системы правильно введенных данных в результате ошибок обработки или преднамеренных действий используются средства контроля (в зависимости от характера бизнес-приложения и последствий для бизнеса любого искажения данных): а) средства контроля сеансовой или пакетной обработки с целью выверки контрольных данных (остатков/контрольных сумм) в файлах, данных после транзакционных обновлений; б) средства контроля входящих остатков с целью их проверки с предыдущими закрытыми остатками, а именно: – средства контроля «от выполнения — к выполнению»; – общие суммы измененных данных в файле; – средства контроля «от программы — к программе»; в) подтверждение корректности данных, генерированных системой; г) проверки целостности полученных или переданных данных (программного обеспечения) между центральным (главным) и удаленными компьютерами д) контрольные суммы записей и файлов; е) проверки для обеспечения уверенности в том, что прикладные программы выполняются в нужное время; Не выполняются проверки для обеспечения уверенности в том, что программы выполняются в правильном порядке и прекращают работу в случае отказа, и что дальнейшая обработка приостанавливается до тех пор, пока проблема не будет разрешена. Не для всех файлов высчитываются контрольные суммы.
Разделение ресурсов Для уменьшения риска случайного изменения или неавторизованного доступа к программному обеспечению и бизнес-данным среды промышленной эксплуатации произведено разделение сред по целям использования: среда разработки, среда тестирования, среда эксплуатации. При разделении ресурсов были учтены следующие требования: – программное обеспечение для разработки и эксплуатации, по возможности, должно работать на различных компьютерных процессорах или в различных доменах или директориях; – действия по разработке и тестированию должны быть разделены, насколько это возможно; – компиляторы, редакторы и другие системные утилиты не должны быть доступны в операционной среде без крайней необходимости.

Продолжение табл. Б.3

Не учтенные требования: – чтобы уменьшить риск ошибок, для операционных и тестовых систем должны использоваться различные процедуры регистрации (входа в систему); разработчики могут иметь доступ к паролям систем операционной среды только в том случае, если внедрены специальные мероприятия по порядку предоставления паролей для поддержки среды промышленной эксплуатации. Эти меры должны обеспечивать смену паролей после использования.
Проверка на соответствие требованиям Регулярно проверяются на соответствие ПБ: – информационные системы и ресурсы; – поставщики систем; – владельцы информации и информационных активов; – пользователи. На соответствие ПБ не проверяется руководство.

Табл. Б.4. Описание системы, вариант №4

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная Советом директоров организации Политика информационной безопасности. Политика не соответствует законодательным требованиям РФ и не учитывает требования по обеспечению непрерывности ведения бизнеса. Данная Политика доведена до сведения всех сотрудников организации в доступной и понятной форме. Для гарантии качественного выполнения требований Политики безопасности на практике 2 раза в год проводится аудит.
Защита от перебоев в подаче электроэнергии Для защиты оборудования от перебоев в подаче электроэнергии и других сбоев, связанных с электричеством надлежащая подача электропитания обеспечено наличие нескольких источников электропитания. Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, поддерживающих критические бизнес-процессы, подключается через устройства бесперебойного электропитания UPS. – резервный генератор. На случай длительного отказа подачи электроэнергии от общего источника не предусмотрены резервные генераторы.
Классификация информации Все информация, циркулирующая в организации, классифицирована по принципу критичности и необходимости ограничения доступа к ней. При этом не учитывается возможный ущерб от НСД к ней.
Система управления паролями Система управления паролями имеет следующие свойства: – предписывает использование индивидуальных паролей для обеспечения установления ответственности;

Продолжение табл. Б.4

– позволяет пользователям выбирать и изменять их собственные пароли, а также включать подтверждающую процедуру для учета ошибок ввода при необходимости; – предписывать выбор высококачественных паролей; – там, где пользователи отвечают за поддержку своих собственных паролей, принуждает их к изменению паролей; – там, где пользователи выбирают пароли, обеспечивает изменение временных паролей при первой регистрации; – поддерживает хранение истории предыдущих пользовательских паролей (за предыдущий год) и предотвращает их повторное использование; – не отображает пароли на экране при их вводе; – обеспечивает смену паролей поставщика, установленных по умолчанию, после инсталляции программного обеспечения. Не соблюдены требования хранения паролей в зашифрованной форме (с помощью одностороннего алгоритма шифрования) отдельно от данных прикладных программ.
Информирование о форс-мажорах Все сотрудники и подрядчики ознакомлены с процедурой информирования: – об инцидентах нарушения информационной безопасности; – о недостатках в системе безопасности; – о сбоях и неисправностях компьютерных систем. Об этих событиях незамедлительно информируется руководство в соответствии с установленным порядком (в виде письменного отчета). Сотрудники проинформированы о процедурах составления отчетов.
Требования к резервированию В соответствии с утвержденной стратегией установлены регулярные процедуры резервирования прикладного программного обеспечения, формирования копий, данных и тестирования, их своевременного восстановления, регистрации событий и ошибок, мониторинга состояния аппаратных средств. Проводится ряд мероприятий по резервированию информации с соблюдением требований: – минимально необходимый объем резервной информации, вместе с точными и полными регистрационными записями по содержанию резервных копий, а также документация по процедурам восстановления во избежание любого повреждения от стихийных бедствий хранится в отдаленном от основного здания месте; – резервная информация обеспечивается гарантированным уровнем физической защиты и защиты от воздействий окружающей среды в соответствии с уровнем безопасности в основном здании; – резервное оборудование регулярно подвергается тестированию для обеспечения уверенности в том, что в случае возникновения чрезвычайных ситуаций на его работу можно положиться; – с целью поддержания возможности восстановления данных в установленном порядке и за гарантированный промежуток времени не реже, чем раз в четыре месяца проводятся практические тренинги с персоналом. Несоблюдаемые требования: – для важных бизнес-приложений сохраняются по крайней мере три поколения (цикла) резервной информации;

Продолжение табл. Б.4

– процедуры восстановления регулярно тестируются для обеспечения уверенности в их эффективности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем определено операционными процедурами восстановления.
Защита данных от утраты, разрушения и подделки Важные данные организации защищаются от утраты, разрушения и фальсификации. Система предоставляет возможности по уничтожению данных после того периода, когда у организации отпадет потребность в их хранении. Порядок обращения с ПДн сотрудников соответствует требованиям ФЗ «О персональных данных». Для выполнения обязательств хранения и защиты информации в организации приняты следующие меры: – составлены инструкции по хранению и обращению с информацией и документацией, а также их уничтожению; – составлен график хранения для различных типов данных; – реализованы надлежащие меры по защите основной документации и информации от потери, уничтожения и подделки. Не проводится инвентаризация всех источников основной информации.
Внедрение нового обрудования В организации четко определены и описаны все материальные активы. В случае необходимости внедрения нового оборудования обязательно: – утверждение у руководства с определением его назначения и порядка использования; – получение разрешения у менеджера, ответственного за поддержание режима безопасности локальной информационной системы. Проверка на совместимость с другими компонентами системы осуществляется не всегда.
9 Управление непрерывностью бизнеса Для обеспечения уверенности в актуальности и эффективности планов проводится их регулярное тестирование, пересмотр и обновление согласно графику и инструкциям. При этом используются следующие методы: – тестирование («имитация прогона») различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний); – моделирование (для тренировки персонала по выполнению своих функций после инцидента и перехода к кризисному управлению); – тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем); – проверка восстановления в альтернативном месте (бизнес-процессы осуществляются параллельно с операциями по восстановлению в удаленном альтернативном месте); – тестирование средств и сервисов-поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями сервисы и программные продукты удовлетворяют контрактным обязательствам). В организации не проводятся «генеральные репетиции» - тестирования того, что организация, персонал, оборудование, средства и процессы могут справляться с прерываниями.

Продолжение табл. Б.4

Требования, обеспечивающие выполнение контрольных проверок С целью обнаружения искажений внутри системы правильно введенных данных в результате ошибок обработки или преднамеренных действий в функции системы включены требования, обеспечивающие выполнение контрольных проверок: – использование места в программах для функций добавления и удаления данных; – процедуры для предотвращения выполнения программ в неправильной последовательности или ее исполнения после сбоя на предыдущем этапе обработки данных. Корректирующие программы для восстановления после сбоев и обеспечения правильной обработки данных не используются.

Табл. Б.5. Описание системы, вариант №5

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная генеральным директором организации Политика информационной безопасности. В политике содержатся: – определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации; – изложение целей и принципов информационной безопасности, сформулированных руководством; – ответственность за нарушения политики безопасности. ПБ не содержит положения по обучению персонала вопросам безопасности и ссылок на документы, дополняющие ПБ.
Порядок обмена между организациями Для предотвращения потери, модификации или неправильного использования информации при обмене ею между организациями учитывается следующее: – порядок обмена информацией и программным обеспечением (как электронным способом, так и вручную) между организациями, включая передачу на хранение исходных текстов программ третьей стороне, строго формализован и документирован и происходит на основе соглашений; – процедуры для уведомления отправителя о передаче, отправке и получении информации; – минимальные технические требования по формированию и передаче пакетов, данных; – требования к курьерской службе; – ответственность и обязательства в случае потери данных; – определение владельцев информации и программного обеспечения, а также обязанностей по защите данных, учет авторских прав на программное обеспечение и аналогичных вопросов; – технические требования в отношении записи и считывания информации и программного обеспечения; – использование шифрования при передачи критичной информации.

Продолжение табл. Б.5

Для защиты информации, передаваемой между организациями применяются следующие меры: а) используются только надежные перевозчики или курьеры. Список авторизованных курьеров согласован с руководством, выполняется процедура идентификации личности курьера; б) упаковка является достаточной для защиты содержимого от любого физического повреждения, которое может иметь место при транспортировке, и соответствует требованиям изготовителей носителей информации; в) применяются специальные средства контроля для защиты важной информации от неавторизованного раскрытия и модификации: – использование запертых контейнеров; – личная доставка; – использование упаковки, которую нельзя нарушить незаметно (на которой видна любая попытка вскрытия); – в исключительных случаях, разбивка отправления на несколько частей, пересылаемых различными маршрутами; – использование цифровых подписей и шифрования для обеспечения конфиденциальности. Не используется согласованная система маркировки для важной или критичной информации, обеспечивающая уверенность в том, что значение этой маркировки будет сразу же понятно, и информация будет соответственно защищена.
Работа с лицензионным ПО В организации ведется строгое следование требованиям авторского права на программное обеспечение, которое определяет законное использование программных и информационных продуктов. Ведется контроль за соблюдением ограничений максимального числа разрешенных пользователей программными продуктами. Для обеспечения выполнения условий лицензионных соглашений, в том числе для ПО, полученного из общедоступных сетей, требуется проводить регулярный аудит. Это требование на настоящий момент не выполнено.
Классификация информации Все информация, циркулирующая в организации, классифицирована. При классификации информационных активов учтены принципы: – критичность с точки зрения ее конфиденциальности, целостности и доступности. – степень влияния доступа к информации на бизнес (ущерб от НСД). При этом не определены процедуры снятия категории критичности с информации.
Расположение оборудования Оборудование расположено и защищено так, чтобы уменьшить риски от воздействий окружающей среды и возможности неавторизованного доступа: а) оборудование размещено таким образом, чтобы свести до минимума излишний доступ в места его расположения; б) средства обработки и хранения важной информации размещены так, чтобы уменьшить риск несанкционированного наблюдения за их функционированием; в) отдельные элементы оборудования, требующие специальной защиты, изолированы, чтобы повысить общий уровень необходимой защиты;

Продолжение табл. Б.5

г) курение вблизи средств обработки информации строго запрещено;
д) для защиты клавиатуры от пыли в производственных цехах используются специальные защитные пленки;
е) разработаны меры по ликвидации последствий бедствий, случающихся в близлежащих помещениях, например, пожар в соседнем здании, затопление в подвальных помещениях или протекание воды через крышу, взрыв на улице.
В организации разрешен прием пищи, напитков вблизи средств обработки информации.
Мониторинг состояния окружающей среды в целях выявления условий, которые могли бы неблагоприятно повлиять на функционирование средств обработки информации, не проводится.
Меры по управлению информационной безопасностью сводят к минимуму риск потенциальных угроз, включая:
– воровство;
– пожар, взрыв;
– пыль;
– химические эффекты;
– помехи в электроснабжении;
– электромагнитное излучение.
Не учтены потенциальные угрозы задымления, затопления, перебои в подаче воды, вибрации.

Обучение персонала

Для того чтобы свести к минимуму риски ИБ, весь персонал обучают процедурам безопасности и правильному использованию средств обработки информации. Обучение сотрудников сторонних организаций, имеющих доступ к ценной информации компании, проводится, прежде чем им будет предоставлен доступ к информации, и должно обеспечить:
– знание ими требований ИБ;
– правильное использование средств обработки информации, например, процедур регистрации в системах, использования пакетов программ и пр.
Информирование пользователей о существующих юридических нормах и изменениях в законодательстве не проводится.

Процедура входа в информационную систему

Процедура входа в информационную систему обладает свойствами:
а) не отображать наименований системы или приложений, пока процесс регистрации не будет успешно завершен;
б) отображать общее уведомление, предупреждающее, что доступ к компьютеру могут получить только авторизованные пользователи;
в) подтверждать информацию регистрации только по завершении ввода всех входных данных. В случае ошибочного ввода система не показывает, какая часть данных является правильной или неправильной;
г) ограничивать число разрешенных неудачных попыток регистрации тремя и предусматривать включение временной задержки прежде, чем будут разрешены дальнейшие попытки регистрации, или отклонение любых дальнейших попыток регистрации без специальной авторизации;
– разъединение сеанса связи при передаче данных;

Продолжение табл. Б.5

д) фиксировать информацию в отношении успешно завершенной регистрации: – дату и время предыдущей успешной регистрации; – детали любых неудачных попыток регистрации, начиная с последней успешной регистрации. Не соблюденные требования при процедуре входа: – не предоставлять сообщений-подсказок в течение процедуры регистрации, которые могли бы помочь неавторизованному пользователю; – ограничивать максимальное и минимальное время, разрешенное для процедуры регистрации. Если оно превышено, система должна прекратить регистрацию; предусматривать запись неудачных попыток.
Тестирование планов Для обеспечения уверенности в актуальности и эффективности планов проводится их регулярное тестирование, пересмотр и обновление согласно графику и инструкциям. При этом используются следующие методы: – тестирование («имитация прогона») различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний); – моделирование (для тренировки персонала по выполнению своих функций после инцидента и перехода к кризисному управлению); – тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем); – проверка восстановления в альтернативном месте (бизнес-процессы осуществляются параллельно с операциями по восстановлению в удаленном альтернативном месте); – тестирование средств и сервисов-поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями сервисы и программные продукты удовлетворяют контрактным обязательствам); – «генеральные репетиции» (тестирование того, что организация, персонал, оборудование, средства и процессы могут справляться с прерываниями). Неиспользуемые методы: – моделирование (для тренировки персонала по выполнению своих функций после инцидента и перехода к кризисному управлению); – тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем).
Политика использования криптографических средств защиты информации Чтобы максимизировать преимущества и минимизировать риски, связанные с использованием криптографических средств, а также избежать неадекватного или неправильного их использования, в организации разработана политика использования криптографических средств защиты информации. При этом определены: а) методика использования криптографических средств в организации, включая общие принципы, в соответствии с которыми следует защищать служебную информацию; б) принципы управления ключами, включая методы восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей; в) роли и обязанности должностных лиц за:

Продолжение табл. Б.5

– реализацию политики; – управление ключами; г) перечень мероприятий, которые должны обеспечивать эффективность внедрения методов криптозащиты в организации; е) требования законодательства и ограничения Не определен порядок определения адекватного уровня криптографической защиты.
Связи с общественностью У организации налажены контакты с внешними специалистами по безопасности для того, чтобы быть в курсе отраслевых тенденций, способов и методов ее оценки, а также с целью адекватного реагирования на инциденты нарушения информационной безопасности. Для своевременного получения рекомендаций в случае инцидента в системе ИБ налажены контакты с поставщиками информационного оборудования и телекоммуникационными операторами. Контакты с правоохранительными органами еще не налажены.

Табл. Б.6. Описание системы, вариант №6

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная Советом директоров организации Политика информационной безопасности. В политике содержится: – изложение целей и принципов информационной безопасности, сформулированных руководством; – требования в отношении обучения персонала вопросам безопасности; – ответственность за нарушения политики безопасности; – ссылки на документы, дополняющие политику информационной безопасности. ПБ не содержит: – определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации; – инструкций предупреждения и обнаружения вредоносного ПО.
Трудовой договор Трудовой договор организации содержит следующие положения: – положение, определяющее ответственность сотрудников за поддержание ИБ; – положение, описывающее меры дисциплинарного воздействия, которые будут применимы в случае нарушения сотрудником требований безопасности; – положение, определяющее юридические права и обязанности, в соответствии с законами об авторском праве или о защите информации. Трудовой договор не содержит: – положение, определяющее срок ответственности за обеспечение ИБ.

Продолжение табл. Б.6

Маршрутизация в сети Сети организации спроектированы с учетом обеспечения максимальных возможностей для совместного использования ресурсов и гибкости маршрутизации. Для снижения риска неавторизованного доступа к бизнес-приложениям или неавторизованного использования информационного оборудования используется принудительная маршрутизация. Принцип заключается в ограничении вариантов маршрутизации в каждой точке сети посредством определенных способов: – распределения выделенных линий или номеров телефона; – автоматического подключения портов к определенным системным приложениям или шлюзам безопасности; – ограничения опций меню и подменю для индивидуальных пользователей; – использования определенных прикладных систем и/или шлюзов безопасности для внешних пользователей сети; – активного контроля разрешенного источника с целью направления соединения через шлюзы безопасности, например, межсетевые экраны; Не используются предотвращения неограниченного сетевого роуминга, а также ограничение доступа к сети посредством создания отдельных логических доменов, например, виртуальных частных сетей для пользовательских групп в пределах организации.
Непрерывность бизнеса Особое внимание уделяется оценке зависимости бизнеса от внешних факторов и существующих контрактов. Проводится обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление; Все согласованные процедуры по обеспечению непрерывности ведения бизнеса требуют документации. Тестирование планов обеспечения непрерывности бизнеса требует установки определенной периодичности.
Комитет по безопасности Для координации внедрения различных мер обеспечения безопасности из числа руководителей основных подразделений создан комитет, задачи которого: – способствовать демонстрации поддержки информационной безопасности со стороны высшего руководства организации; – согласовывать методики и процедуры ИБ (анализ рисков, классификация информации с точки зрения требований безопасности); – оценивать адекватность и координировать внедрение конкретных мероприятий по управлению информационной безопасностью для новых систем или услуг; В задачи комитета не входит: – выработка конкретных соглашений о разграничении ответственности за обеспечение ИБ внутри организации; – информирование персонала по вопросам ИБ; – учет требований безопасности при планировании; – анализ инцидентов нарушения информационной безопасности.

Продолжение табл. Б.6

Приемка и отгрузка материальных ценностей Зоны приемки и отгрузки материальных ценностей находятся под контролем и изолированы от средств обработки информации во избежание неавторизованного доступа. В связи с этим: – доступ к зоне складирования с внешней стороны здания разрешен только определенному и авторизованному персоналу; – зона складирования организована так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания; – обеспечена безопасность внешней(их) двери(ей) помещения для складирования, когда внутренняя дверь открыта. Поступающие материальные ценности не всегда осматриваются на предмет потенциальных опасностей прежде, чем они будут перемещены из помещения для складирования к местам использования. Их регистрация осуществляется только для особо важных объектов.
Классификация информации Все информация, циркулирующая в организации, классифицирована. При обработке информации, полученной от других организаций, не учитывается возможное различие категорий критичности.
Использование лицензионного ПО В организации ведется строгое следование требованиям авторского права на программное обеспечение, которое определяет законное использование программных и информационных продуктов. После покупки лицензионного ПО оно регистрируется в журнале инвентаризации. Лицензии, сертификаты и финансовые документы не всегда сохраняются до конца срока использования ПО.
Предотвращение утечки данных через скрытые каналы Для предотвращения утечки данных через скрытые каналы и «троянские» программы используются следующие мероприятия: – закупка программного обеспечения осуществляется только у доверенного источника; – по возможности программы закупаются в виде исходных текстов с целью их проверки; – используется программное обеспечение, прошедшее оценку на соответствие требованиям информационной безопасности; – осуществляется контроль доступа к установленным программам и их модификациям; – используются проверенные сотрудники для работы с ключевыми системами. Проверка исходных текстов программ перед их эксплуатационным применением не осуществляется.
Управлению инцидентами Для обеспечения быстрой, эффективной и организованной реакции на нарушения информационной безопасности определены обязанности и процедуры по управлению инцидентами. При этом: а) определены процедуры в отношении возможных типов инцидентов нарушения информационной безопасности, в том числе:

Продолжение табл. Б.6

– сбои информационных систем и утрата сервисов; – отказ в обслуживании; – нарушения конфиденциальности; б) в дополнение к обычным планам обеспечения непрерывности (предназначенных для скорейшего восстановления систем или услуг) существуют процедуры выполнения требований: – анализа и идентификации причины инцидента; – использования журналов аудита и аналогичных свидетельств; – взаимодействия с лицами, на которых инцидент оказал воздействие или участвующих в устранении последствий инцидента; – информирования о действиях соответствующих должностных лиц; в) журналы аудита и аналогичные свидетельства собраны и защищены соответствующим образом с целью: – внутреннего анализа проблемы; – использования как доказательство в отношении возможного нарушения условий контракта, нарушения требований законодательства или, в случае гражданских или уголовных судебных разбирательств, касающихся, например, защиты персональных данных или неправомочного использования компьютеров; – ведения переговоров относительно компенсации ущерба с поставщиками программного обеспечения и услуг; г) действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения информационной безопасности находятся под тщательным и формализованным контролем. Процедуры осуществляются с целью обеспечения уверенности в том, что: – только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации; – все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены; – о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству организации, и они проанализированы в установленном порядке; – целостность бизнес-систем и систем контроля подтверждена в минимальные сроки. Не определены процедуры в отношении нарушения информационной безопасности вследствие неполных или неточных данных. После произошедшего инциденты не производится планирование и внедрение средств, предотвращающих повторное проявление инцидента.

Табл. Б.7. Описание системы, вариант №7

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная генеральным директором организации Политика информационной безопасности. Регулярному анализу подлежат только эффективность ПБ, характеризуемой природой, количеством и степенью влияния фиксируемых инцидентов в области

Продолжение табл. Б.7

ИБ. Стоимость и степень влияния контрмер на эффективность деятельности организации, а также результаты технологических изменений не анализируются.
Использование лицензионного ПО В организации ведется следование требованиям авторского права на программное обеспечение, которое определяет законное использование программных и информационных продуктов. После покупки лицензионного ПО оно регистрируется в журнале инвентаризации, все лицензии, сертификаты и финансовые документы сохраняются до конца срока использования ПО. Запрещается создание резервных копий лицензионного ПО. Все пользователи системы осведомлены об авторских правах на ПО, правилах приобретения ПО. Периодически происходят нарушения, связанные с получением ПО из общедоступных сетей. Пользователи не уведомлены, что в случае нарушения авторских прав будут предприняты дисциплинарные действия.
Классификация информации, регламенты Все информация, циркулирующая в организации, классифицирована. Для каждой категории критичности регламентированы условия для: – копирования; – хранения; – передачи по почте, факсом и электронной почтой; – уничтожения. Не регламентированы условия для передачи критичной информации голосом, включая мобильный телефон, голосовую почту, автоответчики.
Размещение ресурсов Все критические информационные ресурсы организации размещаются за охраняемым периметром и физически защищены от неавторизованного доступа и повреждений. При этом персонал информирован о существовании охраняемых зон и о проводимых в них работах только в необходимом объеме. Из соображений безопасности и предотвращения возможности злонамеренных действий в охраняемых зонах запрещена возможность работы в охраняемом помещении без надлежащего контроля со стороны уполномоченного персонала. Доступ третьих лиц для обслуживания оборудования является строго контролируемым и ограничен на время такой необходимости. Для третьих лиц обязательна процедура получения разрешения на доступ. В здании есть несколько неиспользуемых помещений, которые не запираются. Их проверка осуществляется крайне редко. В здании не запрещено использование фото, видео, аудио и другого записывающего оборудования.
Проверка корректности входных данных для прикладных систем Особое внимание обращается на корректность входных данных для прикладных систем. При вводе бизнес-транзакций, постоянных данных (имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (цены продаж, курсы валют, ставки налогов) применяется проверка корректности ввода для обеспечения уверенности в их соответствии исходным данным. В числе проводимых мероприятий: – периодическая анализ (просмотр) содержимого ключевых полей или файлов данных для подтверждения их достоверности и целостности;

Продолжение табл. Б.7

– процедуры проверки правдоподобия вводимых данных; – определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных. Не осуществляется сверка твердых (печатных) копий вводимых документов с вводимыми данными на предмет выявления любых неавторизованных изменений этих данных (необходимо, чтобы все изменения во вводимых документах были авторизованы). Не предусмотрены процедуры реагирования на ошибки, связанные с подтверждением данных.
Управление инцидентами Для обеспечения быстрой, эффективной и организованной реакции на нарушения информационной безопасности определены обязанности и процедуры по управлению инцидентами. При этом: а) определены процедуры в отношении возможных типов инцидентов нарушения информационной безопасности, в том числе: – сбои информационных систем и утрата сервисов; – отказ в обслуживании; – нарушения конфиденциальности; б) в дополнение к обычным планам обеспечения непрерывности (предназначенных для скорейшего восстановления систем или услуг) существуют процедуры выполнения требований: – анализа и идентификации причины инцидента; – использования журналов аудита и аналогичных свидетельств; – взаимодействия с лицами, на которых инцидент оказал воздействие или участвующих в устранении последствий инцидента; – информирования о действиях соответствующих должностных лиц; в) журналы аудита и аналогичные свидетельства собраны и защищены соответствующим образом с целью: – внутреннего анализа проблемы; – использования как доказательство в отношении возможного нарушения условий контракта, нарушения требований законодательства или, в случае гражданских или уголовных судебных разбирательств, касающихся, например, защиты персональных данных или неправомочного использования компьютеров; – ведения переговоров относительно компенсации ущерба с поставщиками программного обеспечения и услуг; г) действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения информационной безопасности находятся под тщательным и формализованным контролем. Процедуры осуществляются с целью обеспечения уверенности в том, что: – только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации; – все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены; – о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству организации, и они проанализированы в установленном порядке; – целостность бизнес-систем и систем контроля подтверждена в минимальные сроки.

Продолжение табл. Б.7

Не определены процедуры в отношении нарушения информационной безопасности вследствие неполных или неточных данных. После произошедшего инциденты не производится планирование и внедрение средств, предотвращающих повторное проявление инцидента.
Политика использования сетевых служб Для уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым сервисам, не компрометируют их безопасность, создана политика использования сетевых служб, содержащая: – положение, определяющее сети и сетевые услуги, к которым разрешен доступ; – положение, описывающее процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ; – положение, определяющее мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам. Все пользователи и подрядчики ознакомлены с требованиями безопасности и методами защиты оставленного без присмотра оборудования: – завершать активные сеансы по окончании работы, если отсутствует механизм блокировки, например, хранитель экрана, защищенный паролем; – защищать PC или терминалы от неавторизованного использования посредством замка или эквивалентного средства контроля, например, защита доступа с помощью пароля, когда оборудование не используется. Пользователи не ознакомлены с требованием отключаться от сервера, когда сеанс закончен (то есть не только выключать PC или терминал).
Соглашение о неразглашении Неотъемлемой частью условий трудового договора является подписание сотрудниками соглашения о неразглашении. Временные сотрудники и представители третьих сторон, не попадающие под стандартный трудовой договор, подписывают отдельно соглашение о соблюдении конфиденциальности до того, как им будет предоставлен доступ к средствам обработки информации. Соглашения о соблюдении конфиденциальности не пересматриваются при изменении условий трудового договора.
Тестирование планов Для обеспечения уверенности в актуальности и эффективности планов проводится их регулярное тестирование, пересмотр и обновление согласно графику и инструкциям. При этом используются следующие методы: – тестирование («имитация прогона») различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний); – моделирование (для тренировки персонала по выполнению своих функций после инцидента и перехода к кризисному управлению); – тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем); – «генеральные репетиции» (тестирование того, что организация, персонал, оборудование, средства и процессы могут справляться с прерываниями).

Продолжение табл. Б.7

Неиспользуемые методы: – проверка восстановления в альтернативном месте (бизнес-процессы осуществляются параллельно с операциями по восстановлению в удаленном альтернативном месте); тестирование средств и сервисов-поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями сервисы и программные продукты удовлетворяют контрактным обязательствам).
Совещания, вопросы обеспечения ИБ На совещаниях Совета директоров регулярно поднимаются вопросы обеспечения информационной безопасности: – назначение ответственных лиц в области информационной безопасности; – изменения в воздействиях основных угроз информационным активам; – анализ и мониторинг инцидентов нарушения информационной безопасности. На совещаниях не рассматриваются вопросы: – утверждение и пересмотр Политики информационной безопасности; – утверждение основных проектов в области информационной безопасности.

Табл. Б.8. Описание системы, вариант №8

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная Советом директоров организации Политика информационной безопасности. Положения ПБ не обновляются с 2002 года.
Классификация информации Все информация, циркулирующая в организации, классифицируется по принципам: – критичность с точки зрения ее конфиденциальности, целостности и доступности. – степень влияния доступа к информации на бизнес (ущерб от НСД). За присвоение категории критичности конкретному виду информации и периодичные проверки этой категории несет ответственность руководитель организации.
Расположение и безопасность информационных систем Все ключевые информационные системы расположены таким образом, чтобы исключить к ним случайный доступ неавторизованных лиц. Охраняемые объекты не выделяются на общем фоне. не имеют вне и внутри здания очевидных вывесок, по которым можно сделать вывод о выполняемых функциях обработки информации. Дополнительное оборудование (фотокопировальные устройства и факсы) расположены соответствующим образом в пределах зоны безопасности во избежание доступа, который мог бы скомпрометировать информацию. Все двери и окна надежно запираются. Но окна нижних этажей требуют установки дополнительной внешней защиты. Сигнализация установлена не на всех окнах охраняемого здания.

Продолжение табл. Б.8

Процесс регистрации пользователей Для контроля за предоставлением права доступа к информационным системам и сервисам существуют формализованные процедуры, охватывающие все стадии жизненного цикла пользовательского доступа от начальной регистрации новых пользователей до конечного снятия с регистрации пользователей, которым больше не требуется доступ к информационным системам и сервисам. Доступ к многопользовательским информационным сервисам контролируется посредством формализованного процесса регистрации пользователей, включающего: – использование уникальных ID (идентификаторов или имен) пользователей таким образом, чтобы действия в системе можно было бы соотнести с пользователями и установить ответственных; – проверку того, что пользователь имеет авторизацию от владельца системы на пользование информационной системой или сервисов; – проверку того, что уровень предоставленного доступа соответствует производственной необходимости, а также учитывает требования политики безопасности организации, например, не нарушает принципа разделения обязанностей; – предоставление пользователям письменного документа, в котором указаны их права доступа; – обеспечение уверенности в том, что поставщики услуг не предоставляют доступ, пока процедуры авторизации не завершены; – ведение формализованного учета в отношении всех лиц, зарегистрированных для использования сервисов; – обеспечение того, чтобы избыточные пользовательские ID не были переданы другим пользователям. Не выполняется: – требование того, чтобы пользователи подписывали документ о том, что они понимают условия предоставления доступа; – немедленная отмену прав доступа пользователей, у которых изменились должностные обязанности или уволившихся из организации; – периодическая проверка и удаление избыточных пользовательских ID и учетных записей.
Управление средствами обработки информации Для обеспечения уверенности в надлежащем и безопасном функционировании средств обработки информации установлены обязанности и процедуры по управлению и функционированию всех средств обработки информации. Операционные процедуры, определяемые политикой безопасности, задокументированы и обязательны к исполнению. Все изменения к ним утверждаются руководством. Процедуры содержат детальную инструкцию выполнения конкретного задания (работы) и включают: – обработку и управление информацией; – определение требований в отношении графика выполнения заданий, включающих взаимосвязи между системами; время начала выполнения самого раннего задания и время завершения самого последнего задания;

Продолжение табл. Б.8

– обработку ошибок или других исключительных ситуаций, которые могут возникнуть в течение выполнения заданий, включая ограничения на использование системных утилит; – специальные мероприятия по управлению выводом данных, например, использование специальной бумаги для печатающих устройств или особых процедур применительно к выводу конфиденциальной информации, включая процедуры для безопасной утилизации выходных данных, не завершенных в процессе выполнения заданий; – перезапуск системы и процедуры восстановления в случае системных сбоев. Процедуры не содержат необходимых контактов на случай неожиданных операционных или технических проблем. С целью минимизации риска нештатного использования систем вследствие ошибочных или злонамеренных действий пользователей используется разграничение обязанностей.
Проверка репутации сотрудников В сотрудников, имеющих значительные полномочия по работе с критичными данными, регулярно проводится проверка репутации. Не проводится проверка репутации сотрудников, работающих по контракту, временных служащих.
План обеспечения непрерывности План обеспечения непрерывности бизнеса предусматривает специальные процедуры в случае чрезвычайных ситуаций, которые обеспечат возможность восстановления бизнес-процессов в течение требуемого времени. Необходимо определить и согласовать все обязанности должностных лиц и процедур на случай чрезвычайных ситуаций.
Сбор улик Для поддержания исков и мер воздействия против нарушителей правил управления ИБ собираются улики. Для соответствия требования судов существуют правила обращения с уликами и критерии ее сохранения – допустимость свидетельств: действительно ли свидетельства могут использоваться в суде или нет; – весомость свидетельств: качество и полнота свидетельств. Не учитывается степень адекватности улики: адекватное свидетельство того, что процесс сбора свидетельств осуществлялся корректно и последовательно в течение всего периода, когда установленное свидетельство инцидента нарушения информационной безопасности было сохранено и обработано системой.
Совет директоров, вопросы обеспечения ИБ На совещаниях Совета директоров регулярно поднимаются вопросы обеспечения информационной безопасности. Один из членов Совета директоров (руководитель Службы безопасности) назначен ответственным за все вопросы, связанные с информационной безопасностью. Несмотря на масштабы организации совещания руководителей основных подразделений для координации действий по внедрению мер обеспечения безопасности проводятся крайне редко.

Продолжение табл. Б.8

Контроль доступа к библиотекам исходных текстов программ Для снижения риска искажения компьютерных программ обеспечивается строгий контроль доступа к библиотекам исходных текстов программ, для чего: – по возможности, исходные библиотеки программ хранятся отдельно от бизнес-приложений, находящихся в промышленной эксплуатации; – назначен специалист-библиотекарь программ для каждого бизнес-приложения; – персоналу поддержки информационных технологий предоставляется ограниченный доступ к исходным библиотекам программ; – программы, находящиеся в процессе разработки или текущего обслуживания, не хранятся в библиотеках с исходными текстами программ, находящихся в промышленной эксплуатации; – обновление библиотек и обеспечение программистов исходными текстами осуществляется только назначенному специалисту-библиотекарю после авторизации, полученной от менеджера, отвечающего за поддержку конкретного бизнес-приложения; – листинги программ хранятся в безопасном месте; – ведется журнал аудита для всех доступов к исходным библиотекам; – старые версии исходных текстов архивируются с указанием точных дат и времени, когда они находились в промышленной эксплуатации, вместе со всем программным обеспечением поддержки, управления заданиями, определениями данных и процедурами; – поддержка и копирование исходных библиотек проводится под строгим контролем с целью предотвращения внесения неавторизованных изменений. Не соблюдено требования по безопасному хранению листингов программ и ведению журнала аудита для всех доступов к исходным библиотекам.

Табл. Б.9. Описание системы, вариант №9

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная Советом директоров организации Политика информационной безопасности. В организации не определен сотрудник, ответственный за процедуры пересмотра и обновления положений ПБ.
Контролируемая зона Территория по периметру ограждена забором высотой 2 метра и круглосуточно охраняется. Въезд на территорию осуществляется через шлагбаум. Вход на территорию разрешен только после предъявления пропуска. Все посетители регистрируются в журнале с фиксацией времени и даты посещения. При доступе к защищаемой информации используются соответствующие процедуры аутентификации при помощи паролей, PIN-кодов, смарт-карт и tokenов. Персонал не носит никаких признаков видимой идентификации. Права доступа сотрудников в зоны информационной безопасности пересматриваются не достаточно регулярно.

Продолжение табл. Б.9

Анализ требований ИБ На стадии анализа требований к проекту разработки систем проводится и анализ требования к безопасности. Требования безопасности и соответствующие мероприятия по обеспечению информационной безопасности учитывают ценность информационных активов, потенциальный ущерб бизнесу, который может стать результатом отсутствия мер безопасности. Не учитывается ущерб, который может стать результатом неэффективности мер безопасности.
Управляемый процесс развития и поддержания непрерывности бизнеса С целью противодействия прерываниям бизнеса и защиты критических бизнес-процессов от последствий при значительных сбоях или бедствиях в организации существует управляемый процесс развития и поддержания непрерывности бизнеса. Этот процесс объединяет следующее: – понимание рисков, с которыми сталкивается организация, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение приоритетов критических бизнес-процессов; – понимание возможных последствий нарушения бизнес-процессов в случае незначительных или существенных инцидентов, потенциально угрожающих жизнедеятельности организации, а также выбора средств и способов обработки информации, которые соответствовали бы целям бизнеса; – формулирование и документирование стратегии непрерывности бизнеса в соответствии с согласованными бизнес-целями и приоритетами; – формулирование и документирование планов обеспечения непрерывности бизнеса в соответствии с согласованной стратегией; – обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса. Не учтено: – организация оптимального страхования результатов обработки информации, которое должно быть частью процесса обеспечения непрерывности бизнеса; – регулярное тестирование и обновление планов развития информационных технологий и существующих процессов.
Проверка репутации В отношении подрядчиков, временного персонала, а также сотрудников, имеющих значительные полномочия, регулярно проводится проверка репутации. Внедрены процедуры по периодическому контролю действий всех сотрудников со стороны вышестоящих руководителей. Не определяется требуемый уровень контроля для новых и неопытных сотрудников при их доступе к критичным системам.
Сбор улик Чтобы достичь качества и полноты свидетельств, необходимо наличие убедительных подтверждений свидетельств. В общем случае, такие убедительные подтверждения достигаются только для бумажных документов: обеспечивается безопасность хранения оригинала; регистрируется, кто, где и когда нашел улику, кто был свидетелем обнаружения. Для информации на компьютерных носителях подлинность улики не гарантируется.

Продолжение табл. Б.9

Регистрация действий персонала Все действия персонала регистрируются в специальном системном журнале с указанием: – времени начала и завершения работы системы; – ошибок системы и предпринятых корректирующие действия; – подтверждения правильной обработки данных файлов и выходных данных компьютера. Фиксация личных данных специалиста, производящего записи, не осуществляется. Регулярно производятся независимые проверки журнала оператора на соответствие требованиям операционных процедур. Все системные сбои информационные системы регистрируются. Затем производится: – анализ ошибок для обеспечения уверенности в том, что они были удовлетворительным образом устранены; – анализ предпринятых корректирующих мер, обеспечивающих уверенность в том, что мероприятия по управлению информационной безопасностью не были скомпрометированы (нарушены) и предпринятые действия надлежащим образом авторизованы.
Политика контроля доступа Правила контроля доступа и права каждого пользователя или группы пользователей однозначно определяются политикой безопасности по отношению к логическому доступу. Пользователи и поставщики услуг оповещены о необходимости выполнения требований в отношении логического доступа. В политике контроля доступа учтено следующее: – требования безопасности конкретных бизнес-приложений; – идентификация всей информации, связанной с функционированием бизнес-приложений; – согласованность между политиками по контролю доступа и классификации информации применительно к различным системам и сетям; – применяемое законодательство и любые договорные обязательства относительно защиты доступа к данным или сервисам; – управление правами доступа в распределенной сети с учетом всех типов доступных соединений. При авторизации доступа не используется принцип «need to know» (пользователь получает доступ только к данным, безусловно необходимым ему для выполнения конкретной функции). Политика контроля доступа не содержит стандартные профили доступа для типовых категорий пользователей.
Классификация информации Все информация, циркулирующая в организации, классифицирована. Для каждой категории критичности регламентированы условия для: – копирования; – хранения; – передачи критичной информации голосом, включая мобильный телефон, голосовую почту, автоответчики. – уничтожения.

Продолжение табл. Б.9

Не регламентированы условия для передачи по почте, факсом и электронной почтой.
Активы организации, ответственность Для каждого материального и информационного актива и процесса, связанного с информационной безопасностью, назначен ответственный администратор (владелец) из числа руководителей. Все детали обязанностей и ответственности четко определены и зафиксированы документально. Не все уровни полномочий ответственных лиц закреплены документально. Администратор может передавать свои полномочия по обеспечению безопасности какому-либо руководителю среднего звена или поставщикам услуг. При этом ответственность за обеспечение безопасности актива передается тому, кому переданы обязанности.

Табл. Б.10. Описание системы, вариант №10

Политика информационной безопасности Общие принципы и порядок обеспечения информационной безопасности в организации определяет действующая и утвержденная Советом директоров организации Политика информационной безопасности. Политика соответствует законодательным требованиям РФ. С политикой безопасности ознакомлены только руководители высшего и среднего звена.
Размещение критических ресурсов организации Все критические информационные ресурсы организации размещаются за охраняемым периметром и физически защищены от неавторизованного доступа и повреждений. Территория по периметру ограждена забором высотой 2 метра и круглосуточно охраняется. По периметру расположены камеры видеонаблюдения. Въезд на территорию осуществляется через шлагбаум. Пожарные входы защищены сигнализацией и запираются. Вход на территорию разрешен только после предъявления пропуска. Не предусмотрена физическая защита от пожара и затопления для части помещений, в которых расположены особо важные объекты.
Соглашение о неразглашении Неотъемлемой частью условий трудового договора является подписание сотрудниками соглашения о неразглашении. Временные сотрудники и представители третьих сторон, не попадающие под стандартный трудовой договор, не подписывают отдельно соглашение о соблюдении конфиденциальности.
Контроль действий системного аудита Проверка технического соответствия требованиям безопасности включает испытания операционных систем для обеспечения уверенности в том, что мероприятия по обеспечению информационной безопасности функционирования аппаратных и программных средств были внедрены правильно. Проверка осуществляются вручную штатным специалистом и включает тестирование на наличие попыток несанкционированного доступа к системе (проникновение),

Продолжение табл. Б.10

которое выполняется специально приглашенным независимым экспертом под наблюдением штатного специалиста. Для того чтобы свести к минимуму риск для бизнес-процессов, требования и действия системного аудита тщательно планируются. Учитываются следующее: – требования аудита согласовываются с руководством; – объем работ по проверкам согласовывается и контролируется; – другие виды доступа могут быть разрешены только в отношении изолированных копий файлов системы, которые удаляются по завершению аудита; – требования в отношении специальной или дополнительной обработки данных следует идентифицировать и согласовывать; – весь доступ подвергается мониторингу и регистрируется с целью обеспечения протоколирования для последующих ссылок. Не соблюдены требования: – информационные ресурсы до проверки четко идентифицируется, обеспечивается их доступность; – при проведении проверок используется доступ «только для чтения» к программному обеспечению и данным; все процедуры, требования и обязанности аудита документируются.
Управляемый процесс развития и поддержания непрерывности бизнеса С целью противодействия прерываниям бизнеса и защиты критических бизнес-процессов от последствий при значительных сбоях или бедствиях в организации существует управляемый процесс развития и поддержания непрерывности бизнеса. Этот процесс объединяет следующее: – понимание рисков, с которыми сталкивается организация, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение приоритетов критических бизнес-процессов; – понимание возможных последствий нарушения бизнес-процессов в случае незначительных или существенных инцидентов, потенциально угрожающих жизнедеятельности организации, а также выбора средств и способов обработки информации, которые соответствовали бы целям бизнеса; – организация оптимального страхования результатов обработки информации, которое должно быть частью процесса обеспечения непрерывности бизнеса; – регулярное тестирование и обновление планов развития информационных технологий и существующих процессов; – обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса. Не учтено: – формулирование и документирование стратегии непрерывности бизнеса в соответствии с согласованными бизнес-целями и приоритетами; – формулирование и документирование планов обеспечения непрерывности бизнеса в соответствии с согласованной стратегией.
Проверка корректности входных данных Особое внимание обращается на корректность входных данных для прикладных систем. При вводе бизнес-транзакций, постоянных данных (имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (цены продаж, курсы валют, ставки налогов) применяется проверка корректности

Продолжение табл. Б.10

ввода для обеспечения уверенности в их соответствии исходным данным. Для этого проводятся проверки исключения двойного ввода или другие проверки ввода с целью обнаружения следующих ошибок: – значений, выходящих за допустимый диапазон; – недопустимых символов в полях данных; – неавторизованные или противоречивые контрольные данные. Не учитываются возможные ошибки, связанные с: – отсутствующими или неполными данные; превышением верхних и нижних пределов объема данных.
Правила контроля доступа При определении правил контроля доступа принимается во внимание, следующее: – дифференциация между правилами, обязательными для исполнения, и правилами, которые являются общими или применяемыми при определенных условиях; – установление правил, основанных на предпосылке «все должно быть в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «все в общем случае разрешено, пока явно не запрещено»; – изменения в признаках маркировки информации как генерируемых автоматически средствами обработки информации, так и инициируемых по усмотрению пользователей; – изменения в правах пользователя как устанавливаемых автоматически информационной системой, так и определенных администратором; – правила, которые требуют одобрения администратора или другого лица перед применением, а также те, которые не требуют специального одобрения.
Установка системного времени Часы на компьютере устанавливаются по Универсальному Скоординированному Времени (UCT). В случае сбоев время системных часов компьютера могут настраивать пользователи.
Маркировка информационных активов Информационным активам организации, независимо от формы представления (физическая или электронная), присвоена соответствующая маркировка категории критичности. Соответствующие маркировки не присваиваются при осуществлении вывода данных из системы, содержащей критичную информацию.
Совет директоров, вопросы обеспечение ИБ На совещаниях Совета директоров регулярно поднимаются вопросы обеспечения информационной безопасности: – утверждение и пересмотр Политики информационной безопасности; – анализ и мониторинг инцидентов нарушения информационной безопасности; – утверждение основных проектов в области информационной безопасности. На совещаниях не рассматриваются вопросы: – назначение ответственных лиц в области информационной безопасности; – изменения в воздействиях основных угроз информационным активам.

Продолжение табл. Б.10

Процедуры обращения с информацией и ее хранения Процедуры обращения с информацией и ее хранения, определенные в организации: – обработка и маркирование всех носителей информации; – ограничение доступа с целью идентификации неавторизованного персонала; – обеспечение формализованной регистрации авторизованных получателей, данных; – обеспечение уверенности в том, что данные ввода являются полными, процесс обработки завершается должным образом и имеется подтверждение вывода данных; – хранение носителей информации в соответствии с требованиями изготовителей; – сведение рассылки данных к минимуму; – четкая маркировка всех копий данных, предлагаемых вниманию авторизованного получателя; – регулярный пересмотр списков рассылки и списков авторизованных получателей. Не обеспечивается защита информации, находящейся в буфере данных и ожидающей вывода в соответствии с важностью этой информации.

Литература

1. Курило, А.П. Основы управления информационной безопасностью. Учебное пособие для вузов. — 2-е изд., испр. — М.: Горячая линия-Телеком, 2014. — 244 с.

2. Милославская Н.Г., Сенаторов М.Ю. Технические, организационные и кадровые аспекты управления информационной безопасностью. М.: Горячая линия. – Телеком, 213. — 216 с.

3. Васильева И.Н. Управление информационной безопасностью. СПб.: Изд-во СПбГЭУ, 2014. — 82 с.

4. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2: учеб. пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 130 с.

5. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3: учеб. пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 170 с.