Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»
(ТУСУР)

УТВЕРЖДАЮ
Заведующий кафедрой
«Управление инновациями»
_____ /*А.Ф.Уваров*
(подпись) *(ФИО)*
"_____" _____ 2013 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

по дисциплине

«Информационные технологии в управлении качеством и защита информации»

Составлены кафедрой «Управление инновациями»

Для студентов, обучающихся
по направлению подготовки бакалавров
221400.62 «Управление качеством»

Форма обучения: очная

Составитель
Доцент каф. УИ, к.ф.-м.н. Годенова Е.Г.

" 31 " января 2013 г.

Томск 2013 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ КУРСА

Изучению дисциплины «Информационные технологии в управлении качеством и защита информации» отводится одно из важнейших мест при подготовке бакалавров по направлению 221400.62 «Управление качеством». Об этом, в частности, свидетельствует тот факт, что согласно ФГОС направления «Управление качеством» данная дисциплина отнесена к разделу базовых дисциплин профессионального блока подготовки бакалавров.

Целью курса «Информационные технологии в управлении качеством и защита информации» является формирование у студентов целостного представления о роли современных информационных технологий в управлении качеством организаций и обеспечении безопасности информационных ресурсов предприятий.

Задачи курса:

✓ ознакомить обучающихся с рядом графических нотаций, применяемых для разработки альбомов бизнес-процессов организаций;

✓ сформировать у обучающихся навыки работы с рядом современных программных продуктов для визуализации, оценки и анализа эффективности деятельности организаций;

✓ ознакомить обучающихся с международными стандартами информационной безопасности, российской нормативно-правовой базой в области защиты информации;

✓ освоить базовые понятия и навыки по разработке политики безопасности компании;

✓ ознакомить студентов с методологией построения комплексной защиты информационной среды предприятия.

В результате изучения дисциплины студент должен:

Знать: основные информационные технологии в управлении качеством;

Уметь: использовать технологии проектирования моделей данных на различных уровнях: концептуальном, логическом и физическом;

Владеть: методами защиты информации.

2. СТРУКТУРА КУРСА

По курсу «Информационные технологии в управлении качеством и защита информации» предусмотрены лабораторные работы в двух семестрах, ориентированные на практическое закрепление лекционного материала и самостоятельной работы студентов. Лабораторные работы направлены на формирование у студентов навыков разработки моделей бизнес-процессов организаций (предприятий) различного уровня; знаний о классах и критериях существующих угроз информационной безопасности; понимание важности защиты конфиденциальной информации, практических умений по защите документооборота и файлов от различных форм несанкционированного доступа и непреднамеренного воздействия, навыков разработки управленческих мер по защите информации организации.

На изучение курса «Информационные технологии в управлении качеством и защита информации» согласно учебному плану направления 221400.62 «Управление качеством» отводится два семестра. Курс логически разбит на два блока. Лабораторные работы первого блока «Информационные технологии в управлении качеством» проводятся в осеннем семестре и направлены на приобретение студентами компетенций в области разработки моделей бизнес-процессов предприятия, как простого уровня, так и комплекса моделей. При этом в ходе выполнения лабораторных работ студенты осваивают три различные нотации визуального моделирования бизнес-процессов. Второй блок «Защита информации» содержит курс лабораторных работ, направленных на формирование компетенций в области защиты документооборота, разработки управленческих документов по защите информации, защиты файлов от несанкционированного доступа и использования. Данное разбиение курса является логическим и целесообразным с точки зрения последовательности изложения материала и взаимодействия с другими дисциплинами учебного плана.

В первый блок входит 8 лабораторных работ. Восьмая лабораторная работа является итоговой работой семестра, при выполнении которой студенты должны продемонстрировать компетенции, полученные ими на лекциях, за время самостоятельной работы и лабораторных работ. Один академический час отводится на написание итогового тестирования за семестр. Тестовые задания представлены в приложении А к данным методическим рекомендациям. В ходе выполнения лабораторных работ студенты осваивают три нотации моделировании бизнес-процессов, которые рекомендуются в дальнейшем для применения при выполнении итоговой работы. Таким образом,

максимально оптимизируется учебный процесс при посещении студентами лекций, лабораторных работ и самостоятельной работе.

Во второй блок входит 9 лабораторных работ по защите информации (физической, криптографической и т.д.), выполнение которых позволит студентом приобрести компетенции для выполнения итоговой работы по разработке политики безопасности компании. Изучение блока приходится на весенний семестр. В восьмом семестре курс заканчивается экзаменом, бально-рейтинговая система, для которого приведена в рабочей программе дисциплины.

В настоящих методических рекомендациях представлена методика организации самостоятельной работы студентов в процессе изучения дисциплины «Информационные технологии в управлении качеством и защита информации» и базовые положения, необходимые для успешного ее выполнения.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

3.1. Общие положения

Самостоятельная работа студентов - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процессе преподавателей[1].

Организационные мероприятия, обеспечивающие нормальное функционирование самостоятельной работы студента, должны основываться на следующих предпосылках:

- ✓ самостоятельная работа должна быть конкретной по своей предметной направленности;
- ✓ самостоятельная работа должна сопровождаться эффективным, непрерывным контролем и оценкой ее результатов.

Предметно и содержательно самостоятельная работа студентов определяется образовательным стандартом, рабочими программами учебных дисциплин, содержанием учебников, учебных пособий и методических руководств. Контроль самостоятельной работы и оценка ее результатов организуется как единство двух форм:

- ✓ контроль и оценка со стороны преподавателей, государственных экзаменационных и аттестационных комиссий, государственных инспекций и др.;
- ✓ самоконтроль и самооценка студента.

Способы самостоятельной работы студентов должны быть установлены рабочей программой учебной дисциплин, входящих в соответствующую профессиональную образовательную программу.

Конкретные способы реализации самостоятельной работы выбираются студентом, а в необходимых случаях - по согласованию с преподавателем (преподавателями) в пределах условий (ограничений), устанавливаемых действующими нормативными документами.

3.2. Содержание самостоятельной работы студентов

В процессе изучения дисциплины студентам предстоит выполнить виды самостоятельной работы, представленные в таблице 1.

---

[1] Самостоятельная работа студентов. Сайт Алтайского государственного университета. Режим доступа URL: http://www.asu.ru/structure/admin_edu/umu/proz_edu/umo_students/ (Дата обращения 10.12.2011 г.).

Подготовка к лабораторным работам занятиям включает в себя изучение лекционного материала и рекомендованной литературы (подготовка доклада). Для успешной подготовки к итоговому тестированию и экзамену рекомендуется изучение лекционного материала и выполнение всего комплекса лабораторных работ.

Таблица 1. – Виды самостоятельной работы

Виды самостоятельной работы	**Число часов**	
	7 семестр	**8 семестр**
Подготовка к опросу на лекциях	4,5	4
Подготовка к тестированию	2	2
Подготовка к защите лабораторных работ	6	7
Ответы на контрольные вопросы	6	7
Анализ деятельности предприятия	6	-
Разработка общей политики безопасности организации	-	20
Подготовка к круглому столу по заданной теме	2	-
Подготовка доклада по заданной теме	-	4
Подготовка презентации по заданной теме	4	4
Анализ статей по заданной теме	4	-
Составление карт процессов для моделей бизнес-процессов	6	-
Работа с электронными ресурсами	6	6
Работа в команде по разработке комплекса моделей бизнес-процессов предприятия	1,5	-
Подготовка кейсов по заданной теме	6	6
Подготовка к экзамену		**36**
Общая трудоемкость час	**108**	**144**
Зачетные Единицы Трудоемкости (ЗЕТ)	**3**	**4**

Далее приводится детализация деятельности по каждому виду самостоятельной работы.

3.2.1 Подготовка к опросу на лекциях

На каждой лекции предусмотрен краткий опрос по теме предыдущей лекции. Это необходимо для актуализации знаний студентов при изучении новой темы, а также для организации самостоятельной работы студентов с конспектами лекций.

Опрос студентов проводится выборочно. Задаются 5-6 вопросов нескольким студентам по выбору. Ответы на вопросы могут влиять на компонент своевременности балльно-рейтинговой системы. В случае неготовности студента к опросу баллы за компонент своевременности могут отниматься.

Для успешного ответа на вопросы студентам рекомендуется 20-30 мин поработать с конспектом лекций самостоятельно накануне лекции. При этом нужно акцентировать внимание на моменты, которые преподаватель выделял в лекционном материале. Кроме того, важно понять общую структуру лекции и логику изложения материала. На опрос выделяется 5-10 мин.

3.2.2 Подготовка к тестированию

Каждое последнее занятие семестра уделяется проведению итогового тестирования за семестр. Примерные вопросы к тестам приводятся в методических указаниях к лабораторным работам, расположенных на научно-образовательном портале ТУСУРа (http://edu.tusur.ru/training/publications/2917).

Примерные вопросы приводятся для того, чтобы студенты имели возможность самостоятельно подготовиться к написанию теста. Для успешного прохождения семестрового тестирования студентам рекомендуется определить принадлежность каждого вопроса к теме лекции или лабораторной работы и изучить эти материалы. Также рекомендуется чтение основной и дополнительной литературы, указанной в рабочей программе дисциплины. Для эффективной и полноценной подготовки к тестам рекомендуется потратить не менее 2-х часов в каждом семестре на изучение типовых вопросов и изучение дополнительного материала по схожим темам.

3.2.3 Подготовка к защите лабораторных работ

Целью проведения лабораторных работ является закрепление полученного на лекциях теоретического материала, развитие логического мышления и аналитических способностей, формирование необходимых компетенций у будущих бакалавров по направлению «Управление качеством»

Методика проведения лабораторных работ предусматривает помимо стандартной работы за компьютером также групповое решение общих (типовых) задач, творческих задач для индивидуального рассмотрения, а также различных интерактивных форм организации лабораторных работ. Для решения ряда задач требуются навыки использования стандартных офисных программ и ресурсов сети Интернет.

В таблице 2 представлены темы лабораторных работ по данному курсу с указанием аудиторных часов на их выполнение. Каждая лабораторная работа требует самостоятельной подготовки. На каждой лабораторной работе студентам выдаются методические рекомендации для выполнения данной лабораторной работы, в которых кратко изложен основной теоретический материал по теме, указан порядок выполнения работы, контрольные вопросы и требования к оформлению отчета (если таковые имеются). Описание всех лабораторных работ и контрольные вопросы к ним расположены на научно-образовательном портале ТУСУРа (http://edu.tusur.ru/training/publications/2917).

Таблица 2. – Темы лабораторных работ

№ п/п	№ раздела дисциплины из табл.	Наименование лабораторных работ	Трудоемкость (час.)

	5.1		
7 семестр			
1	**1, 2**	Моделирование бизнес-процесса предприятия с использованием методологии IDEF0	4
2	**1, 2**	Применение нотации IDEF0 при проектировании бизнес-процессов	4
3	**3**	Построение диаграммы деятельности в нотации UML	4
4	**3**	Построение диаграммы вариантов использования в нотации UML	4
5	**3**	Построение диаграммы последовательностей в нотации UML	4
6	**1, 2**	Изучение интерфейса программы TIBCO BUSINESS STUDIO и нотации BPMN	4
7	**1, 2**	Моделирование бизнес-процессов предприятия в нотации BPMN	4
8	**1, 2, 3, 5**	Разработка комплекса моделей бизнес-процессов предприятия	6
9	**7**	Контроль знаний за семестр по пройденному материалу	2
		Итого за 7 семестр:	**36**
8 семестр			
10	**8**	Изучение Международных и отечественных стандартов в области информационной безопасности	4
11	**10**	Изучение существующих методик оценки рисков	4
12	**10**	Разработка плана аудита информационной безопасности	4
13	**11**	Анализ внутренней сети	4
14	**12**	Выявление уязвимостей в компьютерных системах и построение локальной политики паролей	4
15	**12**	Исследование надежности системы идентификации пользователя	2
16	**13**	Средства защиты и удостоверения подлинности электронных документов на примере пакета Open Office	4
17	**14**	Шифрование текста как метод защиты информации.	2
18	**14**	Исследование электронной цифровой подписи на основе алгоритма RSA	2
19	**15**	Контроль знаний за семестр по пройденному материалу	2
		Итого за 8 семестр:	**32**
		ИТОГО:	**68**

3.2.4. Ответы на контрольные вопросы

Для защиты лабораторной работы требуется ответить на все контрольные вопросы, расположенные после описания каждой лабораторной работы, исключая творческие. При ответе на контрольные вопросы требуется руководствоваться теоретическим материалом к лабораторным работам, поскольку она в полной мере содержит информацию необходимую для построения ответа.

3.2.5. Анализ деятельности предприятия

При выполнении последней лабораторной работы в седьмом семестре необходимы аналитические данные о деятельности какого-либо предприятия, поскольку это требуется для разработки комплекса моделей бизнес-процессов этого предприятия. Поскольку данная работа выполняется в команде и требует последующей публичной защиты, то анализ деятельности предприятия необходимо предварительно провести самостоятельно.

На сайте http://www.businessstudio.ru/ приводится большое количество примеров, построенных при помощи функционального моделирования IDEF0. Знакомство с этими примерами, поможет понять суть данной работы и увидеть примерный результат своей работы, который необходимо получить при работе в команде. Изучение стандартных заготовок моделей также позволит сформировать список вопросов, на которые необходимо найти ответы при построении модели.

Предприятие для построения комплекса моделей полностью определяется выбором студентов. Это может быть предприятие, где была пройдена производственная практика или реализовывался проект ГПО. Кроме того, можно найти предприятие в структуре МСБИ «Дружба» ТУСУР.

Для выполнения командной работы необходимо получить следующие данные:

1) информацию о предприятии;
2) организационная структура отделов;
3) методы получения информации для работы (интервью, анкеты, анализ документов);
4) описание основных, вспомогательных и управленческих процессов (можно в форме карты процессов);
5) и т.д. по желанию студентов.

При подготовке к выполнению лабораторной работы команда может разделить деятельность по сбору данных для оптимизации процесса.

3.2.6 Разработка общей политики безопасности организации

Политика безопасности (ПБ) – это комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии. Политика безопасности включает в себя требования в адрес персонала, менеджеров и технических служб. Стандартными и основными направлениями разработки политики безопасности являются следующие:

- ✓ определение того какие данные и насколько серьезно необходимо защищать,
- ✓ определение того кто и какой ущерб может нанести фирме в информационном аспекте,
- ✓ вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Любую отечественную компанию можно сравнить с небольшим государством. И если в каждом государстве существует законодательство, регламентирующее деятельность граждан, то в компании роль законов выполняют правила политики

безопасности. За нарушение законов государства граждане несут ответственность, за нарушения политики безопасности компании сотрудники также должны нести ответственность.

Политика информационной безопасности определяет стратегию и тактику построения корпоративной системы защиты информации. В российской терминологии документ определяющий стратегию часто называют концепцией, а документ определяющий тактику - политикой. На Западе принято создавать единый документ включающий в себя стратегию и тактику защиты. Политика безопасности компании является основой для разработки целого ряда документов безопасности: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и пр.

Что должно мотивировать отечественные предприятия и компании разрабатывать политику информационной безопасности? Как объяснить актуальность подобных разработок? К таким мотивам можно отнести следующее:[2]

1. Выполнение требований руководства компании. Как правило, руководство компании проявляет внимание к проблемам информационной безопасности под воздействием "фактора страха" или после нескольких серьезных инцидентов повлекших за собой остановку или замедление работы компании. Например, в результате вирусной атаки или атаки "отказ в обслуживании", разглашения конфиденциальной информации или кражи компьютеров с ценной информацией.

2. Выполнение требований российского законодательства. Каждая компания обладает информацией, представляющей некоторую ценность, и по понятным причинам она не желала бы разглашения этой информации. Политика информационной безопасности позволяет определить правила, в соответствии с которыми информация будет отнесена к категории коммерческой или служебной тайны. Это позволит компании юридически защитить информацию (статья 139 Гражданского Кодекса и Закон о защите коммерческой тайны). В зависимости от сферы действия компании, она должна выполнять требования существующего законодательства применимые к ее отрасли. Например, банки, в соответствии со статьей 857 Гражданского Кодекса должны гарантировать защиту банковской тайны клиентов. Страховые компании должны защищать тайну страхования (статья 946 Гражданского Кодекса) и так далее. Кроме этого, в соответствии с Указом №188 от 06.03.97 "Об утверждении перечня сведений

[2] Петренко С., Курбатов В. Политики безопасности компании при работе в Internet [Электронный ресурс]. Режим доступа URL: http://citforum.ru/security/internet/security_pol/ (Дата обращения 05.10.2012 г.)

конфиденциального характера", компании должны обеспечивать защиту персональных данных сотрудников.

3. Выполнение требований клиентов и партнеров. Клиенты и партнеры компании часто желают получить некоторые гарантии того, что их конфиденциальная информация защищена надлежащим образом и могут потребовать юридического подтверждения этого в контрактах. В этом случае политика информационной безопасности компании и является доказательством предоставления подобных гарантий. Так как в политике безопасности декларируются намерения компании относительно качества обеспечения информационной безопасности. Интересно, что партнеров по бизнесу и клиентов компании, как правило, интересуют именно эти "намерения", а не технические средства, с помощью которых эти намерения могут быть достигнуты.

4. Подготовка к сертификации ISO 9001, ISO 15408 и ISO 17799. Сертификация по одному из вышеперечисленных стандартов подтверждает необходимый уровень обеспечения информационной безопасности компании. В настоящее время фокус создания продуктов и услуг смещается в страны с дешевой рабочей силой и одним из доказательств того, что компании этих стран они смогут адекватно защитить передаваемую информацию производителей, является сертификация на соответствие требованиям стандартов по информационной безопасности, например ISO 17799 (BS 7799 часть 2). На сайте www.xisec.com ведется реестр компаний подтвердивших свое соответствие требованиям этого стандарта. Список увеличивается примерно на 50-100 компаний ежемесячно, что показывает возросшее внимание к этой теме.

5. Устранение замечаний аудиторов. Любая внешняя аудиторская проверка обращает внимание на необходимость защищенности бизнес-процесов компании, в том числе особое внимание уделяется наличию политики информационной безопасности.

6. Получение конкурентного преимущества на рынке. Правильно разработанная и реализованная политика безопасности позволяет увеличить время доступности и коэффициент готовности сервисов копании. Таким образом, увеличивается общая живучесть компании и обеспечивается непрерывность бизнеса. По словам ведущих аналитиков Gartner Group "обеспечение информационной безопасности является ключевым моментом устойчивости и непрерывности бизнеса".

7. Демонстрация заинтересованности руководства компании. Вовлечение руководства в организацию режима информационной безопасности компании значительно увеличивает приоритет безопасности, что положительно сказывается на общем уровне безопасности компании. Без демонстрации заинтересованности руководства компании сотрудники не станут воспринимать политику информационной

безопасности всерьез. Цель политики безопасности - разъяснение и доведение позиции руководства по обеспечению информационной безопасности в соответствии с принципами безопасности и бизнес целями компании.

8. Создание корпоративной культуры безопасности. "Образно организацию режима информационной безопасности можно сравнить с цепью: рвется там где самое тонкое звено цепи"(Б. Шнайер). Сотрудники являются как самым сильным, так одновременно и самым слабым звеном в обеспечении информационной безопасности. Необходимо донести до сотрудников мысль о том, что "обеспечение информационной безопасности - обязанность всех сотрудников". Это достигается путем введения процедуры ознакомления с требованиями политики безопасности и подписания соответствующего документа о том, что сотрудник ознакомлен, ему понятны все требования политики и он обязуется их выполнять. Политика позволяет ввести требования по поддержанию необходимого уровня безопасности в перечень обязанностей каждого сотрудника. В процессе выполнения ими трудовых обязанностей для сотрудников необходимо периодически проводить ознакомление и обучение вопросам обеспечения информационной безопасности. Критически важным условием для успеха в области обеспечения информационной безопасности компании становится создание в компании атмосферы, благоприятной для создания и поддержания высокого приоритета информационной безопасности. Чем крупнее компания, тем более важной становится информационная поддержка сотрудников по вопросам безопасности.

9. Уменьшение стоимости страхования. Страхование - важная составляющая управления информационными рисками. Наличие политики информационной безопасности является необходимым и обязательным условием страхования. В России уже появились фирмы предлагающие страховать информационные риски, например "Ингосстрах" и "РОСНО". Стоимость страхования страховая компания определяет путем проведения аудита информационной безопасности независимой компанией, специализирующейся в этой области. Например, компания Центр финансовых технологий (интернет-проект Faktura.ru) заключила договор комплексного страхования информационных рисков с "Ингосстрахом". Сумма ответственности составила $500 000. Аудит проводила компания ОАО "Элвис-Плюс".

10. Экономическая целесообразность. По рекомендациям ведущих компаний в области безопасности от 60 до 80 процентов всех усилий по обеспечению безопасности должны быть направлены на разработку политики безопасности и сопутствующих ей документов. Как показала диаграмма, разработанная Стивеном Россом (Delloitte&Touche)

политика безопасности может являться как самым дешевым, так и одновременно самым эффективным способом обеспечения информационной безопасности.

11. Хорошая бизнес практика. Наличие политики информационной безопасности является правилом хорошего тона. В опросе, проведенном в Великобритании компанией PriceWaterHouseCoopers в 2002 году, 67% компаний назвали именно эту причину создания политики информационной безопасности. Даже такие высокотехнологичные компании как Cisco заявляют, что правильно сформулированная политика информационной безопасности лучше технических средств обеспечения информационной безопасности. Подход Cisco к проблемам создания защищенной инфраструктуры показывает, что именно политика информационной безопасности является краеугольным камнем безопасности, вокруг которого строится вся система обеспечения безопасности.

Таким образом, политика обеспечения информационной безопасности необходима для успешной организации режима информационной безопасности любой отечественной компании. Политика безопасности минимизирует влияние "человеческого фактора" и недостатки существующих технологий защиты информации. Кроме того политика безопасности дисциплинирует сотрудников компании и позволяет создать корпоративную культуру безопасности.

Этапы разработки типовой политики безопасности

Существуют две системы оценки текущей ситуации в области информационной безопасности на предприятии. Они получили образные названия "исследование снизу вверх" и "исследование сверху вниз". Первый метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями. Он основан на известной схеме: "Вы – злоумышленник. Ваши действия?". То есть служба информационной безопасности, основываясь на данных обо всех известных видах атак, пытается применить их на практике с целью проверки, а возможно ли такая атака со стороны реального злоумышленника.

Метод "сверху вниз" представляет собой, наоборот, детальный анализ всей существующей схемы хранения и обработки информации. Первым этапом этого метода является, как и всегда, определение, какие информационные объекты и потоки необходимо защищать. Далее следует изучение текущего состояния системы информационной безопасности с целью определения, что из классических методик защиты информации уже реализовано, в каком объеме и на каком уровне. На третьем этапе производится классификация всех информационных объектов на классы в соответствии с ее конфиденциальностью, требованиями к доступности и целостности (неизменности).

Далее следует выяснение того насколько серьезный ущерб может принести фирме раскрытие или иная атака на каждый конкретный информационный объект. Этот этап носит название "вычисление рисков". В первом приближении риском называется произведение "возможного ущерба от атаки" на "вероятность такой атаки". Существует множество схем вычисления рисков, остановимся на одной из самых простых. Вычисление рисков можно производить либо вручную, с привлечением соотвествующих специалистов. Либо при помощи специализированных программных средств, позволяющих оценить риски предприятия на основе большого массива вопросов. При чем, как правило, в данных программах заложены разные массивы вопросов для разного рода предприятий.

На самом ответственном этапе производится собственно разработка политики безопасности предприятия, которая обеспечит надлежащие уровни как отдельных рисков, так и интегрального риска. При ее разработке необходимо, однако, учитывать объективные проблемы, которые могут встать на пути реализации политики безопасности. Такими проблемами могут стать законы страны и международного сообщества, внутренние требования корпорации, этические нормы общества.

После описания всех технических и административных мер, планируемых к реализации, производится расчет экономической стоимости данной программы. В том случае, когда финансовые вложения в программу безопасности являются неприемлемыми или просто экономически невыгодными по сравнению с потенциальным ущербом от атак, производится возврат на уровень, где мы оценивали риски и меняем их значения.

Завершается разработка политики безопасности ее утверждением у руководства фирмы и детальным документированием. За этим должна следовать активная реализация всех указанных в плане компонентов. Перерасчет таблицы рисков и, как следствие, модификация политики безопасности фирмы чаще всего производится раз в два года.

Подготовительный этап

Обеспечение комплексной безопасности является необходимым условием функционирования любой компании. Эта "комплексность" заключается, прежде всего, в продуманности, сбалансированности защиты, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

Всякой успешной деятельности должен предшествовать этап планирования. Шахматисты знают, что, не создав четкого плана, выиграть партию у сколько-нибудь серьезного соперника невозможно. А соперник — "промышленный шпион" — у нас достаточно серьезный. Планирование обеспечения безопасности заключается в разработке политики безопасности.

Вначале необходимо провести аудит информационных процессов фирмы, выявить критически важную информацию, которую необходимо защищать. Иногда к этому делу подходят однобоко, полагая, что защита заключается в обеспечении конфиденциальности информации. При этом упускаются из виду необходимость обеспечения защиты информации от подделки, модификации, парирования угроз нарушения работоспособности системы. Например, обиженный чем-то программист может вставить деструктивную закладку в программное обеспечение, которая сотрет ценную базу данных уже намного позднее времени его увольнения. Аудит информационных процессов должен заканчиваться определением перечня конфиденциальной информации предприятия, участков, где эта информация обращается, допущенных к ней лиц, а также последствий утраты (искажения) этой информации.

После этого становится ясно, что защищать, где защищать и от кого защищать: ведь в подавляющем случае инцидентов в качестве нарушителей будут выступать — вольно или невольно — сами сотрудники фирмы. На самом деле, с этим ничего нельзя поделать: это надо принять как данность. Различным угрозам безопасности можно присвоить вероятности их реализации. Умножив вероятность реализации угрозы на причиняемый этой реализацией ущерб, получим риск угрозы. После этого можно приступать к разработке политики безопасности.

Содержание политики безопасности

Политика безопасности — это документ "верхнего" уровня, в котором должно быть указано:

- ✓ ответственные лица за безопасность функционирования фирмы;
- ✓ полномочия и ответственность отделов и служб в отношении безопасности;
- ✓ организация допуска новых сотрудников и их увольнения;
- ✓ правила разграничения доступа сотрудников к информационным ресурсам;
- ✓ организация пропускного режима, регистрации сотрудников и посетителей;
- ✓ использование программно-технических средств защиты;
- ✓ другие требования общего характера.

Таким образом, политика безопасности — это организационно-правовой и технический документ одновременно. При ее составлении надо всегда опираться на принцип разумной достаточности и не терять здравого смысла.

Например, в политике может быть указано, что все прибывающие на территорию фирмы сдают мобильные телефоны вахтеру (такие требования встречаются в некоторых организациях). Будет ли кто-нибудь следовать этому предписанию? Как это проконтролировать? К чему это приведет с точки зрения имиджа фирмы? Ясно, что это

требование нежизнеспособное. Другое дело, что можно запретить использование на территории мобильных телефонов сотрудникам фирмы, при условии достаточного количества стационарных телефонов.

Принцип разумной достаточности означает, что затраты на обеспечение безопасности информации должны быть никак не больше, чем величина потенциального ущерба от ее утраты. Анализ рисков, проведенный на этапе аудита, позволяет ранжировать эти риски по величине и защищать в первую очередь не только наиболее уязвимые, но и обрабатывающие наиболее ценную информацию участки. Если в качестве ограничений выступает суммарный бюджет системы обеспечения безопасности, то задачу распределения этого ресурса можно поставить и решить как условную задачу динамического программирования.

Особое внимание в политике безопасности надо уделить разграничению зоны ответственности между службой безопасности и IT-службой предприятия. Зачастую сотрудники службы безопасности, в силу низкой технической грамотности, не осознают важности защиты компьютерной информации. С другой стороны, IT-сотрудники, являясь "творческими" личностями, как правило, стараются игнорировать требования службы безопасности. Кардинально решить эту проблему можно было бы, введя должность CEO по информационной безопасности, которому бы подчинялись обе службы.

В политике безопасности не надо детализировать должностные обязанности каких бы то ни было сотрудников (хотя приходилось видеть и такое). Эти обязанности должны разрабатываться на основе политики, но не внутри нее.

Обеспечение безопасности компьютерной информации

Значительное внимание в политике безопасности уделяется вопросам обеспечения безопасности информации при ее обработке в автоматизированных системах: автономно работающих компьютерах и локальных сетях. Необходимо установить, как должны быть защищены серверы, маршрутизаторы и другие устройства сети, порядок использования сменных носителей информации, их маркировки, хранения, порядок внесения изменений в программное обеспечение.

Можно привести по этому поводу следующие общие рекомендации:

- ✓ в системе должен быть администратор безопасности;
- ✓ за каждое устройство должен быть назначен ответственный за его эксплуатацию;
- ✓ системный блок компьютера надо опечатывать печатями ответственного и работника IT-службы (или службы безопасности)

- ✓ жесткие диски лучше использовать съемные, а по окончании рабочего дня убирать их в сейф;
- ✓ если нет необходимости в эксплуатации CD-ROM, дисководов, они должны быть сняты с компьютеров;
- ✓ установка любого программного обеспечения должна производиться только работником IT-службы;
- ✓ для разграничения доступа сотрудников лучше всего использовать сочетание паролей и смарт-карт (токенов). Пароли должны генерироваться администратором безопасности, выдаваться пользователю под роспись и храниться им также как и другая конфиденциальная информация;
- ✓ должно быть запрещено использование неучтенных носителей информации. На учтенных носителях выполняется маркировка, например, гриф, номер, должность и фамилия сотрудника.

Еще раз напомним о разумной достаточности и здравом смысле. Внедрение любой защиты приводит к определенным неудобствам пользователя. Однако эти неудобства не должны быть существенными, иначе человек будет игнорировать существующие правила. Например, можно потребовать завести журнал пользователя персонального компьютера, в котором он должен отмечать время начала и конца работы, характер выполняемых действий, наименование созданных файлов и т.д. Можно предусмотреть процедуру удаления файлов под две росписи в журнале, да мало ли что еще взбредет в голову! Никто и никогда не будет выполнять такие вздорные требования. Другое дело, если подготовка каких-то важных документов предусмотрена на специальном компьютере в службе безопасности. Здесь журнал учета работы пользователей будет не только уместным, но и необходимым.

Крайне внимательно надо отнестись к подключению своих информационных ресурсов к Интернету. В политике безопасности этот вопрос должен быть выделен в отдельный раздел. Подключение к Интернету обычно преследует следующие цели:

- ✓ получение информации из Интернета;
- ✓ размещение в Интернете своей информации о предоставляемых услугах, продаваемых товарах и т.д.
- ✓ организация совместной работы удаленных офисов или работников на дому.

В первых двух случаях идеальным с точки зрения безопасности было бы выделение для Интернета автономного компьютера, на котором ни в коем случае не должна храниться конфиденциальная информация. На компьютере должны быть обязательно установлены антивирусные средства защиты с актуальной базой, а также правильно

настроенный Firewall. При этом особый контроль надо уделить работе на этом компьютере со сменными носителями информации, а также перлюстрации исходящей почты. В некоторых организациях вся исходящая почта попадает вначале в руки администратора безопасности, который контролирует ее и пересылает дальше.

При необходимости организации распределенной работы сотрудников фирмы наиболее приемлемым решением являются виртуальные частные сети (VPN). В настоящее время имеется много отечественных фирм-разработчиков, представляющих также услуги по установке и настройке соответствующего программного обеспечения.

Несмотря на все принятые меры, нарушения информационной безопасности могут произойти. В политике безопасности должны быть обязательно предусмотрены меры ликвидации этих последствий, восстановления нормальной работоспособности фирмы, минимизации причиненного ущерба. Большое значение здесь имеет применение средств резервирования электропитания, вычислительных средств, данных, а также правильная организация документооборота.

Аудит безопасности

Итак, вы разработали политику безопасности, претворили ее положения в жизнь. Как теперь оценить информационную безопасность вашей фирмы? Может быть, все усилия потрачены втуне? — На эти вопросы поможет ответить аудит безопасности. Существуют фирмы, предоставляющие подобные услуги, и, по крайней мере, два подхода к оценке.

Первый подход — оценка безопасности на качественном уровне. Проводящий оценку эксперт высказывает свое видение состояния дел в фирме, дает рекомендации по устранению замеченных им изъянов. В таком подходе нет ничего предосудительного, однако, субъективизм все же может присутствовать. Хотелось бы иметь действительно независимую, объективную оценку информационной безопасности. Причем было бы неплохо, чтобы эту, количественную, оценку признавали и другие фирмы — ваши потенциальные партнеры. Очевидно, что для этого необходима разработка некоторого набора правил или стандарта в области безопасности информационных систем.

К счастью, почти ничего разрабатывать не надо: стандарт, позволяющий дать количественную оценку информационной безопасности, уже имеется. Речь идет о международном стандарте ISO 17799. Этот документ был принят международным институтом стандартов в конце 2002 года на основе ранее разработанного Великобританией стандарта BS7799. И хотя он пока не является общепринятым документом в нашей стране, этот стандарт не противоречит руководящим документам Гостехкомиссии и приказам ФАПСИ.

Стандарт ISO 17799 позволяет получить количественную оценку комплексной безопасности фирмы. Этот процесс настолько формализован, что существует (и продается в нашей стране) программное обеспечение, позволяющее самостоятельно выполнить оценку безопасности своей компании. Это программное обеспечение представляет собой, по существу, вопросник. Сгенерированный программой отчет высылается в адрес фирмы, имеющей полномочия на проведение сертификации на соответствие этому стандарту, и та присылает вам соответствующий знак и процент соответствия стандарту, как показано на рисунке. Этот знак компания может разместить на своем корпоративном сайте. Трудно сказать, насколько эта процедура актуальна для российских фирм, но сам подход любопытен.

В заключении, необходимо особо подчеркнуть, что необходим постоянный и эффективный контроль над реализацией политики безопасности, потому, что все технические ухищрения в области обеспечения безопасности могут оказаться бесполезными без организации должного контроля.

Итак, адекватный уровень ИБ в современной организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных ПБ. Эффективные ПБ определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации. Для того чтобы ПБ оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах ИБ и обучать их выполнению правил, предписываемых ПБ. Регулярный пересмотр и корректировка правил ПБ необходимы для поддержания ее в актуальном состоянии.

Разработка и внедрение ПБ в организации – процесс коллективного творчества, в котором должны участвовать представители всех подразделений, затрагиваемых производимыми изменениями. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение ИБ. Этот специалист координирует деятельность рабочей группы по разработке и внедрению ПБ на протяжении всего жизненного цикла, включающего в себя проведение аудита безопасности, разработку, согласование, внедрение, обучение, контроль исполнения, пересмотр и корректировку ПБ.

Для разработки эффективной ПБ, помимо профессионального опыта, знания нормативной базы в области ИБ и писательского таланта, необходимо также учитывать

основные факторы, влияющие на эффективность ПБ, и следовать основным принципам разработки ПБ, к числу которых относятся: минимизация влияния на производительность труда, непрерывность обучения, контроль и реагирование на нарушения безопасности, поддержка руководства организации и постоянное совершенствование ПБ.

Содержание типовой политики безопасности компании

Как правило, целью политики безопасности является защита информационных ресурсов компании от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, обеспечение непрерывности бизнеса и минимизация ущерба, наносимого бизнесу в результате осуществления инцидентов информационной безопасности, максимизация прибыли на инвестированный капитал и получение дополнительных возможностей для бизнеса.

Политика безопасности редко разрабатывается с нуля, поскольку это совершенно нецелесообразно. Есть два подхода к разработке политики безопасности: а) использование международных стандартов информационной безопасности; б) переработка стандартных политик безопасности (шаблонов) под конкретную компанию.

В пример первому подходу можно указать применение для разработки политики безопасности серии международных стандартов ISO 27001/17799. Они являются одними из самых важных документов для информационной безопасности организации. Относительно второго подхода можно отметить, что существуют компании специализирующиеся на разработке типовых политик безопасности, а также индивидуальной разработкой политик для компании [1]. Однако зачастую такие типовые политики являются платными, как, например, в Гипермаркете информационной безопасности[3]. Шаблон типовой политики безопасности для индивидуального предприятия приведен в Приложении А к данным требованиям.

Однако, типичная политика безопасности, состоит зачастую из следующих разделов:

- ✓ Термины и определения;
- ✓ Общие положения;
- ✓ Область действия;
- ✓ Положение об управляющем комитете;
- ✓ Соответствие требованиям;
- ✓ Управление рисками;

---

[3] GTrusr. Гипермаркет информацоинной безопасности. [Электронный ресурс] Режим доступа: http://shop.globaltrust.ru/show_good.php?idtov=1055 (Дата обращения 11.10.2012 г).

- ✓ Управление непрерывностью бизнеса;
- ✓ Оповещение о нарушениях безопасности;
- ✓ Повышение осведомленности, обучение и тренинги;
- ✓ Контроль и пересмотр;
- ✓ Ответственность;
- ✓ История изменений.

Требования к содержанию творческой работы

Разрабатываемая творческая работа должна быть написана не более чем на 40 страницах и не менее чем на 10. Работа должна состоять из следующих основных пунктов:

1. ***Титульный лист***. Шаблон оформления титульного листа представлен в Приложении А к данным методическим рекомендациям.

2. ***Содержание*** должно отражать все разделы творческой работы и номера соответствующих страниц.

3. ***Введение*** должно отражать следующие моменты: актуальность разработки политики безопасности, отношение к политике безопасности организации в разных странах, примеры использования политики безопасности в организациях и мнения экспертов, цель и задачи творческой работы, описание составных частей и их краткую характеристику, описание используемой методологии разработки политики безопасности.

4. ***Разделы работы.*** Поскольку данная работа относится к категории творческих работ, то разделы работы остаются на усмотрение студента. Однако существует определенный минимум содержания, который включает в себя разделы:

4.1. Описание проблемы;

4.2. Область применения;

4.3. Позиция организации;

4.4. Распределение ролей и обязанностей;

4.5. Санкции;

4.6. Дополнительная информация.

Описания указанных разделов вполне достаточно для получения зачета.

Как правило, политика безопасности состоит из нескольких уровней: верхнего, среднего и нижнего. Нижний уровень – это уровень специализированных политик безопасности, на которые опирается базовая политика. В данной творческой работе требуется разработать политику верхнего уровня, определяющую действие всей организации в целом.

Детализация политики безопасности до среднего и нижнего уровня не является обязательным требованием к работе и остается на усмотрение студента.

5. ***Список использованных источников и литературы***. В данном разделе приводятся справочные ресурсы, используемые для написания творческой работы. Все информационные ресурсы подразделяются на источники и литературу. Под ***источниками*** те ресурсы, которые являются только лишь поставщиком информации, без подведения аналитических выводов и заключений, например, стандарты информационной безопасности [2]. Под ***литературой*** подразумевается информация, уже переработанная и содержащая выводы, заключения и обобщения, например, учебники, статьи, тезисы и т.д. Кроме того при подготовке творческой работы будет целесообразно использовать конспекты лекций. Пример оформления списка источников и литературы можно посмотреть в данных методических рекомендациях. Пример оформления списка использованной литературы и источников находится в приложении Б к данным методическим рекомендациям.

6. ***Приложения***. В приложения выносятся необходимые справочные материалы и иллюстрации, являющиеся дополнением к тексту основной работы. Приложения нумеруются заглавными буквами русского алфавита и должны иметь заголовок, поясняющий содержание данного приложения.

Требования к оформлению творческой работы

Творческая работа оформляется машинописным текстом на листе формата А4. Все иллюстрации, таблицы, формулы, заголовки должны быть оформлены в соответствии с Образовательным стандартом ТУСУР [4]. Работа должна быть структурирована в четкой логической последовательности, заголовки - отражать суть раздела или подраздела.

При написании работы соблюдать следующие параметры страницы:

Ориентация – книжная;

Поля: Левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см.

Требования к параметрам форматирования приведены в таблице 3.

Таблица 3. - Требования к параметрам форматирования документа

Параметр форматирования	Требования
Межстрочный интервал	1,5
Размер шрифта	12 или 14 кегль
Начертание заголовков	Жирный шрифт

[4] Правила оформления студенческих работ [Электронный ресурс] Режим доступа http://www.tusur.ru/ru/students/educational/. (Дата обращения 11.10.12 г.)

Красная строка	1 см
Выравнивание заголовков	По центру страницы
Выравнивание основного текста	По ширине страницы
Отступы между абзацами	0 пт
Начертание шрифта	Times New Roman

Все заголовки оформляются стилями и должны иметь отражение в содержании текста работы. Список литературы оформляется по аналогии со списком, приведенным в данных требованиях. Окончательный вариант творческой работы должен быть переплетен в твердый переплет.

Литература и источники для подготовки работы

Источники

1. Security policy - Документы по информационной безопасности [Электронный ресурс]. - Режим доступа http://www.securitypolicy.ru/index.php (Дата обращения 10.10.2012 г.);

2. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799-2055 «Информационная технология. Практические правила управления информационной безопасностью». – М.: Стандартинформ, 2006. – 62 с. [Электронный ресурс]. Режим доступа www.npo-echelon.ru/common_files/**gost**/**GOST-17799-2005**.pdf. (Дата обращения 17.10.2012 г.)

Литература

3. Шаньгин В.Ф. Защита информации в корпоративных системах – М.: ИД «Форум»: ИНФРА-М, 2010. – 592 с.

4. Астахов А. Разработка и внедрение эффективных политик безопасности [Электронный ресурс]. - Режим доступа http://www.bre.ru/security/20198.html; (Дата обращения 10.10.2012 г.);

5. HR-portal. Сообщество HR-менеджеров. Типовая политика информационной безопасности. [Электронный ресурс]. – Режим доступа http://www.hr-portal.ru/pages/kb/tib.php; (Дата обращения 17.10.2012 г.);

3.2.7 Подготовка к круглому столу по заданной теме

Занятие по защите комплекса бизнес-моделей предприятия проводится в форме круглого стола. В связи с этим студентам рекомендуется предварительно провести самостоятельную работу по подготовке к данному занятию. Для эффективной организации круглого стола рекомендуется составить список вопросов, которые они хотели бы озвучить в рамках данного стола. Подготовить выдержки из статей по данной

проблеме и пути их решения. Подготовить небольшой рассказ о том, чем они пользовались при решении возникающих проблем, и насколько сложно было организовать командную работу. Какие рекомендации они бы дали сами себе перед выполнением данной работы.

3.2.8 Подготовка доклада по заданной теме

Лабораторная работа № 9, посвященная изучению стандартов в области информационной безопасности, проводится в форме круглого стола и презентации. Однако предварительно студенты должны подготовить доклад по заданной теме. Темы докладов выдаются предварительно не менее чем за неделю до проведения занятия. Темы для подготовки докладов представлены в таблице 4. Допускается тема по выбору студента при предварительном согласовании с преподавателем.

Таблица 4. - Темы для подготовки докладов

Номер темы	Наименование темы
1	Стандарт ISO/IEC 15408. Критерии оценки безопасности информационных технологий;
2	Стандарт ISO/IEC 27001:2005 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования»
3	Стандарт ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"
4	Стандарт ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".
5	Стандарт BS 7799-1:2005
6	Стандарты безопасности в сети Интернет;
7	Стандарты безопасности для беспроводных сетей;
8	ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты

3.2.9 Подготовка презентации по заданной теме

В рамках нескольких лабораторных работ, а именно работ № 4, № 7 и № 9 занятие проводится в интерактивной форме с использованием презентации. Студентам предварительно выдается задание для разработки презентации. Презентация разрабатывается самостоятельно индивидуально, либо в команде.

К занятиям № 4 и № 7 необходимо разработать презентации карт процессов «Деятельность магазина по продаже и прокату видеоносителей» и «Деятельность туристической фирмы». К занятию № 9 требуется подготовить презентацию по теме доклада.

После демонстрации презентации происходит ее обсуждение с остальными участниками занятия. Если занятие включает в себя также элементы круглого стола, то ребята обсуждают представленную презентацию с современными данными, найденными в статьях и Интернете, и в затем подводят итог занятия.

Презентация может быть представлена в любом формате, подходящем для демонстраций. Допустимы такие форматы как ppt, pdf, html и т.д.. Перед занятиям студенты должны ознакомится с техническими возможностями аудитории, где будет проходить занятие на возможность воспроизведения указанных форматов.

3.2.10 Анализ статей по заданной теме

При подготовке кейсов, презентаций и круглого стола требуется не только представить заданную тему, но и владеть информацией об альтернативных путях решения проблемы, современных тенденциях в данной области. С этой целью преподаватель рекомендует статьи для самостоятельного анализа студентами при подготовке к интерактивным занятиям. Студенту нужно в течение 15-20 мин поработать со статьей и уметь ориентироваться в указанной теме, отвечать на вопросы и вступать в дискуссию.

Для того чтобы статьи были актуальными, отражающими реальное положение вещей в данных методических рекомендациях они не приводятся. Студентам рекомендуются статьи года издания, совпадающего с годом обучения группы на данном курсе или на год ранее. Поскольку сфера IT является очень динамичной, то статьи более ранних годов издания не желательны для рекомендации студентам.

3.2.11 Составление карт процессов для моделей бизнес-процессов

Основное назначение карты процесса – это представлять технологию выполнения процесса. За счет создания карты процесса осуществляется его документирование, в результате у организации появляется возможность управлять этим процессом, вносить в него изменения, оценивать результативность и эффективность процесса[5].

В ходе создания системы качества, карты процессов разрабатываются на все процессы, входящие в область действия системы качества.

Карты процессов составляются на основе анализа данных о предприятии (опросов, анализа документов, анкетирования и проч.). Как правило, модели бизнес-процессов не существуют обособленно, а тесно связаны с картами процессов.

---

[5] Назначение карты процессов. [Электронный ресурс]. Режим доступа URL http://www.kpms.ru/Procedury/Q_Process_Map.htm (Дата обращения 05.02.2013 г.)

В блоке лабораторных работ «информационные технологии в управлении качеством» студентам требуется самостоятельно разработать карты процессов на три модели бизнес-процессов:

1. модель бизнес-процесса в нотации IDEF0, разработанная по заданию другого студента (название зависит от задания);

2. модель бизнес-процесса «Деятельность магазина по продаже и прокату видеоносителей»;

3. модель бизнес-процесса «Деятельность туристической фирмы».

Все указанные бизнес-процессы разрабатывались студентами в ходе лабораторных работ. К занятию, следующему за данной лабораторной работой, требуется разработать карту процессов для необходимой модели. На каждую карту процессов рекомендуется затратить не менее 2 – х часов. При этом студенты должны самостоятельно изучить принципы построения карт процессов, используя литературу и электронные ресурсы.

Стандартная карта процессов должна содержать следующую информацию:

1. входы и выходы процесса;

2. начальная точка процесса;

3. участники процесса и подпроцессов;

4. владелец и ответственный за процесс;

5. поставщики и потребители процесса;

6. требования к поставщикам;

7. структура процесса;

8. контроль процесса;

9. документация, регламентирующая процесс;

10. записи процесса;

11. валидация процесса.

Карта процесса готовится в текстовом формате (сдается преподавателю) и в любом формате для представления аудитории (ppt., pdf, и др.).

3.2.12 Работа с электронными ресурсами

На протяжении всего периода изучения дисциплины студентам необходимо пользоваться электронными ресурсами для всех видов деятельности. При подготовке к лабораторным работам, самостоятельной работы и лекциям. Электронные ресурсы необходимы для поиска информации о предприятиях, нотациях, примерах бизнес-процессов, статей, ГОСТов и зарубежных стандартов и т.д. Минимальное время

рекомендуемое для работы с электронными ресурсами в каждом семестре составляет 6 часов. Однако при желании студента оно может быть увеличено.

3.2.13 Работа в команде по разработке комплекса моделей бизнес-процессов предприятия

При разработке комплекса моделей бизнес-процессов вся работа выполняется в команде. При этом задания распределяются в группе полностью по желанию студентов. Помимо разработки моделей бизнес-процессов для выполнения данной лабораторной работы требуется большая предварительная подготовка по сбору данных. Таким образом, неотъемлемой частью самой лабораторной работы являются встречи членов команды для решения текущих вопросов и сведения работы каждого студенты в единый общий комплекс. Минимальное рекомендуемое время для проведения таких встреч 1,5 часа на все лабораторную работу суммарно. Однако при возникающей необходимости студенты могут обсуждать необходимые рабочие вопросы гораздо чаще.

3.2.14 Подготовка кейсов по заданной теме

В некоторых из цикла лабораторных работ вводятся элементы интерактивных занятий, где используется метод кейсов. ***Метод кейсов*** *(англ. Case method, кейс-стади, case-study, метод конкретных ситуаций, метод ситуационного анализа) — техника обучения, использующая описание реальных экономических, социальных и бизнес-ситуаций.* Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации[6].

Решение кейсов на лекциях и лабораторных работах происходит в форме тренингов. Темы кейсов студентам либо во время аудиторных занятий, либо при проведении он-лайн консультаций через социальные сети. На заданную тему студенты должны подготовить описание конкретной ситуации и проработать решение проблемы. По итогам разработки кейсов каждым студентом формируется пакет кейсов для проведения занятия. Во время проведения занятия студенты решают кейсы из данного пакета. Примеры для составления кейсов по блоку «Защита информации» представлены ниже.

Примеры кейсов

[6] Метод кейсов. Материал из Википедии свободной энциклопедии. Режим доступа: URL: http: // wikipedia.org. (Дата обращения 10.12.2011 г.).

1) К диспетчеру по работе с абонентами компании «Мегафон» по ICQ обратился человек, представившийся администратором данного отдела с просьбой предоставить логин и пароль для входа в систему с целью обновления рабочих приложений.

2) Менеджер по работе с клиентами компании «TOMTEL» получил по почте exe файл от неизвестного отправителя с предложением улучшить качество работы на рабочем компьютере.

3) К менеджеру по ипотечному кредитованию коммерческого банка «Промсвязьбанк» обратился человек, представившийся новым сотрудником службы безопасности с просьбой освободить рабочее место на 10 мин для обновления рабочих приложений и антивируса.

4) Начальник отдела оптовых продаж гипермаркета «Стройпарк» получил по электронной почте письмо с предупреждением о том, что его логин и пароль для работы с базой данных о поставщиках будет заблокирован через 3 часа в связи с политикой безопасности. Кроме того сообщалось, что необходимо сообщить логин и пароль по указанному адресу для обновления.

5) Специалист по снабжению компании ОАО «Томритейл» (сеть магазинов «Абрикос») получает по электронной почте письмо. Письмо представляет собой фрагмент переписки двух человек, который якобы ошибочно был прислан другому сотруднику компании («жертве»). В переписке обсуждается возможность оплаты каких-либо услуг с помощью электронных денежных средств. Один из адресатов предлагает другому оплатить услуги с помощью электронного кошелька, при этом в письме приводятся номер электронного кошелька, пароль, инструкция по использованию. К письму прикреплен «плагин для совершения денежных операций» – троянское программное обеспечение. Таким образом, получатель попадает в положение выбора, находясь между двумя альтернативами: украсть или нет, воспользоваться чужими денежными средствами или нет.

6) Сотрудник финансово-аналитического отдела компании ОАО «Ростелеком» в конце рабочего дня выбросила черновые листы с реквизитами, платежными поручениями, накопленные в течение всего дня в корзину для бумаг.

7) Забывчивая сотрудница ИФНС записала на листочке логин и пароль для работы с базой данных о налогоплательщиках и приклеила на монитор.

8) PR-менеджеру сибирского отделения Сбербанка России, которому недавно уменьшили заработную плату предложили работу в АКБ «Газпромбанк» с зарплатой вдвое превышающей предыдущую.

3.2.15 Подготовка к экзамену

Поскольку итоговый контроль знаний студентов по данному курсу осуществляется в форме экзамена, то студентам необходимо представить список вопросов для подготовки не менее чем за месяц до даты экзамена. В данном разделе представлено 28 контрольных вопросов по курсу «Информационные технологии в управлении качеством и защита информации». Представленные вопросы входят в состав экзаменационных билетов. Данные вопросы являются теоретической составляющей итоговой проверки знаний студентов на экзамене.

1) Основные объекты безопасности. Виды безопасности.
2) Виды угроз информационной безопасности.
3) Место системы обеспечения информационной безопасности в системе национальной безопасности РФ.
4) Цели управления информационной безопасностью организации. Активы и их оценка.
5) Типы методик оценки рисков. Методики CRAMM, FRAP, OCTAVE, Risk Watch, Microsoft и их характеристики.
6) Модели нарушителя, угроз и уязвимостей. Их назначение и принцип построения.
7) Оценка рисков. Составление отчета об оценке рисков. Политика безопасности.
8) Автоматизированные системы обработки информации, структура элементов и их уязвимость.
9) Виды угроз безопасности субъектам информационных отношений и их классификация.
10) Принцип алгоритма RSA для формирования цифровой подписи. Его достоинства и недостатки.
11) Электронная цифровая подпись, способы приобретения, необходимая документация. Опасность использования.
12) Стандарты безопасности в интернете. Общие характеристики.
13) Криптосистемы с симметричными и асимметричными ключами.
14) Российское законодательство в области защиты информации.
15) Назначение, содержание и особенности Международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий».
16) Компьютерные преступления и особенности их расследования.
17) Типы и виды компьютерных вирусов. Особенности поражающего воздействия.
18) Политика безопасности. Назначение и структура документа.
19) Информационные ресурсы РФ.

20) Содержание и особенности Международных стандартов серии ISO/IEC 17799:2002.
21) Права на доступ к информации.
22) Идентификация и механизмы подтверждения подлинности пользователя.
23) Брандмауэры. Назначение и принцип действия.
24) Криптография, криптоанализ, криптостойкость и ее параметры.
25) Метод перестановки для шифрования текста.
26) Наиболее популярные программные продукты антивирусной защиты. Сравнительный анализ возможностей.
27) Организационные требования к системам информационной защиты.
28) Методология проектирования защиты.

Примечание: каждый вопрос экзаменационного билета содержит также практическое задание. Все практические задания, содержащиеся в билетах, были проделаны в курсе лабораторных работ. Балльно-рейтинговая система оценки знаний студентов на экзамене представлена в рабочей программе данной дисциплины. Не менее чем за три дня до экзамена преподаватель должен организовать консультацию, где все вопросы, вызывающие у студентов сложность в подготовке к экзамену необходимо подробно рассмотреть.

3.3 Оценка выполнения самостоятельной работы студентов

В начале семестра всем студентам выдается балльно-рейтинговая раскладка (см. в рабочей программе по дисциплине «Информационные технологии в управлении качеством и защита информации») в соответствии с которой оценка знаний студентов осуществляется непрерывно на основании всех видов самостоятельной работы, рассмотренных выше. Не выполнение или не своевременное выполнение заданий для самостоятельной работы, может служить основанием для снижения баллов за выполнение аудиторной работы по аналогичной теме. Поскольку аудиторные занятия находятся в тесной взаимосвязи с темами самостоятельной работы.

В зависимости от содержания СРС контроль осуществляется в виде оценивания письменного отчета по результатам лабораторных работ, оценивания во время опроса на лекциях, оценок за тестирование, оценок за решение кейсов, общей оценки деятельности студента при проведении интерактивных занятий, оценки за ответы на экзамене.

3.4 Организация консультаций по выполнению самостоятельной работы

На любом этапе обучения студенты могут получать необходимые консультации по выполнению самостоятельной работы не только в аудиторные часы, но и дома в режиме

он-лайн. Для консультирования студентов используются электронные ресурсы: электронная почта, социальная сеть «Facebook», чат ICQ.

ПРИЛОЖЕНИЕ А

ПРИМЕР ОФОРМЛЕНИЯ ТИТУЛЬНОГО ЛИСТА ТВОРЧЕСКОЙ РАБОТЫ

(обязательное)

Министерство образования и науки РФ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«Томский государственный университет систем управления и радиоэлектроники» (ТУСУР)

«Разработка политики безопасности

организации *наименование*»

Творческая работа

по дисциплине

«Защита информации в компьютерных системах»

Выполнил:

Студент гр.____

ФИО

Проверил:

к.ф.-м.н,, доцент каф. УИ

Годенова Е.Г.

Томск, 2012

ПРИЛОЖЕНИЕ Б
ПРИМЕР ОФОРМЛЕНИЯ СПИСКА ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

(обязательное)

В приложении представлен пример оформления списка литературных источников, в скобках указано к какому виду источников относится данное издание.

Список используемой литературы

Оформление монотомного издания

1. Шило В.Л. Популярные цифровые микросхемы.-М.: Радио и связь, 2007.-240с.

Оформление многотомного издания

2. Савельев И.В. Курс общей физики: Учеб. пособие для студентов втузов. - М: Наука, 2008. - Т. 1-3.

Оформление нормативно-технических и патентных документов

3. ГОСТ 8.417-81 Государственная система обеспечения единства измерений. Единицы физических величин.

Оформление составной части документа

4. Андрющенко Б.И. Транзисторно-ламповый выходной каскад усилителя мощности // Радиолюбитель. -1992. - № 6. - С. 38.

Оформление электронного документа

5. Назначение карты процессов. [Электронный ресурс]. Режим доступа URL http://www.kpms.ru/Procedury/Q_Process_Map.htm (Дата обращения 05.02.2013 г.)