Министерство образования и науки Российской Федерации
Государственное образовательное учреждение высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»

УТВЕРЖДАЮ

Заведующий кафедрой
«Управление инновациями»

_____ */А.Ф.Уваров*
(подпись) *(ФИО)*
"_____" _____ 2012 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

по дисциплине

«ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

Составлены кафедрой: «Управление инновациями»

Для студентов, обучающихся
по направлениям подготовки магистров
222000.68 «Инноватика», профиль подготовки «Управление инновациями в электронной технике»

Форма обучения очная

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

" 25 " июня 2012 г.

Томск 2012 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ КУРСА

Дисциплина «Защита информации в компьютерных системах» относится к вариативной части профессионального цикла дисциплин в учебном плане по подготовке магистров по направлению 222000.68 «Инноватика».

Поскольку современные организации невозможно представить без автоматизированных систем обработки информации, вопрос защиты информации в различных компьютерных системах находится на пике актуальности. Кроме того в мире непрерывно происходит процесс наращивания технологических новинок. Как правило, крупные компании, давно занимающие лидирующие позиции на рынке имеют грамотно разработанную политику безопасности. Малые инновационные предприятия не всегда могут позволить себе временные и финансовые затраты на разработку политики безопасности. Поэтому магистру по направлению «Инноватика» необходимо иметь представление об актуальных вопросах защиты информации в компьютерных системах и знать минимальный набор превентивных мер по защите информационных активов предприятия.

Цель курса «Защита информации в компьютерных системах» дисциплины - формирование у студентов целостного представления о методах, средствах, способах и необходимости защиты информации, обрабатываемой в компьютерных системах.

- ✓ ознакомить обучающихся с основными видами, классификациями, типами угроз безопасности информации, существующих в современных компьютерных системах;
- ✓ продемонстрировать студентам важность своевременной защиты компьютерной информации;
- ✓ ознакомить обучающихся с нормативно-правовым обеспечением в области защиты информации международного и отечественного уровней;
- ✓ освоить существующие методики и способы защиты информации в компьютерных системах и сетях.

2. СТРУКТУРА КУРСА

Основные положения курса «Защита информации в компьютерных системах» излагаются в рамках лекционных занятий. Необходимая детализация, освоение курса лекций и более глубокое изучение дисциплины обеспечиваются во время практических занятий, самостоятельной работы и в процессе разработки политики безопасности организации. Дисциплина «Защита информации в компьютерных системах» изучается в первом семестре и заканчивается зачетом.

В объеме курса предусмотрено: 9 лекционных и 18 практических занятиях. Курс заканчивается защитой разработанной политики безопасности и итоговым тестированием, результаты которого оцениваются в соответствии с бально-рейтинговой системой.

3. СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

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

Подготовка к практическим (семинарским) занятиям включает в себя изучение лекционного материала и рекомендованной литературы.

Таблица 1 – Виды самостоятельной работы

Наименование работы	Объем, ч
Проработка конспектов лекций	4,5
Подготовка доклада	2
Подготовка к практическим занятиям	9
Подготовка письменных отчетов	5
Разработка политики безопасности организации	13
Подготовка к итоговому тестированию	2,5
Всего	36

Для успешной подготовки к итоговому тестированию рекомендуется изучение лекционного материала и выполнение всего комплекса практических работ.

4. ПЛАН-ГРАФИК ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТАМИ ПО ДИСЦИПЛИНЕ

График выполнения самостоятельной работы студентов (36 ч) приведен в таблице 2.

Таблица 2 – График выполнения самостоятельной работы

Вид самостоятельной работы	Номер недели семестра																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Проработка конспектов лекций	0,5		0,5		0,5		0,5		0,5		0,5		0,5		0,5		0,5	
Подготовка к практическим (семинарским) занятиям		1		1		1		1		1		1		1		1		1
Подготовка доклада	2																	
Написание отчетов		0,5		0,5		0,5		1		0,5		0,5		0,5		0,5		0,5
Разработка политики безопасности						1	1	1	1	1	1	1	1	1	1	1	1	1
Подготовка к итоговому тестированию																	1	1,5
Итого в	2,5	1,5	0,5	1,5	0,5	2,5	1,5	3	1,5	2,5	1,5	2,5	1,5	2,5	1,5	2,5	2,5	4

неделю часов																	

5. ХАРАКТЕРИСТИКА, ОПИСАНИЕ И ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ И ОФОРМЛЕНИЮ РЕЗУЛЬТАТОВ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1 Самостоятельная работа по подготовке к практическим занятиям

Целью проведения практических занятий является закрепление полученного на лекциях теоретического материала, развитие логического мышления и аналитических способностей у будущих магистров по направлению «Инноватика».

Методика проведения практических занятий предусматривает групповое решение общих (типовых) задач и задач для индивидуального рассмотрения. Для решения ряда задач требуются навыки использования стандартных офисных программ и ресурсов сети Интернет.

Темы практических занятий сообщаются студентам предварительно накануне занятия.

На каждом практическом занятии студентам выдаются методические рекомендации для выполнения практических работ, в которых кратко изложен основной теоретический материал по теме практической работы, а также приведен порядок выполнения работы с требованиями к отчету.

Таблица 3 – Темы практических работ

Номер темы	Наименование темы	Трудоемкость, ч
1	Изучение международных стандартов информационной безопасности	4
2	Анализ внутренней сети	4
3	Методики оценки рисков и политика безопасности. Методика оценки рисков Microsoft.	4
4	Метод перестановки для шифрования текстов. Шифрование по методу Вижинера	2
	Исследование электронной цифровой подписи на основе алгоритма RSA	2
5	Выявление уязвимостей в компьютерных системах и построение локальной политики паролей	2
	Исследование надежности системы идентификации пользователя	2
6	Средства защиты и удостоверения подлинности электронных документов	4

7	Использование технологий виртуализации для обеспечения безопасности	4
8	Брандмауэры и методы защиты компьютера от несанкционированного доступа.	4
9	Типы компьютерных вирусов и методы борьбы с ними	2
10	Итоговое тестирование за семестр	2
	ИТОГО	36

5.2 Самостоятельная работа по разработке политики безопасности организации

Целью разработки политики безопасности является развитие навыков самостоятельной работы с учебной и справочной литературой. Кроме того данная работа призвана унифицировать все знания и практические навыки, полученные за семестр. При разработке политики безопасности студентами актуализируются знания, полученные на лекциях и практических занятиях, учатся анализировать современные проблемы организаций, ставить задачи и выбирать соответствующие методы решения, представлять и применять полученные результаты. Одной из ключевых позиций при разработке политики безопасности является выбор организации. Студентам предоставляется свобода выбора необходимой организации. При этом можно использовать ресурсы сети Интернет, опыт, полученный ранее при прохождении производственной практики, взаимодействие с резидентами бизнес-инкубатора ТУСУР. В процессе выбора нужной организации студенты получают навык анализа основных процессов организации и представление полученной информации в логическом, структурированном виде.

5.3 Самостоятельная работа по подготовке доклада

К первому практическому занятию студентам необходимо подготовить доклад, поскольку занятие организуется в интерактивной форме, где студенты выступают в роли преподавателя. При подготовке доклада студентам необходимо распределить доклады так, чтобы все темы были полностью раскрыты и не остались неохваченными. В процессе распределения происходит взаимодействие студентов во внеучебное время, т.е. реализуются интерактивные формы самостоятельной работы. Темы для подготовки докладов представлены в таблице 4.

Таблица 4 – Темы для подготовки докладов

Номер темы	Наименование темы
1	Стандарты ISO/IEC 15408. Критерии оценки безопасности информационных технологий;
2	Стандарты ISO/IEC 17799/27002 и 27001
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	Нормативные документы РФ в области информационной безопасности.
6	Международные стандарты безопасности для сети Internet;
7	Международные стандарты безопасности для беспроводных сетей;
8	Стандарты ISO/IEC 15408. Критерии оценки безопасности информационных технологий;
9	Стандарты ISO/IEC 17799/27002 и 27001
10	Стандарт ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"
11	Стандарт ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

6. ОЦЕНКА ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

В начале семестра всем студентам выдается рейтинговая раскладка (см. в Рабочей программе по дисциплине «Защита информации в компьютерных системах») в соответствии с которой оценка знаний студентов осуществляется непрерывно на основании:

– текущего контроля выполнения практических работ;

– работы по подготовке политики безопасности;

– опроса на лекциях;

– защиты письменных отчетов;

– итогового тестирования на зачете.

В зависимости от содержания СРС контроль осуществляется в виде оценивания письменного отчета по результатам практических работ, тестирования, защиты отчетов.

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 «ВКонтакте», чат ICQ. Для оптимальной организации помощи студентам ежедневно назначается время он-лайн консультаций.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

При самостоятельной подготовке к практическим занятиям рекомендуется пользоваться конспектами лекций, настоящими методическими рекомендациями, учебными пособиями, ресурсами глобальной сети Интернет.

Основная литература

1. Инженерно-техническая защита информации : учебное пособие [Электронный ресурс] / Титов А. А. – 2010. 195 с. Режим доступа: http://edu.tusur.ru/training/publications/654. ограниченный (требуется регистрация на портале) (Дата обращения 20.06.2012 г.)

2. Информатика. Базовый курс : учебное пособие для вузов / С. В. Симонович [и др.] ; ред. С. В. Симонович. - СПб.: Питер, 2008. - 639с. (6 экз. в библ. ТУСУР).

Дополнительная литература

1. Мельников В.П. Информационная безопасность и защита информации : учебное пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков – М.: Академия, 2009. – 336 с. (1 экз. в библ. ТУСУР);

2. Акулов О.А. Информатика. Базовый курс : учебник для вузов / О.А. Акулов, Н.В., Медведев. – М.: Омега-Л, 2009. – 576 с. (1 экз. в библ. ТУСУР);

3. Куприянов А.И. Основы защиты информации. – М.: Academia, 2006. – 253 с. (50 экз. в библ. ТУСУР);

4. Основы защиты информации: учеб. пособие в 3 ч. Сост. А.А. Шелупанов [и др.]. – Томск: В-Спектр, 2007. – 150 с. (81 экземпляр в библиотеке ТУСУР).

5. Галатенко, Владимир Антонович. Основы информационной безопасности : учебное пособие для вузов / В. А. Галатенко ; ред. В. Б. Бетелин. - М. : Интернет-Университет Информационных Технологий, 2008 ; М. : БИНОМ. Лаборатория знаний, 2008. (1 экз. в библ. ТУСУР);

Базы данных, информационно-справочные и поисковые системы:

1. Информационный портал по компьютерной безопасности [Электронный ресурс]. URL: http://www.securitylab.ru. (дата обращения 11.06.2012 г.)

3. OpenPGP в России. [Электронный ресурс] - URL: http://www.pgpru.com. (Дата обращения 18.06.2012 г.)

4. Официальный сайт компании Doctor Web. [Электронный ресурс] - URL: http://www.drweb.com. (Дата обращения 18.06.2012 г.)

5. Официальный сайт антивирусной лаборатории Касперского. [Электронный ресурс] - URL: http://www.kaspersky.ru (Дата обращения 18.06.2012 г.)

6. Поисковая система Google. [Электронный ресурс] - URL: http://google.com (Дата обращения 18.06.2012 г.)

7. Википедия свободная энциклопедия. [Электронный ресурс] – URL: http://ru.wikipedia.org/wiki. (Дата обращения 18.06.2012 г.)

8. Стандарты информационной безопасности. [Электронный ресурс] – URL: http://www.leta.ru/library/standards/ (Дата обращения 18.06.2012 г.)

9. Microsoft. Центр безопасности. [Электронный ресурс] – URL: http://www.microsoft.com/ru-ru/security/default.aspx. (Дата обращения 18.06.2012 г.)