РУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ имени В.П.Чернова

РИУ

РАБОЧАЯ ПРОГРАММА

дисциплины

Защита информации
для специальности

«Юриспруденция»
(наименование специальности)

квалификация – юрист

«УТВЕРЖДАЮ»

Проректор по учебной работе _____ И.В.Щербакова

Программа одобрена на заседании Ученого совета юридического факультета
от 14. 01. 2011 г., протокол № 1.

Москва 2011

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Рабочая программа учебной дисциплины «Защита информации» предназначена для реализации государственных требований к минимуму содержания и уровню подготовки выпускников по специальности «Юриспруденция». Целью и задачей преподавания дисциплины является ознакомление студентов с основами защиты информации. Эти навыки необходимы при работе специалистов в конкретных информационных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Учебная дисциплина «Защита информации» относится к блоку естественнонаучных дисциплин и способствует закреплению знаний, полученных в ходе изучения дисциплин «Информатика и математика», «Базы данных», «Информационное обеспечение управленческой деятельности».

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате изучения дисциплины:

Студент должен

иметь представление:

- о типовых разработанных средствах защиты информации и возможностях их использования в реальных задачах создания и внедрения информационных систем.

Студент должен

Знать:

- основы информационной безопасности и защиты информации;
- принципы криптографических преобразований,
- типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа.

Уметь

- проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем.

Студент должен

Иметь навыки:

- в реализации мероприятий по обеспечению информационной безопасности на предприятии.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Рабочая программа рассчитана на 40 часов. Из них 36 часов отводится на самостоятельную работу студента и 4 часа на лекционные и практические занятия. В зависимости от личных потребностей, студент может изменить время, отводимое на ту или иную форму учебной нагрузки или на распределение часов по разделам курса.

Изучение материала ведется в форме, доступной пониманию студентов, соблюдается единство терминологии обозначений в соответствии с действующими государственными стандартами.

ТЕМАТИЧЕСКИЙ ПЛАН ДИСЦИПЛИНЫ (курс 5)

Наименование разделов и тем	Учебная нагрузка студента, час.				
	Макси-мальная	Самостоя-тельная	Обязат. при очной форме обучения		
				В том числе:	
			Всего	Обзорно - устан, занятия	Лаб.раб практич занятия
Раздел 1. Введение в информационную безопасность	4	4	-	-	-
Раздел 2. Правовое обеспечение информационной безопасности	6	5,25	0,75	0,5	0,25

Раздел 3. Организационное обеспечение информационной безопасности	6	5.25	0,75	0,5	0,25
Раздел 4. Технические средства обеспечения информационной безопасности	6	5,5	0,5	0,5	-
Раздел 5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах	6	5,5	0,5	0,5	-
Раздел 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	6	5,25	0,75	0,5	0,25
Раздел 7. Защита от компьютерных вирусов	6	5,25	0,75	0,5	0,25
Итого по дисциплине:	**40**	**36**	**4**	**3**	**1**

5.1 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Введение в информационную безопасность

Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов.

Раздел 2. Правовое обеспечение информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Три вида возможных нарушений информационной системы.

Раздел 3. Организационное обеспечение информационной безопасности

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Раздел 4. Технические средства обеспечения информационной безопасности

Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке.

Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации.

Раздел 5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах

Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах.

Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению.

Раздел 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств

Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы.

Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Защита ПК на уровне BIOS.

Раздел 7. Защита от компьютерных вирусов

История появления компьютерных вирусов и факторы, влияющие на их распространение.
Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы.

5.2 НОРМАТИВНЫЙ МАТЕРИАЛ:

Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5.3 УЧЕБНАЯ ЛИТЕРАТУРА

ОСНОВНАЯ:

1. Анин Б.Ю. Защита компьютерной информации:Учебное пособие. – СпБ: БХВ-Петербург, 2008
2. Северин В.А Правовое обеспечение информационной безопасности предприятия: Учебно-практическое пособие. -М.: Городец 2009
3. Лясин Д.Н., СаньковС. Г. Модель безопасности ОС Windows: Сборник «Методические указания». Выпуск 2 Волгоград:ВолгГТУ, 2012
4. Степанов, И. К. Информационная безопасность и защита информации: Учебное пособие. – М.ИНФРА-М, 2009.

ДОПОЛНИТЕЛЬНАЯ:

1. В. С. Люцарев, Безопасность компьютерных сетей на основе Windows NT: Учебное пособие, - М. Русская редакция, 1998
2. А. В. Соколов, Защита от компьютерного терроризма: Справочное пособие. - СпБ: БХВ-Петербург, 2002
3. В. Н. Лопатин Информационная безопасность России: Справочное пособие. - СпБ: БХВ-Петербург, 2000
4. Д. Бэндл; Пер. с англ. Защита и безопасность в сетях LINUX: Справочное пособие. - СпБ: БХВ-Петербург, 2002

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Компьютерный класс, оборудованный для проведения практических работ средствами оргтехники, персональными компьютерами, объединенными в сеть с выходом в Интернет;
2. Установленное лицензионное программное обеспечение.

7. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Учебно-методический комплекс по дисциплине " Защита информации ", составленный в соответствии с государственным образовательным стандартом по специальности "Юриспруденция", включает в себя пособие (в объеме 40 часов), два вида тестовых заданий (семинары и сборник вопросов, 108 и 90 заданий, соответственно), контрольную, практическую и зачетную работы, которые дают целостную систему знаний, обеспечивая их глубину и прочность. Особое внимание уделено формированию профессиональной компетентности будущих юристов, развитию навыков самостоятельного применения знаний.

Предлагаемые учебно-методические материалы должны выработать у студентов знания в области теоретических основ информационной безопасности; навыки практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.
Получение углубленных знаний по изучаемой дисциплине достигается путем знакомства со специальными источниками и дополнительной научной литературой по проблематике дисциплины.

Разработчик:
К.ф-м.н., доцент Башарули Н.В., доцент РИУ
Рецензент:
к.т.н., доцент Першиков В.И., доцент РИУ

Утверждение рабочей программы учебной дисциплины

Уполномоченный орган (должностное лицо)	Дата принятия решения	№ документа
Ученый совет юридического факультета	14.01.2011	Протокол № 1

Внесение изменений в рабочую программу учебной дисциплины

Уполномоченный орган (должностное лицо)	Дата принятия решения	№ документа
Ученый совет юридического факультета	26.01.2012	Протокол № 1
Ученый совет юридического факультета	17.01.2013	Протокол № 1
Ученый совет юридического факультета	14.01.2014	Протокол № 1