РУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ
имени В.П.Чернова

РИУ

РАБОЧАЯ ПРОГРАММА

дисциплины

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

для направления
«Экономика»
(наименование направления)

«УТВЕРЖДАЮ»

Проректор по учебной работе _____ И.В. Щербакова

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

Москва 2011

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Учебная дисциплина «Основы защиты информации» предназначена для реализации государственных требований к минимуму содержания и уровню подготовки выпускников по направлению «Экономика». **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 «Основы защиты информации» относится к вариативной части математического цикла дисциплин, является дисциплиной по выбору студентов (Б2.В.ДВ.1:1) и способствует закреплению знаний, полученных в ходе изучения дисциплин «Экономическая информатика», «Профессиональные компьютерные программы», «Информационное обеспечение управления».

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате изучения дисциплины "Основы защиты информации" у студента должны быть сформированы следующие компетенции:

владеет культурой мышления, способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения (ОК-1);

умеет использовать нормативные правовые документы в своей деятельности (ОК-5);

способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-12);

владеет основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией, способен работать с информацией в глобальных компьютерных сетях (ОК-13);

- способен собрать и проанализировать исходные данные, необходимые для расчета экономических и социально-экономических показателей, характеризующих деятельность хозяйствующих субъектов (ПК-1);

- способен осуществлять сбор, анализ и обработку данных, необходимых для решения поставленных экономических задач (ПК-4);

- способен выбрать инструментальные средства для обработки экономических данных в соответствии с поставленной задачей, проанализировать результаты расчетов и обосновать полученные выводы (ПК-5);

- способен, используя отечественные и зарубежные источники информации, собрать необходимые данные проанализировать их и подготовить информационный обзор и/или аналитический отчет (ПК-9);

- способен использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-10);

- способен использовать для решения коммуникативных задач современные технические средства и информационные технологии (ПК-12).

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.

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.

иметь навыки:

- в реализации мероприятий по обеспечению информационной безопасности на предприятии.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Рабочая программа рассчитана на 72 часа. Из них 64 часа отводится на самостоятельную работу студента и 8 часов 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 1)

Наименование разделов и тем	**Учебная нагрузка студента, час.**				
	Макси-мальная	Самостоя-тельная	Обязат. при очной форме обучения		
			Всего	В том числе:	
				Обзорно - устан, занятия	Лаб.раб практич занятия
Раздел 1. Введение в информационную безопасность	9	9	-	-	-
Раздел 2. Правовое обеспечение информационной безопасности	10	9	1	0,5	0,5
Раздел 3. Организационное обеспечение информационной безопасности	11	10	1	0,5	0,5
Раздел 4. Технические средства обеспечения информационной безопасности	11	9,5	1,5	1	0,5
Раздел 5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах	11	9,5	1,5	1	0,5
Раздел 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	10	8,5	1,5	1	0,5
Раздел 7. Защита от компьютерных вирусов	10	8,5	1,5	1	0,5
Итого по дисциплине:	**72**	**64**	**8**	**5**	**3**
Зачетные единицы	**2**				

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 от 6 апреля 2011 г. № 63 - ФЗ «Об электронной цифровой подписи» (с изменениями и дополнениями, вступающими в силу с 1 сентября 2013 г).

Федеральный закон от 27 июля 2006 г. № 149 – ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 21 июля 1993 г. № 5485 - 1 «О государственной тайне» (с изменениями на 18 июля 2011 г.).

Федеральный закон от 27 декабря 2002 г. № 184 - ФЗ «О техническом регулировании»

Федеральный закон от 2 мая 2006 г. № 59 - ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»

Федеральный закон от 29 июля 2004 г. № 98 - ФЗ «О коммерческой тайне».

5.3 ОСНОВНАЯ ЛИТЕРАТУРА

1.Северин В.А Правовое обеспечение информационной безопасности предприятия: Учебно-практическое пособие. -М.: Городец 2009.
2.Анин Б.Ю. Защита компьютерной информации:Учебное пособие. – СпБ: БХВ-Петербург, 2010.
3 Степанов, И. К. Информационная безопасность и защита информации: Учебное пособие. – М.ИНФРА-М, 2009.
Информационные технологии в науке и образовании: Уч. пос. / Е.Л.Федотова -М.:ИД ФОРУМ,2011

5.4 ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

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.

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Учебно-методический комплекс по дисциплине "Основы защиты информации", составленный в соответствии с федеральным государственным образовательным стандартом и основной образовательной программой института по направлению «Экономика», включает в себя пособие (в объеме 72 часов), два вида тестовых заданий (семинары и сборник вопросов, 108 и 90 заданий, соответственно), которые дают целостную систему знаний, обеспечивая их глубину и прочность. Особое внимание уделено формированию профессиональной компетентности будущих экономистов, 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 работы студента с учебной и научной литературой – основной и дополнительной – по проблематике дисциплины и знакомства с работами ведущих российских и зарубежных ученых.

Промежуточный контроль знаний студентов осуществляется на основе выполнения двух видов тестовых заданий, позволяющих оценить уровень теоретических знаний студентов по каждому разделу изучаемой дисциплины, а также контрольной и практической работ, способствующих систематизации знаний – в том числе конкретизации, сравнению и обобщению фактического материала в соответствии с поставленным заданием и дающих возможность выявить общекультурные и профессиональные компетенции студентов, определяемые содержанием дисциплины «Основы защиты информации».

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 ЭФ	14.01.2011	Протокол № 1

Внесение изменений в рабочую программу учебной дисциплины

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