МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 24.04.2017 г., №10

Рабочая программа дисциплины
Защита информации в корпоративных системах

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 5 ЗЕТ

Виды контроля в семестрах:
экзамен(ы) 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	34	34	34	34
Лабораторные	34	34	34	34
В том числе инт.	16	16	16	16
Итого ауд.	68	68	68	68
Контактная работа	68	68	68	68
Сам. работа	76	76	76	76
Часы на контроль	36	36	36	36
Итого	180	180	180	180

Курск 2017

Рабочая программа дисциплины Защита информации в корпоративных системах / сост. ; Курск. гос. ун-т. - Курск, 2017. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 1 декабря 2016 г. № 1515 "Об утверждении ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)" (Зарегистрировано в Минюсте России 20 декабря 2016 г. № 44821)

Рабочая программа дисциплины "Защита информации в корпоративных системах" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цель освоения дисциплины «Защита информации в корпоративных системах»
1.2	- заложить методически правильные основы знаний по информационной безопасности (ИБ), необходимых специалистам, занимающимся вопросами проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ОД

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОК-6: Способностью работать в коллективе , толерантно воспринимая социальные , культурные и иные различия
Знать:
Теоретические основы безопасности электронного бизнеса
Уметь:
Управлять проектами по созданию и развитию систем защиты для электронного бизнеса
Владеть:
Навыками обоснования необходимости внедрения систем защиты в электронный бизнес

ОПК-7: Способностью определять информационные ресурсы , подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты
Знать:
Методы защиты и упреждения атак на электронный бизнес
Уметь:
Выбирать инструментальные средства для реализации защищенных систем электронного бизнеса
Владеть:
Навыками выбора и применения инструментальных средств создания систем безопасности для электронного бизнеса

ПК-6: Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
Знать:
Методы оценки эффективности средств защиты Интернет-технологий
Уметь:
Оценивать результат деятельности компании по защите электронного бизнеса
Владеть:
Навыками взаимодействия с разработчиками при создании систем защиты электронного бизнеса

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)					
Код занятия	**Наименование разделов и тем**	**Вид занятий**	**Семестр / Курс**	**Часов**	**Интеракт.**
	Раздел 1. Раздел 1	Раздел			
1.1	Предпосылки становления предметной об-ласти информационной безопасности. Клю-чевые вопросы информационной безопасно-сти . Концепция информационной безопас-ности Российской Федерации. Разработка корпоративной концепции информационной безопасности	Лек	6	4	2
1.2	Лабораторная работа №1	Лаб	6	4	2
1.3	Правовые аспекты информационной безо-пасности. Международное и российское за-конодательство в сфере информационной безопасности	Лек	6	4	2
1.4	Лабораторная работа №2	Лаб	6	4	2
1.5	Виды защищаемой информации. Модель угроз и модель информационной безопасно-сти	Лек	6	4	2
1.6	Лабораторная работа №3	Лаб	6	4	0
1.7	Понятие защищенной информационной сис-темы. Программа информационной безопас-ности. Организационно-распорядительные документы в сфере информационной безо-пасности. Политика информационной безо-пасности	Лек	6	6	0
1.8	Лабораторная работа №4	Лаб	6	4	0
1.9	Управление информационными рисками	Лек	6	4	0
1.10	Лабораторная работа №5	Лаб	6	4	0
1.11	Стандартизация в сфере информационной безопасности	Лек	6	4	0
1.12	Лабораторная работа №6	Лаб	6	4	2
1.13	Математические модели систем и процессов защиты информации. Сервисы ИБ и защита от инсайдеров	Лек	6	4	0
1.14	Лабораторная работа №7	Лаб	6	6	2
1.15	Комплексная защита информационной ин-фраструктуры и ресурсов. Оценка эффек-тивности СЗИ	Лек	6	4	2
1.16	Самостоятельная работа №4	Ср	6	8	0
1.17	Лабораторная работа №8	Лаб	6	4	0
1.18	Самостоятельная работа №1	Ср	6	14	0
1.19	Самостоятельная работа №2	Ср	6	12	0
1.20	Самостоятельная работа №3	Ср	6	10	0
1.21	Самостоятельная работа №5	Ср	6	10	0
1.22	Самостоятельная работа №6	Ср	6	12	0
1.23	Самостоятельная работа №7	Ср	6	10	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Защита информации в корпоративных системах" рассмотрены и одобрены на заседании кафедры от «30» марта 2017 г. протоколом № 8, является приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине "Защита информации в корпоративных

системах" рассмотрены и одобрены на заседании кафедры от «30» марта 2017 г. протоколом № 8, является приложением к рабочей программе.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Прохорова О. В. - Информационная безопасность и защита информации: Учебник - Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.	http://www.iprbookshop.ru/43183	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Шаньгин В. Ф. - Информационная безопасность и защита информации: учебное пособие - Москва: ДМК Пресс, 2014.	http://www.iprbookshop.ru/29257	1
Л2.2	Некраха А. В., Шевцова Г. А. - Организация конфиденциального делопроизводства и защита информации: Учебное пособие - Москва: Академический Проект, 2015.	http://www.iprbookshop.ru/36849	1

6.3.1 Перечень программного обеспечения

7.3.1.1	199:
7.3.1.2	Microsoft Windows 7 (Open License: 47818817)
7.3.1.3	Microsoft Office 2007 (OpenLicense: 43136274)
7.3.1.4	Adobe Acrobat Reader DC (Бес-платное программное обеспечение)
7.3.1.5	GoogleChrome (Свободная лицензия BSD)
7.3.1.6	7-Zip (Свободная лицензия GNU LGPL),
7.3.1.7	Visual Studio Community (Проприе-тарная академическая лицензия)
7.3.1.8	СКЗИ "КриптоПроCSP" версии 4.0
7.3.1.9	СС КонсультантПлюс (Договор № 7/3Ц от 14.02.2017),
7.3.1.10	СКМ-21 ПО (Компакт-диск со специ-альным программным обеспечением)
7.3.1.11	Смарт-ПО (Компакт-диск с про-граммным обеспечением)
7.3.1.12	Code::Blocks (Свободная лицензия GNU GPLv3)
7.3.1.13	EclipseNeon (Открытое программное обеспечение EclipsePublicLicense)
7.3.1.14	
7.3.1.15	146:
7.3.1.16	Microsoft Windows 7 (OpenLi-cense: 47818817)
7.3.1.17	Ms OfficeProfessional 2007 (OpenLicense: 47818817
7.3.1.18	Google Chrome (Свободная ли-цензия BSD)
7.3.1.19	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.20	Adobe Acrobat Reader DC (Бес-платное программное обеспе-чение)

6.3.2 Перечень информационных справочных систем

7.3.2.1	Каталог библиотеки КГУ. - Режим доступа: http://195.93.165.10:2280
7.3.2.2	Электронная библиотека.- Режим доступа: http://elibrary.ru
7.3.2.3	Университетская информационная система «Россия» – http://uisrussia.msu.ru
7.3.2.4	Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
7.3.2.5	Электронная библиотечная система издательства «Лань» − http://e.lanbook.com/
7.3.2.6	Электронная библиотечная система «IPRbooks» − http://www.iprbookshop.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лаборатория программно-аппаратных средств обеспечения информационной безопас-ности;
7.2	Лаборатория технических средств защиты информации;
7.3	для проведения занятий лекци-онного типа, занятий семинаркого типа, курсового проекти-рования (выполнения курсовых работ), групповых и индивиду-альных консультаций, текуще-го контроля и промежуточной аттестации, самостоятельной работы,
7.4	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 199.
7.5	Моноблок LenovoC560 – 9 шт.
7.6	Стенд информационный 1,4м*0,9м – 9 шт.
7.7	Малогабаритный камуфлирован-ный блокиратор работы сотовых телефонов и закладных устройств – 1 шт.
7.8	Селективный обнаружитель циф-ровых радиоустройств ST062 – 1 шт.
7.9	Устройство защиты объектов ин-форматизации от утечки инфор-мации за счет ПЭМИН «Блокада» – 1 шт.
7.10	Нелинейный локатор «Буклет-2» – 1 шт.
7.11	Устройство МП—1А – 1 шт.
7.12	Электронно-оптическое устройст-во для обнаружения любых типов оптических устройств «Гранат» – 1 шт.
7.13	Программно-аппаратный ком-плекс «Соболь» – 1 шт.
7.14	ИМФ-3 имитатор многофункцио-нальный – 1 шт.
7.15	МониторЖК-панель 17 Асер – 1 шт.
7.16	Жалюзи вертикальные тканевые – 1 шт.
7.17	Концентратор 24порт – 1 шт.
7.18	Лабораторный комплекс «Беспро-водные сети ЭВМ»
7.19	Система активной защиты рече-вой акустической информации SEL-157 "Шагрень",
7.20	Устройство «Смарт (Комплекс оценки эффективности защиты речевой информации от утечки по акустическому, виброакустиче-скому и акустоэлектрическому каналам),
7.21	Программно-аппаратные средства защиты информации от НСД .
7.22	
7.23	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техни-кой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета.
7.24	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.25	Столов – 61
7.26	Посадочных мест – 162
7.27	Компьютеров:
7.28	Для пользователей – 40
7.29	Для библиотекаря – 2
7.30	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памяти, Athlon CPU D525 1.80GHz
7.31	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Планирование и организация времени, необходимого для изучения дисциплины.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:
Изучение конспекта лекции в тот же день, после лекции - 10-15 минут.
Изучение конспекта лекции за день перед следующей лекцией - 10-15 минут.
Изучение теоретического материала по учебнику и конспекту - 1 час в неделю.
Подготовка к лабораторному занятию - 30 мин.
Всего в неделю - 2 часа 55 минут.

2. Описание последовательности действий студента («сценарий изучения дисциплины»).

При изучении дисциплины очень полезно самостоятельно изучать материал, который еще не прочитан на лекции. Тогда лекция будет гораздо понятнее. Однако легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
3. В течение недели выбрать время (1 час) для работы с литературой по криптографическим методам в библиотеке или изучить дополнительную литературу в электронной форме.

3. Методические рекомендации по подготовке лабораторные занятий.
По данному курсу предусмотрены лабораторные занятия. При подготовке к лабораторным занятиям следует изучить соответствующий теоретический материал по криптографическим методам и, если предусмотрено темой, изучить работу программ-калькуляторов или функций криптографического модуля Python.
Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по криптоанализу. Литературу по курсу рекомендуется изучать в библиотеке. Полезно использовать несколько учебников. Однако легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия вве-дены, каков их смысл?, какие математические принципы используются в этом параграфе и каков их смысл «своими словами»?. Сами криптографические алгоритмы следует не заучивать, а «понять». С этой целью рекомендуется записать идею алгоритма, составить план преобразования открытого текста в шифртекст и обратно, сравнить используемые алгоритмы и теоремы в конспекте и в учебнике. При изучении теоретического материала всегда нужно рисовать схемы или графики.
4. Рекомендации по работе с литературой.
5. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по криптографии и криптоанализу. Литературу по курсу рекомендуется изучать в библиотеке. Полезно использовать несколько учебников по изучаемому курсу. Однако легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, какие математические принципы используются в этом параграфе и каков их смысл «своими словами»?. Сами криптографические алгоритмы следует не заучивать, а «понять». С этой целью рекомендуется записать идею алгоритма, составить план преобразования открытого текста в шифртекст и обратно, сравнить используемые алгоритмы и теоремы в конспекте и в учебнике. При изучении теоретического материала всегда нужно рисовать схемы или графики.