Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор по
образовательной деятельности
_____ А.А.Панфилов
«_21_» _02_____ 20_17_г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА СОХРАННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И РЕСУРСОВ ОРГАНИЗАЦИИ
(наименование дисциплины)

Специальность подготовка	38.05.01 "Экономическая безопасность "
Специализация подготовка	«Экономико-правовое обеспечение экономической безопасности»
Уровень высшего образования	Специалитет
Форма обучения	Очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	4 ЗЕТ/144 час.	18	18	18	45	Экзамен (45)
Итого	4 ЗЕТ/144 час.	18	18	18	45	Экзамен (45)

Владимир 20_14_

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА СОХРАННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И РЕСУРСОВ ОРГАНИЗАЦИИ»

Целью дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов» является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз информационным системам и ресурсам организации, знанием моделей нарушителя безопасности, постановкой конкретных задач обеспечения информационной безопасности автоматизированных систем, знанием средств и методов обеспечения сохранности информационных систем и ресурсов (ИСиР).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Программно-аппаратные средства сохранности информационных систем и ресурсов» относится к базовой части.

Изучение её базируется на следующих дисциплинах: «Информационные системы в экономике», «Современные модели управления информационными технологиями».

Дисциплина «Программно-аппаратные средства сохранности информационных систем и ресурсов» обеспечивает изучение следующих дисциплин:

Задачи дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов» - обеспечить:

- изучение моделей угроз и модели нарушителя информационной безопасности ИСиР;
- ознакомление с правовыми основами информационной безопасности при решении задач обеспечения сохранности ИСиР.
- изучение методов и решений по обеспечению сохранности ИСиР;
- получение практических навыков использования средств защиты информации ИСиР;
- изучение методов анализа угроз и уязвимостей, проектируемых и эксплуатируемых ИСиР;
- получение навыков использования программно-аппаратных средств обеспечения безопасности ИСиР.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе освоения дисциплины формируются следующие компетенции:

- способностью работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12);

В результате освоения дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов» обучающийся должен демонстрировать следующие результаты образования:

1) знать:

- программно-аппаратные средства обеспечения информационной безопасности в операционных системах, системах управления базами данных, компьютерных сетях (ОК-12);

2) уметь:

- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня сохранности ИС и Р (ОК-12);

- выбирать и применять средства защиты ИСиР от вредоносного программного обеспечения (ОК-12);
- средства защиты ИСиР от несанкционированного доступа (ОК-12);
- выбирать и применять аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации (ОК-12).

3) владеть:

- навыками эксплуатации и администрирования в части, касающейся разграничения доступа, аутентификации и аудита баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности (ОК-12);
- навыками использования программно-аппаратных средств обеспечения безопасности и сохранности ИС и Р (ОК-12).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144часа.

№ пп	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах/%)	Формы текущего контроля успеваемости форма промежуточной аттестации (по сем.)
				Лекции	Практ. занятия	Лабор. занятия	Контрол. работы	СРС	КП/КР		
1	2	3	4	5	7	8	9	10	11	12	13
	Тема 1. Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации	5	1-2	2	2	2		5		3/50	
	Тема 2. Программные средства обеспечения сохранности ИСиР средствами операционных система и систем управления базами данных		3 - 4	2	2	2		5		3/50	
	Тема 3. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа		5 - 6	2	2	2		5		3/50	Рейтинг-контроль № 1
	Тема 4. Средства защиты ИСиР от вредоносного программного обеспечения		7 - 8	2	2	2		5		3/50	
	Тема 5. Аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации		9 - 10	2	2	2		6		3/50	
	Тема 6. Комплексные системы обеспечения сохранности ИСиР		11 - 12	2	2	2		6		3/50	Рейтинг-контроль № 2
	Тема 7. Организационно-правовое обеспечение сохранности ИСиР в Российской Федерации		13 - 14	2	2	2		6		3/50	

	Тема 8. Современные тенденции развития технологий и средств обеспечения сохранности ИСиР организации		15 - 18	4	4	4		7		6/50	Рейтинг-контроль № 3
	Итого			**18**	**18**	**18**		**45**		**27/50%**	**Экзамен (45)**

СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

Перечень тем лекционных занятий

Тема 1. Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации

Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий.

Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации. Понятие безопасности информации и комплекс угроз в отношении оборудования пользователя и вычислительной сети.

Несанкционированный доступ (НСД). Политика безопасности организации и определение субъекта, потенциально совершающего несанкционированные действия. Статьи уголовного кодекса, предусматривающие ответственность за компьютерные преступления. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

Классы защищенности автоматизированных систем. Сертификация средств защиты информации; Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно- аппаратные средства защиты информации в сетях передачи данных.

Стандарты и рекомендации в области информационной безопасности. Сущность и общее содержание комплексной системы обеспечения безопасности ЭВМ и сетей на их основе с применением программно- аппаратных средств защиты информации в информационных технологиях коммерческой организации. Задачи и методологические основы использования программно- аппаратных средств защиты информации в компьютерах. Технические требования стандартов к программно-аппаратным средствам защиты информации. Международный стандарт критериев оценки безопасности информационных технологий и ГОСТ Р ИСО/МЭК 15408-2002. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Концепция диспетчера доступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем

Тема 2. Программные средства обеспечения сохранности ИСиР средствами операционных система и систем управления базами данных

Основные компоненты подсистемы защиты операционных систем. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Политика безопасности. Понятие домена. Особенности установления доверительных отношений. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защита информации на машинных носителях. Защита остатков информации. Понятие межсетевых экранов. Их классификация. Основные примеры конфигурации защищенных сетей с использованием межсетевых экранов. Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов. Проблемы обеспечения

безопасности при удалённом доступе. Протоколы аутентификации и идентификации пользователей в компьютерных сетях. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Классификация моделей безопасности. Особенности применения моделей безопасности в СУБД. Дискреционные (избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS). Основные виды и причины возникновения угроз целостности СУБД, способы противодействия. Организация взаимодействия СУБД и базовой ОС. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации в СУБД. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

Тема 3. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа (НСД)

Применение современных средств защиты от НСД. Установка и регистрация в системе защиты. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Регистрация событий. Гарантированное удаление данных. Л Обеспечение защищенного подключения автономного (не входящего в состав ЛВС) компьютера к ресурсам корпоративной сети. Программно-аппаратный комплекс шифрования трафика IP. Межсетевые защитные экраны. Руководящий документ, устанавливающий классификацию межсетевых экранов.

Тема 4. Средства защиты ИСиР от вредоносного программного обеспечения

Проблема обеспечения технологической безопасности программного обеспечения. Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Классификация программ по степени опасности для Л защищаемой информации и компьютерной системы. Алгоритмические и программные закладки, мотивы злоумышленных действий. Распространение компьютерных вирусов. Спам (несанкционированные электронные письма). Классификация компьютерных вирусов. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры. Качество антивирусной программы. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности.

Тема 5. Аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации

Шифрование файлов и областей оперативной памяти, формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами. Основные функции криптобиблиотек. Пластиковые карты – характерный пример аппаратных средств. Многоуровневые схемы управления доступом. Два типа аутентификации: статическая и динамическая. Идентификационные карты. Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки. Среда использования смарт-карт в персональных компьютерах. Аппаратный ключ или токен.

Процедуры биометрического опознания. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.

Тема 6. Комплексные системы обеспечения сохранности ИСиР

Системный подход при комплексной системе обесепечения сохранности ИсиР. Оюъект защиты. Системность и комплексность рот защите ИСиР Учет совокупной эффективности системы защиты. Макроструктурные компоненты системы защиты ИСиР. Функциональные системы. Обеспечивающие системы. Технологическая составляющая системы защиты ИСиР. Управление защитой ИСиР. Информационное обеспечение защиты ИСиР.

Перечень тем практических работ

Тема 1. Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации
Тема 2. Программные средства обеспечения сохранности ИСиР средствами операционных систем.
Тема 3. Программные средства обеспечения сохранности ИСиР средствами систем управления базами данных
Тема 4. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа (НСД)
Тема 5. Средства защиты ИСиР от вредоносного программного обеспечения
Тема 6. Аппаратные средства защиты ИСиР
Тема 8. Средства криптографической защиты ИСиР
Тема 9. Изучение концепции информационной безопасности информационных систем персональных данных на примере департамента социальной защиты населения администрации Владимирской области

Перечень тем лабораторных работ

Лабораторная работа №1. Защита документов MS Word
Лабораторная работа №2. Защита книг MS Excel
Лабораторная работа №3. Изучение дискреционных (избирательных) и мандатных (полномочных) моделей безопасности на примере действующих информационных систем
Лабораторная работа №4. Настройка уровней доступа пользователей к файловым ресурсам средствами операционных систем
Лабораторная работа №5. Настройка прав пользователей информационной системы при работе с базами данных
Лабораторная работа №6. Использование и основы создания защищенных каналов передачи данных для информационных систем
Лабораторные работа №7. Шифрование файлов и областей оперативной памяти, формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами.
Лабораторные работа №8. Ознакомление с основными программными средствами обеспечения сохранности информационных систем и ресурсов, применяемыми в государственных учреждениях РФ
Лабораторные работа №9. Основы обеспечения сохранности информационных систем и ресурсов с применением облачных технологий

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения дисциплины предполагается использование инновационных информационных технологий преподавания:

Занятия проводятся в аудиториях, оборудованных электронными проекторами, что позволяет сочетать активные и интерактивные формы проведения занятий, сопровождать их демонстрацией слайдов или готовых копий рисунков, как раздаточного материала.

Это позволяет довести удельный вес занятий в интерактивной форме до величин от 40 до 80 процентов (в зависимости от разделов дисциплины).

Студенты создают резервные копии всех файлов и используют их при подготовке к занятиям в порядке самостоятельной работы на своем компьютере.

Студенты используют общее информационное пространство на дисках локальной сети кафедры, облачном диске группы и в социальной сети для взаимодействия в группе и с преподавателем.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Контроль освоения дисциплины производится в соответствии с положением о рейтинговой системе комплексной оценки знаний студентов ФГБОУ ВО ВлГУ.

Рейтинг-контроль студентов предполагает использование преподавателем заданий, включающих теоретические вопросы, который проводится 3 раза в семестр. Оцениваются также следующие элементы:

- посещение лекций;
- работа на практических занятиях;
- работа на лабораторных занятиях;
- контрольные работы.

Промежуточная аттестация по результатам семестра по дисциплине проходит в форме экзамена, который включает в себя ответы на теоретические вопросы.

Примеры заданий для проведения рейтинг-контроля
Рейтинг-контроль №1

1. Понятия сохранности ИС и Р.
2. Объективная необходимость обеспечения сохранности ИС и Р.
3. Объекты администрирования.
4. Структура ИС.
5. Доменная организация ИС.
6. Модели доменов.
7. Серверные службы.
8. Учетные записи пользователей.
9. Служба управления конфигурациями и изменениями.
10. Идентификация конфигураций.
11. Контроль за конфигурациями.
12. Аудиты/обзоры конфигураций.
13. Служба управления безопасностью.
14. Аспекты информационной безопасности.
15. Угрозы ИС и Р.
16. Классы рисков.

Рейтинг-контроль №2

1. Программные средства обеспечения информационной безопасности.
2. Аппаратные средства обеспечения информационной безопасности.
3. Методы защиты компьютерных сетей организации.
4. Модели администрирования сети.
5. Аудит ИС.
6. Аппаратно-программные платформы администрирования.
7. Программы защиты данных и ресурсов в информационных системах госучреждений РФ.
8. Эксплуатация и сопровождение средств защиты ИС.
9. Управление и обслуживание технических средств защиты ИС.

10. Средства операционных систем, обеспечивающие сохранность информационных ресурсов.
11. Журналирование как метод защиты ИС.
12. Резервное копирование как метод защиты ИС.
13. Шифрование файлов и областей оперативной памяти
14. Формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами.
15. Основные функции криптобиблиотек.
16. Пластиковые карты – характерный пример аппаратных средств.
17. Многоуровневые схемы управления доступом.
18. Два типа аутентификации: статическая и динамическая.

Рейтинг-контроль №3

1. Идентификационные карты. Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки.
2. Среда использования смарт-карт в персональных компьютерах.
3. Аппаратный ключ или токен.
4. Процедуры биометрического опознания.
5. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.
6. Системный подход при комплексной системе обеспечения сохранности ИсиР. Объект защиты. Системность и комплексность рот защите ИСиР
7. Учет совокупной эффективности системы защиты.
8. Макроструктурные компоненты системы защиты ИСиР.
9. Функциональные системы.
10. Обеспечивающие системы.
11. Технологическая составляющая системы защиты ИСиР.
12. Управление защитой ИСиР.
13. Информационное обеспечение защиты ИСиР.

Вопросы для подготовки к экзамену

1. Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации
2. Общие положения теории информационной безопасности.
3. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий.
4. Место программно-аппаратных средств защиты информации в общей проблеме информационной безопасности.
5. Информационные риски и статистика угроз для информации.
6. Понятие безопасности информации и комплекс угроз в отношении оборудования пользователя и вычислительной сети.
7. Несанкционированный доступ (НСД). Политика безопасности организации и определение субъекта, потенциально совершающего несанкционированные действия.
8. Статьи уголовного кодекса, предусматривающие ответственность за компьютерные преступления.
9. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
10. Классы защищенности автоматизированных систем. Сертификация средств защиты информации.
11. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
12. Программно- аппаратные средства защиты информации в сетях передачи данных.
13. Стандарты и рекомендации в области информационной безопасности.

14. Сущность комплексной системы обеспечения безопасности ЭВМ и сетей на их основе с применением программно- аппаратных средств защиты информации в информационных технологиях коммерческой организации.
15. Задачи и методологические основы использования программно- аппаратных средств защиты информации в компьютерах.
16. Технические требования стандартов к программно-аппаратным средствам защиты информации.
17. Международный стандарт критериев оценки безопасности информационных технологий и ГОСТ Р ИСО/МЭК 15408-2002.
18. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите.
19. Программные средства обеспечения сохранности ИСиР средствами операционных система и систем управления базами данных
20. Основные компоненты подсистемы защиты операционных систем. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Политика безопасности. Понятие домена. Особенности установления доверительных отношений.
21. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности.
22. Защита информации на машинных носителях. Защита остатков информации. Понятие и классификация межсетевых экранов. Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов.
23. Проблемы обеспечения безопасности при удалённом доступе. Протоколы аутентификации и идентификации пользователей в компьютерных сетях.
24. Угрозы безопасности БД: общие и специфичные.
25. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит.
26. Задачи и средства администратора безопасности баз данных. Классификация моделей безопасности. Особенности применения моделей безопасности в СУБД.
27. Дискреционные (избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS).
28. Основные виды и причины возникновения угроз целостности СУБД, способы противодействия. Организация взаимодействия СУБД и базовой ОС.
29. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя.
30. Управление набором регистрируемых событий. Анализ регистрационной информации.
31. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа (НСД)
32. Применение современных средств защиты от НСД. Установка и регистрация в системе защиты.
33. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа.
34. Контроль целостности. Регистрация событий. Гарантированное удаление данных.
35. Обеспечение защищенного подключения автономного (не входящего в состав ЛВС) компьютера к ресурсам корпоративной сети.
36. Программно-аппаратный комплекс шифрования трафика IP.
37. Межсетевые защитные экраны. Руководящий документ, устанавливающий классификацию межсетевых экранов.
38. Средства защиты ИСиР от вредоносного программного обеспечения
39. Проблема обеспечения технологической безопасности программного обеспечения. Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам.

40. Классификация компьютерных вирусов. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ.
41. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры. Качество антивирусной программы.
42. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности.
43. Аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации
44. Шифрование файлов и областей оперативной памяти, формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами.
45. Основные функции криптобиблиотек.
46. Пластиковые карты как пример аппаратных средств.
47. Среда использования смарт-карт в персональных компьютерах. Аппаратный ключ или токен.
48. Процедуры биометрического опознания.
49. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.
50. Комплексные системы обеспечения сохранности ИСиР
51. Системный подход при комплексной системе обесепечения сохранности ИсиР. Объект защиты. Учет совокупной эффективности системы защиты.
52. Макроструктурные компоненты системы защиты ИСиР.
53. Функциональные системы.
54. Обеспечивающие системы.
55. Технологическая составляющая системы защиты ИСиР.
56. Управление защитой ИСиР.
57. Информационное обеспечение защиты ИСиР.

Пример практического задания

Тема: Практическое использование программных средств обеспечения сохранности информационных ресурсов средствами операционных систем.

Задание: Настроить уровни доступа к информационным ресурсам организации, хранящимся на дисках компьютера, таким образом, чтобы участники каждой рабочей группы (отдела) имели неограниченный доступ к собственным ресурсам, а к ресурсам всех остальных рабочих групп (отделов) имели уровень доступа «только чтение».

Для одной из групп пользователей скрыть информационные ресурсы остальных групп.

Указание: Использовать материалы теоретических занятий по настройке средств операционной системы для регламентации уровня доступа пользователей к информационным ресурсам на диске компьютера при локальном доступе и доступе по компьютерной сети.

Примечание: Тип операционной системы и расположение ресурсов задается преподавателем.

Задания для самостоятельной работы студентов

Задания для самостоятельной работы предназначены для дополнительного изучения вопросов и систем, рассматриваемых на аудиторных занятиях, а также включают в себя некоторые темы, полностью изучаемые студентами самостоятельно по заданию преподавателя.

1. Ознакомиться с законодательством РФ в области правового обеспечения ИС:
- ознакомление с определением ИС, данном в федеральном законе ФЗ - 149 «Об информации информационных технологиях и о защите информации». Составить краткое резюме статей закона №№ 1, 2, 13, 14, 16, 17.

- ознакомление с содержанием Федерального закон N 152-ФЗ "О персональных данных".

Составить краткое резюме статей закона, касающихся ИС.

2. Изучить проблему, каким образом решается вопрос об электронной подписи документов для систем электронного документооборота. Составить краткое сообщение по теме «Электронная подпись в информационной системе»

3. О каких основных аспектах следует говорить при построении систем корпоративной информационной безопасности?

4. Для чего необходимо формировать политику информационной безопасности, и из каких основных разделов она состоит?

5. В каком случае ИС считается защищенной?

6. Каким образом архитектура ИС может способствовать общей информационной безопасности и почему?

7. Из каких элементов состоит трехуровневая модель оценки защищенности ИС?

Тематика контрольных работ

Контрольная работа №1. Выполнить классификацию моделей нарушителя безопасности и выбрать модель, адекватную для заданного вида организации (по заданию преподавателя).

Контрольная работа №2. Выполнить классификацию моделей угроз безопасности и выбрать модель, адекватную для заданного вида организации (по заданию преподавателя).

Контрольная работа №3. Определить угрозы на уровне программных приложений организации, выбрать методы и средства устранения данного класса угроз.

Контрольная работа №4. Определить угрозы на уровне файлов и папок в компьютерной сети организации, выбрать методы и средства устранения данного класса угроз.

Контрольная работа №5. Определить угрозы на уровне узлов компьютерной сети организации и выбрать методы и средства устранения данного класса угроз.

Контрольная работа №6. Защита от внутренних угроз - разработать внутреннюю политику безопасности и разграничение прав доступа к информации.

Указания: необходимо определить группы пользователей разрабатываемой системы и назначить им соответствующие права доступа к папкам и модулям системы, определить требования к паролям и частоте их смены, а также другие параметры использования ИС. Данные рекомендуется представить в форме таблиц.

Контрольная работа №7. Защита от внешних угроз (безопасность каналов, протоколы, аутентификация, шифрование, безопасная пересылка ключей и т.д.).

Состав проектируемых программных и аппаратных средств может быть оформлен в виде таблицы с содержанием граф:

- нормативно-правовые акты организации, стандарты (международные и отечественные);
- антивирусные и антишпионские средства;
- проактивная защита от внешних угроз и защита внешнего периметра;
- защита от сетевых угроз;
- защита от инсайдерских угроз и защита информационных ресурсов;
- физическая защита информации.

Контрольная работа №8. Обоснование выбора политики безопасности, а также тех или иных программных и аппаратных средств, где должно быть:

- обоснование организационно-правовым методам и программно-аппаратным средствам (средства должны быть конкретные, лицензионные, с требованиями соответствующих стандартов);
- обоснование различным аспектам защиты системы: защита базы, резервное копирование, защита от хищения данных, защита от порчи данных, защита от инсайдерских угроз, уровни или сферы защиты (обоснование разрабатываемого решения на предмет уязвимостей, в том числе ошибки кода, ошибочные действия пользователя «защита от дурака»).

Контрольная работа №9. Обзор современных устройств биометрической идентификации и аутентификации для ИС и выбор средств для конкретного вида организации (по заданию преподавателя).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - http://www.studentlibrary.ru/book/ISBN9785940747680.html
2. Введение в информационную безопасность [Электронный ресурс] : Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.; Под ред. В.С. Горбатова. - М. : Горячая линия - Телеком, 2011. - http://www.studentlibrary.ru/book/ISBN9785991201605.htm
3. Бизнес-безопасность [Электронный ресурс] / Кузнецов И.Н. - М. : Дашков и К, 2012. - http://www.studentlibrary.ru/book/ISBN9785394014383.html
4. Технические, организационные и кадровые аспекты управления информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - http://www.studentlibrary.ru/book/ISBN9785991202749.html

б) дополнительная литература

1. Основы управления информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Вып. 1. - М.: Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - http://www.studentlibrary.ru/book/ISBN9785991202718.html
2. Комплексные (интегрированные) системы обеспечения безопасности [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 7. - М. : Горячая линия - Телеком, 2013. - (Серия "Обеспечение безопасности объектов"). - http://www.studentlibrary.ru/book/ISBN9785991202381.html
3. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М. : Горячая линия - Телеком, 2012. - http://www.studentlibrary.ru/book/ISBN9785991202572.html

в) интернет-ресурсы

1. Сервер информационных технологий: www.citforum.ru
2. Учебный центр Softline: www.edu.softline.ru
3. Интернет – университет информационных технологий www.intuit.ru

г) периодические издания

1. Информационные технологии - Ежемесячный теоретический и прикладной научно-технический журнал. Издательство «Новые технологии», Москва (имеется в электронной библиотеке ВлГУ).

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

При изучении дисциплины необходим электронный мультимедийный проектор и компьютер преподавателя, для выполнения лабораторных работ необходимы персональные компьютеры студентов.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по специальности 38.05.01 «Экономическая безопасность» и специализации «Экономико-правовое обеспечение экономической безопасности»

Рабочую программу составил к.т.н., доцент Карповский В.А. _____
(ФИО, подпись)

Рецензент
(представитель работодателя) Генеральный директор ООО «АЙТИМ» Ланцов Е.А.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ВТиСУ
Протокол № 6/1 от 13.02.17 года
Заведующий кафедрой В.Н. Ланцов _____
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии специальности 38.05.01 «Экономическая безопасность»
Протокол № 1 от 21.02.17 года
Председатель комиссии д.э.н., профессор О.А. Доничев _____
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____