

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 \_\_\_\_\_ 2017 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)

## **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, 144 часа.

№ пп	Раздел (тема) дисциплины	Семестр	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.)
			Неделя семестра	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 организации ИСиР	15 - 18	4	4	4	7	6/50	Рейтинг-контроль № 3
<b>Итого</b>		<b>18</b>	<b>18</b>	<b>18</b>	<b>45</b>	<b>27/50%</b>	<b>Экзамен (45)</b>

## 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 опознавания. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.

#### **Тема 6. Комплексные системы обеспечения сохранности ИСиР**

Системный подход при комплексной системе обеспечения сохранности ИСиР. Объект защиты. Системность и комплексность при 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
- Лабораторная работа №7. Шифрование файлов и областей оперативной памяти, формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами.
- Лабораторная работа №8. Ознакомление с основными программными средствами обеспечения сохранности информационных систем и ресурсов, применяемыми в государственных учреждениях РФ
- Лабораторная 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 опознавания.
49. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.
50. Комплексные системы обеспечения сохранности ИСиР
51. Системный подход при комплексной системе обеспечения 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, данным 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](http://www.citforum.ru)
2. Учебный центр Softline: [www.edu.softline.ru](http://www.edu.softline.ru)
3. Интернет – университет информационных технологий [www.intuit.ru](http://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. В.А. Карповский  
(ФИО, подпись)

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

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

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Владимирский государственный университет  
имени Александра Григорьевича и Николая Григорьевича Столетовых»

Институт Информационных технологий и радиоэлектроники  
Кафедра «Вычислительная техника и системы управления»

УТВЕРЖДАЮ  
Заведующий кафедрой

  
подпись

В.Н. Ланцов  
инициалы, фамилия

« 13 » 02 20 17

Основание:  
решение кафедры  
от « 13 » 02 20 17

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ  
ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ  
ПРИ ИЗУЧЕНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА СОХРАННОСТИ  
ИНФОРМАЦИОННЫХ СИСТЕМ И РЕСУРСОВ ОРГАНИЗАЦИИ**

наименование дисциплины

38.05.01 «Экономическая безопасность»

код и наименование направления подготовки

«Экономико-правовое обеспечение экономической безопасности»

наименование специализации

специалитет

Уровень высшего образования

Владимир, 2017

## ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (ФОС) для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» разработан в соответствии с рабочей программой, входящей в ОПОП специальности 38.05.01 «Экономическая безопасность» специализации «Экономико-правовое обеспечение экономической безопасности».

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Тема 1. Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации	ОК-12	Тест, доклады, контрольная работа
2	Тема 2. Программные средства обеспечения сохранности ИСиР средствами операционных система и систем управления базами данных	ОК-12	Тест, доклады, контрольная работа
3	Тема 3. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа	ОК-12	Тест, доклады, контрольная работа
4	Тема 4. Средства защиты ИСиР от вредоносного программного обеспечения	ОК-12	Тест, кейс, доклады, контрольная работа
5	Тема 5. Аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации	ОК-12	Тест, кейс, доклады, контрольная работа
6	Тема 6. Комплексные системы обеспечения сохранности ИСиР	ОК-12	Тест, кейс, доклады, контрольная работа
7	Тема 7. Организационно-правовое обеспечение сохранности ИСиР в Российской Федерации	ОК-12	Тест, доклады, контрольная работа
8	Тема 8. Современные тенденции развития технологий и средств обеспечения сохранности ИСиР организации	ОК-12	Тест, доклады, контрольная работа

Комплект оценочных средств по дисциплине «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» предназначен для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы, в том числе рабочей программы дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов организации», для оценивания результатов обучения: знаний, умений, владений и уровня приобретенных компетенций.

Комплект оценочных средств по дисциплине «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» включает:

1. Оценочные средства для проведения текущего контроля успеваемости:
  - комплект тестовых вопросов для выбора ответа студентами, который позволяет оценивать и диагностировать знание фактического материала, умение правильно использовать специальные термины и понятия, распознавать объекты изучения

в рамках определенного раздела дисциплины, а также провести процедуру измерения уровня знаний и умений обучающихся.

2. Оценочные средства для проведения промежуточной аттестации в форме  
 – контрольных вопросов для проведения экзамена.

**Перечень компетенций, формируемых в процессе изучения дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» при освоении образовательной программы по специальности 38.05.01 «Экономическая безопасность»**

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

<b>Знать</b>	<b>Уметь</b>	<b>Владеть</b>
<ul style="list-style-type: none"> <li>программно-аппаратные средства обеспечения информационной безопасности в операционных системах, системах управления базами данных, компьютерных сетях</li> </ul>	<ul style="list-style-type: none"> <li>проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня сохранности ИС и Р</li> <li>выбирать и применять средства защиты ИСиР от вредоносного программного обеспечения</li> <li>средства защиты ИСиР от несанкционированного доступа</li> <li>выбирать и применять аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>навыками использования программно-аппаратных средств обеспечения безопасности и сохранности ИС и Р</li> </ul>

**Показатели, критерии и шкала оценивания компетенций текущего контроля знаний по учебной дисциплине «Программно-аппаратные средства сохранности информационных систем и ресурсов организации»**

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» предполагает выполнение тестовых заданий студентами.

**Критерии оценки ответов студентов**



Для рейтинг-контроля №1

Критерии оценки ответа на задание	Распределение баллов за ответ
Нет ответа (ошибочный ответ) /Верный ответ	0 / 0,625 баллов (за каждое задание)

Для рейтинг-контроля №2

Критерии оценки ответа на задание	Распределение баллов за ответ
Нет ответа (ошибочный ответ) /Верный ответ	0 / 0,56 баллов (за каждое задание)

Для рейтинг-контроля №3

Критерии оценки ответа на задание	Распределение баллов за ответ
Нет ответа (ошибочный ответ) /Верный ответ	0 / 1,15 баллов (за каждое задание)

Регламент проведения мероприятия и оценивания

№	Вид работы	Продолжительность
1.	Предел длительности	20-25 мин.
2.	Внесение исправлений	до 5 мин.
	Итого	до 30 мин.

**ОЦЕНОЧНЫЕ СРЕДСТВА  
ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ  
«Программно-аппаратные средства сохранности информационных систем и  
ресурсов организации»**

**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.

### Оценочные средства для проведения контроля выполнения по осваиваемой дисциплине самостоятельной работы студента

#### Содержание (структура) заданий самостоятельной работы студентов

*Примерная тематика докладов*

№	Тема (раздел) самостоятельной работы студентов	Контролируемые компетенции
1	Ознакомиться с законодательством РФ в области правового обеспечения ИС: - ознакомление с определением ИС, данным в федеральном	ОК-12

	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»	ОК-12
3	О каких основных аспектах следует говорить при построении систем корпоративной информационной безопасности?	ОК-12
4	Для чего необходимо формировать политику информационной безопасности, и из каких основных разделов она состоит?	ОК-12
5	В каком случае ИС считается защищенной?	ОК-12
6	Каким образом архитектура ИС может способствовать общей информационной безопасности и почему?	ОК-12
7	Из каких элементов состоит трехуровневая модель оценки защищенности ИС?	ОК-12
8	Изучить комплекс мер по защите ресурсов персонального компьютера, реализуемый средствами операционной системы Windows.	ОК-12
9	Изучить комплекс мер по защите ресурсов персонального компьютера, реализуемый средствами операционной системы Linux.	ОК-12
10	Каковы основные современные тенденции развития технологий и средств обеспечения сохранности ИСиР организации.	ОК-12
11	Составить обзор и привести классификацию устройств биометрической идентификации и аутентификации, применяемых для обеспечения сохранности ресурсов организации.	ОК-12

*Примерная тематика контрольных работ*

№	Тема (раздел) самостоятельной работы студентов	Контролируемые компетенции
1	Выполнить классификацию моделей нарушителя безопасности и выбрать модель, адекватную для заданного вида организации (по заданию преподавателя).	ОК-12
2	Выполнить классификацию моделей угроз безопасности и выбрать модель, адекватную для заданного вида организации (по заданию преподавателя).	ОК-12
3	Определить угрозы на уровне программных приложений организации, выбрать методы и средства устранения данного класса угроз.	ОК-12
4	Определить угрозы на уровне файлов и папок в компьютерной сети организации, выбрать методы и средства устранения данного класса угроз.	ОК-12
5	Определить угрозы на уровне узлов компьютерной сети, выбрать методы и средства устранения данного класса угроз.	ОК-12
6	Защита от внутренних угроз - разработать внутреннюю	ОК-12

№	Тема (раздел) самостоятельной работы студентов	Контролируемые компетенции
	<p>политику безопасности и разграничение прав доступа к информации.</p> <p>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.</p>	
7	<p>Защита от внешних угроз (безопасность каналов, протоколы, аутентификация, шифрование, безопасная пересылка ключей и т.д.).</p> <p>Состав проектируемых программных и аппаратных средств может быть оформлен в виде таблицы с содержанием граф:</p> <ol style="list-style-type: none"> <li>1. нормативно-правовые акты организации, стандарты (международные и отечественные);</li> <li>2. антивирусные и антишпионские средства;</li> <li>3. проактивная защита от внешних угроз и защита внешнего периметра;</li> <li>4. защита от сетевых угроз;</li> <li>5. защита от инсайдерских угроз и защита информационных ресурсов;</li> <li>6. физическая защита информации.</li> </ol>	ОК-12
8	<p>Обоснование выбора политики безопасности, а также тех или иных программных и аппаратных средств, где должно быть:</p> <ol style="list-style-type: none"> <li>1. обоснование организационно-правовым методам и программно-аппаратным средствам (средства должны быть конкретные, лицензионные, с требованиями соответствующих стандартов);</li> <li>2. 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»).</li> </ol>	ОК-12
9	Обзор современных устройств биометрической идентификации и аутентификации для ИС и выбор средств для конкретного вида организации (по заданию преподавателя).	ОК-12

**Оценочный лист (показатели) выполнения и защиты самостоятельной работы студента по осваиваемой дисциплине**

Наименование показателя		Оценка
<b>I. Качество выполнения контрольной работы студента</b>		
1.	Соответствие содержания работы заданию	2
2.	Грамотность изложения и качество оформления работы	2
3.	Самостоятельность выполнения работы, глубина проработки материала, использование рекомендованной справочной литературы	2
Общая оценка за выполнение		6

<b>II. Качество доклада</b>		
1.	Соответствие содержания доклада заявленной теме	2
2.	Выделение основной мысли работы	2
3.	Качество изложения материала	2
Общая оценка за доклад		6
<b>III. Ответы на дополнительные вопросы</b>		
Общая оценка за ответы на вопросы		3
<b>ИТОГОВАЯ ОЦЕНКА ЗА САМОСТОЯТЕЛЬНУЮ РАБОТУ СТУДЕНТА</b>		<b>15</b>

**Общее распределение баллов текущего контроля по видам учебных работ для студентов (в соответствии с Положением)**

Рейтинг-контроль 1	До 10 баллов
Рейтинг-контроль 2	До 10 баллов
Рейтинг контроль 3	До 10 баллов
Посещение занятий студентом	До 5 баллов
За выполнение практических занятий	
За выполнение лабораторных занятий	До 15 баллов
Выполнение семестрового плана самостоятельной работы	До 10 баллов

**Регламент проведения мероприятия и оценивания работы на лабораторных занятиях**

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» в учебном плане предусмотрены лабораторные задания, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

**Регламент проведения мероприятия**

№	Вид работы	Продолжительность
1.	Выполнение задания	60-65 мин.
2.	Внесение исправлений в представленное решение	до 10-20 мин.
3.	Комментарии преподавателя	до 10 мин.
	Итого	до 90 мин.

**Перечень лабораторных занятий:**

- 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

Варианты заданий приведены в методических указаниях к лабораторным занятиям.

### *Шкала формирования оценки выполнения плана*

Оценка в баллах	Критерии
5	Выполнены все пункты задания, студент сумел рассчитать время, необходимое для выполнения задания, четко понимает его цель. Работа выполнена с минимальной помощью или без нее; Свободно использует полученные ранее знания из лекционного курса; При подготовке и выполнении заданий использован достаточный объем необходимой литературы; Студент понимает связь формы и содержания. Хорошая графика, соблюдение стандартов.
4	Выполнены все пункты задания, студент сумел рассчитать время, необходимое для выполнения задания, четко понимает его цель. Работа выполнена с минимальной помощью; Использует полученные ранее знания из лекционного курса; При подготовке и выполнении заданий использовалась дополнительная литература; Мелкие ошибки при выполнении расчетов; Хорошая графика, соблюдение стандартов.
3	Выполнены не все пункты задания, студент не сумел рассчитать время, необходимое для выполнения задания, но понимает его цель. При выполнении работы требовалась помощь преподавателя. Прослеживается затруднение в привлечении полученных ранее знаний из соответствующих курсов для решения конкретных заданий; При подготовке и выполнении дополнительная литература использовалась в недостаточном объеме; Выполнение отчета с отступлениями от стандартов и небрежным оформлением.

Менее 3	<p>Демонстрирует полное безразличие к выполняемой работе. Требуется постоянное давление для реализации задания. Требуется дополнительная проверка, подтверждающая самостоятельность выполнения работы.</p> <p>Использованная информация и иные данные отрывисты и второстепенны. Полученные результаты не внушают доверия и требуют доскональной проверки.</p> <p>Не способен привлечь полученные ранее знания (даже после консультации) из соответствующих курсов для решения конкретных задач при выполнении заданий.</p> <p>Выполнение отчета не соответствует стандартам. Оформление в высшей степени небрежное.</p>
---------	--

### Регламент проведения мероприятия и оценивания работы на практических занятиях

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» в учебном плане предусмотрены практические задания, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

#### Регламент проведения мероприятия

№	Вид работы	Продолжительность
1.	Выполнение задания	60-65 мин.
2.	Внесение исправлений в представленное решение	до 10-20 мин.
3.	Комментарии преподавателя	до 10 мин.
	Итого	до 90 мин.

Оценка	Критерии оценивания
<b>5 баллов</b>	Решение выполнено полностью, в представленном решении обоснованно получен правильный ответ.
<b>4 балла</b>	Решение выполнено полностью, но нет достаточного обоснования или при верном решении допущена ошибка, не влияющая на правильную последовательность рассуждений, и, возможно, приведшая к неверному ответу.
<b>3 балла</b>	Решение выполнено частично.
<b>2 балла</b>	Решение неверно или отсутствует.

#### 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

**Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» на экзамене**

Промежуточная аттестация по итогам освоения дисциплины (экзамен) проводится в экзаменационную сессию. Экзамен проводится по билетам, содержащим 2 вопроса. Студент пишет ответы на вопросы экзаменационного билета на листах белой бумаги формата А4, на каждом из которых должны быть указаны: фамилия, имя, отчество студента; шифр студенческой группы; дата проведения экзамена; номер экзаменационного билета. Листы ответов должны быть подписаны и студентом и экзаменатором после получения студентом экзаменационного билета.

Максимальное количество баллов, которое студент может получить на экзамене, в соответствии с Положением составляет 40 баллов.

Оценка в баллах	Оценка за ответ на экзамене	Критерии оценивания компетенций
30-40 баллов	«Отлично»	Студент глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач, подтверждает полное освоение компетенций, предусмотренных программой экзамена.
20-29 баллов	«Хорошо»	Студент показывает, что твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, допуская некоторые неточности; демонстрирует хороший уровень освоения материала, информационной и коммуникативной культуры и в целом подтверждает освоение компетенций, предусмотренных программой экзамена.
10-19 баллов	«Удовлетворительно»	Студент показывает знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, что в целом не препятствует усвоению последующего программного материала,



		допускает нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, подтверждает освоение компетенций, предусмотренных программой экзамена на минимально допустимом уровне.
Менее 10 баллов	«Неудовлетворительно»	Студент не знает значительной части программного материала (менее 50% правильно выполненных заданий от общего объема работы), допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, не подтверждает освоение компетенций, предусмотренных программой экзамена.

**ОЦЕНОЧНЫЕ СРЕДСТВА  
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ  
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «Программно-аппаратные средства сохранности  
информационных систем и ресурсов организации»**

**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 обеспечения 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.

Максимальная сумма баллов, набираемая студентом по дисциплине «Программно-аппаратные средства сохранности информационных систем и ресурсов организации» в течение семестра равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	Уровень сформированности компетенций
91 - 100	«Отлично»	Теоретическое содержание курса освоено полностью, без пробелов необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	<b>Высокий уровень</b>
74-90	«Хорошо»	Теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество	<b>Продвинутый уровень</b>

		выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	
61-73	«Удовлетвори-тельно»	Теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.	<i>Пороговый уровень</i>
Менее 60	«Неудовлетворительно»	Теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	<i>Компетенции не сформированы</i>

Разработчик



В.А.Карповский