

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Макаренко Елена Николаевна

Должность:

Документ подписан в:

Дата подписания: 20.06.2026 11:52:57

Уникальный программный ключ:

c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Ростовский государственный экономический университет (РИНХ)»

**УТВЕРЖДАЮ**

Начальник

учебно-методического управления

Т.К. Платонова

«25» мая 2026 г.

**Рабочая программа дисциплины  
Управление информационной безопасностью**

Направление подготовки

10.04.01 Информационная безопасность

Направленность (профиль) программы магистратуры

10.04.01.02 Программно-аппаратные методы расследования компьютерных преступлений

Для набора 2026 года

Квалификация  
магистр

**КАФЕДРА            Информационная безопасность**

**Распределение часов дисциплины по семестрам / курсам**

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
	14			
Неделя	14			
Вид занятий	уп	рп	уп	рп
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Практические	32	32	32	32
Итого ауд.	80	80	80	80
Контактная работа	80	80	80	80
Сам. работа	28	28	28	28
Часы на контроль	36	36	36	36
Итого	144	144	144	144

**ОСНОВАНИЕ**

Учебный план утвержден учёным советом Университета (протокол № 9 от 03.03.2026 г.).

Программу составил(и): к.т.н., доцент, Лапсарь А.П.

Зав. кафедрой: к.э.н., доцент Ю.В. Радченко

Методический совет направления: д.э.н., профессор Е.Н. Тищенко

Директор института магистратуры: д.э.н., профессор Е.А. Иванова

### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	получение обучающимися теоретических знаний по организации управления информационной безопасностью на объектах информатизации и в организациях, использующих в своей деятельности информационные системы; изучение и последующее освоение современных технологий защиты информации ограниченного доступа на объектах; оптимизация организационных и технических мероприятий по обеспечению информационной безопасности организации
-----	--

### 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели**

**ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;**

#### В результате освоения дисциплины обучающийся должен:

**Знать:**

методики формирования команд; методы эффективного руководства коллективами.(соотнесено с индикатором УК-3.1.)  
основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов (соотнесено с индикатором ОПК-3.1.)

**Уметь:**

разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом;разрабатывать мероприятия по личностному, образовательному и профессиональному росту(соотнесено с индикатором УК-3.2.)  
разрабатывать технические задания на создание подсистем обеспечения информационной безопасности.(соотнесено с индикатором ОПК-3.2.)

**Владеть:**

методами организации и управления коллективом, планированием его действий.(соотнесено с индикатором УК-3.3.)  
навыками разработки политик безопасности различных уровней.(соотнесено с индикатором ОПК-3.3.)

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### Раздел 1. Системы управления информационной безопасности

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Тема 1 "Основные положения теории информационной безопасности». Исследование архитектуры построения систем управления информационной безопасностью. Оформление при помощи LibreOffice	Лабораторные занятия	1	4	УК-3 ОПК-3
1.2	Тема 1 "Основные положения теории информационной безопасности». Исследование архитектуры построения систем управления информационной безопасностью.	Лекционные занятия	1	4	УК-3 ОПК-3
1.3	Тема 1 "Основные положения теории информационной безопасности». Управление информационной безопасностью объекта информатизации.	Практические занятия	1	6	УК-3 ОПК-3
1.4	Тема 1 "Основные положения теории информационной безопасности». Информационная безопасность: основные определения. Понятие конфиденциальности, целостности, доступности информации. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Белла Ла-Падулы. Формальные модели целостности: модель Кларка-Вилсона, модель Биба. Совместное использование моделей безопасности. Рольное управление доступом.	Самостоятельная работа	1	10	УК-3 ОПК-3
1.5	«Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Исследование свойств локальной политики безопасности.	Лекционные занятия	1	4	УК-3 ОПК-3
1.6	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Исследование свойств локальной политики безопасности. Оформление при помощи MS Office	Лабораторные занятия	1	4	УК-3 ОПК-3
1.7	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Управление средствами защиты информации на объекте.	Практические занятия	1	6	УК-3 ОПК-3
1.8	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».	Самостоятельная работа	1	4	УК-3 ОПК-3

	Классификация угроз информационной безопасности. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит. Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.				
<b>Раздел 2. Методы и технологии информационной безопасности</b>					
№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
2.1	"Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Исследование функционирования систем управления информационной безопасностью на объекте защиты.	Лекционные занятия	1	4	УК-3 ОПК-3
2.2	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Исследование функционирования систем управления информационной безопасностью на объекте защиты.	Лабораторные занятия	1	12	УК-3 ОПК-3
2.3	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Аудит состояния информационной безопасности на объектах информатизации.	Практические занятия	1	8	УК-3 ОПК-3
2.4	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Классификация возможных каналов утечки информации. Технологии защиты акустической информации от утечки. Технологии защиты информации от утечки по каналам ПЭМИН. Технологии защиты видовой информации от утечки.	Самостоятельная работа	1	4	УК-3 ОПК-3
2.5	«Управление безопасностью в компьютерной системе». Классификация методов защиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий	Лекционные занятия	1	4	УК-3 ОПК-3
2.6	Тема 2 «Управление безопасностью в компьютерной системе». Классификация методов защиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий.	Лабораторные занятия	1	12	УК-3 ОПК-3
2.7	Тема 2 «Управление безопасностью в компьютерной системе». Оценка эффективности проводимых мероприятий по совершенствованию системы управления информационной безопасностью.	Практические занятия	1	12	УК-3 ОПК-3
2.8	Тема 2 «Управление безопасностью в компьютерной системе». Термины и определения. Системы удаленного управления безопасностью: в отсутствие локального объекта управления, при локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной системы.	Самостоятельная работа	1	10	УК-3 ОПК-3
2.9	Подготовка к промежуточной аттестации	Экзамен	1	36	УК-3 ОПК-3

#### 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

#### 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

##### 5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2013	ЭБС «Университетская библиотека онлайн»
2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	ЭБС «Университетская библиотека онлайн»
3	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	ЭБС «IPR SMART»
4	Морозов, А. В., Филатова, Л. В., Полякова, Т. А.	Информационное право и информационная безопасность. Часть 2: учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	ЭБС «IPR SMART»
5	Морозов, А. В., Филатова, Л. В., Полякова, Т. А.	Информационное право и информационная безопасность. Часть 1: учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	ЭБС «IPR SMART»

### 5.2. Профессиональные базы данных и информационные справочные системы

ИСС "КонсультантПлюс"  
ИСС "Гарант" <http://www.internet.garant.ru/>  
ЭБС «IPR Books» <http://www.iprbookshop.ru/>  
Библиоклуб.ру <http://biblioclub.ru/>

### 5.3. Перечень программного обеспечения

Операционная система РЕД ОС  
LibreOffice

### 5.4. Учебно-методические материалы для обучающихся с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет, и/или в специализированных лабораториях, предусмотренных образовательной программой.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

## 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

**1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
<b>УК-1 –способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели</b>			
З. методики формирования команд; методы эффективного руководства коллективами.	поиск и сбор необходимой литературы, использование различных баз данных	полнота и содержательность ответа умение приводить примеры	Т (тесты Раздел 1 тема 1 вопрос 1-2; Раздел 2 тема 1 вопрос 1), Э (вопросы 1-4, 9-11, 25-26)
У. разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту	использование информационных технологий в практической деятельности для приобретения новых знаний и умений	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 1 практическое задание 1, часть 1); ЛЗ (Раздел 1 лабораторное задание 1, часть 1) ПОЗЭ (1-5)
В. методами организации и управления коллективом, планированием его действий.	использование современных информационно-коммуникационных технологий и различных информационных ресурсов	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 1 практическое задание 1, часть 2); ЛЗ (Раздел 1 лабораторное задание 1, часть 2) ПОЗЭ (1-5)
<b>ОПК-3- способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности</b>			

З. основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов	актуальность тем исследований и ее практическая новизна	полнота и содержательность ответа умение приводить примеры	Т (тесты Раздел 1 тема 1 вопрос 3; Раздел 2 тема 1 вопрос 2-3), Э (вопросы 5-8, 16-18, 27-30)
У. разрабатывать технические задания на создание подсистем обеспечения информационной безопасности.	поиск и сбор необходимой литературы, анализ фундаментальных и прикладных проблем информационной безопасности	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 2 практическое задание 1, часть 1) ЛЗ (Раздел 2 лабораторное задание 1, часть 1) ПОЗЭ (1-5)
В. навыками разработки политик безопасности различных уровней.	использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 2 практическое задание 1, часть 2); ЛЗ (Раздел 2 лабораторное задание 1, часть 2) ПОЗЭ (1-5)

*ЛЗ – лабораторные задания, ПЗ- практические задания; Т – тест, Э – вопросы к экзамену ПОЗЭ – практико-ориентированные задания к экзамену*

## 1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

84-100 баллов (оценка «отлично»)

67-83 баллов (оценка «хорошо»)

50-66 баллов (оценка «удовлетворительно»)

0-49 баллов (оценка «неудовлетворительно»)

## **2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

### **Вопросы к экзамену**

1. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
2. Специальные проверки и специальные исследования.
3. Информационная безопасность: основные определения.

4. Понятие конфиденциальности, целостности, доступности информации.
5. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Белла Ла-Падулы. Формальные модели целостности: модель Кларка-Вилсона, модель Биба.
6. Совместное использование моделей безопасности.
7. Ролевое управление доступом.
8. Выбор и оптимизация требуемых мер и средств защиты информации на объектах.
9. Аттестация объектов информатизации.
10. Контроль за обеспечением безопасной эксплуатации объектов информатизации.
11. Теоретические основы построения систем защиты от угроз».
12. Классификация угроз информационной безопасности.
13. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит.
14. Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы.
15. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
16. Информационное противоборство, информационная война.
17. Методы нарушения конфиденциальности, целостности и доступности информации в условиях информационного противоборства.
18. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
19. Правовые, организационно-технические и экономические методы обеспечения ИБ.
20. Модели, стратегии и системы обеспечения информационной безопасности в условиях информационного противоборства.
21. Классификация возможных каналов утечки информации.
22. Технологии защиты акустической информации от утечки.
23. Технологии защиты информации от утечки по каналам ПЭМИН.
24. Технологии защиты видовой информации от утечки.
25. Классификация методов защиты информации от программно-математических воздействий.
26. Категорирование объектов информатизации.
27. Деятельность администратора безопасности по предотвращению программно-математических воздействий.
28. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий.
29. Системы удаленного управления безопасностью: в отсутствие локального объекта управления, при локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления.
30. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной системы.

### **Практико-ориентированные задания к экзамену**

1. Установить угрозы, атаки и риски сетевой безопасности.
2. Установить антивирусное программное обеспечение.
3. Установить Linux-подобную операционную систему.
4. Настроить впервые установленную Linux-подобную операционную систему.
5. Установить шифровальную систему.

### **Критерии оценивания:**

- 84-100 баллов (оценка «отлично») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности; усвоена основная литература, рекомендованная в рабочей программе дисциплины;

- 50-66 баллов (оценка «удовлетворительно») - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; выполняются в целом корректные действия по применению знаний на практике;

- 0-49 баллов (оценка «неудовлетворительно») - ответы не связаны с вопросами, наличие грубых ошибок в ответе, демонстрирующие непонимание сущности излагаемого вопроса и неумение применять знания на практике; отсутствие уверенности и неточность ответов на дополнительные и наводящие вопросы.

## **Тесты**

### **Раздел 1 Системы управления информационной безопасности**

Тема 1 " Основные положения теории информационной безопасности "

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- а) сотрудники
- б) хакеры
- в) атакующие
- г) контрагенты (лица, работающие по договору)

2. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- а) владельцы данных
- б) пользователи
- в) администраторы
- г) руководство

3. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

- а) поддержка высшего руководства
- б) эффективные защитные меры и методы их внедрения
- в) актуальные и адекватные политики и процедуры безопасности
- г) проведение тренингов по безопасности для всех сотрудников

Тема 2 " Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

1. Что такое политики безопасности?

- а) инструкции по выполнению задач безопасности
- б) общие руководящие требования по достижению определенного уровня безопасности
- в) широкие, высокоуровневые заявления руководства
- г) детализированные документы по обработке инцидентов безопасности

2. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
- а) анализ рисков
  - б) анализ затрат / выгоды
  - в) результаты ALE
  - г) выявление уязвимостей и угроз, являющихся причиной риска
3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
- а) анализ рисков
  - б) анализ затрат / выгоды
  - в) результаты ALE
  - г) выявление уязвимостей и угроз, являющихся причиной риска

## **Раздел 2. Методы и технологии информационной безопасности**

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

1. Для решения каких задач предназначены статические оболочки экспертных систем?
- а) для управления и диагностики в режиме реального времени
  - б) для решения статических задач
  - с) для решения задач анализа и синтеза с разделением времени
  - д) для разработки динамических систем
  - е) нет правильного ответа
2. Эффективная программа безопасности требует сбалансированного применения:
- а) технических и нетехнических методов
  - б) контрмер и защитных механизмов
  - в) физической безопасности и технических средств защиты
  - г) процедур безопасности и шифрования
3. Что из перечисленного не является целью проведения анализа рисков?
- а) делегирование полномочий
  - б) количественная оценка воздействия потенциальных угроз
  - в) выявление рисков
  - г) определение баланса между воздействием риска и стоимостью необходимых контрмер

Тема 2. «Управление безопасностью в компьютерной системе».

1. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
- а) поддержка
  - б) выполнение анализа рисков
  - в) определение цели и границ
  - г) делегирование полномочий
2. Целостность и наглядность описания предметной области сохраняется в семантических сетях с увеличением размеров и усложнением связей
- а) да
  - б) нет
3. Задачи аппаратного моделирования деятельности человека могут относиться к задачам искусственного интеллекта
- а) да
  - б) нет

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его

взгляд, варианта ответа. Тестовое задание содержит 10 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается. Время прохождения тестирования 20 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

### **3. Критерии оценки:**

- 1-20 баллов выставляется обучаемому. За один правильный ответ обучаемый получает 2 балла.

## **Лабораторные задания**

### **1. Тематика лабораторных заданий по разделам и темам**

#### **Раздел 1 «Системы управления информационной безопасности»**

Тема 1 «Основные положения теории информационной безопасности»

Лабораторная работа 1 Исследование архитектуры построения систем управления информационной безопасностью. Оформление при помощи LibreOffice.

Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

Лабораторная работа 2. Теоретические основы построения систем защиты от угроз. Исследование свойств локальной политики безопасности. Оформление при помощи LibreOffice.

#### **Раздел 2. «Методы и технологии информационной безопасности».**

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

Лабораторная работа 1. Исследование функционирования систем управления информационной безопасностью на объекте защиты.

Тема 2. «Управление безопасностью в компьютерной системе».

Лабораторная работа 2. Классификация методов защиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий.

### **Критерии оценки:** всего- 40 баллов.

- (для каждого задания):

10 б. – задание выполнено верно;

9-7 б. – при выполнении задания были допущены неточности, не влияющие на результат;

6-3 б. – при выполнении задания были допущены ошибки;

2 - 1 б. – при выполнении задания были допущены существенные ошибки;

0 б. – задание не выполнено.

## **Практические задания**

### **1. Тематика практических заданий по разделам и темам**

#### **Раздел 1 «Системы управления информационной безопасности»**

Тема 1 «Основные положения теории информационной безопасности»

Практическое занятие 1 Управление информационной безопасностью объекта информатизации.

Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

Практическое занятие 2. Управление средствами защиты информации на объекте.

Раздел 2. «**Методы и технологии информационной безопасности**».

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

Практическое занятие 1. Аудит состояния информационной безопасности на объектах информатизации.

Тема 2. «Управление безопасностью в компьютерной системе».

Практическое занятие 2. Оценка эффективности проводимых мероприятий по совершенствованию системы управления информационной безопасностью.

## **2. Критерии оценки:** всего – 40 баллов.

10 б. – задание выполнено верно;

9-7 б. – при выполнении задания были допущены неточности, не влияющие на результат;

6-3 б. – при выполнении задания были допущены ошибки;

2 - 1 б. – при выполнении задания были допущены существенные ошибки;

0 б. – задание не выполнено.

## **3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

**Текущий контроль** успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Экзамен проводится по расписанию **промежуточной аттестации** в письменном виде. Количество вопросов в экзаменационном задании – 3. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

### МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия;
- лабораторные занятия.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем.

При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- подготовить ответы на все вопросы по изучаемой теме;
- письменно решить домашнее задание, рекомендованные преподавателем при изучении каждой темы.

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лабораторному занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.