Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Директор Института магистратуры
Иванова Е.А.
«01» июня 2023г.

Рабочая программа дисциплины
Защищенные информационные системы

Направление 10.04.01 Информационная безопасность
магистерская программа 10.04.01.02 "Программно-аппаратные методы расследования компьютерных преступлений"

Для набора 2023 года

Квалификация
магистр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	10	10	10	10
Лабораторные	20	20	20	20
Практические	20	20	20	20
Итого ауд.	50	50	50	50
Контактная работа	50	50	50	50
Сам. работа	121	121	121	121
Часы на контроль	9	9	9	9
Итого	180	180	180	180

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.03.2023 протокол № 9.

Программу составил(и): к.т.н., доцент, Серпенинов О.В.

Зав. кафедрой: к.э.н.Радченко Ю.В.

Методическим советом направления: д.э.н., профессор, Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Овладение основными методами научного исследования; ознакомление с методами и способами организации защиты информационных систем.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-1:Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2:Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

В результате освоения дисциплины обучающийся должен:

Знать:

Знать методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности; современную нормативную базу и ГОСТы, регламентирующие процесс разработки технического задания; правила, способы и методы организации совместных разработок.(соотнесено с индикатором ОПК- 1.1.)
Знать методы концептуального проектирования технологий обеспечения информационной безопасности.(соотнесено с индикатором ОПК-2.1.)

Уметь:

Уметь обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности.(соотнесено с индикатором ОПК-1.2.)
Уметь выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения (соотнесено с индикатором ОПК-2.2.)

Владеть:

Владеть навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений(соотнесено с индикатором ОПК-1.3.)
Владеть навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности(соотнесено с индикатором ОПК-2.3.)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Раздел 1. Принципы организации защищённых информационных систем

№	Наименование темы / Вид занятия	Семестр	Часов	Компетенции	Литература
1.1	Тема 1 "Основные принципы организации защищённых ИС". Концепция создания защищенных информационных систем. Защищённость как понятие. Защищенные технологии в целом. Защищенные информационные системы.Модель защищенных информационных систем. / Лек /	1	2	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.2	Тема 1 "Основные принципы организации защищённых ИС". Концепция создания защищенных информационных систем. Защищённость как понятие. Защищенные технологии в целом. Защищенные информационные системы. Модель защищенных информационных систем. / Лаб /	1	6	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.3	Тема 2 «Уязвимость защищённых ИС». Анализ причин уязвимости ЭИС. Методы и механизмы защиты от НСД. Модель системы безопасности РЭИС / Лек /	1	2	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.4	Тема 2 «Уязвимость защищённых ИС». Анализ причин уязвимости ЭИС. Методы и механизмы защиты от НСД. Модель системы безопасности РЭИС. РедОС / Лаб /	1	4	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.5	Тема 2 «Уязвимость защищённых ИС». Анализ причин уязвимости ЭИС. Методы и механизмы защиты от НСД. Модель системы безопасности РЭИС / Пр /	1	4	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.6	Тема 2 «Уязвимость защищённых ИС». Анализ причин уязвимости ЭИС. Методы и механизмы защиты от НСД. Модель системы безопасности РЭИС. РедОС / Ср /	1	20	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.7	Тема 3 «Требования к архитектуре ИС для обеспечения безопасности ее функционирования». Идеология открытых информационных систем. Анализ безопасности ИС при отсутствии злоумышленных факторов. Стандартизация подходов к обеспечению	1	2	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3

	информационной безопасности. / Лек /				
1.8	Тема 3 «Требования к архитектуре ИС для обеспечения безопасности ее функционирования». Идеология открытых информационных систем. Анализ безопасности ИС при отсутствии злоумышленных факторов. Стандартизация подходов к обеспечению информационной безопасности. / Лаб /	1	4	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.9	Тема 3 «Требования к архитектуре ИС для обеспечения безопасности ее функционирования». Идеология открытых информационных систем. Анализ безопасности ИС при отсутствии злоумышленных факторов. Стандартизация подходов к обеспечению информационной безопасности. / Пр /	1	4	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.10	Тема 3 «Требования к архитектуре ИС для обеспечения безопасности ее функционирования». Идеология открытых информационных систем. Анализ безопасности ИС при отсутствии злоумышленных факторов. Стандартизация подходов к обеспечению информационной безопасности. / Ср /	1	20	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3

Раздел 2. Раздел 2. Технологии обеспечения безопасности

№	Наименование темы / Вид занятия	Семестр	Часов	Компетенции	Литература
2.1	Тема 4 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Особенности сетевых систем. Общие угрозы сетевых систем. Требования для защиты конфиденциальной информации в органах исполнительной власти. Средства защиты информации для коммерческих структур. / Лек /	1	2	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.2	Тема 5 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Защита информации в информационных системах и компьютерных сетях. Особенности, которые делают сети уязвимыми. Причины, приводящие к крупным проблемам. Наиболее часто встречающиеся дефекты защиты. Причинами появления уязвимостей в сетях. / Ср /	1	20	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.3	Тема 5 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Защита информации в информационных системах и компьютерных сетях. Особенности, которые делают сети уязвимыми. Причины, приводящие к крупным проблемам. Наиболее часто встречающиеся дефекты защиты. Причинами появления уязвимостей в сетях. / Лаб /	1	2	ОПК-1	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.4	Тема 5 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Защита информации в информационных системах и компьютерных сетях. Особенности, которые делают сети уязвимыми. Причины, приводящие к крупным проблемам. Наиболее часто встречающиеся дефекты защиты. Причинами появления уязвимостей в сетях. / Пр /	1	4	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.5	Тема 5 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Защита информации в информационных системах и компьютерных сетях. Особенности, которые делают сети уязвимыми. Причины, приводящие к крупным проблемам. Наиболее часто встречающиеся дефекты защиты. Причинами появления уязвимостей в сетях. / Ср /	1	19	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.6	Тема 6 «Технологическая модель подсистемы информационной безопасности». Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны. Концепция защищенных виртуальных частных сетей. / Лек /	1	2	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.7	Тема 6 «Технологическая модель подсистемы информационной безопасности». Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны. Концепция защищенных виртуальных частных сетей. / Лаб /	1	4	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.8	Тема 6 «Технологическая модель подсистемы информационной безопасности». Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны. Концепция защищенных виртуальных частных сетей. / Пр /	1	8	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.9	Курсовая работа. Темы курсовых работ представлены в Приложении 1. / Ср /	1	42	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3

2.10	/ Экзамен /	1	9	ОПК-1,ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Трипкош В. А., Матвеев А. Г.	Электронная цифровая подпись в деятельности предприятий и организаций: учебное пособие	Оренбург: Оренбургский государственный университет, 2012	https://biblioclub.ru/index.php?page=book&id=270314 неограниченный доступ для зарегистрированных пользователей
Л1.2	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.3	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	https://biblioclub.ru/index.php?page=book&id=438331 неограниченный доступ для зарегистрированных пользователей
Л1.4	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	https://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1		Информационная безопасность: журнал	Москва: Гротек, 2014	https://biblioclub.ru/index.php?page=book&id=364894 неограниченный доступ для зарегистрированных пользователей
Л2.2	Нужнов Е. В.	Компьютерные сети: учебное пособие	Таганрог: Южный федеральный университет, 2015	https://biblioclub.ru/index.php?page=book&id=461991 неограниченный доступ для зарегистрированных пользователей
Л2.3	Пуговкин А. В.	Сети передачи данных: учебное пособие	Томск: Факультет дистанционного обучения ТУСУРа, 2015	https://biblioclub.ru/index.php?page=book&id=480793 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ИСС "КонсультантПлюс"

ИСС "Гарант" http://www.internet.garant.ru/

Федеральная служба по техническому и экспортному контролю https://fstec.ru/

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций https://rkn.gov.ru/

5.4. Перечень программного обеспечения

Libreoffice

5.5. Учебно-методические материалы для студентов 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 (МОДУЛЯ)

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.

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

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

Приложение 1

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
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание			
З: Знать методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности; современную нормативную базу и ГОСТы, регламентирующие процесс разработки технического задания; правила, способы и методы организации совместных разработок	ориентировка в понятиях основ абстрактного мышления, анализа, синтеза	полнота и содержательность ответа; умение приводить примеры	Экзаменационные вопросы 1-30 Тестовые вопросы 1-6 Курсовой проект КП(1-15)
У: Уметь обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности.	проявление умений абстрактно мыслить, анализировать и синтезировать информацию	полнота и содержательность ответа; умение приводить примеры; умение самостоятельно находить решение поставленных задач	ПОЗЭ (1-5) Лабораторное занятие 1-5 Практическое занятие 1-4 КП (1-15)
В: Владеть навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений.	демонстрация навыков абстрактного мышления, анализа, синтеза	полнота и содержательность ответа; умение приводить примеры; умение самостоятельно находить решение поставленных задач	ПОЗЭ (1-5) Лабораторное занятие 1-5 Практическое занятие 1-4 КП (1-15)
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности			
З: Знать методы концептуального проектирования технологий обеспечения информационной безопасности	ориентировка в понятиях основ разработки систем, комплексов, средств и технологий обеспечения информационной безопасности	полнота и содержательность ответа; умение приводить примеры	Экзаменационные вопросы 30-57 Тестовые вопросы 7-12 КП (1-10)

У: Уметь выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.	проявление умений разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	полнота и содержательность ответа; умение приводить примеры; умение самостоятельно находить решение поставленных задач	ПОЗЭ (1-5) Лабораторное занятие 1-5 Практическое занятие 1-4 КП (1-15)
В: Владеть навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности.	демонстрация навыков разработки систем, комплексов, средств и технологий обеспечения информационной безопасности	полнота и содержательность ответа; умение приводить примеры; умение самостоятельно находить решение поставленных задач	ПОЗЭ (1-5) Лабораторное занятие 1-5 Практическое занятие 1-4 КП (1-15)

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

Теоретические вопросы к экзамену

1. Экономические аспекты проблем защиты информации.
2. Объекты информационной защиты.
3. Основные принципы информационной безопасности.
4. Общие проблемы безопасности.
5. Национальная безопасность и уровни её обеспечения.
6. Виды информации, подлежащие защите.
7. Комплексный подход к обеспечению безопасности.
8. Потенциальные угрозы безопасности.
9. Случайные угрозы: причины. Уязвимость информации.
10. Каналы несанкционированного получения информации в информационных системах.
11. Преднамеренные угрозы: по цели эксплуатации, по принципу воздействия, по характеру воздействия.
12. Защита информации в современных информационных системах: межсетевые экраны, брандмауэры, прокси-серверы, системы активного аудита.
13. Методы криптографической защиты информации: функции и задачи защиты; модели и системы защиты информации.
14. Криптографическое преобразование информации методом подстановки и монофонической замены.
15. Криптографичекое преобразование информации методом перестановки.
16. Криптографическое преобразование информации методом гаммирования и аналитических

преобразований.
17. Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам.
18. Методы идентификации и установления подлинности субъектов и различных объектов.
19. Понятие сервисов безопасности. Стандарты безопасности.
20. Архитектура механизмов защиты информации в современных АИС.
21. Методы цифровой подписи.
22. Биометрические системы идентификации.
23. Административные и организационные мероприятия по обеспечению информационной безопасности.
24. Методологические подходы к оценке уязвимости информации.
25. Модель защиты системы с полным перекрытием.
26. Рекомендации по использованию моделей оценки уязвимости информации.
27. Допущения в моделях оценки уязвимости информации.
28. Анализ существующих методик определения требований к защите информации.
29. Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения.
30. Руководящем документе Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации", выпущенном в 1992 году. Часть 1.
31. Классы защищенности средств вычислительной техники от несанкционированного доступа.
32. Функции защиты информации.
33. Стратегии защиты информации.
34. Способы и средства защиты информации.
35. Архитектура систем защиты информации.
36. Требования защиты информации.
37. Общеметодологических принципов архитектуры системы защиты информации.
38. Средства защиты информации.
39. Антивирусы, средства анализа защищенности, средства обнаружения вторжений
40. Подходы к организации системы защиты.
41. Этапы построения систем защиты.
42. Методы противодействия различным угрозам информационной безопасности.
43. Возможности средств обнаружения вторжения.
44. Классификация средств обнаружения уязвимостей.
45. Методы выявления сетевых атак.
46. Способы противодействия сетевым атакам
47. Общие принципы построения информационных сетей.
48. Топология физических связей информационных сетей.
49. Семиуровневая модель организации сети. Общая характеристика модели OSI.
50. Классификация линий связи. Их основные характеристики.
51. Сетевые IP-адреса. Формат IP-адреса. Использование масок при IP-адресации.
52. Протоколы транспортного уровня TCP и UDP.
53. Общие свойства и классификация протоколов маршрутизации.
54. Беспроводные информационные сети стандарта 802.11. Мобильные телефонные сети. Спутниковая связь.
55. Сетевые службы: электронная почта, веб-служба, протокол HTTP.
56. Методы обеспечения качества обслуживания в информационных сетях.
57. Сетевая безопасность.

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 основных знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, 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.

Тестовые вопросы

1. Банк тестов по модулям и (или) темам

Принципы организации защищённых информационных систем.

Тема 1 "Основные принципы организации защищённых ИС". Концепция создания защищенных информационных систем. Защищённость как понятие. Защищенные технологии в целом. Защищенные информационные системы. Модель защищенных информационных систем.

1. С точки зрения ГТК основной задачей средств безопасности является обеспечение:
сохранности информации
защиты от НСД
простоты реализации
надежности функционирования

2. Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев:
D
A
B
C

3. При качественном подходе риск измеряется в терминах
денежных потерь:
заданных с помощью шкалы или ранжирования
оценок экспертов
объема информации

4. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:
область равной критичности
область равного доступа
уровень безопасности
уровень доступности

5. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне:
E5
E7

E4
E6

6. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это:
уязвимость информации
надежность информации
защищенность информации
безопасность информации

Тема 2 «Уязвимость защищённых ИС». Анализ причин уязвимости ЭИС. Методы и механизмы защиты от НСД. Модель системы безопасности РЭИС.

7. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это:
аудит
аутентификация
авторизация
идентификация

8. Согласно «Европейским критериям» минимальную адекватность обозначает уровень:
E1
E7
E0
E6

9. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь:
наиболее важные субъекты
наиболее важные объекты
все субъекты
все объекты

10. Программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа:
фильтр
заместитель
перехватчик
имитатор

11. Согласно «Европейским критериям» предъявляет повышенные требования и к целостности, и к конфиденциальности информации класс:
F-IN
F-AV
F-DX
F-DI

12. Соответствие средств безопасности решаемым задачам характеризует:
эффективность
корректность
адекватность
унификация

13. С помощью закрытого ключа информация:
копируется
транслируется
расшифровывается
зашифровывается

14. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется:

актуальностью информации
доступностью
качеством информации
целостностью

Тема 3 «Требования к архитектуре ИС для обеспечения безопасности ее функционирования». Идеология открытых информационных систем. Анализ безопасности ИС при отсутствии злоумышленных факторов. Стандартизация подходов к обеспечению информационной безопасности.

15. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев:

C
A
B
D

16. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности:

LWM
На основе анализа угроз
Лендвера
С полным перекрытием

17. Недостатком модели конечных состояний политики безопасности является:

изменение линий связи
статичность
сложность реализации
низкая степень надежности

18. По документам ГТК количество классов защищенности АС от НСД:

8
7
9
6

19. Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:

избирательным
мандатным
привилегированным
идентифицируемым

20. Организационные требования к системе защиты:

управленческие и идентификационные
административные и аппаратурные
административные и процедурные
аппаратурные и физические

21. На многопользовательские системы с информацией одного уровня конфиденциальности согласно «Оранжевой книге» рассчитан класс:

C1
B2
C2
B1

Технологии обеспечения безопасности.

Тема 4 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Особенности сетевых систем. Общие угрозы сетевых систем. Требования для защиты конфиденциальной

информации в органах исполнительной власти. Средства защиты информации для коммерческих структур.

22. Основу политики безопасности составляет:
программное обеспечение
управление риском
способ управления доступом
выбор каналов связи

23. При избирательной политике безопасности в матрице доступа субъекту системы соответствует:
ячейка
строка
прямоугольная область
столбец

24. Наименее затратный криптоанализ для криптоалгоритма DES:
перебор по выборочному ключевому пространству
разложение числа на сложные множители
перебор по всему ключевому пространству
разложение числа на простые множители

25. Недостаток систем шифрования с открытым ключом:
при использовании простой замены легко произвести подмену одного шифрованного текста другим
относительно низкая производительность
необходимость распространения секретных ключей
на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

26. По документам ГТК самый высокий класс защищенности СВТ от НСД к информации:
1
6
9
7

27. Наукой, изучающей математические методы защиты информации путем ее преобразования, является:
криптоанализ
криптология
стеганография
криптография

28. Обеспечение целостности информации в условиях случайного воздействия изучается:
стеганографией
теорией помехоустойчивого кодирования
криптологией
криптоанализом

Тема 5 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Защита информации в информационных системах и компьютерных сетях. Особенности, которые делают сети уязвимыми. Причины, приводящие к крупным проблемам. Наиболее часто встречающиеся дефекты защиты. Причинами появления уязвимостей в сетях.

29. Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа:
перехват
уборка мусора
наблюдение

компрометация

30. Конечное множество используемых для кодирования информации знаков называется:
шифром
кодом
алфавитом
ключом

31. Недостатком дискретных моделей политики безопасности является:
изначальное допущение вскрываемости системы
необходимость дополнительного обучения персонала
статичность
сложный механизм реализации

32. Первым этапом разработки системы защиты ИС является:
анализ потенциально возможных угроз информации
изучение информационных потоков
стандартизация программного обеспечения
оценка возможных потерь

33. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет:
криптология
стеганография
криптоанализ
криптография

34. Недостатком модели политики безопасности на основе анализа угроз системе является:
изначальное допущение вскрываемости системы
статичность
необходимость дополнительного обучения персонала
сложный механизм реализации

35. По документам ГТК количество классов защищенности СВТ от НСД к информации:
9
6
8
7

Тема 6 «Технологическая модель подсистемы информационной безопасности». Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны. Концепция защищенных виртуальных частных сетей.

36. Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему:
всех средств безопасности
аудита
пароля
хотя бы одного средства безопасности

37. При избирательной политике безопасности в матрице доступа объекту системы соответствует:
ячейка
столбец
прямоугольная область
строка

38. Надежность СЗИ определяется:
усредненным показателем

самым слабым звеном
количеством отраженных атак
самым сильным звеном

39. Политика информационной безопасности — это:
профиль защиты
итоговый документ анализа рисков
стандарт безопасности
совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации

40. Обеспечением скрытности информации в информационных массивах занимается
криптография
криптоанализ
криптология
стеганография

41. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты:
ограниченной компетенцией злоумышленника
за определенное время
фиксированными затратами
фиксированным ресурсом

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 20 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.

Критерии оценивания:
правильный и полный ответ на 1 вопрос – 1 балл;
неправильный ответ на 1 вопрос – 0 баллов.
Количество баллов за семестр – 20 баллов.

Лабораторные задания

1.Тематика лабораторных работ по разделам и темам:

Раздел 1 «**Принципы организации защищённых информационных систем**».

Тема 1 "Основные принципы организации защищённых ИС". Концепция создания защищенных информационных систем. Защищённость как понятие. Защищенные технологии в целом. Защищенные информационные системы. Модель защищенных информационных систем.

Лабораторная работа 1. Установка антивирусного программного обеспечения.

Тема 2 «Уязвимость защищённых ИС». Анализ причин уязвимости ЭИС. Методы и механизмы защиты от НСД. Модель системы безопасности РЭИС.

Лабораторная работа 2. Пользовательская политика.

Тема 3 «Требования к архитектуре ИС для обеспечения безопасности ее функционирования». Идеология открытых информационных систем. Анализ безопасности ИС при отсутствии злоумышленных факторов. Стандартизация подходов к обеспечению информационной безопасности.

Лабораторная работа 3. Установка Linux-подобной операционной системы.

Раздел 2. «**Технологии обеспечения безопасности**».

Тема 5 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Защита информации в информационных системах и компьютерных сетях. Особенности, которые делают сети уязвимыми. Причины, приводящие к крупным проблемам. Наиболее часто встречающиеся дефекты защиты. Причинами появления уязвимостей в сетях.

Лабораторная работа 4. Установка шифровальных систем.

Тема 6 «Технологическая модель подсистемы информационной безопасности». Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны. Концепция защищенных виртуальных частных сетей.

Лабораторная работа 5. Установка межсетевого экрана.

Критерии оценивания:

- (для каждого задания):

8 баллов. – задание выполнено верно;

5-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;

3-4 баллов. – при выполнении задания были допущены ошибки;

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

0 баллов. – задание не выполнено.

Максимальное количество баллов, которые могут быть получены обучающимся - 40.

Практические задания

1.Тематика практических заданий по разделам и темам:

Раздел 1 «**Принципы организации защищённых информационных систем**».

Тема 1 "Основные принципы организации защищённых ИС". Концепция создания защищенных информационных систем. Защищённость как понятие. Защищенные технологии в целом. Защищенные информационные системы. Модель защищенных информационных систем.

Практическая работа 1. Настройка антивирусного программного обеспечения.

Тема 2 «Уязвимость защищённых ИС». Анализ причин уязвимости ЭИС. Методы и механизмы защиты от НСД. Модель системы безопасности РЭИС.

Практическая работа 2. Настройка пользовательских групп.

Тема 3 «Требования к архитектуре ИС для обеспечения безопасности ее функционирования». Идеология открытых информационных систем. Анализ безопасности ИС при отсутствии злоумышленных факторов. Стандартизация подходов к обеспечению информационной безопасности.

Практическая работа 3. Настройка впервые установленной Linux-подобной операционной системы.

Раздел 2. «**Технологии обеспечения безопасности**».

Тема 5 «Технологии и инструменты обеспечения безопасности информации в системах и сетях». Защита информации в информационных системах и компьютерных сетях. Особенности, которые делают сети уязвимыми. Причины, приводящие к крупным проблемам. Наиболее часто встречающиеся дефекты защиты. Причинами появления уязвимостей в сетях.

Практическая работа 4. Использование шифровальных систем.

Тема 6 «Технологическая модель подсистемы информационной безопасности». Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны. Концепция защищенных виртуальных частных сетей.

Практическая работа 5. Настройка межсетевого экрана.

Критерии оценивания:

- (для каждого задания):

8 баллов. – задание выполнено верно;

5-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;

3-4 баллов. – при выполнении задания были допущены ошибки;

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

0 баллов. – задание не выполнено.

Максимальное количество баллов, которые могут быть получены обучающимся - 40.

Темы курсовых проектов

В курсовом проекте в соответствии с полученным вариантом необходимо выполнить этап концептуального проектирования системы информационной безопасности:
материалы исследования, разработки, анализа различных методов, методик, способов, алгоритмов в области обработки и защиты информации

Варианты курсового проекта
1 Отделение коммерческого банка.
2 Поликлиника.
3 Университет.
4 Офис страховой компании.
5 Интернет-магазин.
6 Офис адвоката.
7 Агентство недвижимости.
8 Туристическое агентство.
9 Издательство.
10 Отделение налоговой службы.
11 Гостиница.
12 Железнодорожная касса.
13 Офис нотариуса.
14 Администрация завода.
15 Администрация города.

Шкалы 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 основных знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, 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.

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.

В билете два вопроса: один теоретический и один практико-ориентированный. Объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Защита курсового проекта проводится за счет времени, отведенного на изучение дисциплины.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекционные занятия;
- лабораторные занятия;
- практические занятия;
- самостоятельные работы.

В ходе лабораторных и практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки защиты информационных систем.

При подготовке к лабораторным и практическим занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– подготовить ответы на все вопросы по изучаемой теме.

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

Вопросы, не рассмотренные на лекциях, лабораторных и 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 практическому и лабораторному занятиям 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.