МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ,
МИНИСТЕРСТВО НАУКИ, ВЫСШЕГО ОБРАЗОВАНИЯ И ИННОВАЦИЙ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

ГОУ ВПО Кыргызско-Российский Славянский университет
имени первого Президента Российской Федерации Б.Н. Ельцина

УТВЕРЖДАЮ
и.о. декана ЕТФ
Комарцов Н.М.
4.11.24

Информационная безопасность открытых систем

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационных и вычислительных технологий**

Учебный план g09040440_24_1пи_рпис.plx
Направление подготовки 09.04.04 - РФ, 710400 - КР Программная инженерия
Магистерская программа "Разработка программно-информационных систем"

Квалификация **магистр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 128
в том числе:
аудиторные занятия 38
самостоятельная работа 89,9

Виды контроля в семестрах:
зачеты с оценкой 3

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на	3 (2.1)		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	12	12	12	12
Практические	26	26	26	26
Контактная работа в период теоретического	0,1	0,1	0,1	0,1
В том числе инт.	8	8	8	8
Итого ауд.	38	38	38	38
Контактная работа	38,1	38,1	38,1	38,1
Сам. работа	89,9	89,9	89,9	89,9
Итого	128	128	128	128

Программу составил(и):
к.т.н., доцент кафедры ИВТ, Демиденко А.П.;;ст.преп. кафедры ИВТ, Беляев А.А.

Рабочая программа дисциплины
Информационная безопасность открытых систем

разработана в соответствии с ФГОС 3++:
Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.04 Программная инженерия (приказ Минобрнауки России от 19.09.2017 г. № 932)

Рабочая программа одобрена на заседании кафедры
Информационных и вычислительных технологий

Протокол от 02.10.2024 г. № 2
Срок действия программы: 2024-2028 уч.г.
Зав. кафедрой д.т.н., проф. Лыченко Н.М.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
9 сентября 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информационных и вычислительных технологий

Протокол от 3 сентября 2025 г. № 1
Зав. кафедрой д.т.н., проф. Лыченко Н.М.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Информационных и вычислительных технологий

Протокол от __ _____ 2026 г. № __
Зав. кафедрой д.т.н., проф. Лыченко Н.М.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
__ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Информационных и вычислительных технологий

Протокол от __ _____ 2027 г. № __
Зав. кафедрой д.т.н., проф. Лыченко Н.М.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
__ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
Информационных и вычислительных технологий

Протокол от __ _____ 2028 г. № __
Зав. кафедрой д.т.н., проф. Лыченко Н.М.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Изучение дисциплины «Информационная безопасность
1.2	открытых систем» направлено на достижение следующих
1.3	основных целей:
1.4	1) заложить терминологический фундамент;2) рассмотреть особенности построения
1.5	открытых систем;
1.6	3) приобрести навыки аудита
1.7	открытых систем; 4) научить правильно проводить оценку рисков информационной
1.8	безопасности для
1.9	открытых систем; 5) изучить методы и средства обеспечения информационной
1.10	безопасности
1.11	открытых систем; 6) рассмотреть основные общеметодологические принципы
1.12	построения системы защиты информации для
1.13	открытых систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Технологическая (проектно-технологическая) практика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Преддипломная практика
2.2.2	Спецкурс по технологиям проектирования программного обеспечения

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-7: Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях;	
Знать:	
Уровень 1	- особенности построения открытых систем и системы защиты информации для них.
Уметь:	
Уровень 1	- применять методы и средства обеспечения информационной безопасности открытых систем
Владеть:	
Уровень 1	- навыками аудита открытых систем.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	- угрозы информационной безопасности;
3.1.2	- современные подходы к построению систем защиты информации; - компьютерные системы и сети как объект информационного воздействия,
3.1.3	- критерии оценки
3.1.4	защищенности и методы обеспечения их информационной безопасности
3.2	**Уметь:**
3.2.1	- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;
3.2.2	- применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований;
3.3	**Владеть:**
3.3.1	- анализом информационной инфраструктуры;
3.3.2	- методами формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)								
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Пр. подг.**	**Примечание**
	Раздел 1. Стандартизация и модельное представление открытых информационных систем							
1.1	Основные элементы технологии открытых информационных систем. Основные модели открытых систем /Лек/	3	2	ОПК-7	Л1.1 Л1.2Л2.3 Э2			
1.2	Практическая работа №1. Построение модели открытых систем. /Пр/	3	6	ОПК-7	Л1.1 Л1.2Л2.2 Л2.3 Э1 Э2	2		презентация и обсуждение разработанных моделей
1.3	Интранет как открытая система /Ср/	3	26	ОПК-7	Л1.1 Л1.2Л2.3 Э1 Э2			
	Раздел 2. Атаки на открытые системы							
2.1	Классические и современные методы проникновения в открытые системы /Лек/	3	2	ОПК-7	Л1.1 Л1.2Л2.2 Л2.3 Э1 Э2	1		Интерактивное обсуждение методов проникновения в открытые системы
2.2	Практическая работа №2. Исследование защищенности сетей передачи данных. /Пр/	3	4	ОПК-7	Л1.1 Л1.2Л2.2 Л2.3 Э2	2		Обсуждение проблемы защиты сетей передачи даных
2.3	Практическая работа №2. Разработка политик безопасности. /Пр/	3	6	ОПК-7	Л1.1 Л1.2Л2.2 Э2			
2.4	Обеспечение информационной безопасности в открытых системах /Ср/	3	27	ОПК-7	Л1.1 Л1.2Л2.2 Э1 Э2			
2.5	Удаленные атаки на открытые системы /Лек/	3	2	ОПК-7	Л1.1 Л1.2Л2.3 Э2	1		Интерактивное обсуждение проблемы удаленных атак
	Раздел 3. Аутентификация субъектов и объектов взаимодействия в открытых системах. Межсетевые экраны							
3.1	Сетевая аутентификация. Подсистема аутентификации /Лек/	3	2	ОПК-7	Л1.1 Л1.2Л2.3 Э2			
3.2	Практическая работа №3. Выбор реализации межсетевых экранов. /Пр/	3	4	ОПК-7	Л1.1 Л1.2Л2.2 Э1 Э2			
3.3	Межсетевые экраны /Ср/	3	10	ОПК-7	Л1.1 Л1.2Л2.2 Л2.3 Э2			
	Раздел 4. Криптографическая защита в открытых системах							
4.1	Управление криптографическими ключами /Лек/	3	2	ОПК-7	Л1.1 Л1.2Л2.1 Э2			

4.2	Новые направления: идентификационные и бессертификационные криптосистемы /Лек/	3	2	ОПК-7	Л1.1 Л1.2Л2.1 Э2	2		Презентация и обсуждение новых направлений
4.3	Практическая работа №4. Система PGP. Установка и исследование. /Пр/	3	6	ОПК-7	Л1.1 Л1.2Л2.1 Л2.2 Э2			
4.4	Система Керберос.Применение. /Ср/	3	26,9	ОПК-7	Л1.1 Л1.2Л2.2 Э2			
4.5	/КрТО/	3	0,1	ОПК-7	Л1.1 Л1.2Л2.1 Л2.2 Э2			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Перечень контрольных вопросов
Вопросы для проверки уровня обученности ЗНАТЬ
1. Концепция безопасности.
2. Сетевые и системные угрозы (атаки).
4. Аудит сетевых систем.
5. Брандмауэры.
6. Обнаружение попыток взлома.
7. Криптография.
8. SSL.
9. Уровни безопасности компьютеров.
10. Решение проблем безопасности в Windows NT.
11. Политики безопасности.
12. Управление правами доступа.
13. Матричная модель доступа (модель Харрисона-Руззо-Ульмана).
14. Многоуровневая модель доступа (модель Белла-Лападулы).
15. Защита информации от несанкционированного доступа.
16. Защита от несанкционированного копиро-вания.
17. Аутентификация сообщений. Типы функций аутентификации.
18. Традиционное шифрование и аутентификация.
19. Шифрование с открытым ключом. Аутентификация и цифровая подпись.
20. Шифрование с открытым ключом. Аутентификация, цифровая подпись и конфиденциальность.
21. Код аутентичности сообщений (MAC).
22. Код аутентичности сообщений на основе DES.
23. Защита от разрушающих программных воздействий.
24. Вредоносные программы и их классификация.
26. Проблемы обеспечения безопасности при удаленном доступе.
27. Персональные и межсетевые защитные средства.

Задания для проверки уровня обученности УМЕТЬ
1. Авторизация в доменах Windows.
2. Защита от несанкционированного копирования.
3. Борьба с сетевыми атаками.
4. Методы обнаружения и удаления вирусов и восстановления программного обеспечения.

Навыки для проверки уровня обученности ВЛАДЕТЬ
1. Использовать классические алгоритмы шифрования.
2. Применять алгоритмы шифрования с открытым ключом для обеспечения конфиденциальности, аутентификации и цифровой подписи.
3. Владеть приемами использования MAC.
4. Владеть постановкой задачи создания политик безопасности.

5.2. Темы курсовых работ (проектов)

Не предусмотрены

5.3. Фонд оценочных средств

Практическая работа1: исследование функций физического уровня модели OSI;канальный уровень модели OSI: исследование корректности передачи каждого кадра. Практическая работа2:исследование защищенности сетей передачи данных.Проверка политики безопасности и других документов в области информационной безопасности конкретного предприятия.Разработка политик безопасности.Предмет политики. Описание позиции организации.

Применимость.Практическая работа №3: выбор реализации межсетевых экранов. Оценка критериев реализации межсетевых экранов. Практическая работа №4: система PGP. Установка и исследование. Установка Mozilla Thunderbird. Установка Enigmail.

Контрольная работа

Вариант1
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Дайте определения криптографии, криптоанализу, криптологии.
2. Дифференциальный и линейный криптоанализ
3. Даны p=11, q=13. Алгоритмом RSA зашифруйте слово “весна”.

Вариант2
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Что такое аутентификация? Назовите функции, порождающие аутентификатор .
2. Надежность DES
3. Используя задачу о рюкзаке, зашифруйте слово “ЗАЩИТА”

Вариант3
Необходимо подробно в письменной форме ответить на следующие вопросы
1 Что такое шифр Вернама или одноразовый блокнот.
2. Как осуществляется дешифрование в DES. Лавинный эффект в DES.
3. Даны p=17, q=11. Алгоритмом RSA зашифруйте слово “лето”.

Вариант4
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Конфузия и диффузия в шифрах.
2. Как осуществляется аутентификация с помощью симметричной схемы шифрования
3. Используя задачу о рюкзаке, зашифруйте слово “РЮКЗАК”

Вариант5
Необходимо подробно в письменной форме ответить на следующие вопросы
1.Что такое цифровая подпись, как реализуется. Виды цифровых подписей.
2. Шифрование на основе гаммирования. Схема Вернама.
3. С помощью упрощенного DES выполните один раунд шифрования, если подключ есть 10000001, а блок −11011101

Вариант6
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Абсолютно секретные и стойкие по вычислениям шифры.
2. Как осуществляется аутентификация с помощью асимметричной схемы шифрования
3. Даны p=17, q=7. Алгоритмом RSA зашифруйте слово “утро”.

Вариант7
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Шифрование с открытым ключом. Как реализовать аутентификацию, цифровую подпись и конфиденциальность.
2. Алгоритм RSA. Для каких целей применяется. Подробно
3. Используя задачу о рюкзаке, зашифруйте слово “ШИФР”

Вариант8
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Блочные и поточные схемы шифрования: достоинства и недостатки.
2. Начальная и конечная перестановки в DES.Свойства этих перестановок
3. Скремблеры. Определение, реализация. Недостатки

Вариант9
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Шифр Файстеля. Алгоритм дешифрования
2. Идеально стойкие шифры.
3. Даны p=13, q=7. Алгоритмом RSA зашифруйте слово “ТОКМАК”.

Вариант10
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Шифр Файстеля. Понятие раунда. Схема реализации
2. Диффузия и конфузия. Их назначение
3. С помощью упрощенного DES выполните один раунд шифрования, если подключ есть 10011001, а блок −00011101

Вариант11
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Какие схемы распределения открытых ключей вам известны. Их достоинства и недостатки.
2. Алгоритмы шифрования с открытым и закрытым ключом. Особенности. Способ использования. Достоинства и недостатки
3. Используя задачу о рюкзаке, зашифруйте слово “Файстель”

Вариант12
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Шифрование с открытым ключом. Как реализовать аутентификацию и цифровую подпись
2. Классификация алгоритмов по используемым ключам
3. С помощью упрощенного DES выполните один раунд шифрования, если подключ есть 11111001, а блок −11111101

Вариант13
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Какие схемы распределения открытых ключей вам известны. Их достоинства и недостатки.
2. Абсолютно стойкая и защищенные по вычислениям схемы шифрования
3. Даны p=13, q=17. Алгоритмом RSA зашифруйте слово “КОЛЛЕДЖ”

Вариант14
Необходимо подробно в письменной форме ответить на следующие вопросы
1. В чём отличие аутентификации от цифровой подписи. Виды цифровых подписей .
2. Классификация информации, имеющейся у аналитика при криптоанализе
3. С помощью упрощенного DES выполните один раунд шифрования, если подключ есть 00000000, а блок −11111111

Вариант15
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Алгоритмы шифрования с открытым и закрытым ключом. Особенности. Способ использования. Достоинства и недостатки
2. Начальная и конечная перестановки в DES.Свойства этих перестановок
3. С помощью упрощенного DES выполните один раунд шифрования, если подключ есть 11111111, а блок −00000000

Вариант16
Необходимо подробно в письменной форме ответить на следующие вопросы
1. Какие схемы распределения открытых ключей вам известны. Их достоинства и недостатки.
2. Как осуществляется аутентификация с помощью симметричной схемы шифрования
3. Используя задачу о рюкзаке, зашифруйте слово “БЛОК”

Тесты

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:

- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных
тест_20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
- Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальностьl
23) Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
- Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

5.4. Перечень видов оценочных средств

Практическая работа; контрольная работа; тестирование. Зачёт с оценкой.
Виды шкал оценивания представлены в Приложении 1.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Аверченков В.И., Данчул А.А., Ерохин В.Б.	Информационная безопасность: учебник.	Москва: ИНФРА-М, 2023. 416 с.
Л1.2	Шакиров В.А.	Информационная безопасность автоматизированных систем управления.	Москва: Горячая линия - Телеком, 2023. 240 с.

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Музыкантский А.И., Фурин В.В.	Лекции по криптографии	М.: МЦНМО 2011
Л2.2	Глотина И.М.	Средства безопасности операционной системы Windows Server 2008. Учебно-методическое пособи	Саратов: Вузовское образование 2018
Л2.3	С.В. Запечников и др.	Информационная безопасность открытых систем Т.1,2: Учебник для вузов	М.: Горячая линия-Телекои 2006

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Аверченков В.И. Методы и средства инженерно-технической защиты информации: учебное пособие / Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р.— Б.: Брянский государственный технический университет, 2012. 187— с.	http://www.iprbookshop.ru/7000
Э2	Васильев В.И. Интеллектуальные системы защиты информации: учебное пособие / Васильев В.И.— М.: Машиностроение, 2013. 172— с.	http://www.iprbookshop.ru/18519

6.3. Перечень информационных и образовательных технологий

6.3.1 Компетентностно-ориентированные образовательные технологии

6.3.1.1	6.3.1.1 Изучение дисциплины аспирантами осуществляется в форме лекций, практических занятий в аудиторных условиях (компьютерные классы) и в процессе самостоятельной работы, контроля знаний.
6.3.1.2	6.3.1.2 Теоретическая информация, по мере возможности, представляется в виде компьютерных презентаций с использованием мультимедийных средств.
6.3.1.3	6.3.1.3 Практические занятия проводятся в компьютерных классах, оснащенных персональными компьютерами с необходимыми параметрами и с установленным необходимым программным обеспечением. Используется Интернет для получения дополнительной информации. Используется дискуссионный метод проведения занятий, где студенты могут высказать свое мнение по обсуждаемой проблеме.
6.3.1.4	6.3.1.4 Защита практических работ проводится в виде собеседования с преподавателем по теории и программной реализации работы.

6.3.2 Перечень информационных справочных систем и программного обеспечения	
6.3.2.1	Операционная система Ubuntu Linux 18.04 , пакет программ Open Office 4.1, языки программирования
6.3.2.2	высокого уровня, установленные на компьютерах, учебно-методические комплексы по разделам дисциплины,
6.3.2.3	размещенные на серверах компьютерных классов.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебная компьютерная лаборатория :
7.2	ПК - 10 шт;
7.3	сервер - 1;
7.4	ПК преподавателя - 1.
7.5	Локальная сеть кафедры ИВТ КРСУ.
7.6	Интернет со скоростью 70 Мбит/сек.
7.7	Зона WI-FI.
7.8	Интерактивная доска, проектор, обычная доска, 50 посадочных мест

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

Технологическая карта дисциплины представлена в Приложении 2.
Текущий контроль осуществляется в течение семестра и включает в себя проверку подготовки магистранта к выполнению практической работы (т.е.знание теории по теме практической работы), проверку завершения практической работы и оформления отчёта.
Рубежный контроль осуществляется в течение семестра в виде защиты практических работ, выполнения контрольных работ, тестирования.

Методические указания по выполнению практических работ представлены в электронной папке преподавателя (локальная сеть кафедры Информационных и вычислительных технологий КРСУ). Выполнение практических работ завершается оформлением отчета, в котором приводится теория по теме работы, результаты работы прграммы и графики.
Рекомендации по работе с тестами по дисциплине.
Совокупность тестов , представленная в разделе 5.3 может использоваться по частям для текущего контроля освоения предмета по разделам и темам и для итогового контроля знаний по дисциплине в целом.
Предполагается «загрузить» тесты в специализированную ПС или использовать их в форме бланочного контроля. Они могут использоваться студентами для самоконтроля при подготовке к итоговому зачёту по дисциплине.
Вопросы по контрольным работам представлены в разделе РПД Фонд оценочных средств. Ответы на контрольные работы оформляются в письменном виде.