

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.О.43 Защита критической информационной инфраструктуры

Направление подготовки/специальность: 10.05.05 - Безопасность информационных технологий в правоохранительной сфере

Профиль/направленность/специализация: Технологии защиты информации в правоохранительной сфере

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2021

Автор программы:

Кандидат технических наук, доцент Зауголков Игорь Алексеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «26» ноября 2020 г. № 1461).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	8
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	18
6. Учебно-методическое и информационное обеспечение дисциплины.....	20
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	20

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОПК-4 Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), 12 Обеспечение безопасности (в сфере защиты информации), Сфера правоохранительной деятельности

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ОПК-4 Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	Выполняет технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывает рабочую техническую документацию в соответствии требованиям по защите критической информационной инфраструктуры

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОПК-4 Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации

№ п/п	Наименование дисциплин, определяющих	Форма обучения
-------	--------------------------------------	----------------

	междисциплинарные связи	Очная (семестр) 6
1	Правовая защита информации	+

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Защита критической информационной инфраструктуры» относится к обязательной части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Защита критической информационной инфраструктуры» изучается в 9 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	108
Контактная работа	48
Лекции (Лекции)	16
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	60
Зачет	-

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
9 семестр					
1	Комплексный подход к обеспечению информационной безопасности в компьютерных системах	2	4	9	Лабораторная работа
2	Методы и средства защиты информации от несанкционирован ного доступа в компьютерных системах.	3	5	9	Лабораторная работа

3	Защита информации от несанкционированного доступа в операционных системах в компьютерных системах	2	4	9	Лабораторная работа
4	Криптографические методы и средства обеспечения информационной безопасности в компьютерных системах	3	5	6	Лабораторная работа
5	Криптографический интерфейс приложений операционной системы Windows (CryptoApi) в компьютерных системах	2	4	9	Лабораторная работа
6	Защита компьютерных систем от вредоносных программ в компьютерных системах.	2	5	9	Лабораторная работа
7	Защита программных средств от несанкционированного использования и копирования в компьютерных системах.	2	5	9	Лабораторная работа

Тема 1. Комплексный подход к обеспечению информационной безопасности в компьютерных системах (ОПК-4)

Лекция.

Угрозы информационной безопасности и каналы утечки информации. Организационно-правовое обеспечение информационной безопасности. Инженерно-технические методы и средства защиты информации. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. Требования к комплексным системам защиты информации

Лабораторные работы.

Лабораторная работа Политика учетных записей. Утилиты администрирования командной строки.

Задания для самостоятельной работы.

Подготовка конспекта лекций и лабораторных работ, прочтение дополнительной литературы

Тема 2. Методы и средства защиты информации от несанкционированного доступа в компьютерных системах. (ОПК-4)

Лекция.

Способы несанкционированного доступа к информации в компьютерных системах и защиты от него. Аутентификация пользователей на основе паролей и модели рукопожатия». Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью. Программно-аппаратная защита информации от локального несанкционированного доступа. Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях.

Лабораторные работы.

Лабораторная работа №2. Использование реестра для настройки параметров операционной системы.

Задания для самостоятельной работы.

Подготовка конспекта лекций и лабораторных работ, прочтение дополнительной литературы

Тема 3. Защита информации от несанкционированного доступа в операционных системах компьютерных системах (ОПК-4)

Лекция.

Защита информации от несанкционированного доступа в открытых версиях операционной системы Windows. Дискреционное и мандатное управление доступом к объектам компьютерных систем. Подсистема безопасности защищенных версий операционной системы Windows. Аудит событий безопасности в защищенных версиях операционной системы Windows. Защита информации от несанкционированного доступа в операционных системах семейства Unix.

Лабораторные работы.

Лабораторная работа №3. Утилиты администрирования командной строки.

Задания для самостоятельной работы.

Подготовка конспекта лекций и лабораторных работ, прочтение дополнительной литературы

Тема 4. Криптографические методы и средства обеспечения информационной безопасности в компьютерных системах (ОПК-4)

Лекция.

Элементы теории чисел. Основные понятия криптографии. Симметричные и асимметричные криптосистемы. Способы создания симметричных криптосистем. Абсолютно стойкий шифр. Криптографическая система DES и ее модификации. Криптографическая система ГОСТ 28147—89. Принципы построения асимметричных криптографических систем. Электронная цифровая подпись и ее применение. Использование симметричных и асимметричных криптографических систем. Компьютерная стеганография и ее применение.

Лабораторные работы.

Лабораторная работа № 4. Анализ и настройка политики безопасности.

Задания для самостоятельной работы.

Подготовка конспекта лекций и лабораторных работ, прочтение дополнительной литературы

Тема 5. Криптографический интерфейс приложений операционной системы Windows (CryptoApi) в компьютерных системах (ОПК-4)

Лекция.

Принципы построения и использования CryptoAPI. Создание и передача криптографических ключей с помощью функций CryptoAPI. Использование функций CryptoAPI для шифрования и расшифровывания данных. Использование функций CryptoAPI для получения и проверки электронной цифровой подписи. Защита документов MicrosoftOffice от несанкционированного доступа. Шифрующая файловая система в защищенных версиях операционной системы Windows.

Лабораторные работы.

Лабораторная работа № 5. Аудит.

Задания для самостоятельной работы.

Подготовка конспекта лекций и лабораторных работ, прочтение дополнительной литературы

Тема 6. Защита компьютерных систем от вредоносных программ компьютерных системах. (ОПК-4)

Лекция.

Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.

Лабораторные работы.

Лабораторная работа № 6. Использование протокола IPSec.

Задания для самостоятельной работы.

Подготовка конспекта лекций и лабораторных работ, прочтение дополнительной литературы

Тема 7. Защита программных средств от несанкционированного использования и копирования в компьютерных системах. (ОПК-4)

Лекция.

Принципы построения систем защиты от копирования. Методы защиты инсталляционных дисков от копирования. Методы настройки устанавливаемого программного обеспечения на характеристики компьютера. Методы противодействия исследованию алгоритма работы системы защиты.

Лабораторные работы.

Лабораторная работа № 7. Повышение защищенности рабочих станций.

Задания для самостоятельной работы.

Подготовка конспекта лекций и лабораторных работ, прочтение дополнительной литературы

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

9 семестр

- посещаемость – 10 баллов
- текущий контроль – 40 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мак. кол-во баллов	Методика проведения занятия и оценки
--------	------------------------------------	---------------------------------	--------------------	--------------------------------------

1.	Комплексный подход к обеспечению информационной безопасности в компьютерных системах	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
2.	Методы и средства защиты информации от несанкционированного доступа в компьютерных системах.	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

3.	Защита информации от несанкционированного доступа в операционных системах компьютерных системах	Лабораторная работа(контрольный срез)	10	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>6 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>3 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
4.	Криптографические методы и средства обеспечения информационной безопасности в компьютерных системах	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

5.	Криптографический интерфейс приложений операционной системы Windows (CryptoApi) в компьютерных системах	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
6.	Защита компьютерных систем от вредоносных программ в компьютерных системах.	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

7.	Защита программных средств от несанкционированного использования и копирования в компьютерных системах.	Лабораторная работа(контрольный срез)	10	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 6 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 3 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
8.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7-9 баллов – посещаемость студента составляет не менее 80 % занятий 4-6 баллов – посещаемость студента составляет не менее 50 % занятий 1-3 балла – посещаемость студента составляет не менее 25 % занятий
9.	Премияльные баллы		20	Дополнительные премияльные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции
10.	Ответ на экзамене		30	25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично». 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно»
11.	Итого за семестр		100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

4.2 Типовые оценочные средства текущего контроля

Лабораторная работа

Тема 1. Комплексный подход к обеспечению информационной безопасности в компьютерных системах

Лабораторная работа Политика учетных записей. Утилиты администрирования командной строки.

Цель работы: изучение возможных подходов к решению задач администрирования с использованием средств настройки основных параметров безопасности рабочей станции ОС Windows 2000, XP, средств работы с реестром ОС, системных средств администрирования командной строки.

Контрольные вопросы 1. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен. 2. Какие параметры входят в политику блокировки учётной записи? 3. Возможно ли, что учётная запись не будет заблокирована при количестве ошибок большем, чем установленное пороговое значение? 4. Что такое и для чего применяется ММС? 5. Что такое оснастка? 6. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике? 7. Каким образом можно включить автозапуск программ через групповую политику? 8. При помощи какой команды можно получить список пользователей операционной системы? 9. При помощи какой команды можно получить список групп пользователей операционной системы? 10. При помощи какой команды можно создать нового пользователя?

Тема 3. Защита информации от несанкционированного доступа в операционных системах компьютерных системах

Лабораторная работа №3. Утилиты администрирования командной строки.

Цель работы: Изучение возможных подходов к решению задач администрирования с использованием утилит администрирования командной строки ОС Windows 7.

Задания для выполнения

1. Используя утилиту PING определить пропускную способность сети до адресов 10.7.0.120, 10.219.0.1, 10.239.1.1 и 10.7.15.15. Объясните разницу в результатах.
2. Используя утилиту TRACERT и таблицу маршрутизации шлюза (используйте файл «APOS–LR#04–router2», а точнее адреса шлюзов), постройте схему сети университета.
3. Передайте пакеты участникам сети напрямую и через шлюз. Объясните полученные записи в таблице ARP.

Контрольные вопросы

1. Для чего используется утилита PING?
2. Как с помощью утилиты PING оценить пропускную способность сети? Объясните формулу.
3. Что такое петля маршрутизации?
4. Как выглядят правила маршрутизации, образующие петлю?
5. Зачем нужна таблица ARP?
6. Объясните разницу во времени между обращениями к одному и тому же хосту по имени и IP адресу.

Тема 4. Криптографические методы и средства обеспечения информационной безопасности в компьютерных системах

Лабораторная работа № 4. Анализ и настройка политики безопасности.

Цель работы: Изучение технологии настройки параметров безопасности с использованием шаблонов.

Контрольные вопросы.

- 1 Назовите основные средства защиты Windows XP.
- 2 Расскажите алгоритм создания, редактирования и применения шаблонов безопасности в Windows XP.
- 3 Дайте краткую характеристику инструментам аудита безопасности Windows XP.
- 4 Каким образом в оснастке Анализ и настройка безопасности MMC анализируются текущие настройки безопасности?
- 5 Как работает протокол IPSec?
- 6 Какие бывают типы процессов входа в систему Windows XP?
- 7 Какие возможности обеспечивает протокол безопасности Kerberos?
- 8 Как происходит аутентификация пользователя по протоколу NTLM?
- 9 чем аутентификация пользователя отличается от входа в систему?
- 10 Какие стандартные типы учетных записей имеются в Windows XP?
- 11 Какие способы управления паролями существуют в Windows XP и чем они отличаются друг от друга?
- 12 По каким принципам обычно учетные записи объединяют в группы?
- 13 Для чего в Windows XP используется инструмент Whoami?
- 14 Какие списки контроля доступа ACL используются в Windows XP? Дайте им краткую характеристику.

Тема 5. Криптографический интерфейс приложений операционной системы Windows (CryptoApi) в компьютерных системах

Лабораторная работа № 5. Аудит.

Цель работы: Изучение технологии ведения аудита в ОС Windows 2000, XP. Изучение возможности разделения функций администратора системы и администратора безопасности (аудитора).

Контрольные вопросы:

- 1 Что называется мониторингом?
- 2 Чем отличается Мониторинг параметров и Мониторинг состояния?
- 3 Какой программный модуль реализует Мониторинг параметров? Мониторинг состояния?
- 4 Что такое DirectX?

Тема 6. Защита компьютерных систем от вредоносных программ в компьютерных системах.

Лабораторная работа № 6. Использование протокола IPSec.

Цель работы: Изучение механизмов защиты сетевого трафика средствами протокола IPSec.

Отчет о лабораторной работе должен содержать:

1. Исходную топологию;
2. Конфигурационные файлы;
3. IPsec сообщения перехватываемые программой Wireshark.

Контрольные вопросы:

- 1 Понятие VPN (Основные положения, преимущества и недостатки)
- 2 Туннелирование в VPN
- 3 Классификация VPN (общая)
- 4 Протокол PPTP
- 5 Протокол L2F
- 6 Протокол L2TP
- 7 Основные протоколы входящие в IPSec
- 8 Этапы установления соединения
- 9 Алгоритм Диффи-Хеллмана
- 10 Протокол SSL

11 Инфраструктура открытых ключей

12 Сравнение протоколов PPTP, L2F, L2TP, IPSec, SSL (Область применения, основные преимущества и недостатки)

Тема 7. Защита программных средств от несанкционированного использования и копирования в компьютерных системах.

Лабораторная работа № 7. Повышение защищенности рабочих станций.

Цель работы: Изучение способов повышения защищенности рабочих станций под управлением ОС Windows 2000, XP от несанкционированного доступа.

Вопросы и задания

1 Изучить рекомендации к защищенной реализации механизма хранения паролей. Исследовать механизм восстановления паролей выбранного веб-приложения.

2 Исследовать минимально допустимую длину и сложность паролей в произвольных пяти веб-приложениях из рейтинга ALEXA TOP 100

3 Исследовать наличие оракулов в механизмах аутентификации произвольных пяти веб-приложениях из рейтинга ALEXA TOP 100

Лабораторная работа

Тема 2. Методы и средства защиты информации от несанкционированного доступа в компьютерных системах.

Лабораторная работа №2. Использование реестра для настройки параметров операционной системы.

Цель работы: Изучение возможных подходов к решению задач администрирования с использованием средств работы с реестром ОС Windows 7.

Контрольные вопросы. 1. Что такое системный реестр Windows? 2. Расскажите о структуре реестра. 3. Поясните особенности «троянских программ». 4. Почему профилактика «троянских программ» связана с системным реестром? 5. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ОПК-4)

1. Классификации угроз безопасности КС
2. Каналы, способы и средства воздействия угроз
3. Объекты защиты в КС
4. Классификация КС и характеристика классов
5. Системные принципы информационной безопасности
6. Выработка политики безопасности
7. Направления применения методов и средствЗИ
8. Разработка системы организационных и физических мер защиты КС

9. Разработка системы программно-технических мер защиты КС
10. Характеристика организационных мер и средств защиты КС
11. Администрирование КС
12. Документирование мероприятий по ЗИ
13. Технические средства защиты КС от НСД
14. Технические методы и средства защиты целостности и бесперебойности функционирования компонентов КС
15. Классификация систем контроля доступа (СКД)
16. СКД на основе считывания ключевой информации
17. СКД на основе считывания биометрических признаков
18. Исполняющие подсистемы СКД
19. Организация бесперебойного электропитания
20. Устройства бесперебойного электропитания
21. Особенности хранения компьютерной информации на физических носителях
22. Методы и способы уничтожения информации
23. Использование активного коммуникационного оборудования
24. Маршрутизаторы (routers)
25. Аппаратные криптосистемы
26. Система защиты от ПЭМИН
27. Методы снижения вероятности возникновения угрозы утечки информации за счет ПЭМИН
28. Методы и средства оценки уровня ПЭМИН
29. Методы и средства блокирования возможности утечки информации за счет ПЭМИН
30. Технологии организации коммуникационной инфраструктуры
31. Технологии хранения и доступа к информационным ресурсам
32. Классификация программных СЗИ

33. Обзор современных программных СЗИ.
34. Типовая структура подсистемы безопасности ОС
35. Подсистема безопасности в Windows NT/2000
36. Программы для аутентификации доступа к компьютеру.....
37. Программы для защиты целостности ОС
38. Программы для защиты ПК от вторжений из глобальных сетей
39. Программные компоненты сетевых СЗИ
40. МЭ: виды и варианты использования
41. Средства организации виртуальных частных сетей
42. Средства обнаружения сетевых атак
43. Средства защиты электронных сообщений с помощью цифровой подписи
44. Программный комплекс VIPNET
45. Классификация методов и средств контроля эффективности ЗИ в КС
46. Сканеры безопасности КС

Типовые задания для зачета (ОПК-4)

1. Основной проблемой реализации систем защиты является:
 - а) исключение случайного и преднамеренного получения информации посторонними лицами;
 - б) разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;
 - в) системы защиты не должны создавать заметных неудобств пользователям в ходе их работы с ресурсами системы.
 - г) все вышеперечисленное.+
2. Комплексный (системный) подход к построению любой системы включает в себя:
 - а) изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца; +
 - б) совокупности научных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов;

с) разработку единой концепции как полной совокупности научно обоснованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

3. Какими бывают стратегии защиты информации?

- а) оборонительная, наступательная, упреждающая; +
- б) наступательная, инженерная, сигнализационная, адаптивная;
- с) инженерно-техническая, программно-аппаратная, программная, организационная.

4. Что должна включать в себя система защиты от утечки?

- а) защита от наблюдения, прослушивания, перехвата, контроль вещественных носителей (комплексы мероприятий по контролю звукопроницаемости помещений, предотвращение утечки информации путем шифрования, контроль за уничтожением носителей и т.д.)
- б) звукоизоляция, глушение, экранирование);+
- с) защита от перехвата (шифрование, экранирование, зашумление, фильтрация);+ комплекс защиты от перехвата (шифрование, экранирование, зашумление, фильтрация) комплекс предотвр. утечки вещ.носителей (учет и сккрытие отходов, уничтожение отходов)
- д) определение полномочий пользователя (учет и анализ потока информации, распределение полномочий пользователей, ведения журнала учета);
- е) установки пропускного режима (КПП на входе в здание, контроль доступа в помещения для совещаний и хранилищ конфиденциальных данных);

5. Какие элементы входят в состав информационных правоотношений ?

- а) должностные инструкции, обращение, фиксирование, хранение;
- б) права, ограничение прав, обязанности, ответственность;+
- с) права, обязанности, фиксирование, хранение;
- д) права, ограничение прав, должностные инструкции, ответственность.

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ОПК-4	Показывает хороший уровень знаний базовых теоретических знаний и практических навыков для программирования на языках высокого уровня.¶Способен достаточно эффективно применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач
«не зачтено» (0 - 49 баллов)	ОПК-4	Не имеет базовых теоретических знаний и практических навыков для программирования на языках высокого уровня.¶Не способен продемонстрировать методы и инструментальные средства программирования для решения профессиональных задач.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;

- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : Учеб. пособие для вузов. - М.: Академия, 2005. - 255 с.
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие. - М.: ИД "Форум", ИНФРА-М, 2013. - 591 с.

6.2 Дополнительная литература:

1. Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов. - 4-е изд., стер.. - Москва: Флинта, 2016. - 224 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93351>
2. Блинков, Ю. В. Основы теории информационных процессов и систем : учебное пособие. - Весь срок охраны авторского права; Основы теории информационных процессов и систем. - Пенза: Пензенский государственный университет архитектуры и строительства, ЭБС АСВ, 2011. - 184 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/23103.html>
3. Блок 2: Современные системы защиты информации в ведущих зарубежных странах, 2017. - 1 электрон. опт. диск (CD-ROM).

6.3 Иные источники:

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>
2. Портал «Гуманитарное образование» - <http://www.humanities.edu.ru/>
3. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-collection.edu.ru/>
4. Федеральная служба по надзору в сфере образования и науки - <http://obrnadzor.gov.ru>
5. Вопросы образования - <http://www.ecsocman.edu.ru/vo>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyj-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Российская государственная библиотека. – URL: <https://www.rsl.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
8. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.