Аннотация к рабочей программе дисциплины

«Защищенные цифровые системы передачи информации»

Цель преподавания дисциплины

Сформировать основы знаний по принципам построения телекоммуникационных систем (ТКС), а также ознакомление с методами, средствами и системами обеспечения их информационной безопасности.

Задачи изучения дисциплины

Основными задачами изучения дисциплины является: определение места и значения ИБТКС в системе принятия хозяйственных решений и её роли как превентивного механизма предупреждения негативных последствий вредоносных воздействий объективного и субъективного характера на функционирование ТКС; ознакомление с принципами передачи сообщений в основных сетях связи, ознакомление с основами информационной безопасности систем и сетей связи, ознакомление с методами несанкционированного извлечения информации из сигналов и сообщений различных систем связи.

Знания и умения, которыми должен обладать студент, успешно освоивший данную

Индикаторы компетенций, формируемые в результате освоения дисциплины

ПК-3 Способен использовать современные методы оценки параметров безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью, с целью разработки методов устранения выявленных уязвимостей	ПК-3.2 Применяет основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств
	ПК-3.3 Применяет стандартные программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
	ПК-3.4 Пользуется нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных технологий
	ПК-3.5 Осуществляет установку и управление специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа
ПК-4 Способен осуществлять монтаж, наладку, настройку, регулировку, опытную проверку работоспособности, испытания и сдачу в эксплуатацию сооружений, средств и оборудования сетей	ПК-4.3 Использует современные отечественные и зарубежные пакеты программ при решении схемотехнических, системных и сетевых задач, правила и методы монтажа, настройки и регулировки узлов радиотехнических устройств и систем

Разделы дисциплины

1. Проблемы информационной безопасности сетей
2. Политика безопасности
3. Технологии аутентификации
4. Технологии межсетевых экранов
5. Технологии защиты от вирусов
6. Технологии анализа защищенности и обнаружения сетевых атак
7. Требования к системам защиты информации
8. Аудит безопасности информационных систем
9. Разработка и защита Web-сайтов

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)
Т. А. Ширабакина
(подпись, инициалы, фамилия)
«31» 08 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищенные цифровые системы передачи информации

(наименование дисциплины)

ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Системы мобильной связи»

форма обучения заочная
(очная, очно-заочная, заочная)

Курск – 2020

Рабочая программа дисциплины Защищенные цифровые системы передачи информации составлена в соответствии с ФГОС ВО – бакалавриата по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность «Системы мобильной связи», одобренного Ученым советом университета (протокол № *9* «*29*» *марта* 2019 г.).

Рабочая программа дисциплины Защищенные цифровые системы передачи информации обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи на заседании кафедры информационной безопасности протокол № *1* «*31*» *августа* 2019 г.

Зав. кафедрой Таныгин М.О.

Разработчик программы

к.т.н., доцент Марухленко А.Л.

Согласовано: протокол № 19 «31» 08 2019 г.

Зав. кафедрой Андронов В.Г.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Защищенные цифровые системы передачи информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, одобренного Ученым советом университета (протокол № *9* «*29*» *марта* 2019 г.).

Зав. кафедрой _____

протокол № 1 «31» 08 2020 г.

Рабочая программа дисциплины Защищенные цифровые системы передачи информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, одобренного Ученым советом университета (протокол № *9* «*29*» *марта* 2019 г.).

Зав. кафедрой _____

протокол № 11 «30» 06 2021 г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи», одобренного Ученым советом университета протокол № 7 «28» февраля 2022 г., на заседании кафедры информационной безопасности, протокол №11 от «30» июня 2022 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Тапогин М.О. _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи», одобренного Ученым советом университета протокол №7 «28» 02 2022 г., на заседании кафедры информационной безопасности протокол №1 от 30.08.2023

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи», одобренного Ученым советом университета протокол №___ «__» _____ 20___ г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи», одобренного Ученым советом университета протокол №___ «__» _____ 20___ г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Защищенные цифровые системы передачи информации» является формирование знаний по принципам построения телекоммуникационных систем (ТКС), а также ознакомление с методами, средствами и системами обеспечения их информационной безопасности.

1.2. Задачи изучения дисциплины

Основными задачами изучения дисциплины является: определение места и значения ИБТКС в системе принятия хозяйственных решений и её роли как превентивного механизма предупреждения негативных последствий вредоносных воздействий объективного и субъективного характера на функционирование ТКС; ознакомление с принципами передачи сообщений в основных сетях связи, ознакомление с основами информационной безопасности систем и сетей связи, ознакомление с методами несанкционированного извлечения информации из сигналов и сообщений различных систем связи.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-3	Способен использовать современные методы оценки параметров безопасности и защиты программного обеспечения и сетевых устройств	ПК-3.2 Применяет основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств	***Знать:*** классификацию, виды и типы инструментальных средств контроля защищенности информации в автоматизированных системах; Методы и способы контроля защищенности информации; ***Уметь:*** применять инструментальные средства контроля защищенности информации в автоматизированных системах;

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	администрируемой сети с помощью специальных средств управления безопасностью, с целью разработки методов устранения выявленных уязвимостей		производить оценку полученных результатов; сопоставлять результаты измерений с требуемыми значениями. ***Владеть:*** навыками инструментального контроля защищенности информации в автоматизированных системах; анализа защищенности автоматизированных систем; навыками выбора инструментальных средств контроля защищенности информации; навыками интерпретации результатов измерений и определения подхода для повышения защищенности автоматизированных систем.
		ПК-3.3 Применяет стандартные программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения, принципы и способы организации системы защиты информации на объектах информатизации. Порядок и алгоритм проведения организационных мероприятий на объектах информатизации. ***Уметь:*** Выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации на объектах информатизации и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Осуществлять выбор технических средств защиты информации в зависимости от условий эксплуатации объектов

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			информатизации. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками применения технических средств защиты информации, обрабатываемой в сетях ЭВМ.
		ПК -3.4 Пользуется нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных технологий	***Знать:*** классификацию, виды и типы угроз безопасности автоматизированных систем, принципы построения средств защиты информации; основные компоненты автоматизированных систем объекта информатизации; компоненты, назначение и функциональные особенности программно-аппаратных средств защиты информации. ***Уметь:*** определять параметры конфигурирования программно-аппаратных средств в соответствие заданным требованиям политики безопасности. ***Владеть:*** навыками защиты информации в компьютерных сетях; навыками конфигурирования программно-аппаратных средств защиты информации; выбора средств защиты информации; навыками построения системы защиты сетей ЭВМ.
		ПК-3.5 Осуществляет установку и управление специализированными программными средствами защиты сетевых устройств администрируемой сети от	**Знать:** устройство межсетевых экранов, технологию оценки состояния защищенности, совместимость программно-аппаратных средств и варианты обеспечения разграничения доступа на уровне операционной системы и прикладных средств. **Уметь:** настраивать режимы работы межсетевых экранов, проводить

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		несанкционированного доступа	анализ защищенности локальной вычислительной сети ***Владеть:*** навыками эксплуатации и разработки программно-аппаратных средств обеспечения защиты передаваемых в масштабе вычислительной сети
ПК-4	Способен осуществлять монтаж, наладку, настройку, регулировку, опытную проверку работоспособности, испытания и сдачу в эксплуатацию сооружений, средств и оборудования сетей	ПК 4.3 Использует современные отечественные и зарубежные пакеты программ при решении схемотехнических, системных и сетевых задач, правила и методы монтажа, настройки и регулировки узлов радиотехнических устройств и систем	***Знать:*** особенности современных пакетов программ при решении схемотехнических, системных и сетевых задач по организации взаимодействия удаленных абонентов. ***Уметь:*** настраивать существующие каналы связи, расширять и администрировать локальную вычислительную сети, оптимизировать трафик и обеспечивать уверенный прием в случае использования беспроводного доступа. ***Владеть:*** навыками монтажа, настройки и регулировки узлов радиотехнических устройств и систем.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защищенные цифровые системы передачи информации», входит в часть блока 1, формируемую участниками образовательных отношений «Дисциплины (модули)») основной профессиональной образовательной программы – программы бакалавриата 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи». Дисциплина изучается на 3 курсе.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 академических часа.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	8
в том числе:	
лекции	4
лабораторные занятия	4
практические занятия	
Самостоятельная работа обучающихся (всего)	95,9
Контроль (подготовка к экзамену)	
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Проблемы информационной безопасности сетей	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP – сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.
2.	Политика безопасности	Основные понятия политики безопасности. Верхний,

		средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети: физическая безопасность, логическая безопасность, защита ресурсов, определение административных полномочий, аудит и оповещение.
3.	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно – программные системы идентификации и аутентификации.
4.	Технологии межсетевых экранов	Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
5.	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.
6.	Технологии анализа защищенности и обнаружения сетевых атак	Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях.

		Методы реагирования. Обзор современных средств обнаружения атак.
7.	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.
8.	Аудит безопасности информационных систем	Понятие аудита безопасности и цели его проведения. Стандарты, используемые при проведении аудита. Инициирование и планирование процедуры аудита. Сбор информации для аудита. Анализ данных аудита. Разработка рекомендаций. Подготовка отчетных документов. Анализ рисков и управление рисками. Оценка по верхним и нижним значениям. Оценка на основе выявления слабого звена. Оценка риска на основе рассмотрения этапов вторжения. Обзор программных продуктов для анализа и управления рисками: GRAMM, RiskWath, COBRA, ПО компании MethodWare, ПО “Аван Гард”.
9.	Разработка и защита Web-сайтов	Основы языка разметки документов HTML. Структура HTML -документа. Форматирование текста в HTML. Использование графики в HTML. Использование таблиц в HTML. Гиперссылки в HTML. Фреймы в HTML. Каскадные таблицы стилей CSS. Основы языка программирования JavaScript. Методы ввода и вывода информации в языке программирования JavaScript. Операторы в языке программирования JavaScript. Функции в языке программирования JavaScript. Обработчики событий в языке программирования JavaScript. Создание меню в языке программирования JavaScript. Окна в в языке программирования JavaScript. Формы в в языке программирования JavaScript.Защита информации с помощью аутентификации в языке программирования JavaScript. Защита контента от несанкционированного копирования информации в языке программирования JavaScript. Защита Web-сайта от DDoS – атак. Антивирусная защита Web-сайта.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (*по неделям семестра*)	Компетенции
		лек, час	№, лаб.	№, пр.			
1	2	3	4	5	6	7	8
1.	Проблемы информационной безопасности сетей	0,25		1	У-1-3 МУ – 1-4	С – 1-2 ЗЛР - 1-2	ПК-3
2.	Политика безопасности	0,25			У-1-3, 4-6	С – 3-4	ПК-3
3.	Технологии аутентификации	0,5			У-1-3, 4-6	С - 5-6	ПК-3
4.	Технологии межсетевых экранов	0,5		2	У-1-3, 4-6 МУ – 1-4	С – 7-8 ЗЛР - 7-8	ПК-3
5.	Технологии защиты от вирусов	0,5		3	У-1-3, 4-6 МУ – 1-4	С – 9-10 С – 7-8	ПК-3
6.	Технологии анализа защищенности и обнаружения сетевых атак	0,5			У-1-3, 4-6	С – 11-12	ПК-3
7.	Требования к системам защиты информации	0,5		4	У-1-3, 4-6 МУ – 1-4	С – 13-14 ЗЛР – 13-14	ПК-3
8.	Аудит безопасности информационных систем	0,5			У-1-3	С – 15-16	ПК-3
9.	Разработка и защита Web-сайтов	0,5			У-1-3	С – 17-18	ПК-3

С – собеседование, ЗЛР – защита лабораторной работы

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные занятия

Таблица 4.4 – Лабораторные занятия

№	Наименование практической работы	Объем, час.
1.	Изучение существующих каналов утечки информации	1
2.	Настройка межсетевого экрана в операционной системе Windows	1
3.	Антивирусная программа: Kaspersky Internet Security	1
4.	Анализ защищенности компьютерной сети с помощью программ	1

	GFI Languard, Network Security Scanner и XSPIDER	
Итого		4

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№ раздела (Тема)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Проблемы информационной безопасности сетей	2 неделя	10
2.	Политика безопасности	4 неделя	10
3.	Технологии аутентификации	6 неделя	10
4.	Технологии межсетевых экранов	8 неделя	10
5.	Технологии защиты от вирусов	10 неделя	10
6.	Технологии анализа защищенности и обнаружения сетевых атак	12 неделя	10
7.	Требования к системам защиты информации	14 неделя	10
8.	Аудит безопасности информационных систем	16 неделя	10
9.	Разработка и защита Web-сайтов	18 неделя	15,9
Итого			95,9

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачету;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода не предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся.

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий

содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций);

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-3. Способен использовать современные методы оценки параметров безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью, с	Программное обеспечение инфокоммуникаций		Системы коммутации Системы спутникового телерадиовещания

целью разработки методов устранения выявленных уязвимостей.		
ПК-4. Способен осуществлять монтаж, наладку, настройку, регулировку, опытную проверку работоспособности, испытания и сдачу в эксплуатацию сооружений, средств и оборудования сетей	Теоретические основы систем мобильной связи	Обеспечение информационной безопасности в беспроводных сетях

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ПК-3/ завершающий	ПК-3.2 Применяет основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств	***Знать:*** виды и типы инструментальных средств контроля защищенности информации в автоматизированных системах. ***Уметь:*** применять инструментальные средства контроля защищенности информации в автоматизированных системах. ***Владеть:*** навыками инструментального контроля защищенности информации в автоматизированных системах.	***Знать:*** классификацию, виды и типы инструментальных средств контроля защищенности информации в автоматизированных системах; ***Уметь:*** применять инструментальные средства контроля защищенности информации в автоматизированных системах; производить оценку полученных результатов. ***Владеть:***	***Знать:*** классификацию, виды и типы инструментальных средств контроля защищенности информации в автоматизированных системах; Методы и способы контроля защищенности информации; ***Уметь:*** применять инструментальные средства контроля защищенности информации в автоматизированных системах; производить оценку полученных результатов; сопоставлять

			навыками инструментального контроля защищенности информации в автоматизированных системах; анализа защищенности автоматизированных систем.	результаты измерений с требуемыми значениями. ***Владеть:*** навыками инструментального контроля защищенности информации в автоматизированных системах; анализа защищенности автоматизированных систем; навыками выбора инструментальных средств контроля защищенности информации; навыками интерпретации результатов измерений и определения подхода для повышения защищенности автоматизированных систем.
	ПК-3.3 Применяет стандартные программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа	***Знать:*** классификацию, виды и типы угроз безопасности автоматизированных систем, основные компоненты автоматизированных систем объекта информатизации. ***Уметь:*** определять параметры конфигурирования программно-аппаратных средств в соответствие заданным требованиям политики безопасности. ***Владеть:*** навыками конфигурирования программно-	***Знать:*** классификацию, виды и типы угроз безопасности автоматизированных систем, принципы построения средств защиты информации; основные компоненты автоматизированных систем объекта информатизации. ***Уметь:*** определять параметры конфигурирования программно-	***Знать:*** классификацию, виды и типы угроз безопасности автоматизированных систем, принципы построения средств защиты информации; основные компоненты автоматизированных систем объекта информатизации; компоненты, назначение и функциональные особенности программно-аппаратных средств защиты информации.

		аппаратных средств защиты информации.	аппаратных средств в соответствие заданным требованиям политики безопасности. ***Владеть:*** навыками защиты информации в компьютерных сетях; навыками конфигурирования программно-аппаратных средств защиты информации.	***Уметь:*** определять параметры конфигурирования программно-аппаратных средств в соответствие заданным требованиям политики безопасности. ***Владеть:*** навыками защиты информации в компьютерных сетях; навыками конфигурирования программно-аппаратных средств защиты информации; выбора средств защиты информации; навыками построения системы защиты сетей ЭВМ.
	ПК -3.4 Пользуется нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных технологий	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам, ***Уметь:*** Выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации на объектах информатизации и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. ***Владеть:*** навыками применения технических средств	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации. ***Уметь:*** Выполнять требования нормативных и эксплуатационных документов (документации)	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения, принципы и способы организации системы защиты информации на объектах информатизации. Порядок и

		защиты информации, обрабатываемой в сетях ЭВМ.	по обеспечению защиты информации на объектах информатизации и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками применения технических средств защиты информации, обрабатываемой в сетях ЭВМ.	алгоритм проведения организационных мероприятий на объектах информатизации. ***Уметь:*** Выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации на объектах информатизации и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Осуществлять выбор технических средств защиты информации в зависимости от условий эксплуатации объектов информатизации. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками применения технических средств защиты информации, обрабатываемой в сетях ЭВМ.
	ПК-3.5	**Знать**:	**Знать**:	**Знать:** устройство

	Осуществляет установку и управление специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа	используемые в работе с ОС программные средства **Уметь**: использовать в работе с ОС программные средства разработки ПО и администрирования **Владеть навыками**: навыками работы с информационно-техническими средствами	инструментальные средства проведения проверок информационных систем **Уметь**: анализ кода программных средств защиты информации **Владеть навыками**: методы проектирования информационных систем с учетом требований информационной безопасности	межсетевых экранов, технологию оценки состояния защищенности, совместимость программно-аппаратных средств и варианты обеспечения разграничения доступа на уровне операционной системы и прикладных средств. **Уметь:** настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети ***Владеть:*** навыками эксплуатации и разработки программно-аппаратных средств обеспечения защиты передаваемых в масштабе вычислительной
ПК-4, основной	ПК-4.3 Использует современные отечественные и зарубежные пакеты программ при решении схемотехнических, системных и сетевых задач, правила и	***Знать:*** основы работы с программным обеспечением при решении схемотехнических и системных задач связи. ***Уметь:*** настраивать существующие каналы связи. ***Владеть:*** навыками регулировки узлов радиотехнических устройств.	***Знать:*** основы современных пакетов программ при решении и сетевых задач по организации взаимодействия удаленных абонентов. ***Уметь:*** настраивать существующие каналы связи, расширять и	***Знать:*** особенности современных пакетов программ при решении схемотехнических, системных и сетевых задач по организации сетевого взаимодействия. ***Уметь:*** оптимизировать трафик и обеспечивать

	методы монтажа, настройки и регулировки узлов радиотехнических устройств и систем		администрировать локальную вычислительную сеть ***Владеть:*** навыками монтажа и настройки узлов систем связи.	уверенный прием в случае использования беспроводного доступа. ***Владеть:*** навыками монтажа, настройки и регулировки узлов радиотехнических устройств и систем.

7.3Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Проблемы информационной безопасности сетей	ПК-3	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР №1	1-12 1-4	Согласно таблице 7.2
2	Политика безопасности	ПК-3	Лекция, СРС	Собеседование	13-15	Согласно таблице 7.2
3	Технологии аутентификации	ПК-3	Лекция, СРС	Собеседование	16-21	Согласно таблице 7.2
4	Технологии межсетевых экранов	ПК-3	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР №2	22-24 1-5	Согласно таблице 7.2
5	Технологии защиты от вирусов	ПК-3	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР №3	25-32 1-4	Согласно таблице 7.2
6	Технологии анализа защищенности и обнаружения сетевых атак	ПК-3	Лекция, СРС	Собеседование	33-36	Согласно таблице 7.2

7	Требования к системам защиты информации	ПК-3	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР №4	37-41 1-8	Согласно таблице 7.2
8	Аудит безопасности информационных систем	ПК-3	Лекция, СРС	Собеседование	42-45	Согласно таблице 7.2
9	Разработка и защита Web-сайтов	ПК-3	Лекция, СРС	Собеседование	46-48	Согласно таблице 7.2

СРС – самостоятельная работа студента,
КВЗЛР – контрольные вопросы для защиты лабораторных работ,

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы собеседования по разделу (теме) 4. «Технологии межсетевых экранов»:

1. Основные функции и дополнительные возможности межсетевых экранов. Политика работы МЭ.
2. Особенности функционирования межсетевых экранов на уровнях модели OSI. Варианты исполнения МЭ.
3. Основные схемы подключения межсетевых экранов

Контрольные вопросы к лабораторной работе №2 «Настройка межсетевого экрана в операционной системе Windows»:

1) Что такое брандмауэр?
2) Какие бывают брандмауэры?
3) Что фиксирует журнал безопасности брандмауэра?
4) Перечислите основные требования к выбираемым средствам анализа защищенности.
5) Дайте общий обзор современных средств анализа защищенности.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Основной защитой от фишинга являются:

1. Фильтры.
2. Антивирусные программы.
3. Криптографические системы.
4. Системы видеонаблюдения.

Задание в открытой форме:

1. Режим, при котором передача и прием данных происходят одновременно, это …

2. Режим, при котором передача и прием данных происходят по очереди,это …

3. Режим, при котором происходит только передача или только прием данных, это …

Задание на установление правильной последовательности.

Расположить параметры для группировки данных на сервере сбора информации об атаке:

1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

Задание на установление соответствия:

Выберите соответствие между названиями и определениями уровней модели OSI:

1	Прикладной уровень	А	обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений
2	Сетевой уровень	Б	уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью
3	Уровень представления	В	предназначен для обеспечения надёжной передачи данных от отправителя к получателю
4	Канальный уровень	Г	определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому.
5	Физический уровень	Д	предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля ошибок, которые могут возникнуть.
6	Сеансовый уровень	Е	предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.
7	Транспортный уровень	Ж	обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время

Компетентностно-ориентированная задача:

Создать топологию, состоящую из маршрутизатора, к которому подключены 2 компьютера. Между ПК 1 и маршрутизатором подсеть 172.16.0.0, ПК 2 и маршрутизатором подсеть 192.168.0.0. Проверить доступность компьютеров (ПК) с помощью команды ping. Создать Access

list, запрещающий прохождений icmp-пакетов из подсети 192.168.0.0. Выполнить команду ping с ПК 1 на ПК 2 и с ПК2 на ПК 1.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 Обалльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Лабораторная работа №1	1	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Лабораторная работа №2	1	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Лабораторная работа №3	1	Выполнил, доля правильных ответов от 50% до 90%	5	Доля правильных ответов более 90%
Лабораторная работа №4	1	Выполнил, доля правильных ответов от 50% до 90%	5	Доля правильных ответов более 90%
Собеседование по теме 1	1	Доля правильных ответов от 50% до	2	Доля правильных ответов более 90%

		90%		
Собеседование по теме 2	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Собеседование по теме 3	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Собеседование по теме 4	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Собеседование по теме 5	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Собеседование по теме 6	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Собеседование по теме 7	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Собеседование по теме 8	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Собеседование по теме 9	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Итого	13		36	
Посещаемость	0		14	
Зачёт	0		60	
Итого	13		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме –3 балла,
– задание в открытой форме – 3 балла,
– задание на установление правильной последовательности – 3 балла,
– задание на установление соответствия – 3 балла,
– решение компетентностно-ориентированной задачи – 15 баллов.

Максимальное количество баллов за тестирование – 60 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1) Пролубников, А. В. Сети передачи данных : учебное пособие : в 2 частях / А. В. Пролубников. – Омск : Омский государственный университет

им. Ф.М. Достоевского, 2020. – Ч. 1. – 116 с. – URL: https://biblioclub.ru/index.php?page=book&id=614062 . – Режим доступа : по подписке. – Текст : электронный.

2) Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.– URL: https://biblioclub.ru/index.php?page=book&id=429035. – Режим доступа : по подписке. – Текст : электронный.

3) Васяева, Н. С. Проектирование локальных вычислительных сетей: учебное пособие для курсового проектирования / Н. С. Васяева, Е. С. Васяева. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 94 с. – URL: https://biblioclub.ru/index.php?page=book&id=560566. – Режим доступа : по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

4) Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. – Минск : РИПО, 2019. – 180 с. – URL: https://biblioclub.ru/index.php?page=book&id=599948. – Режим доступа : по подписке. – Текст : электронный.

5) Сети и системы телекоммуникаций: учебное электронное издание / В. А. Погонин, А. А. Третьяков, И. А. Елизаров, В. Н. Назаров. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 197 с.– URL: https://biblioclub.ru/index.php?page=book&id=570531 . – Режим доступа : по подписке. – Текст : электронный.

6) Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. – URL: https://biblioclub.ru/index.php?page=book&id=429032. – Режим доступа : по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1) Изучение существующих каналов утечки информации: методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 11 с. - Текст : электронный.

2) Настройка межсетевого экрана в операционной системе Windows : методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 23 с. - Текст : электронный.

3) Антивирусная программа: Kaspersky Internet Security : методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 13 с. - Текст : электронный.

4) Анализ защищенности компьютерной сети с помощью программ GFI Languard, Network Security Scanner и XSPIDER : методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 12 с. - Текст : электронный.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.»- http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку,

способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в

письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14.Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изме-нённых	Заменённых	Аннулированных	новых			