Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

КАФЕДРА ФИНАНСОВОГО МОНИТОРИНГА

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-2/1

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
3	4	144	32	0	16		60	0	Э КП
Итого	4	144	32	0	16	0	60	0	

АННОТАЦИЯ

Дисциплина посвящена освоению технологий, методов и средств обеспечения информационной безопасности объектов в открытых и корпоративных сетях.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является изучение технологий, методов и средств обеспечения информационной безопасности объектов на примере интернета и интранета.

Задачами дисциплины являются:

- привитие обучаемым основ культуры обеспечения ИБ объектов;
- формирование у обучаемых понимания технологий обеспечения ИБ объектов;
- ознакомление обучаемых с основными практическими приемами построения защиты объектов;
- обучение различным средствам обеспечения ИБ ИС.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыки, сформированные в процессе:

− изучения программы общеобразовательной школы;

− освоения программы подготовки бакалавров или программ подготовки специалистов по родственным направлениям высшего профессионального образования;

- изучения дисциплин: «Специальные технологии баз данных и экспертных систем», «Информационные ресурсы в государственно финансовом мониторинге», «Информационные ресурсы в первичном финансовом мониторинге», "Интеллектуальный анализ данных и процессов".

В свою очередь дисциплина обеспечивает необходимую подготовку студентов для производственной практики, дипломного проектирования и подготовки выпускной квалификационной работы.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС,**	**Код и наименование индикатора достижения профессиональной компетенции**

		анализ опыта)	
проектный			
Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности, согласованных со стратегией развития информационных систем; обоснование выбора принципов организации и функциональной структуры программного, программно-аппаратного и технического обеспечения систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и международных стандартов; проектирование и разработка систем, комплексов, средств и технологий обеспечения информационной безопасности; разработка программ и методик испытаний программных, программноаппаратных и технических средств и систем обеспечения информационной безопасности; разработка и применение автоматизированных технологии обработки больших информационных	Система обеспечения информационной безопасности и информационно-аналитического обеспечения финансового мониторинга	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.033	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы

потоков (массивов) финансовой и/или экономической информации в режиме реального времени.			утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами

			предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности, согласованных со стратегией развития информационных систем; обоснование выбора принципов организации и функциональной структуры программного, программно-аппаратного и технического обеспечения систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и международных стандартов; проектирование и разработка систем, комплексов, средств и технологий обеспечения информационной безопасности; разработка программ и методик испытаний программных,	Система обеспечения информационной безопасности и информационно-аналитического обеспечения финансового мониторинга	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.033	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного

программноаппаратных и технических средств и систем обеспечения информационной безопасности; разработка и применение автоматизированных технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени.			доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа.; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее.; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных

			средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	3 Семестр						
1	Виртуальные частные сети (VPN)	1-8	16/0/8	ЛР-4 (10),ЛР-7 (15)	25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2
2	Средства обеспечения ИБ в открытых системах	9-16	16/0/8	ЛР-11 (10),ЛР-13 (15)	25	КИ-16	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2,

							В-ПК-2
	Итого за 3 Семестр		32/0/16		50		
	Контрольные мероприятия за 3 Семестр				50	Э, КП	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
ЛР	Лабораторная работа
КИ	Контроль по итогам
Э	Экзамен
КП	Курсовой проект

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	3 Семестр	32	0	16
1-8	**Виртуальные частные сети (VPN)**	16	0	8
1	**Тема № 1. Введение.** Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Состав и классификация средств обеспечения ИБ объектов.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
2 - 3	**Тема № 2. Базовые сведения о VPN.** Различные подходы к определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Классификация VPN. Специфика построения VPN. Критерии, предъявляемые к VPN. Классификация VPN компании Check Point по типу устанавливаемых соединений: Intranet VPN, Client\Server VPN, Extranet VPN, Remote Access VPN – определения, характерные черты и особенности использования. Классификация VPN	Всего аудиторных часов		
		4	0	2
		Онлайн		
		0	0	0

	согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN – определения, требования, технологии построения. VPN в сетях общего пользования. Специфика использования VPN в сетях Frame Relay, ATM, X.25, TCP/IP. Политики безопасности VPN. Основные варианты создания VPN: защищенные, частные и промежуточные каналы. Варианты политик безопасности при использовании каналов Internet для построения VPN. Интеграция VPN и дополнительных средств защиты: использование PKI, криптографические модули, аудит, антивирусные средства и т.д.			
4	**Тема № 3. Туннелирование.** Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPN-агентов. Обработка входящих и исходящих пакетов. Различные варианты позиционирования и использования VPN-агентов.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
5	**Тема № 4. Варианты построения VPN.** VPN на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств – основные характеристики, сравнительный анализ.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
6	**Тема № 5. Протоколы создания VPN 2-го уровня модели OSI.** Протокол PPTP. Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000. Протокол L2TP. Основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP/IPSec инкапсуляция данных. Обработка входящих и исходящих данных. Настройка VPN на базе протокола L2TP в среде Windows.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
7	**Тема № 6. Протоколы создания VPN 3-го уровня модели OSI.** Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция данных в транспортном и туннельном	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0

	режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка при использовании AH в транспортном режиме. Обработка исходящих (поиск SA, генерация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на соответствие записи в SPD) пакетов. Использование комбинированных криптографических алгоритмов в ESP. Особенности использования расширенных (64-битных) порядковых номеров. Защита от повторной передачи пакетов. Согласование параметров безопасности с использованием протокола IKE. Порядок обмена сообщениями IKE. Сообщения IKE_SA_INIT для согласования параметров безопасности IKE_SA и обмена по протоколу Диффи-Хеллмана. Сообщения IKE_AUTH для аутентификации и установления CHILD_SA для защиты данных с помощью AH или ESP. Сообщения CREATE_CHILD_SA для согласования дополнительных CHILD_SA в рамках данной IKE_SA. Сообщения INFORMATIONAL для сообщения информации о текущем состоянии или ошибках. Детали работы протокола (согласование версий протокола, использование порядковых номеров, генерирование ключевого материала, обработка ошибок и т.д.). Форматы основного заголовка IKE и заголовков сообщений.			
8	**Тема № 7. Протоколы создания VPN 5-го уровня модели OSI.** Протоколы создания VPN 5-го уровня модели OSI SSL/TLS.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
9-16	**Средства обеспечения ИБ в открытых системах**	16	0	8
9	**Тема № 8. Базовые сведения о межсетевых экранах (МЭ).** Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Персональные МЭ. Основные компоненты МЭ. Слабости МЭ. Выбор реализаций МЭ.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
10	**Тема № 9. Примеры МЭ.** Маршрутизаторы Cisco. Назначение и основные характеристики. Операционная система. Интерфейсы маршрутизаторов. Основные разделы и подразделы меню комплекса межсетевых экранов ФПСУ-IP. Идентификация и аутентификация комплекса в сети. Удаленное администрирование. Построение VPN на базе комплекса. Комплекс ФПСУ-IP-клиент.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
11	**Тема № 10. Аудит и мониторинг ИБ в открытых системах.**	Всего аудиторных часов		
		2	0	1

	Методы отражения вторжений: предотвращение, прерывание, сдерживание, отклонение, обнаружение, устранение последствий.	Онлайн		
		0	0	0
12	**Тема № 11. Средства анализа защищенности.** САЗ и их место в защите открытых систем. Классификации САЗ. Сетевые сканеры: размещение агентов, принципы работы, этапы работы; сравнение современных реализаций. Системные сканеры. САЗ для приложений. Критерии выбора САЗ.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
13	**Тема № 12. Системы обнаружения/предотвращения вторжений.** Классификация и структура СОВ/СПВ. Системные и сетевые СОВ/СПВ: принципы работы, достоинства и недостатки. Размещение сетевых СОВ/СПВ. Интеллектуальные и поведенческие СОВ. Обнаружение вторжений/злоупотреблений; обнаружение аномалий/сопоставление с образцом. СОВ, их выбор, применение, ограниченность и примеры систем. СПВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
14	**Тема № 13. Виды виртуальных локальных сетей.** VLAN с группировкой портов, VLAN с маркированными кадрами, VLAN на основе протоколов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимущества VLAN.	Всего аудиторных часов		
		2	0	1
		Онлайн		
		0	0	0
15 - 16	**Тема № 14. Защита от спама. Тема № 15. Другие средства защиты информации.** Защита от спама в электронной почте: определение, методы детектирования, архитектура защищенной от спама электронной почты, примеры систем. Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы обеспечения ИБ на уровне предприятия.	Всего аудиторных часов		
		4	0	2
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	3 Семестр

1 - 4	**Лабораторная работа №1. Построение виртуальных частных сетей средствами ОС Windows. Шифрование файловой системы. Удалённое управление по протоколу SSH.** Ознакомление с построением VPN средствами ОС Windows – поддерживаемыми этой ОС протоколами PPTP, L2TP, IPsec. Изучение и практическое применение шифрованной файловой системы LUKS. Изучение и практическое применение протокола удалённого управления ОС SSH.
5 - 8	**Лабораторная работа №2. Система аутентификации, учёта и аудита.** Изучение и практическое применение auditd, syslog, PAM.
9 - 11	**Лабораторная работа №3. Изучение средств анализа защищенности сетей и систем обнаружения/предотвращения вторжений.** Получение практических навыков работы со средствами анализа защищенности и с системами обнаружения вторжений.
12 - 15	**Лабораторная работа №4 . Построение виртуальных частных сетей на основе программно-аппаратных комплексов ФПСУ-IP.** Изучение и практическое применение программно-аппаратного комплекса ФПСУ-IP как МЭ.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

С целью формирования и развития профессиональных навыков студентов в курсе используются активные и интерактивные формы проведения занятий: доклады и презентации с их обсуждением, ролевые игры с дискуссиями и разбором конкретных ситуаций в сочетании с внеаудиторной работой. В процессе преподавания дисциплины в каждом разделе выделяются наиболее важные темы и внимание обучаемых особо акцентируется на них. В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, разработчиками систем защиты информации для сетей, мастер-классы экспертов и специалистов в области сетевой безопасности.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-1	З-ПК-1	КП, Э, КИ-8, КИ-16, ЛР-4, ЛР-7, ЛР-11, ЛР-13
	У-ПК-1	КП, Э, КИ-8, КИ-16, ЛР-4, ЛР-7, ЛР-11, ЛР-13
	В-ПК-1	КП, Э, КИ-8, КИ-16, ЛР-4, ЛР-7, ЛР-11, ЛР-13
ПК-2	З-ПК-2	КП, Э, КИ-8, КИ-16, ЛР-4, ЛР-7, ЛР-11, ЛР-13
	У-ПК-2	КП, Э, КИ-8, КИ-16, ЛР-4, ЛР-7, ЛР-11, ЛР-13

	В-ПК-2	КП, Э, КИ-8, КИ-16, ЛР-4, ЛР-7, ЛР-11, ЛР-13

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ С 89 Информационная безопасность : учебное пособие для вузов, Суворова Г. М., Москва: Юрайт, 2023

2. 004 И74 Информационная безопасность открытых систем Т.1 Угрозы, уязвимости, атаки и подходы к защите, , : Горячая линия - Телеком, 2006

3. 004 И74 Информационная безопасность открытых систем Т.2 Средства защиты в сетях, , Москва: Горячая линия-Телеком, 2008

4. ЭИ Б 27 Сетевая информационная безопасность : учебник, Басыня Е.А., Москва: НИЯУ МИФИ, 2023

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. ЭИ Т 83 Комплексное обеспечение информационной безопасности на предприятии : учебник для вузов, Петровский М. В., Тумбинская М. В., Санкт-Петербург: Лань, 2022

2. 004 О-75 Основы организации сетей Cisco Т.1 , , М.[и др.]: Вильямс, 2004

3. 004 О-75 Основы организации сетей Cisco Т.2 , , М.[и др.]: Вильямс, 2004

4. 004 З-31 Основы построения виртуальных частных сетей : учебное пособие для вузов, Милославская Н.Г., Запечников С.В., Толстой А.И., Москва: Горячая линия - Телеком, 2011

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. ФСТЭК России (http://www.fstec.ru)

2. Средства защиты информации. (http://www.analitika.info)

3. Ресурсы по методологии и программным продуктам ARIS (http://www.ariscommunity.com/aris-express/tutorials -)

4. Gartner - аналитический ресурс в области ИТ (http://www.gartner.com)

5. Открытые системы (http://www.osp.ru)

6. Обучающие статьи о Computer Science и использование классических алгоритмов и структур данных в реше (https://tproger.ru/tag/algorithms/)

7. ИС "Единое окно доступа к образовательным ресурсам" (http://window.edu.ru/)

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Основными видами учебных занятий в процессе преподавания дисциплины являются лекции и лабораторные работы.

Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:

- изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);

- выполнение необходимых расчетов и экспериментов; оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным заданиям и теоретическим расчетам;

- по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала.

Контроль усвоения теоретического материала является индивидуальным.

Под самостоятельной работой студентов понимается планируемая учебная, учебно-исследовательская, а также научно-исследовательская работа студентов, которая выполняется во внеаудиторное время по инициативе студента или по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Основными видами самостоятельной учебной деятельности студентов высшего учебного заведения являются:

1) предварительная подготовка к аудиторным занятиям, в том числе и к тем, на которых будет изучаться новый, незнакомый материал. Предполагается изучение учебной программы и анализ наиболее значимых и актуальных проблем курса.

2) Своевременная доработка конспектов лекций;

3) Подбор, изучение, анализ и при необходимости – конспектирование рекомендованных источников по учебным дисциплинам;

4) подготовка к контрольным занятиям, зачетам и экзаменам;

5) выполнение специальных учебных заданий, предусмотренных учебной программой, в том числе рефератов, курсовых, контрольных работ

Все виды самостоятельной работы дисциплине могут быть разделены на основные и дополнительные.

К основным (обязательным) видам самостоятельной работы студентов относятся:

а) самостоятельное изучение теоретического материала,

б) решение задач к семинарским занятиям,

в) выполнение письменных заданий к семинарским занятиям,

г) подготовка ролевых игр

Дополнительными видами самостоятельной работы являются:

а) выполнение курсовых работ

б) подготовка докладов и сообщений для выступления на семинарах;

Данные виды самостоятельной работы не являются обязательными и выполняются студентами по собственной инициативе с предварительным согласованием с преподавателем.

Источниками для самостоятельного изучения теоретического курса выступают:

- учебники по предмету;

- курсы лекций по предмету;

- учебные пособия по отдельным темам

- научные статьи в периодической юридической печати и рекомендованных сборниках;
- научные монографии.

Умение студентов быстро и правильно подобрать литературу, необходимую для выполнения учебных заданий и научной работы, является залогом успешного обучения. Самостоятельный подбор литературы осуществляется при подготовке к семинарским, практическим занятиям, при написании контрольных курсовых, дипломных работ, научных рефератов.

Положительный результат может быть достигнут только при условии комплексного использования различных учебно-методических средств, приемов, рекомендуемых преподавателями в ходе чтения лекций и проведения лабораторных работ, систематического упорного труда по овладению необходимыми знаниями, в том числе и при самостоятельной работе.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

При изучении дисциплины рекомендуется использовать следующие средства обучения:
- программу учебного курса:
- рекомендуемую основную и дополнительную литературу;
- методические указания, пособия и учебники (в бумажном виде);
- задания для самостоятельной работы для закрепления теоретического материала;
- описания лабораторных работ и контрольные вопросы к ним;
- методическое обеспечение текущего и итогового контроля знаний.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечение по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и лабораторных работах.

Принципы отбора содержания и организации учебного материала дисциплины

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе выполнения лабораторных работ и самостоятельных занятий. Данная дисциплина выполняет функции теоретической и практической подготовки студентов. В нем заложен деятельностный компонент, наиболее ярко проявляющийся в системе практических лабораторных занятий.

Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и носят ярко выраженный творческий характер. В лекционном курсе главное место отводится общетеоретическим проблемам. Практические занятия рекомендуется использовать для выработки у студентов практических навыков защиты в открытых системах.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

- самостоятельное ознакомление студентов с теоретическим материалом, представленным в основной литературе;

- самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

- подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области обеспечения ИБ, а также российских и зарубежных компаний – разработчиками средств обеспечения ИБ.

За основу логического прохождения курса приняты следующие положения.

1. Изложение теоретических основ курса начинается с изучения базовые сведения о технологиях обеспечения ИБ объектов.

2. Далее в качестве одного из базовых вариантов построения ВЧС рассматривается межсетевой экран.

3. После определения основного предмета изучения вводит понятийный аппарат, используемый при дальнейшем изложении, а именно классы ВЧС, туннелирование, схемы построения ВЧС, политика ИБ для ВЧС, стандартные протоколы построения ВЧС и т.д.

4. Также изучается также часто применяемый вид виртуальных сетей – виртуальные локальные сети.

5. Далее рассматриваются САЗ и СОВ/СПВ и другие средства обеспечения ИБ объектов.

Теоретические положения курса подкрепляются иллюстрациями и выработкой практических навыков при выполнении студентами лабораторных работ по всем основным темам курса.

Автор(ы):

Рычков Вадим Александрович