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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 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**
1	3	108	8	0	24		40	0	Э
Итого	3	108	8	0	24	0	40	0	

Москва, 2020

АННОТАЦИЯ

Дисциплина «Технологии обеспечения информационной безопасности объектов» реализует требования государственного образовательного стандарта по специальности 10.04.01 «Информационная безопасность» (квалификация (степень) выпускника «Магистр») и содействует формированию у студентов профессиональных компетенций, необходимых для решения задач, относящихся к определенному виду профессиональной деятельности.

Курс занимает важное место в общей системе профильной подготовки выпускника, являясь своего рода мостом, связывающим общенаучные и общеобразовательные дисциплины с профильными для будущего специалиста курсами.

В свою очередь дисциплина обеспечивает необходимую подготовку студентов для дипломного проектирования.

Целью преподавания дисциплины является: изучение технологий, методов и средств обеспечения информационной безопасности (ИБ) 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.

Таким образом, дисциплина «Технологии обеспечения информационной безопасности объектов» является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность». Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина реализует требования государственного образовательного стандарта по специальности 10.04.01 «Информационная безопасность» (квалификация (степень) выпускника «Магистр») и содействует формированию у студентов профессиональных компетенций, необходимых для решения задач, относящихся к определенному виду профессиональной деятельности.

Курс занимает важное место в общей системе профильной подготовки выпускника, являясь своего рода мостом, связывающим общенаучные и общеобразовательные дисциплины с профильными для будущего специалиста курсами.

В свою очередь дисциплина обеспечивает необходимую подготовку студентов для дипломного проектирования.

Целью преподавания дисциплины является: изучение технологий, методов и средств обеспечения информационной безопасности (ИБ) 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.

Таким образом, дисциплина «Технологии обеспечения информационной безопасности объектов» является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность». Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Технологии обеспечения информационной безопасности объектов» реализует требования государственного образовательного стандарта по специальности 10.04.01 «Информационная безопасность» (квалификация (степень) выпускника «Магистр») и содействует формированию у студентов профессиональных компетенций, необходимых для решения задач, относящихся к определенному виду профессиональной деятельности.

Курс занимает важное место в общей системе профильной подготовки выпускника, являясь своего рода мостом, связывающим общенаучные и общеобразовательные дисциплины с профильными для будущего специалиста курсами.

В свою очередь дисциплина обеспечивает необходимую подготовку студентов для дипломного проектирования.

Целью преподавания дисциплины является: изучение технологий, методов и средств обеспечения информационной безопасности (ИБ) 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.

Таким образом, дисциплина «Технологии обеспечения информационной безопасности объектов» является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность». Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях,
- творческое мышление,

- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-4 [1] – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	З-УК-4 [1] – Знать: правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном языках; существующие профессиональные сообщества для профессионального взаимодействия У-УК-4 [1] – Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия В-УК-4 [1] – Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий

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, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.030, 06.032, 06.033, 06.034	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 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).
Проектирование систем обеспечения информационной	Средства и технологии обеспечения	ПК-2 [1] - Способен разрабатывать технические задания	З-ПК-2[1] - Знать: формальные модели безопасности

безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	безопасности значимых объектов критической информационной инфраструктуры	на проектирование систем обеспечения ИБ иди информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	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 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
	1 Семестр						
1	Раздел 1	1-8	4/0/12		25	КИ-8	З-ПК-1, У-ПК-1, З-ПК-2, У-ПК-2, З-УК-4, У-УК-4
2	Раздел 2	9-16	4/0/12		25	КИ-16	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-4, У-УК-4, В-

							УК-4
	Итого за 1 Семестр		8/0/24		50		
	Контрольные мероприятия за 1 Семестр				50	Э	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-4, У-УК-4, В-УК-4

* – 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**
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	1 Семестр	8	0	24
1-8	**Раздел 1**	4	0	12
1 - 3	**Межсетевые экраны (МЭ)** Введение. Базовые сведения о межсетевых экранах (МЭ). Примеры МЭ.	Всего аудиторных часов		
		2		4
		Онлайн		
4 - 5	**Виртуальные частные сети (VPN)** Базовые сведения о VPN. Туннелирование. Варианты построения VPN.	Всего аудиторных часов		
		1		4
		Онлайн		
6 - 8	**Стандартные протоколы создания VPN** Протоколы создания VPN 2-го уровня модели OSI. Протоколы создания VPN 3-го уровня модели OSI.	Всего аудиторных часов		
		1		4
		Онлайн		
9-16	**Раздел 2**	4	0	12

9 - 10	**Стандартные протоколы создания VPN** Протоколы создания VPN 5-го уровня модели OSI.	Всего аудиторных часов		
		1		2
		Онлайн		
11	**Базовые сведения о виртуальных локальных сетях (VLAN)** 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		
		1		4
		Онлайн		
12 - 15	**Адаптивное управление ИБ объектов** Аудит и мониторинг ИБ в открытых системах. 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. Методы отражения вторжений: предотвращение, прерывание, сдерживание, отклонение, обнаружение, устранение последствий. Системы обнаружения/предотвращения вторжений (СОВ/СПВ). 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		
		1		4
		Онлайн		
16	**Другие средства обеспечения ИБ в открытых системах** Защита от спама. Защита от спама в электронной почте: определение, методы детектирования, архитектура защищенной от спама электронной почты, примеры систем. Другие средства защиты информации Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы обеспечения ИБ на уровне предприятия.	Всего аудиторных часов		
		1		2
		Онлайн		

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
	1 Семестр
	Лабораторная работа 1. «Построение виртуальных частных сетей средствами ОС Windows. Шифрование файловой системы. Удалённое управление по протоколу SSH» 1. Цель: • 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. 2. Оборудование: компьютерный класс; лабораторный стенд под ОС Windows SP. 3. Требования по предварительной подготовке студентов. Для успешного выполнения лабораторной работы необходимо: • иметь представления о протоколах PPTP, L2TP, IPsec и средствах управления ОС Windows; • иметь представления о протоколах принципах сетевого взаимодействия, стеке протоколов TCP/IP и маршрутизации в IP-сетях; • иметь представления о принципах работы ассиметричной криптографии; • иметь навыки работы в UNIX-подобных системах; • изучить руководства к утилитам (команда man), а также представленные в списке литературы. 4. Этапы выполнения работы. Лабораторная работа – это групповое занятие студентов под руководством преподавателя, направленное на выработку и закрепление профессиональных умений и навыков. Во время проведения лабораторных работ особое внимание уделяется активизации самостоятельной работе студентов над задачами. На лабораторную работу отводится 4 часа. Основные этапы работы: 1) Ознакомление с методическим пособием; 2) Выполнение заданий: PPTP, L2TP, IPsec: • Ознакомление с теорией по протоколам, представленной в ПО ZSPs. • Настройка серверной части протокола PPTP. • Настройка клиентской части протокола PPTP. • Настройка серверной части протокола L2TP. • Настройка клиентской части протокола L2TP. • Настройка серверной части протокола IPsec.

	• Настройка клиентской части протокола IPsec. SSH: • Изучение протокола SSH на примере OpenSSH. • Настройка OpenSSH для аутенфикации по открытому ключу. Для этого объединитесь в пары, сгенерируйте и обменяйтесь открытыми ключами при помощи команд, указанных выше. Проверьте работоспособность при помощи клиента ssh. Убедитесь в том, что трафик между компьютерами зашифрован при помощи tcpdump. • Передайте файл с одного компьютера на другой при помощи программы scp. С помощью сниффера tcpdump убедитесь, что файл не передаётся по сети в открытом виде. • Передайте файл с одного компьютера на другой при помощи sftp. • Настройте туннелирование трафика по протоколу SSH. Шифрование файловой системы: • Создайте шифрованную файловую систему в произвольном файле. • Скопируйте в созданную ФС несколько текстовых файлов. Просмотрите содержимое файла, содержащего шифрованную ФС и убедитесь, что данные не читаемы. 1) Подготовка отчета о выполненной работе и защита результатов работы перед преподавателем посредством демонстрации соответствующих пяти заданиям экранов компьютеров и комментариев к ни.
	Лабораторная работа 2. Система аутентификации, учёта и аудита» 1. Цель: • изучение и практическое применение auditd, syslog, PAM. • Оборудование: компьютерный класс; лабораторный стенд под ОС Windows SP. 2. Требования по предварительной подготовке студентов. Для успешного выполнения лабораторной работы необходимо: • иметь представления об архитектуре UNIX-подобных ОС; • иметь навыки работы в UNIX-подобных системах; • изучить руководства к утилитам (команда man), а также материалы, представленные в списке литературы. 3. Этапы выполнения работы. Лабораторная работа – это групповое занятие студентов под руководством преподавателя, направленное на выработку и закрепление профессиональных умений и навыков. Во время проведения лабораторных работ особое внимание уделяется активизации самостоятельной работе студентов над задачами. На лабораторную работу отводится 4 часа. Основные этапы работы: 1) Ознакомление с методическим пособием;

	2) Выполнение рабочих заданий: PAM: • Настройте парольную политику в соответствии со стандартом PCI DSS. • Изменение пароля пользователя не реже одного раза в 90 дней. • При смене пароля запрещается выбор в качестве нового какого-либо из последних четырех использовавшихся данным пользователем паролей. • Блокирование учетной записи после шести неудачных попыток ввода пароля. • Блокирование учетной записи пользователя не менее чем на 30 минут, либо пока администратор не снимет блокировку. • Использование в пароле не менее семи символов. • Использования в пароле как цифр, так и букв. Система аудита: • Настройте auditd для регистрации событий изменения системной даты и/или времени. Для этого вам потребуется отслеживать следующие системные вызовы: adjtimex(), settimeofday(), stime(), clock_settime(). Кроме того, необходимо отслеживать изменения файла /etc/localtime. • Проверьте работоспособность правила при помощи команды date. • Настройте auditd для регистрации событий загрузки/выгрузки модулей ядра. Для этого вам потребуется отслеживать исполнение следующих файлов: /sbin/insmod, /sbin/rmmod, /sbin/modprobe. Кроме того, необходимо отслеживать системные вызовы init_module() и delete_module(). • Проверьте работоспособность правила. • Получите отчёт auditd, демонстрирующий выполнение предыдущих заданий. Продемонстрируйте преподавателю. Syslog: • Настройте отправку событий с auditd на удаленный сервер. 3) Подготовка отчета о выполненной работе и защита результатов работы перед преподавателем посредством демонстрации соответствующих пяти заданиям экранов компьютеров и комментариев к ним.
	Лабораторная работа 3. «Изучение средств анализа защищенности сетей и систем обнаружения/предотвращения вторжений» 1. Цель: • получить практические навыки работы со средствами анализа защищенности; • получить практические навыки работы с системами обнаружения вторжений. • Оборудование: компьютерный класс; лабораторный стенд под ОС Windows SP. 2. Требования по предварительной подготовке студентов. Для успешного выполнения лабораторной работы

	необходимо: • иметь представления о принципах сетевого взаимодействия, стеке протоколов TCP/IP и маршрутизации в IP-сетях; • иметь навыки работы в UNIX-подобных системах; • изучить руководства к утилитам (команда man), а также представленные в списке литературы. 3. Этапы выполнения работы. 1) Ознакомление с методическим пособием; 2) Выполнение рабочих заданий: • Опробовать на практике настройку и поиск уязвимостей предлагаемым преподавателем сканером. Проэксплуатировать найденные уязвимости. • Опробовать на практике настройку и поиск несанкционированных действия с помощью СОВ Snort. С помощью СОВ обнаружить сканирование портов и эксплуатацию уязвимости MS08-067. 3) Подготовка отчета о выполненной работе и защита результатов работы перед преподавателем посредством демонстрации соответствующих пяти заданиям экранов компьютеров и комментариев к ним.
	Лабораторная работа 4. «Построение виртуальных частных сетей на основе программно-аппаратных комплексов ФПСУ-IP» 1. Цель: • изучение и практическое применение программно-аппаратного комплекса ФПСУ-IP как МЭ. 2. Оборудование: компьютерный класс Оборудование: компьютерный класс; лабораторный стенд. 3. Требования по предварительной подготовке студентов. Для успешного выполнения лабораторной работы необходимо: • иметь представления о принципах сетевого взаимодействия, стеке протоколов TCP/IP и маршрутизации в IP-сетях; • иметь навыки работы в командной строке. 4. Этапы выполнения работы. 1) Ознакомление с методическим пособием; 2) Выполнение рабочих заданий: • Управление администраторами. • Управление начальной загрузкой. • Организация работы ключевой системы. • Настройка сетевых адаптеров. • Режимы отображения при запущенном комплексе. • Настройка портов. • Групповые политики. • Удалённый администратор –конфигурирование, администрирование. • Взаимодействие комплекса с сетевым оборудованием. • Комплексы ФПСУ-IP/Клиент. Центр Генерации Ключей Клиентов. Устройство VPN-key. • Взаимодействие со стандартными межсетевыми

	экранами (Kerio WinRoute firewall, MS ISA Client). 3) Подготовка отчета о выполненной работе и защита результатов работы перед преподавателем посредством демонстрации соответствующих пяти заданиям экранов компьютеров и комментариев к ним.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

С целью формирования и развития профессиональных навыков студентов в дисциплине используются активные и интерактивные формы проведения занятий: лабораторные работы и доклады и презентации с их обсуждением в сочетании с внеаудиторной работой.

В соответствии со спецификой ВУЗа в процессе преподавания дисциплины методически целесообразно в каждом разделе выделить наиболее важные темы и акцентировать на них внимание обучаемых.

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

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	Э, КИ-8, КИ-16
	У-ПК-1	Э, КИ-8, КИ-16
	В-ПК-1	Э, КИ-16
ПК-2	З-ПК-2	Э, КИ-8, КИ-16
	У-ПК-2	Э, КИ-8, КИ-16
	В-ПК-2	Э, КИ-16
УК-4	З-УК-4	Э, КИ-8, КИ-16
	У-УК-4	Э, КИ-8, КИ-16
	В-УК-4	Э, КИ-16

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.

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ П 84 Информационная безопасность и защита информации : учебное пособие, Санкт-Петербург: Лань, 2021

2. 004 М48 Информационная безопасность открытых систем : учебник, Москва: Флинта, 2013

3. ЭИ Д84 Оценка защищенности речевой информации Ч.1 Выявление акустических и вибрационных каналов утечки речевой информации, Москва: НИЯУ МИФИ, 2015

4. ЭИ Д84 Оценка защищенности речевой информации Ч.2 Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

5. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале акустоэлектромагнитного преобразования, Москва: НИЯУ МИФИ, 2018

6. ЭИ Д84 Оценка защищенности речевой информации Ч.4 Проведение инструментального контроля в канале высокочастотного навязывания, Москва: НИЯУ МИФИ, 2018

7. ЭИ Д84 Оценка защищенности речевой информации Ч.5 Проведение инструментального контроля в канале высокочастотного облучения, Москва: НИЯУ МИФИ, 2018

8. 004 М48 Системы и сети передачи данных : учебник, Москва: РадиоСофт, 2015

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

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

Общие рекомендации по изучению курса

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций, лабораторных работ и контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время лабораторных занятий, выполнения всех учебных заданий преподавателя, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Теория ИБ как наука использует свою терминологию,

категориальный, графический и математический аппараты, которыми студент должен научиться пользоваться и применять по ходу записи лекции. Культура записи лекции – один из важнейших факторов успешного и творческого овладения знаниями.

В конце лекции преподаватель оставляет время (5 минут) для того, чтобы студенты имели возможность задать уточняющие вопросы по изучаемому материалу.

Лекции имеют в основном обзорный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов, а также призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Перед выполнением лабораторных работ студент должен заранее изучить теоретический и учебно-методический материалы, относящиеся непосредственно к выполнению данной работы. После этого составляется план выполнения работы в соответствии с ее сценарием и готовятся рабочие материалы, необходимые для выполнения работы и для оформления отчета по ней. По имеющимся у студента контрольным вопросам осуществляется самоконтроль уровня подготовки к выполнению работы. При необходимости студент может обратиться к преподавателю за консультацией по вопросам, относящимся к выполнению данной лабораторной работы.

После допуска преподавателем студента к лабораторной работе, он выполняет все задания, готовит отчет и защищает его.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

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.

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 объектов.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Средства обеспечения освоения учебного курса

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.

Основные формы изучения дисциплины

Курс читается на 1 семестре.

Курс рассчитан на 108 часов, из которых 8 часов лекционных занятий, 24 часа лабораторных занятий (ЛР) и 40 часов самостоятельной работы (СР) студента.

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.

Обоснование логики прохождения учебного курса

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):

Мельников Дмитрий Анатольевич, к.т.н., с.н.с.