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

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

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	3	108	8	0	24		40	0	Э
2, 4	3	108	8	0	22		42	0	Э
Итого	6	216	16	0	46	12	82	0	

АННОТАЦИЯ

Целями освоения учебной дисциплины является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области выявления угроз и оценки уязвимости компьютерных систем и сетей, а также выработке эффективных мер противодействия целенаправленным атакам на них.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Задачами дисциплины являются:

- дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области защиты информации; основ реализации угроз безопасности информации и практической отработки методик выявления, реагирования и предотвращения целенаправленных атак на компьютерные системы и сети.

В результате обучения студенты должны ознакомиться с системой правовых, организационно-распорядительных, нормативных и информационных документов, определяющих организацию, правила и порядок построения компьютерных систем и сетей, а также деятельности в области контроля эффективности их защиты от целенаправленных атак

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками смежных дисциплин «Теоретические основы защиты информации в ключевых системах информационной инфраструктуры», «Организационно-правовые механизмы обеспечения информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Основы аттестации объектов информатизации».

Знания, полученные при изучении дисциплины «Методы и средства контроля эффективности защиты информации от несанкционированного доступа» являются базовыми

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, 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 безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-2.3 [1] - Способен устанавливать требования к обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ *Основание:* Профессиональный стандарт: 06.033, 06.034	З-ПК-2.3[1] - Знать: Отечественные стандарты в области информатизации и обеспечения информационной безопасности АСУ, информационных и телекоммуникационных систем общего и специального назначения; Основные принципы обеспечения безопасности КИИ; Основные положения ядерной безопасности; Причины возникновения инцидентов ядерной безопасности; Основные виды угроз для АСУ ТП на АЭС; Сущность основных физических процессов и информационных угроз в АСУ ТП в ядерном реакторе, их взаимосвязь; Требования по обеспечению безопасности значимых объектов КИИ.; У-ПК-2.3[1] - Уметь: Планировать, разрабатывать, совершенствовать и осуществлять внедрение мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Выявлять

			основные информационные угрозы в АСУ ТП ядерного реактора; Проводить оценку необходимости применения средств ядерной защиты реакторов. ; В-ПК-2.3[1] - Владеть: Навыками внедрения мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Навыками внедрения мероприятий по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности значимых объектов КИИ; Навыком обоснованного выбора средств защиты информации и средств ядерной защиты реакторов с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ; Навыком общего/детального анализа структуры системы безопасности значимого объекта КИИ.
организационно-управленческий			
Организация работы коллектива исполнителей, принятие	Контроль защищенности информации на объектах	ПК-2.4 [1] - Способен обеспечивать безопасность значимого объекта	З-ПК-2.4[1] - Знать: Принципы организации систем безопасности значимых объектов КИИ

управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	информатизации	КИИ на всех стадиях жизненного цикла *Основание:* Профессиональный стандарт: 06.031, 06.033, 06.034	и обеспечения их функционирования; Критерии обеспечения ядерной безопасности значимых объектов КИИ.; У-ПК-2.4[1] - Уметь: Анализировать данные, получаемые при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, признаков компьютерных атак.; В-ПК-2.4[1] - Владеть: Навыком проведения перспективных исследований в области информационной безопасности и ядерной защиты объектов КИИ; Навыком совершенствования системы безопасности значимых объектов КИИ; Навыком управления (администрирования) системой безопасности и реагирования на компьютерные инциденты; Навыком проведения контроля состояния (мониторинг) критических процессов и системы безопасности значимого объекта КИИ.

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	Раздел 1. Принципы построения компьютерных систем и сетей и классификация целенаправленных атак на них	1-8	4/0/12		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1
2	Раздел 2. Стек сетевых протоколов TCP/IP	9-16	4/0/12		25	КИ-16	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-2.4, У-ПК-2.4, В-ПК-2.4
	Итого за 3 Семестр		8/0/24		50		
	Контрольные мероприятия за 3 Семестр				50	Э	У-ПК-2.4, В-ПК-2.4, З-ПК-1, У-ПК-1, В-ПК-1,

							З-ПК-2.4
	4 Семестр						
1	Раздел 3. Основные типы атак на компьютерные системы и сети	1-8	4/0/11		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-2.4, У-ПК-2.4, В-ПК-2.4
2	Раздел 4. Тестирование компьютерных систем и сетей на проникновение	9-15	4/0/11		25	КИ-15	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-2.4, У-ПК-2.4, В-ПК-2.4
	Итого за 4 Семестр		8/0/22		50		
	Контрольные мероприятия за 4 Семестр				50	Э	З-ПК-2.3, У-ПК-

							2.3, В-ПК-2.3, З-ПК-2.4, У-ПК-2.4, В-ПК-2.4

* – 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.**
	3 Семестр	8	0	24
1-8	**Раздел 1. Принципы построения компьютерных систем и сетей и классификация целенаправленных атак на них**	4	0	12
1 - 2	**Тема 1. Нормативное регулирование в сфере обеспечения безопасности информации в компьютерных системах и сетях** Основные термины и определения в сфере обеспечения безопасности информации, обрабатываемой с использованием компьютерных систем и сетей. Обзор отечественных и зарубежных стандартов и нормативных документов по вопросам построения и защиты компьютерных систем и сетей.	Всего аудиторных часов		
		1	0	3
		Онлайн		
		0	0	0
3 - 4	**Тема 2. Классификация целенаправленных атак на компьютерные системы и сети** Классификация целенаправленных атак на компьютерные системы и обзор основных атак каждого класса. Жизненный цикл атак и порядок реагирования на инциденты информационной безопасности.	Всего аудиторных часов		
		1	0	3
		Онлайн		
		0	0	0
5 - 6	**Тема 3. Основные методы оценки безопасности компьютерных систем и сетей.** Основные методы оценки безопасности компьютерных систем и сетей средствами моделирования атак	Всего аудиторных часов		
		1	0	3
		Онлайн		
		0	0	0

	злоумышленника. Стандарты и методология проведения тестирования на проникновение. Обзор основных инструментов для тестирования компьютерных систем и сетей на проникновение.			
7 - 8	**Тема 4. Основы сетевых технологий** Обзор принципов построения современных компьютерных сетей. Отечественные и международные стандарты в сфере построения компьютерных сетей. Сетевые модели OSI и TCP/IP.	Всего аудиторных часов 1 Онлайн 0	 0 0	 3 0
9-16	**Раздел 2. Стек сетевых протоколов TCP/IP**	4	0	12
9 - 10	**Тема 5. Сетевые протоколы канального уровня.** Изучение ключевых сетевых протоколов канального уровня сетевой модели TCP/IP. Обзор структуры сетевого кадра, правил физической адресации, особенностей технологий Ethernet и Wi-Fi для построения проводных и беспроводных сетей, а также соответствующих стандартов.	Всего аудиторных часов 1 Онлайн 0	 0 0	 3 0
11 - 12	**Тема 6. Протоколы сетевого уровня.** Изучение ключевых сетевых протоколов сетевого уровня сетевой модели TCP/IP. Обзор структур сетевых пакетов, правил логической адресации, особенностей реализации протоколов IPv4, IPv6, ICMP, ARP, DHCP и описывающих их стандартов.	Всего аудиторных часов 1 Онлайн 0	 0 0	 3 0
13 - 14	**Тема 7. Сетевые протоколы транспортного уровня.** Изучение ключевых сетевых протоколов транспортного уровня сетевой модели TCP/IP. Обзор структур сетевых сегментов и датаграмм, портов, особенностей реализации протоколов TCP и UDP, а также описывающих их стандартов.	Всего аудиторных часов 1 Онлайн 0	 0 0	 3 0
15	**Тема 8. Сетевые протоколы прикладного уровня.** Изучение ключевых сетевых протоколов прикладного уровней сетевой модели TCP/IP. Обзор структур сетевых сообщений, правил идентификации ресурсов, языка разметки HTML, особенностей реализации протоколов HTTP, HTTPS, DNS, а также стандартов, описывающих соответствующие протоколы.	Всего аудиторных часов 1 Онлайн 0	 0 0	 3 0
	4 Семестр	8	0	22
1-8	**Раздел 3. Основные типы атак на компьютерные системы и сети**	4	0	11
1 - 2	**Тема 9. Атаки на сетевые протоколы.** Моделирование, обнаружение и противодействие атакам на сетевые протоколы. Анализ уязвимостей сетевых протоколов и основных векторов атаки на них. Обзор основных способов проведения атак, порядка выявления атак и мер противодействия.	Всего аудиторных часов 1 Онлайн 0	 0 0	 1 0
3 - 4	**Тема 10. Поиск и эксплуатация уязвимостей** Изучение методов поиска и эксплуатации уязвимостей в компьютерных системах и сетях. Защита компьютерных систем и сетей от целенаправленных атак, использующих эксплуатацию уязвимостей.	Всего аудиторных часов 1 Онлайн 0	 0 0	 4 0
5 - 6	**Тема 11. Парольные атаки** Изучение методов проведения и противодействия парольным атакам, направленным на получение доступа к	Всего аудиторных часов 1 Онлайн	 0 	 4

	компьютерным системам и сетям от имени легитимных пользователей.	0	0	0
7 - 8	**Тема 12. Атаки на веб-приложения** Изучение методов проведения и противодействия атакам, направленных против веб-приложений и сервисов.	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0
9-15	**Раздел 4. Тестирование компьютерных систем и сетей на проникновение**	4	0	11
9 - 10	**Тема 13. Разведка и сбор данных** Классификация и изучение методов сбора информации о структуре и составе сети для проверки её безопасности. Технологии сканирования сетей, применяемые злоумышленниками для их взлома.	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0
11 - 12	**Тема 14. Получение доступа** Изучение методов проникновения в компьютерные системы и сети через уязвимые подсистемы.	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
13 - 14	**Тема 15. Повышение привилегий и поддержание доступа** Изучение методов расширения привилегий и сохранения доступа, применяемых злоумышленниками после проникновения в компьютерные системы и сети.	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
15	**Тема 16. Анализ результатов и подготовка итогового отчета** Проведение анализа результатов тестирования на проникновение и подготовка итогового отчёта, содержащего описание условий и использованных методов тестирования, достигнутых результатов, оценку рисков информационной безопасности, а также рекомендации по устранению выявленных уязвимостей и совершенствованию процессов обеспечения информационной безопасности.	Всего аудиторных часов		
		1	0	1
		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	**Лабораборатная работа № 1:** Подготовка стенда для моделирования и анализа целенаправленных атак на компьютерные системы и сети.
2 - 3	**Лабораборатная работа № 2:** Знакомство с графическим симулятором сети GNS3.
4	**Лабораборатная работа № 3:** Знакомство с терминалом Linux
5	**Лабораборатная работа № 4:** Сетевое окружение Linux
6 - 7	**Лабораборатная работа № 5:** Знакомство в Kali Linux
8	**Лабораборатная работа № 6:** Знакомство с Wireshark
9 - 10	**Лабораборатная работа № 7: Моделирование компьютерных сетей.** Моделирование компьютерных сетей.
11 - 12	**Лабораборатная работа № 8:** Исследование протоколов канального уровня
13 - 15	**Лабораборатная работа № 9:** Исследование протоколов сетевого уровня
	4 Семестр
1	**Лабораборатная работа № 1:** Атаки на протокол ARP
2	**Лабораборатная работа № 2:** Атаки на протокол DHCP
3	**Лабораборатная работа № 3:** Атаки на протокол VLAN
4	**Лабораборатная работа № 4:** Знакомство со сканерами уязвимостей.
5	**Лабораборатная работа № 5:** Знакомство с базами данных эксплойтов и инструментами для эксплуатации уязвимостей.
6	**Лабораборатная работа № 6:** Лабораборатная работа № 6: Парольные атаки в режиме онлайн
7	**Лабораборатная работа № 7:** Парольные атаки в режиме оффлайн
8	**Лабораборатная работа № 8:** Атаки на веб-приложения
9 - 10	**Лабораборатная работа № 9:** Сбор информации в сети Интернет
11	**Лабораборатная работа № 10:** Сканирование сетей
12	**Лабораборатная работа № 11:** Поиск уязвимостей
13	**Лабораборатная работа № 12:** Эксплуатация уязвимостей
14	**Лабораборатная работа № 13:** Расширение привилегий
15	**Лабораборатная работа № 14:** Поддержание доступа

16	**Лабораборатная работа № 15:** Анализ результатов тестирования и подготовка итогового отчёта

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документ, государственные и международные стандарты, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы обеспечения защиты компьютерных систем и сетей от целенаправленных атак. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по выявлению угроз безопасности информации в компьютерных системах и сетях, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети. При проведении лабораторных работ необходимо отрабатывать задания, в том числе с проведением деловых игр (эпизодов).

Лабораторные работы проводятся на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть развёрнуто необходимое ПО для моделирования и анализа целенаправленных атак на компьютерные системы и сети. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

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)**	**Аттестационное мероприятие (КП 2)**
ПК-1	З-ПК-1	Э, КИ-8, КИ-16	КИ-8, КИ-15
	В-ПК-1	Э, КИ-8, КИ-16	КИ-8, КИ-15
	У-ПК-1	Э, КИ-8, КИ-16	КИ-8, КИ-15
ПК-2.3	З-ПК-2.3	КИ-16	Э, КИ-8, КИ-15
	У-ПК-2.3	КИ-16	Э, КИ-8, КИ-15

	В-ПК-2.3	КИ-16	Э, КИ-8, КИ-15
ПК-2.4	З-ПК-2.4	Э, КИ-16	Э, КИ-8, КИ-15
	У-ПК-2.4	Э, КИ-16	Э, КИ-8, КИ-15
	В-ПК-2.4	Э, КИ-16	Э, КИ-8, КИ-15

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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>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.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">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.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>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.</td></tr>
</table>

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ М 42 Атака на Internet : учебное пособие, Москва: ДМК Пресс, 2006

2. ЭИ А 95 Защита от хакеров корпоративных сетей : учебное пособие, Москва: ДМК Пресс, 2008

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

4. ЭИ Ш 44 Самоподобие и фракталы. Телекоммуникационные приложения : учебное пособие, Москва: Физматлит, 2008

5. ЭИ Б 24 Семь безопасных информационных технологий : учебное пособие, Москва: ДМК Пресс, 2017

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 О-54 Безопасность компьютерных сетей : , Москва: Горячая линия - Телеком, 2019

2. ЭИ М60 Сетевые атаки на открытые системы на примере Интранета : учебное пособие для вузов, Москва: НИЯУ МИФИ, 2012

3. ЭИ Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, ред. М. А. Иванов, Москва: НИЯУ МИФИ, 2011

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

1. Kali Linux ()

2. GNS3 ()

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Вузовские электронно-библиотечные системы учебной литературы ()

2. База научно-технической информации (например, ВИНИТИ РАН) ()

3. www.fstec.ru; www.gost.ru; www.fsb.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

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - Обеспечение безопасности информации ключевых систем информационной инфраструктуры, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР15 - максим.балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При неаттестации хотя бы по одному из разделов, студент не допускается к зачёту, экзамену

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - Обеспечение безопасности значимых объектов критической информационной инфраструктуры, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР15 - максим.балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех практических работ раздела.

При неаттестации хотя бы по одному из разделов, студент не допускается к зачёту.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите

информации и аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по моделированию и анализу целенаправленных атак на компьютерные системы и сети, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

Особенности изучения разделов дисциплины

Учебная дисциплина «Целенаправленные атаки на компьютерные системы» может быть охарактеризована как прикладная дисциплина технической направленности, является достаточно сложной, поскольку требует хорошей физико-математической подготовки. Необходимо глубокое знание смежных дисциплин специализации.

В процессе изучения данной программы необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Вопросы по тематике курса, являющиеся теоретическим обоснованием наиболее важных направлений в практической профессиональной деятельности студентов, включаются в практические занятия. В практические занятия включаются вопросы, усвоение которых требуется на уровне практических навыков и умений.

Для проведения всех практических занятий должны использоваться методические разработки, позволяющие индивидуализировать задания обучаемым. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями объектов информатизации и набором конкретных действий, объединённых в соответствующую подгруппу.

В качестве форм промежуточного (межсеместрового) контроля полученных знаний могут быть использованы письменные работы (рефераты) в сочетании с собеседованием, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

Студенты, прослушавшие курс, обладают умениями и навыками, необходимыми для корректного применения и разработки средств защиты информации.

Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Муравьёв Сергей Константинович, к.т.н.

Рецензент(ы):

Горбатов В.С.