Аннотация к рабочей программе дисциплины «Основы мониторинга безопасности инфокоммуникационных систем и сетей»

Цель преподавания дисциплины

Дисциплина «Основы мониторинга безопасности инфокоммуникационных систем и сетей»формирует у студентов теоретических знаний в области организации и применения современных технологий и средств мониторинга инфокоммуникационных систем и сетей, практических навыков использования, соответствующих программных и технических средств информационных сетей и коммуникационных.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:
– изучение базовых теоретических принципов построения инфокоммуникационных сетей;
– изучение основных технологий сетей;
– реализовывать правильный подход к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС)
– выработка навыков и умений эксплуатации и мониторинга работоспособности инфокоммуникационных сетей.

Компетенции, формируемые в результате освоения дисциплины

– Способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9);
– Способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать, проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13).

Разделы дисциплины

Введение. Анализ современного состояния сетевой безопасности. Назначение сетевых пакетов и их структура. Анализ сетевого трафика. Программные утилиты для мониторинга сет. Контроль трафика с помощью виртуальных частных сетей. Угрозы информации в беспроводных сетях Получение информации от сетевых сервисов. Системы мониторинга сетей связи.

Системы обнаружения вторжений. Автоматическая валидация уязвимостей с множеств и нейронных сетей.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики
Т.А. Ширабакина
(подпись, инициалы, фамилия)
«01» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы мониторинга безопасности инфокоммуникационных систем и сетей
(наименование дисциплины)

направление подготовки (специальность) 10.05.02
(шифр согласно ФГОС
Информационная безопасность телекоммуникационных систем
и наименование направление подготовки (специальности)

Защита информации в системах связи и управления
наименование профиля, специализации или магистерской программы)

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

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем и на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем (специализация Защита информации в системах связи и управления), одобренного Учёным советом университета, протокол №5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем на заседании кафедры информационной безопасности № «9» 01.02 2017.

Зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Спеваков А.Г.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № 1 «28» 08 2017 г. на заседании кафедры Таныгин М.О.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол №5 «30» 01 2017 г. на заседании кафедры КПиСС 28.06.2018 г. протокол № 23
(наименование кафедры, дата, номер протокола)

Зав. кафедрой В.Г. Андронов

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019 №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н. доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_1_ от «_31_» _08_ 20_20_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_28_» _06_ 20_21_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_30_» _06_ 20_22_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

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

1.1. Цель преподавания дисциплины

Дисциплина «Основы мониторинга безопасности инфокоммуникационных систем и сетей» формирует у студентов теоретических знаний в области организации и применения современных технологий и средств мониторинга инфокоммуникационных систем и сетей, практических навыков использования соответствующих программных и технических средств информационных сетей и коммуникационных технологий.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

– изучение базовых теоретических принципов построения инфокоммуникационных сетей;

– изучение основных технологий сетей;

– реализовывать правильный подход к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС)

– выработка навыков и умений эксплуатации и мониторинга работоспособности инфокоммуникационных сетей.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

– принципы организации инфокоммуникационных сетей;

– инструментальные средства мониторинга сетей и сетевых пакетов;

уметь:

– разрабатывать протоколы мониторинга инфокоммуникацонных систем и сетей;

– использовать стандарты Ethernet: для получения информации о структуре сетей и процессах, в них протекающих;

владеть:

– практическими навыками использования средств анализа информации в сетях TCP/IP;

– навыками анализа схем IP-маршрутизации; методов маршрутизации информационных потоков;

Процесс изучения дисциплины направлен на формирование

следующих компетенций

– способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9);

– способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам базовой части (Б1.В.ОД.9). Изучается на 5 курсе в 10 семестре.

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

Общая трудоёмкость (объём) дисциплины составляет 6 зачётных единицы, 108 часов

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	216
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	90,15
лекции	36
лабораторные занятия	36
практические занятия	18
экзамен	0,15
зачет	
курсовая работа (проект)	
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	90
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	18
Самостоятельная работа обучающихся (всего)	90
Контроль/экз (подготовка к экзамену)	36

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

4.1. Содержание дисциплины

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

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Введение. Анализ современного состояния сетевой безопасности	Эволюция угроз. Сдвиги в потребительском восприятии угроз сетевой безопасности. Актуальность технологий предотвращения утечек. Шифрование и многофакторная аутентификация как наиболее эффективные методы защиты. Амплификация. BGP и утечки информации
2.	Назначение сетевых пакетов и их структура	Необходимость упаковки информации. Заголовки пактов. Формат данных в пакте. Методы управления обменом данными. Управление обменом данными в системах с различной топологией. Адресация пакетов.
3.	Анализ сетевого трафика	APM-решения. Признаки комплексного подхода а анализу трафика. Методы анализа сетевого трафика. Парадигмы сетевого мониторинга. Решения в области анализа трафика.
4.	Программные утилиты для мониторинга сети	Назначение, состав, функционал, особенности лицензирования средств мониторинга сети. Состояние рынка средств мониторинга сети. Виды собираемой информации в сетевых мониторах
5.	Контроль трафика с помощью виртуальных частных сетей	Определение виртуальных частных сетей. Принцип действия VPN. Создание туннеля. Процесс инкапсуляции. Туннелирование на уровне 2. Туннелирование IPSec. Поддержка VPN операционными системами. VPN и коммутируемые сети: преимущества и недостатки. Сценарии VPN. VPN удаленного доступа. Виртуальные частные экстрасети. Протоколы туннелирования. Технология PPTP. Технология L2F. Технология L2TP. Режимы тунеллирования. Протоколы шифрования.
6.	Угрозы информации в беспроводных сетях	Особенности беспроводных сетей. Периметр беспроводных сетей. Риски для информации в беспроводных сетях. Уязвимости устройств беспроводной связи. Ошибки конфигурации точек беспроводного доступа. Ошибки конфигурации клиентов беспроводных сетей. Уязвимость криптографических протоколов беспроводных сетей. Утечки информации в беспроводных сетях. Физические особенности среды, влияющие на безопасность
7.	Получение информации от сетевых сервисов	Сканирование портов. Получение информации от DNS-сервера. Перебор имен. Перебор обратных записей. Получение информации с использованием SNMP. Получение информации с использованием NetBIOS. Работа с электронной почтой. Анализ баннеров. Получение информации от NTP-сервера.
8.	Системы мониторинга сетей связи	Контроль точек взаимодействия сетей. Управление сетью. Возможности современных систем контроля сетей связи.

		учёт разговорного трафика. Функциональные возможности систем мониторинга сетей связи. Анализ качества функционирования сети. Анализ разговорной нагрузки по каналам.
9.	Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей	Проверка конфигураций и поиск уязвимости ИС. Принципы работы систем обнаружения вторжений. Состав системы обнаружения вторжений. Классификация систем обнаружения вторжений. Размещение компонентов системы обнаружения вторжений в сети. Постановка задачи нечеткой классификации уязвимостей при использовании нейросетей. Принципы работы систем обнаружения вторжений на основе нейросетей.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Введение. Анализ современного состояния сетевой безопасности	4		1	У-4,5 МО-1,7	С	ПК-9, ПК-13
2.	Назначение сетевых пакетов и их структура	4	1		У-2,6,7 МО-1,2	С	ПК-9, ПК-13
3.	Анализ сетевого трафика	4	2		У-1,2 МО-2,3	С	ПК-9, ПК-13
4.	Программные утилиты для мониторинга сети	4		2	У-1-3 МО-1,8	С	ПК-9, ПК-13
5.	Контроль трафика с помощью виртуальных частных сетей	4	3		У-1,5,6 МО-1,4	С	ПК-9, ПК-13
6.	Угрозы информации в беспроводных сетях	4	4		У-3 МО-1,5	С	ПК-9, ПК-13
7.	Получение информации от сетевых сервисов	4	5		У-2,6,8 МО-1,6	С	ПК-9, ПК-13
8.	Системы мониторинга сетей связи	4		3	У-1,2 МО-1,9	С	ПК-9, ПК-13
9.	Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей	4			У-2,7 МО-1	С	ПК-9, ПК-13

С – собеседование

4.2. Лабораторные работы и практические занятия

4.2.1. Лабораторные занятия

Таблица 4.3 – Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1.	Средства устранения неисправностей в TCP/IP	6
2.	Протокол управления транспортом	6
3.	Контроль сетевой активности через VPN	8
4.	Беспроводные технологии Bluetooth	8
5.	Сетевые утилиты и их использование	8
Итого		36

4.2.2. Практические занятия

Таблица 4.4 – Практические занятия

№	Наименование лабораторной работы	Объем, час.
1.	Назначение пакетов и их структура, адресация пакетов	6
2.	Анализаторы сетевых протоколов	6
3.	Исследование работы телефонной сети на базе АТС Panasonic	6
Итого		18

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Введение. Анализ современного состояния сетевой безопасности	1-2 недели	10
2.	Назначение сетевых пакетов и их структура	3-4 недели	10
3.	Анализ сетевого трафика	5-6 недели	10
4.	Программные утилиты для мониторинга сети	7-8 недели	10
5.	Контроль трафика с помощью виртуальных частных сетей	9-10 недели	10
6.	Угрозы информации в беспроводных сетях	11-12 недели	10
7.	Получение информации от сетевых сервисов	13-14 недели	10
8.	Системы мониторинга сетей связи	15-16 недели	10
9.	Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей	17-18 недели	10
Итого			36

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

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

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

библиотекой университета:

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

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

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

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

– путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. **Образовательные технологии**

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 35.2% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы №1 Назначение пакетов и их структура, адресация пакетов	Выполнение таблицы, иллюстрирующей методы управления обменом в различных топологиях	6
2.	Выполнение практической работы №2 Анализаторы сетевых протоколов	Изучение концепции беспроводных сетевых технологий, классификацию беспроводных сетей	6
3.	Выполнение практической работы №1 Исследование работы телефонной сети на базе АТС Panasonic	Ознакомление с оборудованием для сетей Ethernet и Fast Ethernet	6
	Итого		18

7. **Фонд оценочных средств для проведения промежуточной аттестации**

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9)			Измерения в телекоммуникационных системах Планирование и управление информационной безопасностью Основы мониторинга безопасности инфокоммуникационных систем и сетей Система сертификации и аттестации телекоммуникационных систем Порядок

			проведения аттестации объектов информатизации Технологическая практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13)			Защита информации в системах беспроводной связи Системы коммутации Основы мониторинга безопасности инфокоммуникационных систем и сетей Практика по получению профессиональных умений и опыта профессиональной деятельности Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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

Таблица 7.2 – Критерии и шкала оценивания компетенций

Наименование	Показатели оценивания	Критерии и шкала оценивания компетенций		
		Пороговый	Продвинутый	Высокий уровень

компетенции	компетенций	уровень («удовлетворительно)	уровень (хорошо»)	(«отлично»)
способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знает**: С пробелами основное техническое оборудование защищенных телекоммуникационных сетей. **Умеет**: В недостаточной форме формулировать технические требования средств защиты информации в телекоммуникационных системах. **Владеет**: Слабо владеет навыками решения профессиональных задач.	**Знает**: Углубленно, но с некоторыми пробелами в отдельных областях технические средств мониторинга информационной безопасности телекоммуникационных систем. **Умеет**: В достаточной мере формулировать технические требования средств защиты информации в телекоммуникационных системах. **Владеет**: Навыками программирования в профессиональной сфере**.**	**Знает**: Углубленно техническое обслуживание средств мониторинга информационной безопасности телекоммуникационных сетей. **Умеет**: успешно формулировать технические требования к телекоммуникационным системам и нормам. **Владеет**: Развитыми навыками проведения аудита безопасности телекоммуникационных сетей.
способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информацио	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения,	**Знает:** Основные правила организации режима защиты информации на объектах. **Умеет:** Формулировать отдельные условия проведения мониторинга безопасности сетей связи. **Владеет:** Навыками участия в мониторинга	**Знает:** Основные принципы организации режима защиты информации на объектах. **Умеет:** Формулировать документы регламентирующих режим безопасной передачи трафика по сетям и системам связи. **Владеет:** Организации	**Знает:** Глубокие знания в области организации режима защиты информации на объектах **Умеет:** Формировать комплект документов, регламентирующих режим ограниченного доступа к информации. **Владеет:** Навыками организации

нной безопасности и телекоммуникационных систем (ПК-13)	навыки в типовых и нестандартных ситуациях	безопасности систем и сетей связи.	отдельных процессов аудита безопасности систем связи.	режима безопасной передачи данных по сетям и системам связи..

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

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1.	Введение. Анализ современного состояния сетевой безопасности	ПК-9, ПК-13	Лекция, Практическая работа, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ПР№1		
2.	Назначение сетевых пакетов и их структура	ПК-9, ПК-13	Лекция, Лабораторная работа, СРС	собеседование	1-15	Согласно табл.7.2
				контрольные вопросы к ЛР№1		
3.	Анализ сетевого трафика	ПК-9, ПК-13 ПК-9, ПК-13	Лекция, Лабораторная работа, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№2		
4.	Программные утилиты для мониторинга сети	ПК-9, ПК-13	Лекция, Практическая работа, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ПР№2		

5.	Контроль трафика с помощью виртуальных частных сетей	ПК-9, ПК-13	Лекция, Лабораторная работа, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№3	1-5	
6.	Угрозы информации в беспроводных сетях	ПК-9, ПК-13	Лекция, Лабораторная работа, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№4		
7.	Получение информации от сетевых сервисов	ПК-9, ПК-13	Лекция, Лабораторная работа, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№5		
8.	Системы мониторинга сетей связи	ПК-9, ПК-13	Лекция, Практическая работа, СРС	собеседование		Согласно табл.7.2
				контрольные вопросы к ПР№3		
9.	Получение информации от сетевых сервисов	ПК-9, ПК-13	Лекция, СРС	собеседование		Согласно табл.7.2

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

7.4. Рейтинговый контроль изучения учебной дисциплины

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

– Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;

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

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Средства устранения неисправностей в TCP/IP»	3	Выполнил, но «не защитил»	7	Выполнил и «защитил»
Выполнение лабораторной работы №2 «Протокол управления транспортом»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Контроль сетевой активности через VPN»	3	Выполнил, но «не защитил»	7	Выполнил и «защитил»
Выполнение лабораторной работы №4 «Беспроводные технологии Bluetooth»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы №5 «Сетевые утилиты и их использование»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение практической работы №1 «Назначение пакетов и их структура, адресация пакетов»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение практической работы №2 «Анализатор сетевых протоколов»	3	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение практической работы №3 «Исследование работы телефонной сети на базе АТС Panasonic»	3	Выполнил, но «не защитил»	7	Выполнил и «защитил»
СРС	0		9	
ИТОГО	24		48	
Посещаемость	0		16	
Экзамен	0		36	
ИТОГО	24		100	

При итоговом контроле в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (максимум 15) переводят в баллы на экзамене (максимум 36) путём умножения на 2.4 и округления до целого значения. Пример билета в тестовой форме приведён в приложении В

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

8.1. Основная и дополнительная учебная литература

8.1.1. Основная литература

1) Громов Юрий Юрьевич. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - ТНТ, 2013. - 384 с.

2) Лукьянюк, Сергей Георгиевич. Теория электрической связи. Помехоустойчивость и эффективность систем связи [Текст] : учебное пособие / С. Г. Лукьянюк, А. М. Потапенко. - ЮЗГУ, 2013. - 263 с.

3) Олифер, Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с.

8.1.2. Дополнительная литература

4) Гордиенко В. Н. Многоканальные телекоммуникационные системы [Текст] : учебник / В. Н. Гордиенко, М. С. Тверецкий. - Горячая линия - Телеком, 2007. - 416 с.

5) Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / М. А. Иванов, И. Чугунков. - Москва : МИФИ, 2012. - 400 с.

6) Крук, Борис Иванович. Телекоммуникационные системы и сети [Текст] : учебное пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком. Т. 1: Современные технологии. - 2013. - 620 с.

7) Крухмалев В. В. Цифровые системы передачи [Текст] : учебное пособие / В. В. Крухмалев, В. Н. Гордиенко, А. Д. Моченов. - Горячая линия - Телеком, 2007. - 352 с.

8) Онокой, Людмила Сергеевна. Компьютерные технологии в науке и образовании [Текст]: учебное пособие / Л. С. Онокой, В. М. Титов. - Москва: ФОРУМ : ИНФРА-М, 2014. – 223 с.

8.2. Перечень методических указаний

1) Таныгин М.О. Основы мониторинга безопасности инфокоммуникационных систем и сетей [Текст] : методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 10 с. – Библиогр.: с. 10.

2) Таныгин М.О. Средства устранения неисправностей в TCP/IP [Текст] : методические указания к лабораторной работе / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 6 с.: ил. 1, табл. 1. – Библиогр.: с. 6..

3) Таныгин М.О. Протокол управления транспортом TCP [Текст] : методические указания к лабораторной работе / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 19 с.: ил. 12, табл. 2. – Библиогр.: с. 19.

4) Таныгин М.О. Контроль сетевой активности через VPN [Текст] : методические указания к лабораторной работе / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 32 с.: ил. 30. – Библиогр.: с. 32.

5) Таныгин М.О. Беспроводные технологии Bluetooth [Текст] : методические указания к лабораторной работе / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 8 с.: ил. 9. – Библиогр.: с. 8.

6) Таныгин М.О. Сетевые утилиты и их использование [Текст] : методические указания к лабораторной работе / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 4 с. – Библиогр.: с. 4.

7) Назначение пакетов и их структура, адресация пакетов [Текст] : методические указания к практической работе / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 9 с.: ил. 4. – Библиогр.: с. 9..

8) Таныгин М.О. Анализаторы сетевых протоколов [Текст] : методические указания к практической работе / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 20 с.: ил. 13, табл. 2. – Библиогр.: с. 9..

9) Таныгин М.О. Исследование работы телефонной сети на базе АТС Panasonic [Текст] : методические указания к практической работе / Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 31 с.: ил. 29, табл. 4. – Библиогр.: с. 31.

9. **Перечень ресурсов информационно-телекоммуникационной сети Интернет**

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
4) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
5) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
6) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
7) База данных "Патенты России"
8) Компания Cisco [официальный сайт] https://www.cisco.com/c/ru_ru/index.html
9) ЗАО «Лаборатория Касперского» [корпоратвный блог] https://www.kaspersky.ru/blog/
10) Аналитический раздел комании «Код Безопасности» https://www.securitycode.ru/documents/analytics/

11) Сайт для IT-специалистов www/habrahabr.ru

10. **Методические указания для обучающихся по освоению дисциплины**

Основными видами аудиторной работы студента при изучении дисциплины «Основы мониторинга безопасности инфокоммуникационных систем и сетей» являются лекции, практические работы. Студент не имеет права пропускать занятия без уважительных причин.

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

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

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

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

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Основы мониторинга безопасности инфокоммуникационных систем и сетей»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

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

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность операционных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Основы мониторинга безопасности инфокоммуникационных систем и сетей» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, анализатор WireShark, монитор трафика TrafficMonitor (пробная версия)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

13. **Лист дополнений и изменений, внесенных в рабочую программу дисциплины**

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изменённых	заменённых	аннулированных	новых			
1		4, 14			2	23.08.18	

ПРИЛОЖЕНИЕ А Образец экзаменационного билета в тестовой форме

ЮГО-ЗАПАДНЫЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ	
Факультет ФиПИ Специальность 10.05.02 курс 5, семестр 10 Дисциплина **«Основы мониторинга безопасности инфокоммуникационных систем и сетей»**	Утверждено на заседании кафедры ИБ, Протокол № __ от ____ 201__ г. Зав. кафедрой _____ М.О. Таныгин
1. В настоящее время угрозы и вредоносный код разрабатываются с целью • досаждать или мешать пользователям работать • для хищения денег и критически важной корпоративной информации • отслеживания нажимаемых пользователем клавиш и копирования данных отправляемых форм • наделения новых средств и систем сетевыми возможностями	
2. Основным средством предотвращения утечек из корпоративных информационных систем являются • Файрволы • IDS • VPN • DLP • AAA	
3. Что такое неотчуждаемый аутентифицирующий признак? • Признак, который не может быть похищен у пользователя • Признак, который не может быть потерян пользователем • Признак, который не может быть забыт пользователем • Признак, утрату которого пользователь сразу обнаружит • Всё вместе	
4. На что нацелен фишинг? • на доверчивость пользователя • на сообразительность пользователя • на интересность пользователя • на ответственность пользователя	
5. Особенностью современных злоумышленников, организующих атаки типа отказ в обслуживании является • Падение уровеня необходимого опыта и знаний для организации DDoS атак • Объдинение злоумышленников в трансграничные организации • Возможность использования «серых зон» интернета для осуществления своих планов • Использование технологии блокчейн • Массовая рассылка вредоносного кода	

6. Как называется процесс формирования кадра из данных прикладного уровня? • Буферизация • Управление • Инкапсуляция • Кодирование
7. Что такое префикс сети (network prefix)? • десятичное число, равное числу разрядов маски подсети, установленных в ноль • шестнадцатеричное число, равное числу разрядов маски подсети, установленных в единицу • десятичное число, равное числу разрядов маски подсети, установленных в единицу • первый октет IP-адреса
8. VPN работают на уровне модели OSI • 2 • 3 • 4 • 5 • 6
9. Современные VPN-решения состоят из • Центрального сервера, VPN – шлюзов и VPN – клиентов • Сети VPN – шлюзов • Сети независимых VPN – клиенов • Множества VPN – клиентов и центрального сервера
10. Протоколы тунеллирования обеспечивают • Скрытие заголовков сетевых пакетов, передаваемых по защищённому каналу • Шифрование содержимого сетевых пакетов, передаваемых по защищённому каналу • Коммуникацию узлов VPN • Взаимное опознавание узлов VPN
11. Комплексный мониторинг безопасности в информационной системе необходим для • быстрого определения «масштабов бедствия» и корневых причин сбоев необходимо одновременно контролировать метрики, характеризующие работу приложений, и метрики, характеризующие работу всей ИТ-инфраструктуры без исключения. • понимания качества предоставления ИТ-сервисов в масштабе всего предприятия. • быстрого устранения проблем и планирования мощностей необходима кооперация между различными отделами ИТ-Службы. • возможности воспроизвести сетевую активность и работу приложения в тот момент (а также до и после), когда произошло критическое событие ускорения диагностики проблем
12. Выберете методы управления производительностью приложений: • решения, основанные на синтетических транзакциях (GUI-роботы) • решения, использующие программные агенты на стороне сервера • решения, использующие программные агенты на стороне клиента • решения, основанные на анализе сетевого трафика • все перечисленные
13. К недостаткам систем ретроспективного анализа трафика модно отнести • доступ к очень большому дисковому • возможность посмотреть, что происходило в сети в произвольный момент прошлого • низкая скорость анализа • невозможность анализа сложных задач анализа

- высокие требования по скорости работы мониторов

14. Вторжение в беспроводную сеть не может произойти с
роутера с Wi-Fi,
программной точка доступа Soft AP
ноутбука с одновременно включенными проводным и беспроводным интерфейсом,
сетевого принтера
концентратора

15. Отключения ответа в беспроводных точках доступа на широковещательный запрос ESSID (Broadcast ESSID) позволяет предотвратить сканирование беспроводной сети злоумышленником

- Да
- Нет
- Да, если в сети не происходили регистрации новых легальных узлов

16. Основной способ мониторинга состояния сети это

- Сканирование портов
- Получение информации от DNS-сервера
- Определение активных хостов
- Перебор обратных записей
- Извлечение информации из сетевых протоколов

17. Чем отличается сканирование по протоколу TCP от сканирования по протоколу UDP

- Отсутствие ответа при сканировании по TCP протоколу позволяет сканеру принять решение о том, что порт открыт
- Отсутствие ответа при сканировании по TCP протоколу позволяет сканеру принять решение о том, что работает брандмауэр
- Отсутствие ответа при сканировании по UDP протоколу позволяет сканеру принять решение о том, что порт открыт
- Отсутствие ответа при сканировании по UDP протоколу позволяет сканеру принять решение о том, что работает брандмауэр

18. Неправильная конфигурация DNS-сервера позволяет злоумышленнику

- Получить информацию о структуре внутренней сети атакуемого предприятия
- Получить список доменных имён сервисов, действующих в сети
- Получить список используемых атакуемым сетевых сервисов
- Количество активных компьютеров в сети

19. Сетевые анализаторы работают в режимах:

- в реальном времени
- в режиме полного заркалирования
- в режиме превентивного анализа
- по предварительно сохранённому трафику

20. Что из приведенного ниже правильно описывает протокол SNMP?

- Входит в стандарт протокола TCP/IP
- Редко используется во вновь создаваемых сетях
- Использует концепцию, известную под названием MIB
- Является лучшим выбором для сетей с высоким объемом трафика