



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.10 Информационная безопасность GPRS и IP телефонии

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	4		
Семестр	8		

Лекции	24		
Лабораторные занятия	38		
Практические (семинарские) занятия	24		
в т. ч. практическая подготовка	8		
Форма(ы) промежуточной аттестации	Зачет с оценкой		
Контроль			
Иные формы работы			
Самостоятельная работа	58		

Всего часов: 144

Трудоемкость: 4 зачетных единицы.

Разработчик(и) рабочей программы:

кандидат физико-математических наук, доцент

С.А. Рощупкин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

формирование взгляда на информационную безопасность GPRS и IP- телефонии как на научно-практическую деятельность, носящую прикладной характер; представления о роли информационной безопасности GPRS и IP- телефонии, как о значимом месте в области информационных технологий, связанной с передачей конфиденциальной информации по каналам связи.

Задачи изучения дисциплины:

создание представления о правилах организации передачи данных по каналам GPRS и IP- телефонии, о структурах систем GPRS и IP-телефонии, а также угрозах информационной безопасности этих систем, а также развитие способностей по использованию существующих методов обеспечения информационной безопасности в каналах связи.

Место дисциплины в структуре ОПОП: реализуется в вариативной части (части, формируемой участниками образовательных отношений) блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
УК-8	Знать: – факторы вредного влияния на жизнедеятельность элементов среды обитания; – алгоритмы действий при возникновении чрезвычайных ситуаций и военных конфликтов; – правила техники безопасности на рабочем месте.	Знает: - правила организации информационной безопасности GPRS и IP- телефонии;
	Уметь: – идентифицировать опасные и вредные факторы в рамках осуществляемой деятельности, создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности.	Умеет: - применять основные механизмы защиты информации на практике.
	Владеть: – действиями по предотвращению возникновения чрезвычайных ситуаций (природного и техногенного происхождения) на рабочем месте и осуществлению спасательных и неотложных аварийно-восстановительных мероприятий в случае возникновения чрезвычайных ситуаций.	Владеет: - навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.
УК-9	Знать: - понятийный аппарат	Знает:

	экономической науки и базовые принципы функционирования экономики; – цели и механизмы основных видов социальной экономической политики.	- цели и механизмы организации информационной безопасности GPRS и IP- телефонии;
	Уметь: - использовать методы экономического и финансового планирования для достижения поставленной цели; – использовать финансовые инструменты для управления личными финансами (личным бюджетом).	Умеет: - использовать методы экономического и финансового планирования для обеспечения информационной безопасности GPRS и IP-телефонии.
	Владеть: - навыками применения экономических инструментов для управления финансами, с учетом экономических и финансовых рисков в различных областях жизнедеятельности.	Владеет: - навыками применения информационной безопасности в компьютерных системах.
ПКС-1	Знать: - сущность и понятие информационной безопасности, характеристику ее составляющих, источники угроз и меры по их предотвращению; - методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, диагностике, анализу, сопровождению и совершенствованию систем защиты информации.	Знает: - основные понятия, архитектуру и структуру каналов связи GPRS и IP- телефонии; - механизмы обеспечения информационной безопасности GPRS и IP- телефонии; - протоколы каналов связи GPRS и IP-телефонии.
	Уметь: - оценивать защищенность, классифицировать основные угрозы, обеспечивать информационную безопасность компьютерных систем, применяя необходимые программно-аппаратные средства и системы защиты информации; - принимать управленческие и административные решения в сфере защиты информации.	Умеет: - применять известные методы и средства обеспечения информационной безопасности GPRS и IP- телефонии.
	Владеть: - категориальным аппаратом в области обеспечения комплекса мер по администрированию и диагностике систем защиты информации; - правилами, методами, средствами,	Владеет: - методами управления информационной безопасностью GPRS и IP- телефонии.

	процедурами управления и администрирования информационной безопасностью объекта.	
--	--	--

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего ча- сов	Аудиторные заня- тия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
7 семестр						
Раздел 1. «Структура сети GPRS»		13	4	4	4	1
1	Тема 1. Современное состояние информационной безопасности GPRS и IP- телефонии. Мобильная станция. Базовая станция. Узел обслуживания абонентов GPRS. Узел маршрутизации GPRS.	13	4	4	4	1
Раздел 2. «Механизмы обеспечения информационной безопасности GPRS»		7	2	2	2	1
2	Тема 2. Безопасность мобильной станции (SIM-карта). Безопасность соединения. Процедура подключения мобильной станции к сети GPRS.	7	2	2	2	1
Раздел 3. «Структура системы IP-телефонии»		8	2	2	2	2
3	Тема 3. Узел передачи данных (шлюз), «диспетчер», «монитор», абонентский пункты	8	2	2	2	2
Раздел 4. «Организация электронного документооборота»		8	2	2	2	2
4	Тема 4. Перехват данных. Отказ в обслуживании. Подмена номера. Атака на абонентский пункт. Атака на диспетчера	8	2	2	2	2
	Форма отчетности					
	Контроль					
	Итого за 7 семестр	36	10	10	10	6
	в т.ч. практическая подготовка	4				
8 семестр						
Раздел 5. «Обеспечение информационной безопасности IP-телефонии»		20	2	2	6	10
5	Тема 5. Выбор правильной топологии. Физическая безопасность. Контроль доступа. VLAN. Шифрование. Межсетевые экраны. Аутентификация. RFC 1918. Системы обнаружения атак.	20	2	2	6	10
Раздел 6. «Построение сети на базе рекомендации H.323»		20	2	2	6	10
6	Тема 6. Терминал. Шлюз. Привратник. Устройство организации конференций.	20	2	2	6	10
Раздел 7. «Протокол RAS»		20	2	2	6	10
7	Тема 7. Обнаружение привратника. Регистрация оборудования. Доступ к сетевым ресурсам. Определение местоположения оборудования в сети. Опрос текущего состояния. Освобождение поло-	20	2	2	6	10

	сы пропускания.					
Раздел 8. «Сигнальный канал Н.225.0. Управляющий канал Н.245»		26	4	4	6	12
8	Тема 8. Основные сообщения канала. Принципы работы. Определение ведущего и ведомого оборудования. Обмен данными о функциональных возможностях оборудования. Открытие логических каналов.	26	4	4	6	12
Раздел 9. «Построение сетей IP-телефонии на базе протокола SIP»		22	4	4	4	10
9	Тема 9. Функциональные возможности протокола. Адресация. Элементы SIP-сети. Перспективы развития GPRS и IP-телефонии, а также методов их защиты.	22	4	4	4	10
	<i>Форма отчетности</i>	Зачет с оценкой				
	<i>Контроль</i>					
	Итого за 8 семестр	108	14	14	28	52
	в т.ч. практическая подготовка	4				
	ИТОГО	144	24	24	38	58

Очно-заочная форма обучения не реализуется

Заочная форма обучения не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме контрольной работы.

Типовой вариант контрольной работы

1. Структура сети GPRS.
2. Механизмы обеспечения информационной безопасности GPRS.
3. Структура системы IP-телефонии.
4. Угрозы информационной безопасности IP-телефонии.
5. Обеспечение информационной безопасности IP-телефонии.
6. Построение сети на базе рекомендации Н.323.
7. Протокол RAS.
8. Сигнальный канал Н.225.0.
9. Управляющий канал Н.245.
10. Построение сетей IP-телефонии на базе протокола SIP.

Промежуточная аттестация обучающихся осуществляется в форме зачета с оценкой с использованием следующих оценочных материалов: *перечень вопросов к зачету*.

Вопросы к зачету (8 семестр, очная форма обучения)

1. Современное состояние информационной безопасности GPRS и IP- телефонии. Мобильная станция. Базовая станция.
2. Узел обслуживания абонентов GPRS. Узел маршрутизации GPRS.
3. Механизмы обеспечения информационной безопасности GPRS Безопасность мобильной станции (SIM-карта). Безопасность соединения. Процедура подключения мобильной станции к сети GPRS.
4. Структура системы IP-телефонии Узел передачи данных (шлюз), «диспетчер», «монитор», абонентский пункт.
5. Угрозы информационной безопасности IP-телефонии. Перехват данных. Отказ в обслуживании.
6. Подмена номера. Атака на абонентский пункт. Атака на диспетчера.
7. Обеспечение информационной безопасности IP-телефонии Выбор правильной топологии. Физическая безопасность. Контроль доступа. VLAN. Шифрование. Межсетевые экраны. Аутентификация. RFC 1918. Системы обнаружения атак.
8. Построение сети на базе рекомендации H.323 Терминал. Шлюз. Привратник. Устройство организации конференций.
9. Протокол RAS. Обнаружение привратника. Регистрация оборудования. Доступ к сетевым ресурсам.
10. Определение местоположения оборудования в сети. Опрос текущего состояния. Освобождение полосы пропускания.
11. Сигнальный канал H.225.0 Основные сообщения канала. Принципы работы.
12. Управляющий канал H.245 Определение ведущего и ведомого оборудования. Обмен данными о функциональных возможностях оборудования. Открытие логических каналов.
13. Построение сетей IP-телефонии на базе протокола SIP Функциональные возможности протокола. Адресация. Элементы SIP-сети. Перспективы развития GPRS и IP-телефонии, а также методов их защиты.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Демидов, Л.Н. Основы эксплуатации компьютерных сетей: учебник для бакалавров : / Л.Н. Демидов. – Москва : Прометей, 2019. – 799 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576033> (дата обращения: 01.09.2021). – Библиогр.: с. 750 - 752. – ISBN 978-5-907100-01-5. – Текст : электронный.

4.2. Дополнительная литература

1. Попов, М.В. Анализ систем безопасности, использующих GSM каналы связи : практическое пособие / М.В. Попов. – Москва : Лаборатория книги, 2010. – 92 с. – Режим доступа: по

подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=86424> (дата обращения: 01.09.2021). – Текст : электронный.

2. IP-телефония в компьютерных сетях : учебное пособие / И.В. Баскаков, А.В. Пролетарский, С.А. Мельников, Р.А. Федотов. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) : Бином. Лаборатория знаний, 2008. – 184 с. : ил.,табл. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=232984> (дата обращения: 01.09.2021). – ISBN 978-5-94774-978-6. – Текст : электронный.

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ

4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ
----	-------------------	--	------------------

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.