Учреждение образования
«Белорусский государственный университет транспорта»

УТВЕРЖДАЮ
Первый проректор
учреждения образования
«Белорусский государственный
университет транспорта»
_____ Ю.Г. Самодум
«24» «03» 2021
Регистрационный № УД-56.33 / уч.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕЙ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-37 02 04 Автоматика, телемеханика и связь на железнодорожном транспорте

2021

Учебная программа составлена на основе образовательного стандарта ОСВО 1-37 02 04-2018 «Автоматика, телемеханика и связь на железнодорожном транспорте»

СОСТАВИТЕЛЬ:
П.М. Буй, доцент кафедры «Автоматика, телемеханика и связь» учреждения образования «Белорусский государственный университет транспорта», кандидат технических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой «Автоматика, телемеханика и связь» учреждения образования «Белорусский государственный университет транспорта»
(протокол № 11 от 10 декабря 2020 г.);
методической комиссией электротехнического факультета учреждения образования «Белорусский государственный университет транспорта»
(протокол № 1 от 21 января 2021 г.);
научно-методическим советом заочного факультета учреждения образования «Белорусский государственный университет транспорта»
(протокол № 1 от 27 января 2021 г.);
научно-методическим советом учреждения образования «Белорусский государственный университет транспорта»
(протокол № 1 от 23 марта 2021 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Актуальность изучения учебной дисциплины

В последнее время наблюдается резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации, а также резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с их помощью в инфокоммуникационных системах и сетях. Доступ к сетевым ресурсам на железнодорожном транспорте постоянно расширяется, увеличивается круг пользователей, использующих сетевые приложения. В связи с этим все более актуальным становится вопрос об обеспечении безопасности информационных технологий и сетей железнодорожного транспорта. Важными задачами являются анализ угроз и уязвимостей информационной безопасности, анализ рисков, а также грамотная организация и построение комплексной системы защиты информации. Необходимо, чтобы в процессе обучения студент уяснил опасности, которые грозят информационным технологиям и информации, которая ими обрабатывается, в современном мире, а также освоил методы защиты информационных технологий и сетей при условии возникновения угроз.

Программа разработана на основе компетентностного подхода, требований к формированию компетенций, сформулированных в образовательном стандарте ОСВО 1-37 02 04-2018 «Автоматика, телемеханика и связь на железнодорожном транспорте».

Дисциплина относится к компоненту дисциплин учреждения высшего образования, осваиваемых студентами специальности 1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте», входит в модуль «Программирование» и является дисциплиной по выбору студентов.

Цели и задачи учебной дисциплины

Целью преподавания дисциплины «Безопасность информационных технологий и сетей» является получение студентами базовых знаний по вопросам обеспечения информационной безопасности современных технологий и сетей в условиях возникновения угроз различных по виду, происхождению и характеру.

Основными задачами дисциплины являются:

– освоение общих принципов организации цифровых сетей;

– изучение модели взаимодействия открытых систем;

– изучение основных угроз информационной безопасности и уязвимостей информационных систем;

– получение знаний о методах защиты информации, способах криптографического преобразования информации;

– освоение ключевых технологий канального уровня модели OSI;

– изучения стека протоколов TCP/IP;

– изучение методов и средств разграничения доступа, аутентификации субъектов;

– изучение основных сетевых информационных служб;

– получение представлений о протоколах сетевой безопасности.

Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен обладать следующей специализированной компетенцией (СК), предусмотренной типовым учебным планом специальности 1-37 02 04-2018 «Автоматика, телемеханика и связь на железнодорожном транспорте»:

СК-2. Уметь настраивать локальные вычислительные сети и производить конфигурирование сетевого оборудования с учетом возможных угроз их информационной безопасности, производить выбор аппаратных и программных средств защиты информации, оценивать их эффективность.

Для приобретения специализированной компетенции СК-2 в результате изучения дисциплины студент должен.

знать:

- системную методологию, правовое и нормативное обеспечение защиты информации;
- организационные и технические методы защиты информации;

– алгоритмы криптографического преобразования информации;

– основные принципы адресации, коммутации, маршрутизации в цифровых сетях;

– технологии, применяемые на физическом уровне для организации связи;

– особенности протоколов канального, сетевого и транспортного уровней модели взаимодействия открытых систем;

– назначение и принцип работы наиболее распространенных сетевых информационных служб;

уметь:

– проводить анализ вероятных угроз и уязвимостей информационной безопасности для заданных объектов;

– определять риски нарушения информационной безопасности телекоммуникационных систем;

– организовывать виртуальные локальные сети;

– осуществлять адресацию сетевых интерфейсов с применением масок;

– использовать протоколы сетевой безопасности и анализировать особенности их использования;

– производить конфигурирование маршрутизаторов цифровых сетей;

владеть:

– методами защиты проводных и беспроводных каналов связи;

– способами настройки таблиц маршрутизации сетевых устройств.

Структура содержания учебной дисциплины

Содержание дисциплины представлено в виде тем, которые характеризуются относительно самостоятельными укрупненными дидактическими единицами содержания обучения. Содержание дисциплины опирается на приобретенные ранее студентами компетенции при изучении дисциплин «Высшая математика», «Информатика».

Форма получения высшего образования – дневная и заочная сокращенная. По дневной форме обучения дисциплина изучается в 3 семестре. По заочной сокращенной форме обучения дисциплина изучается в 7 и 8 семестрах.

В соответствии с учебным планом дневной формы обучения на изучение дисциплины отведено всего 120 часов, в том числе 72 аудиторных часа, из них лекции – 38 часов, лабораторные занятия – 16 часов, практические занятия – 18 часов. Форма текущей аттестации – зачет. Трудоемкость дисциплины составляет 3 зачетных единицы.

Распределение аудиторных часов по семестрам, видам занятий дневной формы обучения

Семестр	Всего часов	Зачетных единиц	Аудиторных часов	Лекции	Лабораторные занятия	Практические занятия	Форма текущей аттестации
3	120	3	72	38	16	18	Зачет

Распределение аудиторных часов по семестрам, видам занятий заочной сокращенной формы обучения

Курс	Семестр	Всего часов	Зачетных единиц	Аудиторных часов	Часов ауд. занятий в семестре по видам учебной работы				Количество видов отчетности				
					лекции	лабораторные занятия	практические занятия	СУРС	экзамены	зачеты	курсовые проекты	курсовые работы	контрольные работы
4	7	4		4	4								
	8	116	3	12	4	4	4			1			
Итого:		120	3	16	8	4	4						
Всего часов:													
самостоятельное изучение аудиторных тем:									56				

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. **Основные понятия и принципы защиты информации**

Основные понятия информационной безопасности. Государственный стандарт Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения». Особенности информации, как объекта защиты. Краткий исторический экскурс по вопросам информационной безопасности.

Тема 2. **Основы сетевых технологий**

Эволюция сетей. Глобальные сети. Локальные сети. Конвергенция сетей. Интернет, как основной фактор развития сетевых технологий. Стандартизация Интернет. Модель OSI. Уровни модели OSI. Протокол. Интерфейс.

Тема 3. **Общие принципы организации цифровых сетей**

Топология сети. Принципы адресации, маршрутизации, мультиплексирования/демультиплексирования. Коммутация каналов. Коммутация пакетов. Классификация сетей.

Тема 4. **Угрозы, уязвимости и риски информационной безопасности сетевых устройств**

Понятие угрозы. Классификация угроз информационной безопасности сетевых технологий по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков. Понятие атаки. Модель нарушителя информационной безопасности.

Тема 5. **Методы защиты информации на физическом уровне**

Классификация методов защиты информации. Методы защиты информации на физическом уровне модели OSI. Модели информационной безопасности. Триада «Конфиденциальность, доступность, целостность». Гексада Паркера. Модель STRIDE. Особенности беспроводной среды передачи. Множественный доступ с кодовым разделением каналов (CDMA).

Тема 6. **Криптографические методы защиты информации**

Классификация криптографических методов защиты информации. Архивация и кодирование информации. Шифрование информации. Симметричные методы шифрования. Асимметричные методы шифрования. Электронная цифровая подпись. Управление криптографическими ключами: генерация, хранение и распределение ключей. Стеганография.

Тема 7. **Технологии канального уровня**

Технология Ethernet. Локальные адреса (MAC-адреса). Разделяемая среда передачи. Борьба с коллизиями. Беспроводные локальные сети (Wi-Fi). Персональные сети (Bluetooth). Коммутируемые сети Ethernet. Алгоритм прозрачного моста IEEE 802.1D. Коммутаторы и их архитектура. Построение отказоустойчивых сетей с использованием протокола покрывающего дерева. Виртуальные локальные сети и их конфигурирование.

Тема 8. **Стек протоколов TCP/IP**

Протоколы сетевого уровня, протокол IP. Сетевая адресация (IP-адресация). Протокол ARP. Доменные имена. Система DNS. Протокол DHCP. Структура заголовка IP-пакета. Маршрутизаторы, протоколы RIP, OSPF, EIGRP, BGP. Протокол ICMP. IPv6. Понятие порта и сокета. Протоколы UDP и TCP. Методы квитирования. Концепция скользящего окна при передаче данных.

Тема 9. **Средства аутентификации субъектов и управление доступом**

Понятие идентификации и аутентификации. Классификация средств аутентификации. Парольные средства аутентификации для сетевых устройств. Средства аутентификации с использованием смарт-карт и электронных ключей. Биометрические средства аутентификации. Строгая аутентификация в компьютерных сетях. Протоколы аутентификации. Технологии управления доступом и авторизация. Разграничение доступа по спискам. Дискретный и мандатный методы управления доступом. Ролевое управление доступом.

Тема 10. **Сетевые информационные службы**

Общие принципы организации сетевых служб. Веб-служба. Протокол HTTP. Почтовая служба. Протоколы SMTP, POP3, IMAP. Сетевая файловая служба. Протокол FTP. Служба управления сетью. Протоколы SNMP, telnet.

Тема 11. **Протоколы сетевой безопасности**

Фильтрация трафика. Межсетевые экраны. Прокси-серверы. Системы и средства мониторинга трафика. Системы обнаружения вторжений. Защита сетевых соединений. Протокол IPsec. Безопасность сетевых служб. Компьютерные вирусы и механизмы борьбы с ними. Протокол HTTPS. Облачные сервисы и их безопасность. Защита информации беспроводных сетях.

Тема 12. **Обеспечение информационной безопасности при работе в сети Интернет**

Обзор инцидентов в сфере информационной безопасности. Системы автоматизированного сбора и учета фактов нарушения информационной безопасности объектов информатизации. Методы и средства защиты информации от удаленных атак. Безопасность в социальных сетях. Рекомендации по защите персонального компьютера при работе в сети Интернет.

Тема 13. **Комплексный подход при организации защиты информации**

Методы оценки эффективности средств обеспечения информационной безопасности. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем. Концепция национальной безопасности Республики Беларусь. Концепция информационной безопасности Республики Беларусь.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (дневная форма обучения)

Номер темы, занятия	Название темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов			Материальное обеспечение занятия (наглядные методические пособия и др.)	Литература	Форма контроля знаний
		лекции	лабораторные занятия	практические занятия			
1	**Тема 1. Основные понятия и принципы защиты информации (2 ч)**	2			Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,6,7]	
2	**Тема 2. Основы сетевых технологий (8 ч)**	4	4		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
3	**Тема 3. Общие принципы организации цифровых сетей (6 ч)**	4	2		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
4	**Тема 4. Угрозы, уязвимости и риски информационной безопасности сетевых устройств (10 ч)**	4		6	Учебники, методическая литература, конспект лекций, презентации с проек-	[1,4,6,7]	Отчет по практическим работам, защита

					тора и ноутбука, класс персональных компьютеров		практических работ
5	**Тема 5. Методы защиты информации на физическом уровне (1 ч)**	1			Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,6,7]	
6	**Тема 6. Криптографические методы защиты информации (4 ч)**	2		2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,3,5,6,7]	Отчет по практическим работам, защита практических работ
7	**Тема 7. Технологии канального уровня (9 ч)**	5	4		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
8	**Тема 8. Стек протоколов TCP/IP (9 ч)**	5	4		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
9	**Тема 9. Средства аутентификации субъектов и управление доступом (6 ч)**	2		4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,5,6,7,8]	Отчет по практическим работам, защита практических работ

10	**Тема 10. Сетевые информационные службы (6 ч)**	4	2		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,5]	Отчет по лабораторным работам, защита лабораторных работ
11	**Тема 11. Протоколы сетевой безопасности (6 ч)**	2		4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,3,5,6,7]	Отчет по практическим работам, защита практических работ
12	**Тема 12. Обеспечение информационной безопасности при работе в сети Интернет (1 ч)**	1			Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,5,6,7]	
13	**Тема 13. Комплексный подход при организации защиты информации (4 ч)**	2		2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,3,4,6,7]	Отчет по практическим работам, защита практических работ

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (заочная сокращенная форма обучения)

Номер темы, занятия	Название темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов			Самостоятельное изучении материала, час	Материальное обеспечение занятия (наглядные методические пособия и др.)	Литература	Форма контроля знаний
		лекции	лабораторные занятия	практические занятия				
1	**Тема 1. Основные понятия и принципы защиты информации (2 ч)**	1			1	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,6,7]	
2	**Тема 2. Основы сетевых технологий (8 ч)**	1			7	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	
3	**Тема 3. Общие принципы организации цифровых сетей (6 ч)**	1	2		3	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ

4	**Тема 4. Угрозы, уязвимости и риски информационной безопасности сетевых устройств (10 ч)**	1		2	7	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,4,6,7]	Отчет по практическим работам, защита практических работ
5	**Тема 5. Методы защиты информации на физическом уровне (1 ч)**				1	Учебники, методическая литература	[1,6,7]	
6	**Тема 6. Криптографические методы защиты информации (4 ч)**			1	3	Учебники, методическая литература, класс персональных компьютеров	[1,3,5,6,7]	Отчет по практическим работам, защита практических работ
7	**Тема 7. Технологии канального уровня (9 ч)**	1	2		6	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
8	**Тема 8. Стек протоколов TCP/IP (9 ч)**	1			8	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	
9	**Тема 9. Средства аутентификации субъектов и управление доступом (6 ч)**			1	5	Учебники, методическая литература, класс персональных компьютеров	[1,2,5,6,7,8]	Отчет по практическим работам, защита практических работ

10	**Тема 10. Сетевые информационные службы (6 ч)**	1			5	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,5]	
11	**Тема 11. Протоколы сетевой безопасности (6 ч)**	1			5	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,3,5,6,7]	
12	**Тема 12. Обеспечение информационной безопасности при работе в сети Интернет (1 ч)**				1	Учебники, методическая литература	[1,2,5,6,7]	
13	**Тема 13. Комплексный подход при организации защиты информации (4 ч)**				4	Учебники, методическая литература	[1,3,4,6,7]	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

КРИТЕРИИ ОЦЕНОК РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ

Оценка	Показатели оценки
незачет	Недостаточно полный объем знаний в вопросах дисциплины; знание только незначительной части основной литературы, рекомендованной учебной программой дисциплины, использование научной терминологии, изложение ответа на вопросы с существенными ошибками; слабое владение инструментарием учебной дисциплины, некомпетентность в решении стандартных (типовых) задач; пассивность на лабораторных и практических занятиях, низкий уровень культуры исполнения заданий.
зачет	Систематизированные, глубокие и полные знания по всем поставленным вопросам в сфере безопасности информационных технологий и сетей; точное использование научной терминологии, грамотное и логически правильное изложение ответа на вопросы, умение делать обобщения и обоснованные выводы; владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках учебной программы; достаточное усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины; умение оценивать угрозы, уязвимости и риски информационной безопасности, эффективность средств аутентификации, организовывать политику безопасности информационной системы; владение навыками настройки локальной вычислительной сети и конфигурирования сетевого оборудования; систематическая активная самостоятельная работа на лабораторных и практических занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Методы (технологии) обучения

Основными методами (технологиями), отвечающие целям изучения дисциплины, являются:

− элементы проблемного обучения, реализуемые при проведении всех видов учебных занятий по дисциплине;

− элементы учебно-исследовательской деятельности, реализуемые на практических занятиях и при самостоятельной работе.

Организация самостоятельной работы

При изучении дисциплины используются следующие формы самостоятельной работы:

− контролируемая самостоятельная работа в виде решения индивидуальных исследовательских задач в аудитории во время проведения практических занятий под контролем преподавателя в соответствии с расписанием;

− самостоятельная работа при подготовке к практическим занятиям.

Диагностика компетенций студента

Оценка учебных достижений студента на зачете производится по шкале «зачет-незачет».

Для оценки достижений студентов используется следующие формы:

− устные доклады на научно-технических конференциях;

− тесты и контрольные опросы по отдельным темам;

− отчеты по лабораторным работам с их устной защитой;

- отчеты по практическим работам с их устной защитой;
- проведение зачета по дисциплине в письменно-устной форме.

ОСНОВНАЯ ЛИТЕРАТУРА

1. **Олифер, В.** Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание / В. Олифер, Н. Олифер // Учебник для ВУЗов. 6-е изд. – СПб. : Питер, 2020. – 1008 с. (электронная версия)

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

2. **Буй, П.М.** Средства аутентификации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в системах управления на транспорте» / П.М. Буй, Д.Д. Семиход. – Гомель : БелГУТ, 2010. – 39 с.

3. **Буй, П.М.** Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в телекоммуникациооных системах» / П.М. Буй, В.О. Матусевич. – Гомель : БелГУТ, 2011. – 56 с.

4. **Белоусова, Е.С.** Политика безопасности информационных систем : учеб.-метод. пособие для практ. работ / Е.С. Белоусова, П.М. Буй. – Гомель : БелГУТ, 2016. – 38 с.

5. **Таненбаум, Э.** Компьютерные сети / Э. Таненбаум, Д. Уэзеролл // 5-е изд. – Спб. : Питер, 2012. – 960 с. (электронная версия)

6. **Романец, Ю. В.** Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с. (электронная версия)

7. **Домарев, В. В.** Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ООО «ТИД “ДС”», 2001. – 688 с. (электронная версия)

8. **Смит, Ричард Э.** Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. – М.: Издательский дом «Вильямс», 2002. – 432 с. (электронная версия)

ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ РАБОТ

Тема 2

1 Изучение принципов адресации, коммутации и маршрутизации в цифровых сетях;

2 Изучение модели взаимодействия открытых систем;

Тема 3

3 Изучения среды моделирования сетей Cisco Packet Tracer;

Тема 7

4 Изучение коммутируемой сети Ethernet;

5 Изучение виртуальных локальных сетей;

Тема 8

6 Статическая маршрутизация;

7 Изучение протоколов динамической маршрутизации;

Тема 10

8 Изучение работы сетевых информационных служб.

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 4

1 Анализ угроз и уязвимостей безопасности информационной системы;

2 Оценка рисков информационной безопасности;

3 Модель нарушителя информационной безопасности;

Тема 6

4 Оценка эффективности и производительности методов шифрования;

Тема 9

5 Исследование показателей эффективности парольных средств аутентификации;

6 Исследование показателей эффективности биометрических средств аутентификации;

Тема 11

7 Использование списков доступа для защиты информации в локальных сетях;

8 Защита информации в беспроводных сетях;

Тема 13

9 Политика безопасности информационных систем.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
ПО ДИСЦИПЛИНЕ
«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕЙ»
С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
1 Web-технологии	ИУСиТ	Согласовано	
2 Глобальные сети	АТиС	Согласовано	
3 Мультисервисные телекоммуникационные сети	АТиС	Согласовано	