

Учреждение образования
«Белорусский государственный университет транспорта»

УТВЕРЖДАЮ

Первый проректор

учреждения образования

«Белорусский государственный

университет транспорта»

 Ю.Г. Самодум

«24» « 03 » 2021

Регистрационный № УД- 56.34 / уч.

ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности:

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

Учебная программа составлена на основе образовательного стандарта ОСВО 1-37 02 04-2019 «Автоматика, телемеханика и связь на железнодорожном транспорте» и учебного плана ІЗ7-ЭАСМ-133/уч. от 04.07.2018.

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.);
методической комиссией 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 связи с резким увеличением вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации, а также резком увеличении объемов обрабатываемой информации в компьютерных системах и сетях при расширении круга пользователей, имеющих к ним доступ, актуальным становится вопрос об эффективной защите этой информации и оперативном реагировании на появление новых угроз ее информационной безопасности.

В связи с тем, что ни в глобальном, ни в региональном масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации по ее защите, актуальным становится вопрос об внедрении в компьютерные сети современных и эффективных систем защиты информации. Также важными задачами являются анализ угроз и уязвимостей информационной безопасности, анализ рисков, а также грамотная организация и построение комплексной системы защиты информации.

Программа разработана на основе компетентностного подхода, требований к формированию компетенций, сформулированных в образовательном стандарте ОСВО 1-37 02 04-2019 «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 «Основы сетевых технологий и защиты информации» является получение студентами базовых знаний в сфере сетевых технологий и особенностей обеспечения их информационной безопасности 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 учебным планом специальности 1-37 02 04 «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:

- основные принципы адресации, коммутации, маршрутизации в компьютерных сетях;
- уровни модели OSI и их назначение;

- технологии, применяемые на физическом уровне для организации компьютерных сетей;
- особенности протоколов канального, сетевого и транспортного уровней модели взаимодействия открытых систем;
- назначение и принцип работы наиболее распространенных сетевых информационных служб;
-
- Организационные, аппаратные и программные методы защиты информации, применяемые в компьютерных сетях;
- основные алгоритмы криптографического преобразования информации;
- уметь:**
- осуществлять адресацию сетевых интерфейсов с применением масок;
- организовывать виртуальные локальные сети;
- производить конфигурирование маршрутизаторов компьютерных сетей;
- проводить анализ вероятных угроз и уязвимостей информационной безопасности для заданных объектов;
- определять риски нарушения информационной безопасности телекоммуникационных систем;
- использовать протоколы сетевой безопасности и анализировать особенности их использования;
- владеть:**
- способами настройки таблиц маршрутизации сетевых устройств;
- методами защиты проводных и беспроводных каналов связи.

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. **Введение в сетевые технологии**

Эволюция сетей. Глобальные сети. Локальные сети. Конвергенция сетей. Интернет, как основной фактор развития сетевых технологий.

Тема 2. **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. Концепция национальной безопасности Республики Беларусь. Концепция информационной безопасности Республики Беларусь. Краткий исторический экскурс по вопросам информационной безопасности.

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

Топология сети. Принципы адресации, маршрутизации, мультиплексирования/демультиплексирования. Коммутация каналов. Коммутация пакетов. Сравнительный анализ сетей с двумя способами коммутации. 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. **Стандартизация и архитектура построения сетей**

Стандартизация сетевых технологий. Стандартизация Интернет. Понятие открытой системы. Модель OSI. Протокол. Интерфейс. Уровни модели OSI. Стандартные стеки коммуникационных протоколов.

Тема 6. **Технологии физического уровня**

Классификация линий связи и их характеристики. Типы кабелей. Модуляция и манипуляция сигналами. Дискретизация аналоговых сигналов. Методы кодирования. Частотное, временное и спектральное мультиплексирование. Особенности беспроводной среды передачи. Множественный доступ с кодовым разделением каналов (CDMA). Физические стандарты Ethernet, Fast Ethernet, Gigabit Ethernet, 10G Ethernet, 100G Ethernet, IEEE 802.11.

Тема 7. **Методы защиты информации в компьютерных сетях**

Классификация методов защиты информации. Организационные методы. Аппаратные методы. Программные методы. Модели информационной безопасности. Триада «Конфиденциальность, доступность, целостность». Гексада Паркера. Модель STRIDE.

Тема 8. **Технологии канального уровня**

Технология Ethernet. Локальные адреса (MAC-адреса). Разделяемая среда передачи. Борьба с коллизиями. Беспроводные локальные сети (Wi-Fi). Персональ-

ные 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 9. 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 10. Технологии сетевого уровня

Протоколы сетевого уровня. Протокол IP. Сетевая адресация (IP-адресация). Использование масок при адресации. Технология CIDR. Протокол ARP. Доменные имена. Система DNS. Протокол DHCP. Структура заголовка IP-пакета. Маршрутизаторы, протоколы RIP, OSPF, EIGRP, BGP. Протокол ICMP. IPv6.

Тема 11. Технологии транспортного уровня

Понятие порта и сокета. Протокол UDP. Протокол TCP. Установление и разъединение логических соединений. Методы квитирования. Концепция скользящего окна при передаче данных.

Тема 12. 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 13. 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 14. Сетевая безопасность

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. Облачные сервисы и их безопасность. Защита информации в беспроводных сетях. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем.

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. Введение в сетевые технологии (1 ч)	1			Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	
2	Тема 2. Основные понятия и принципы защиты информации (2 ч)	2			Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,6,7]	
3	Тема 3. Общие принципы организации цифровых сетей (5 ч)	3	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 (8 ч)	4		4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,4,6,7]	Отчет по практическим работам, защита практических работ

5	Тема 5. Стандартизация и архитектура построения сетей (3 ч)	1	2		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
6	Тема 6. Технологии физического уровня (5 ч)	3	2		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
7	Тема 7. Методы защиты информации в компьютерных сетях (1 ч)	1			Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5,6,7]	
8	Тема 8. Технологии канального уровня (7 ч)	3	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. Криптографические методы защиты информации (4 ч)	2		2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,3,5,7,8]	Отчет по практическим работам, защита практических работ
10	Тема 10. Технологии сетевого уровня (12 ч)	6	4	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным и практическим работам, защита лабораторных и практических работ

11	Тема 11. Технологии транспортного уровня (2 ч)	2			Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	
12	Тема 12. Средства аутентификации субъектов и управление доступом (8 ч)	2		6	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,5,8]	Отчет по практическим работам, защита практических работ
13	Тема 13. Сетевые информационные службы (5 ч)	3	2		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,5]	Отчет по лабораторным работам, защита лабораторных работ
14	Тема 14. Сетевая безопасность (9 ч)	5		4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,4,5,6,7]	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 изучение материала, час	Материальное обеспечение занятия (наглядные методические пособия и др.)	Литература	Форма контроля знаний
		лекции	лабораторные занятия	практические занятия				
1	Тема 1. Введение в сетевые технологии (1 ч)				1	Учебники, методическая литература	[1,5]	
2	Тема 2. Основные понятия и принципы защиты информации (2 ч)	1			1	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,6,7]	
3	Тема 3. Общие принципы организации цифровых сетей (5 ч)	1	2		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 (8 ч)			2	6	Учебники, методическая литература	[1,4,6,7]	Отчет по практическим работам, защита практических работ

5	Тема 5. Стандартизация и архитектура построения сетей (3 ч)				3	Учебники, методическая литература	[1,5]	
6	Тема 6. Технологии физического уровня (5 ч)	1			4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	
7	Тема 7. Методы защиты информации в компьютерных сетях (1 ч)				1	Учебники, методическая литература	[1,5,6,7]	
8	Тема 8. Технологии канального уровня (7 ч)	1	2		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. Криптографические методы защиты информации (4 ч)				4	Учебники, методическая литература	[1,3,5,7,8]	
10	Тема 10. Технологии сетевого уровня (12 ч)	1		2	9	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	Отчет по практическим работам, защита практических работ
11	Тема 11. Технологии транспортного уровня (2 ч)	1			1	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	
12	Тема 12. Средства аутентификации субъектов и управление доступом (8 ч)				8	Учебники, методическая литература	[1,2,5,8]	

13	Тема 13. Сетевые информационные службы (5 ч)	1			4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,5]	
14	Тема 14. Сетевая безопасность (9 ч)	1			8	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,4,5,6,7]	

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 сферах сетевых технологий и защиты информации; 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:

- 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 используются 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 телекоммуникационных 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 «ГИД “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 3

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

Тема 5

2 Изучение модели взаимодействия открытых систем;

Тема 6

3 Изучения среды моделирования сетей Cisco Packet Tracer;

Тема 8

4 Изучение коммутируемой сети Ethernet;

5 Изучение виртуальных локальных сетей;

Тема 10

6 Изучение работы протокола DHCP;

7 Изучение принципов статической маршрутизации и протоколов динамической маршрутизации;

Тема 13

8 Изучение работы сетевых информационных служб.

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 4

1 Анализ угроз и уязвимостей безопасности компьютерной сети;

2 Оценка рисков информационной безопасности компьютерных сетей;

Тема 9

3 Алгоритмы шифрования для защиты информации в компьютерных сетях;

Тема 10

4 Использование масок для организации перекрытия адресных пространств при конфигурации нескольких подсетей;

Тема 12

5 Исследование показателей эффективности парольных средств аутентификации оконечных сетевых устройств;

6 Исследование показателей эффективности биометрических средств аутентификации;


7 Защита оконечных сетевых устройств и локальных сетей с использованием списков доступа;

Тема 14

8 Защита информации в беспроводных сетях;

9 Политика безопасности информационных систем.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
ПО ДИСЦИПЛИНЕ
«ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ»
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	