Учреждение образования
«Белорусский государственный университет транспорта»

УТВЕРЖДАЮ
Первый проректор
учреждения образования
«Белорусский государственный
университет транспорта
_____ Ю.Г. Самодум
«30» «05» 2017
Регистрационный № УД-20.36 /уч.

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-37 02 04 Автоматика, телемеханика и связь на железнодорожном транспорте
специализации:
1-37 02 04 02 Системы передачи и распределения информации

2017

Учебная программа составлена на основе образовательного стандарта ОСВО 1-37 02 04-2013 «Автоматика, телемеханика и связь на железнодорожном транспорте»

СОСТАВИТЕЛИ:
П.М. Буй, доцент кафедры «Системы передачи информации» учреждения образования «Белорусский государственный университет транспорта», кандидат технических наук, доцент;
Е.С. Белоусова, доцент кафедры «Системы передачи информации» учреждения образования «Белорусский государственный университет транспорта», кандидат технических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой «Системы передачи информации» учреждения образования «Белорусский государственный университет транспорта»
(протокол № 3 от 15 марта 2017 г.);
научно-методической комиссией электротехнического факультета учреждения образования «Белорусский государственный университет транспорта»
(протокол № 2 от 27 апреля 2017 г.);
научно-методической комиссией заочного факультета учреждения образования «Белорусский государственный университет транспорта»
(протокол № 3 от 14 апреля 2017 г.);
научно-методическим советом учреждения образования «Белорусский государственный университет транспорта»
(протокол № от мая 2017 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 информационных и телекоммуникационных системах. Кроме того, в телекоммуникационных системах на транспорте постоянно расширяется круг пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных, повсеместно используются сетевые технологии, происходит объединение локальных сетей с использованием глобальных. В связи с этим все более актуальным становится вопрос о защите информации в телекоммуникационных системах. Важными задачами являются анализ угроз и уязвимостей информационной безопасности, анализ рисков, а также грамотная организация и построение комплексной системы защиты информации в информационных системах. Поэтому важно, чтобы в процессе обучения студент освоил современные методы защиты информации в телекоммуникационных системах при условии возникновения угроз.

Программа разработана на основе компетентностного подхода, требований к формированию компетенций, сформулированных в образовательном стандарте ОСВО 1-37 02 04-2013 «Автоматика, телемеханика и связь на железнодорожном транспорте».

Дисциплина относится к циклу общепрофессиональных и специальных дисциплин, осваиваемых студентами специальности 1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте».

Цели и задачи учебной дисциплины

Целью преподавания дисциплины «Защита информации в телекоммуникационных системах» является получение студентами базовых знаний по вопросам защиты информации телекоммуникационных систем в условиях возникновения угроз различных по виду, происхождению и характеру.

Основными задачами дисциплины являются:

– изучение основных угроз информационной безопасности и уязвимостей объектов информатизации в телекоммуникационных системах;

– изучение методов и средств разграничения доступа, криптографического преобразования информации;

– получение знаний о методах защиты информации в проводных и беспроводных каналах связи;

– получение представлений о протоколах сетевой безопасности и методах удаленной аутентификации субъектов.

Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен закрепить и развить следующие академические (АК) и социально-личностные (СЛК) компетенции, предусмотренные в образовательном стандарте ОСВО 1- 37 02 04-2013:

АК-1. Уметь применять базовые научно-теоретическими знания для решения теоретических и практических задач;

АК-2. Владеть системным и сравнительным анализом;

АК-3. Владеть исследовательскими навыками;

АК-4. Уметь работать самостоятельно;

АК-5. Быть способным порождать новые идеи (обладать креативностью);

АК-6. Владеть междисциплинарным подходом при решении проблем;

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером;

АК-9. Уметь учиться, повышать свою квалификацию в течении всей жизни;

СЛК-5. Быть способным к критике и самокритике;

СЛК-6. Уметь работать в команде.

В результате изучения дисциплины студент должен обладать следующими профессиональными компетенциями (ПК), предусмотренными образовательными стандартами ОСВО 1-37 02 04-2013:

ПК-7. Осуществлять мероприятия по организации и сохранению информационной безопасности систем железнодорожной автоматики, телемеханики и связи в соответствии с действующим законодательством;

ПК-8. Обоснованно выбирать методы и критерии защиты систем железнодорожной автоматики, телемеханики и связи от перенапряжений;

ПК-10. Давать оценку функциональным узлам систем железнодорожной автоматики, телемеханики и связи с точки зрения их информационной и функциональной безопасности;

ПК-44. Содействовать применению систем железнодорожной автоматики, телемеханики и связи, обеспечивающих защиту обрабатываемой информации.

Для приобретения профессиональных компетенций ПК-7, ПК-8, ПК-10 и ПК-44 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;

уметь:

– 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:

– методами защиты проводных и беспроводных каналов связи;
– принципами защиты информации критически важных объектов информатизации.

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 общепрофессиональных и специальных дисциплин «Теория вероятности и математическая статистика», «Надежность устройств автоматики, телемеханики и связи», «Теоретические основы автоматики и телемеханики».

Форма получения высшего образования – дневная и заочная. По дневной форме обучения дисциплина изучается в 9 семестре.

В соответствии с учебным планом на изучение дисциплины отведено всего 110 часов, в том числе 72 аудиторных часа, из них лекции – 38 часов, практические занятия – 34 часа. 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	Практические занятия	Форма текущей аттестации
9	110	3	72	38	34	Зачет

Распределение аудиторных часов по семестрам, видам занятий заочной форме 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
5	9	8		8	4		4						
5	10	102	3	8	2		6			1			
Итого:		110	3	16	6		10						
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 50922-2000 «Защита информации. Основные термины и определения». Особенности информации, как объекта защиты. Виды информации в соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации». Краткий исторический экскурс по вопросам информационной безопасности. Задачи в сфере обеспечения информационной безопасности.

Тема 2. **Угрозы, уязвимости и риски информационной безопасности телекоммуникационных систем**

Понятие угрозы. Классификация угроз информационной безопасности телекоммуникационных систем по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков. Понятие атаки. Модель нарушителя информационной безопасности телекоммуникационных систем. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.

Тема 3. **Методы защиты информации в телекоммуникационных системах**

Классификация методов защиты информации в телекоммуникационных системах по характеру проводимых мероприятий. Организационные методы. Аппаратные методы. Программные методы. Модели информационной безопасности. Триада «Конфиденциальность, доступность, целостность». Гексада Паркера. Модель STRIDE.

Тема 4. **Криптографические методы защиты информации в телекоммуникационных системах**

Классификация криптографических методов защиты информации. Архивация и кодирование информации. Шифрование информации. Симметричные методы шифрования в телекоммуникационных системах. Алгоритмы DES и AES. Режимы шифрования. Асимметричные методы шифрования в телекоммуникационных системах. Алгоритмы RSA и Эль-Гамаля. Цифровая подпись. Хеш-функции. Управление криптографическими ключами: генерация, хранение и распределение ключей. Стеганография.

Тема 5. **Средства аутентификации субъектов и управление доступом**

Понятие идентификации и аутентификации. Классификация средств аутентификации. Парольные средства аутентификации для оконечных устройств телекоммуникационных систем. Средства аутентификации с использованием смарт-карт и электронных ключей. Биометрические средства аутентификации. Строгая аутентификация в компьютерных сетях. Протоколы аутентификации. Технологии управления доступом и авторизация. Дискретный и мандатный методы управления доступом. Ролевое управление доступом. Управление доступом в операционных системах.

Тема 6. **Сетевая безопасность**

Фильтрация трафика. Межсетевые экраны. Прокси-серверы. Системы и средства мониторинга трафика. Системы обнаружения вторжений. Атаки на стек протоколов TCP/IP. Защита сетевых соединений. Протокол IPsec. Использование виртуальных частных сетей для защиты сетевых соединений. Безопасность сетевых служб. Вредоносное программное обеспечение. Протокол HTTPS. Облачные сервисы и их безопасность. Защита информации беспроводных сетях. Безопасность в сетях 802.11. Безопасность систем Bluetooth.

Тема 7. **Защита информации критически важных объектов информатизации**

Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности. Постановление Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации». Особенности функциональной безопасности. Защита информации в АСУ ТП.

Тема 8. **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.

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	практические занятия			
1	**Тема 1. Основные понятия и принципы защиты информации (4 ч)**	2	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,3,8]	Отчет по практическим работам, защита практических работ
2	**Тема 2. Угрозы, уязвимости и риски информационной безопасности телекоммуникационных систем (10 ч)**	4	6	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,7]	Отчет по практическим работам, защита практических работ
2.1	Понятие угрозы. Классификация угроз информационной безопасности телекоммуникационных систем по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков.	2	4			
2.2	Понятие атаки. Модель нарушителя информационной безопасности телекоммуникационных систем. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.	2	2			
3	**Тема 3. Методы защиты информации в телекоммуникационных системах (4 ч)**	2	2	Учебники, методическая литература, конспект лекций,	[1,3,8]	Отчет по практическим рабо-

				презентации с проектора и ноутбука, класс персональных компьютеров		там, защита практических работ
4	**Тема 4. Криптографические методы защиты информации в телекоммуникационных системах (10 ч)**	6	4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,3, 5,8]	Отчет по практическим работам, защита практических работ
4.1	Классификация криптографических методов защиты информации. Архивация и кодирование информации. Шифрование информации.	2				
4.2	Симметричные методы шифрования в телекоммуникационных системах. Алгоритмы DES и AES. Режимы шифрования. Асимметричные методы шифрования в телекоммуникационных системах. Алгоритмы RSA и Эль-Гамаля.	2	2			
4.3	Цифровая подпись. Хеш-функции. Управление криптографическими ключами: генерация, хранение и распределение ключей. Стеганография.	2	2			
5	**Тема 5. Средства аутентификации субъектов и управление доступом (14 ч)**	6	8	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,4, 6,8]	Отчет по практическим работам, защита практических работ
5.1	Понятие идентификации и аутентификации. Классификация средств аутентификации. Парольные средства аутентификации для оконечных устройств телекоммуникационных систем.	2	2			
5.2	Средства аутентификации с использованием смарт-карт и электронных ключей. Биометрические средства аутентификации. Строгая аутентификация в компьютерных сетях. Протоколы аутентификации.	2	4			
5.3	Технологии управления доступом и авторизация. Дискретный и мандатный методы управления доступом. Ролевое управление доступом. Управление доступом в операционных системах.	2	2			
6	**Тема 6. Сетевая безопасность (18 ч)**	10	8	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,3,8]	Отчет по практическим работам, защита практических работ
6.1	Фильтрация трафика. Межсетевые экраны. Прокси-серверы. Системы и средства мониторинга трафика. Системы обнаружения вторжений.	2	4			
6.2	Атаки на стек протоколов TCP/IP. Защита сетевых соединений. Протокол IPsec. Использование виртуальных частных сетей для защиты сетевых соединений.	3	2			
6.3	Безопасность сетевых служб. Компьютерные вирусы и механизмы	3				

	борьбы с ними. Протокол HTTPS. Облачные сервисы и их безопасность.					
6.4	Защита информации беспроводных сетях. Безопасность в сетях 802.11. Безопасность систем Bluetooth.	2	2			
7	**Тема 7. Защита информации критически важных объектов информатизации (6 ч)**	4	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2]	Отчет по практическим работам, защита практических работ
7.1	Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности.	2	2			
7.2	Постановление Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации». Особенности функциональной безопасности. Защита информации в АСУ ТП.	2				
8	**Тема 8. Комплексный подход при организации защиты информации (6 ч)**	4	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,3,7,8]	Отчет по практическим работам, защита практических работ
8.1	Методы оценки эффективности средств обеспечения информационной безопасности. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем.	2	2			
8.2	Концепция национальной безопасности Республики Беларусь.	2				

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (заочная 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	практические занятия				
1	**Тема 1. Основные понятия и принципы защиты информации (4 ч)**			4	Учебники, методическая литература, конспект лекций	[1,2,3,8]	
2	**Тема 2. Угрозы, уязвимости и риски информационной безопасности телекоммуникационных систем (10 ч)**	1	2	7	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,7]	Отчет по практическим работам, защита практических работ
2.1	Понятие угрозы. Классификация угроз информационной безопасности телекоммуникационных систем по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков.		2	4			
2.2	Понятие атаки. Модель нарушителя информационной безопасности телекоммуникационных систем. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.	1		3			
3	**Тема 3. Методы защиты информации в телекоммуникационных системах (4 ч)**	1		3	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,3,8]	

4	**Тема 4. Криптографические методы защиты информации в телекоммуникационных системах (10 ч)**	1	2	7	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,3, 5,8]	Отчет по практическим работам, защита практических работ
4.1	Классификация криптографических методов защиты информации. Архивация и кодирование информации. Шифрование информации.	1		1			
4.2	Симметричные методы шифрования в телекоммуникационных системах. Алгоритмы DES и AES. Режимы шифрования. Асимметричные методы шифрования в телекоммуникационных системах. Алгоритмы RSA и Эль-Гамаля.		2	2			
4.3	Цифровая подпись. Хеш-функции. Управление криптографическими ключами: генерация, хранение и распределение ключей. Стеганография.			4			
5	**Тема 5. Средства аутентификации субъектов и управление доступом (14 ч)**	1	2	11	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,4, 6,8]	Отчет по практическим работам, защита практических работ
5.1	Понятие идентификации и аутентификации. Классификация средств аутентификации. Парольные средства аутентификации для оконечных устройств телекоммуникационных систем.		2	2			
5.2	Средства аутентификации с использованием смарт-карт и электронных ключей. Биометрические средства аутентификации. Строгая аутентификация в компьютерных сетях. Протоколы аутентификации.	1		5			
5.3	Технологии управления доступом и авторизация. Дискретный и мандатный методы управления доступом. Ролевое управление доступом. Управление доступом в операционных системах.			4			
6	**Тема 6. Сетевая безопасность (18 ч)**	2	4	12	Учебники, методическая литература, конспект лекций, класс персональных компьютеров	[1,3,8]	Отчет по практическим работам, защита практических работ
6.1	Фильтрация трафика. Межсетевые экраны. Прокси-серверы. Системы и средства мониторинга трафика. Системы обнаружения вторжений.		2	4			
6.2	Атаки на стек протоколов TCP/IP. Защита сетевых соединений. Протокол IPsec. Использование виртуальных частных сетей для защиты сетевых соединений.	1		4			
6.3	Безопасность сетевых служб. Компьютерные вирусы и механизмы борьбы с ними. Протокол HTTPS. Облачные сервисы и их безопасность.	1		2			

6.4	Защита информации беспроводных сетях. Безопасность в сетях 802.11. Безопасность систем Bluetooth.		2	2			
7	**Тема 7. Защита информации критически важных объектов информатизации (6 ч)**			6	Учебники, методическая литература, конспект лекций	[1,2]	
7.1	Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности.			4			
7.2	Постановление Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации». Особенности функциональной безопасности. Защита информации в АСУ ТП.			2			
8	**Тема 8. Комплексный подход при организации защиты информации (6 ч)**			6	Учебники, методическая литература, конспект лекций	[1,3,7,8]	
8.1	Методы оценки эффективности средств обеспечения информационной безопасности. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем.			4			
8.2	Ценностно-надежностные аспекты при организации комплексной защиты информации. Назначение и цель политики информационной безопасности. Концепция национальной безопасности Республики Беларусь.			2			

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 практических занятиях, низкий уровень культуры исполнения заданий.
зачет	Систематизированные, глубокие и полные знания по всем поставленным вопросам в сфере информационной безопасности систем автоматики и телемеханики; 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; систематическая активная самостоятельная работа на 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 (АК-1, АК-2, АК-3, АК-4, АК-7, АК-9, СЛК-6, ПК-7, ПК-8, ПК-10, ПК-44);

− тесты и контрольные опросы по отдельным темам (АК-1, АК-2, АК-4, АК-9, ПК-7, ПК-8, ПК-10);

− отчеты по практическим работам с их устной защитой (АК-1, АК-2, АК-3, АК-4, АК-7, АК-9, СЛК-5, СЛК-6, ПК-7, ПК-8, ПК-10);

− проведение зачета по дисциплине в устной форме (АК-1, АК-2, АК-4, АК-5, АК-7, СЛК-5, ПК-7, ПК-8, ПК-10, ПК-44).

ОСНОВНАЯ ЛИТЕРАТУРА

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

2. **Яковлев, В. В.** Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта / В. В. Яковлев, А. А. Корниенко // Учебник для ВУЗов ж.-д. транспорта. – М.: УМК МПС России, 2002. – 328 с.

3. **Олифер, В.** Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер // Учебник для ВУЗов. 5-е изд. – СПб. : Питер, 2016. – 992 с.

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

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

5. **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, 2010. – 56 с.

6. **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.

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

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

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 1

1 Основы защиты информации;

Тема 2

2 Анализ угроз и уязвимостей безопасности телекоммуникационной системы;

3 Оценка рисков информационной безопасности;

4 Модель нарушителя информационной безопасности телекоммуникационной системы;

Тема 3

5 Обеспечение конфиденциальности, доступности и целостности информации в телекоммуникационной системе;

Тема 4

6 Оценка эффективности и производительности методов шифрования для применения в телекоммуникационных системах;

7 Исследование методов управления криптографическими ключами;

Тема 5

8 Исследование показателей эффективности парольных средств аутентификации оконечных устройств телекоммуникационных систем;

9 Исследование показателей эффективности биометрических средств аутентификации;

10 Исследование протоколов удаленной аутентификации;

11 Технологии управления доступом;

Тема 6

12 Защита локальной вычислительной сети;

13 Защита сетевых устройств;

14 Защита сетевых соединений;

15 Защита информации в сети 802.11;

Тема 7

16 Обеспечение информационной безопасности критически важных объектов информатизации;

Тема 8

17 Политика безопасности информационной системы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
ПО ДИСЦИПЛИНЕ
«ЗАЩИТА ИНФОРМАЦИИ
В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ»
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 Транспортные радиосистемы	СПИ	Согласовано	
2 Цифровые телекоммуникационные сети	СПИ	Согласовано	