Учреждение образования
«Белорусский государственный университет транспорта»

УТВЕРЖДАЮ
Первый проректор
учреждения образования
«Белорусский государственный
университет транспорта
_____ Ю.Г. Самодум
«30» « 05 » 2017
Регистрационный № УД- 20.37 / уч.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

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 01 Автоматика и телемеханика

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 современных системах автоматики и телемеханики. Кроме того, в системах автоматики и телемеханики постоянно расширяется круг пользователей, имеющих непосредственный доступ к управлению и к массивам данных, повсеместно используются сетевые технологии, происходит объединение локальных сетей в глобальные, применяется удаленное управление. В связи с этим все более актуальным становится вопрос о защите информации в системах управления на транспорте и, в частности, в системах автоматики и телемеханики. Важными задачами являются анализ причин возникновения каналов утечки информации, определение методов и средств их блокировки, а также грамотная организация и построение комплексной системы информационной безопасности для систем автоматики и телемеханики. Поэтому важно, чтобы в процессе обучения студент освоил современные методы обеспечения информационной безопасности таких систем в условиях 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 «Информационная безопасность систем автоматики и телемеханики» является получение студентами базовых знаний по вопросам обеспечения информационной безопасности управляющих систем на транспорте в условиях возникновения угроз различных по виду, происхождению и характеру.

Основными задачами дисциплины являются:

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

– изучение методов и средств аутентификации субъектов и разграничения доступа;

– получение знаний о применяемых методах криптографического преобразования информации;

– получение представлений о построении комплексной системы защиты информации.

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;

– активные и пассивные мероприятия по защите информации и средства их реализации;

уметь:

– проводить анализ вероятных угроз информационной безопасности для заданных объектов;

– определять риски нарушения информационной безопасности систем автоматики и телемеханики;

– разрабатывать рекомендации по защите объектов различного типа от несанкционированного доступа;

владеть:

– современными техническими средствами защиты информации;

– принципами организации и построения комплексных систем защиты информации.

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 полной и сокращенной формам 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. **Введение в информационную безопасность**

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 информационной безопасности систем автоматики и телемеханики**

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

Тема 3. **Правила разграничения доступа**

Смысл и необходимость разграничения доступа при организации информационного взаимодействия на объектах информатизации. Основные принципы организации разграничения доступа, и их применение.

Тема 4. **Методы защиты информации в системах автоматики и телемеханики**

Классификация методов защиты информации в системах автоматики и телемеханики по характеру проводимых мероприятий. Организационные методы. Аппаратные методы. Программные методы. Модели информационной безопасности. Обеспечение конфиденциальности, доступности и целостности информации.

Тема 5. **Сертификация и аттестация систем автоматики и телемеханики в сфере защиты информации**

Государственная политика информационной безопасности. Состав и основные функции государственной системы защиты информации Республики Беларусь. Оперативно-аналитический центр при Президенте Республики Беларусь, его цели и функции. Сертификация и аттестация средств защиты и объектов информации в Республике Беларусь. Стандарты Республики Беларусь серии 34.101. Задание по безопасности. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30 августа 2013 года «О некоторых вопросах технической и криптографической защиты информации».

Тема 6. **Криптографические методы защиты информации в системах автоматики и телемеханики**

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

Тема 7. **Средства аутентификации субъектов в системах автоматики и телемеханики**

Понятие идентификации и аутентификации. Классификация средств аутентификации в системах автоматики и телемеханики. Парольные средства аутентификации в системах автоматики и телемеханики. Средства аутентификации с использованием смарт-карт и электронных ключей в системах автоматики и телемеханики. Биометрические средства аутентификации.

Тема 8. **Информационная безопасность автоматизированных систем управления технологическими процессами**

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 9. **Комплексный подход к обеспечению безопасности информационных систем**

Методы оценки эффективности средств обеспечения информационной безопасности. Методы и средства защиты информации от удаленных атак. Вредоносное программное обеспечение. 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	практические занятия			
1	**Тема 1. Введение в информационную безопасность (2 ч)**	2		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,8]	
2	**Тема 2. Угрозы информационной безопасности систем автоматики и телемеханики (12 ч)**	4	8	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 систем автоматики и телемеханики по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков.	2	6			
2.2	Понятие атаки. Модель нарушителя информационной безопасности систем автоматики и телемеханики. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.	2	2			
3	**Тема 3. Правила разграничения доступа (4 ч)**	2	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука,	[1,2,8]	Отчет по практическим работам, защита практиче-

				класс персональных компьютеров		ских работ
4	**Тема 4. Методы защиты информации в системах автоматики и телемеханики (6 ч)**	4	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,8]	Отчет по практическим работам, защита практических работ
4.1	Классификация методов защиты информации в системах автоматики и телемеханики по характеру проводимых мероприятий. Организационные методы. Аппаратные методы. Программные методы.	2				
4.2	Модели информационной безопасности. Обеспечение конфиденциальности, доступности и целостности информации.	2	2			
5	**Тема 5. Сертификация и аттестация систем автоматики и телемеханики в сфере защиты информации (8 ч)**	4	4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,8]	Отчет по практическим работам, защита практических работ
5.1	Государственная политика информационной безопасности. Состав и основные функции государственной системы защиты информации Республики Беларусь. Оперативно-аналитический центр при Президенте Республики Беларусь, его цели и функции. Сертификация и аттестация средств защиты и объектов информации в Республике Беларусь. Стандарты Республики Беларусь серии 34.101.	2	2			
5.2	Задание по безопасности. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30 августа 2013 года «О некоторых вопросах технической и криптографической защиты информации».	2	2			
6	**Тема 6. Криптографические методы защиты информации в системах автоматики и телемеханики (14 ч)**	6	8	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,3,5]	Отчет по практическим работам, защита практических работ
6.1	Классификация криптографических методов защиты информации в системах автоматики и телемеханики. Архивация и кодирование информации. Шифрование информации. Симметричные методы шифрования. Алгоритмы DES и AES.	4	2			
6.2	Асимметричные методы шифрования. Алгоритмы RSA и Эль-Гамаля. Хэш-функции. Управление криптографическими ключами в системах автоматики и телемеханики: генерация, хранение и распределение ключей. Стеганография.	2	6			
7	**Тема 7. Средства аутентификации субъектов в системах автоматики и телемеханики (12 ч)**	6	6	Учебники, методическая литература,	[1,2,4,6]	Отчет по практиче-

7.1	Понятие идентификации и аутентификации. Классификация средств аутентификации в системах автоматики и телемеханики. Парольные средства аутентификации в системах автоматики и телемеханики.	2	2	конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров		ским работам, защита практических работ
7.2	Средства аутентификации с использованием смарт-карт и электронных ключей в системах автоматики и телемеханики. Биометрические средства аутентификации.	4	4			
8	**Тема 8. Информационная безопасность автоматизированных систем управления технологическими процессами (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
8.1	Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности.	2	2			
8.2	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				
9	**Тема 9. Комплексный подход к обеспечению безопасности информационных систем (8 ч)**	6	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,7,8]	Отчет по практическим работам, защита практических работ
9.1	Методы оценки эффективности средств обеспечения информационной безопасности. Методы и средства защиты информации от удаленных атак. Компьютерные вирусы и механизмы борьбы с ними. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем.	4				
9.2	Концепция национальной безопасности Республики Беларусь. Концепция информационной безопасности Республики Беларусь.	2	2			

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (заочная полная и сокращенная формы 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. Введение в информационную безопасность (2 ч)**			2	Учебники, методическая литература, конспект лекций	[1,2,8]	
2	**Тема 2. Угрозы информационной безопасности систем автоматики и телемеханики (12 ч)**	2	2	8	Учебники, методическая литература, конспект лекций, класс персональных компьютеров	[1,7]	Отчет по практическим работам, защита практических работ
2.1	Понятие угрозы. Классификация угроз информационной безопасности систем автоматики и телемеханики по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков.	1	2	5			
2.2	Понятие атаки. Модель нарушителя информационной безопасности систем автоматики и телемеханики. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.	1		3			
3	**Тема 3. Правила разграничения доступа (4 ч)**			4	Учебники, методическая литература, конспект лекций	[1,2,8]	
4	**Тема 4. Методы защиты информации в системах автоматики и телемеханики (6 ч)**	1		5	Учебники, методическая литература,	[1,2,8]	

4.1	Классификация методов защиты информации в системах автоматики и телемеханики по характеру проводимых мероприятий. Организационные методы. Аппаратные методы. Программные методы.			2	конспект лекций, презентации с проектора и ноутбука		
4.2	Модели информационной безопасности. Обеспечение конфиденциальности, доступности и целостности информации.	1		3			
5	**Тема 5. Сертификация и аттестация систем автоматики и телемеханики в сфере защиты информации (8 ч)**	1	2	5	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,8]	Отчет по практическим работам, защита практических работ
5.1	Государственная политика информационной безопасности. Состав и основные функции государственной системы защиты информации Республики Беларусь. Оперативно-аналитический центр при Президенте Республики Беларусь, его цели и функции. Сертификация и аттестация средств защиты и объектов информации в Республике Беларусь. Стандарты Республики Беларусь серии 34.101.		2	2			
5.2	Задание по безопасности. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30 августа 2013 года «О некоторых вопросах технической и криптографической защиты информации».	1		3			
6	**Тема 6. Криптографические методы защиты информации в системах автоматики и телемеханики (14 ч)**		2	12	Учебники, методическая литература, конспект лекций, класс персональных компьютеров	[1,2,3,5]	Отчет по практическим работам, защита практических работ
6.1	Классификация криптографических методов защиты информации в системах автоматики и телемеханики. Архивация и кодирование информации. Шифрование информации. Симметричные методы шифрования. Алгоритмы DES и AES..		2	4			
6.2	Асимметричные методы шифрования. Алгоритмы RSA и Эль-Гамаля. Хэш-функции. Управление криптографическими ключами в системах автоматики и телемеханики: генерация, хранение и распределение ключей.			8			
7	**Тема 7. Средства аутентификации субъектов в системах автоматики и телемеханики (12 ч)**	1	2	9	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональ-	[1,2,4,6]	Отчет по практическим работам, защита практических работ
7.1	Понятие идентификации и аутентификации. Классификация средств аутентификации в системах автоматики и телемеханики. Парольные средства аутентификации в системах автоматики и телемеханики.		2	2			

7.2	Средства аутентификации с использованием смарт-карт и электронных ключей в системах автоматики и телемеханики. Биометрические средства аутентификации.	1		7	ных компьютеров		
8	**Тема 8. Информационная безопасность автоматизированных систем управления технологическими процессами (6 ч)**		2	4	Учебники, методическая литература, конспект лекций, класс персональных компьютеров	[1,2]	Отчет по практическим работам, защита практических работ
8.1	Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности.		2	2			
8.2	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			
9	**Тема 9. Комплексный подход к обеспечению безопасности информационных систем (8 ч)**	1		7	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,7,8]	
9.1	Методы оценки эффективности средств обеспечения информационной безопасности. Методы и средства защиты информации от удаленных атак. Компьютерные вирусы и механизмы борьбы с ними. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем.	1		3			
9.2	Концепция национальной безопасности Республики Беларусь. Концепция информационной безопасности Республики Беларусь.			4			

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. **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.

2. **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.

3. **Мао, Венбо** Современная криптография: теория и практика / Венбо Мао // Пер с англ. – М.: Издательский дом «Вильямс», 2005. – 768с.

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

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 2

1 Анализ угроз безопасности информационной системы;

2 Количественная оценка рисков информационной безопасности;

3 Качественная оценка рисков информационной безопасности;

4 Модель нарушителя информационной безопасности системы автоматики и телемеханики;

Тема 3

5 Правила разграничения доступа;

Тема 4

6 Обеспечение конфиденциальности, доступности и целостности информации в системе автоматики и телемеханики;

Тема 5

7 Изучение СТБ 34.101.1, СТБ 34.101.2 и СТБ 34.101.3;

8 Анализ структуры задания по безопасности;

Тема 6

9 Оценка симметричных методов шифрования в системах автоматики и телемеханики;

10 Оценка асимметричных методов шифрования в системах автоматики и телемеханики;

11 Формирование электронно-цифровой подписи документа;

12 Исследование методов управления криптографическими ключами;

Тема 7

13 Исследование показателей эффективности парольных средств аутентификации в системах автоматики и телемеханики;

14 Исследование показателей эффективности биометрических средств аутентификации в системах автоматики и телемеханики;

15 Исследование показателей эффективности комбинированных средств аутентификации в системах автоматики и телемеханики;

Тема 8

16 Обеспечение информационной безопасности критически важных объектов информатизации;

Тема 9

17 Политика безопасности информационной системы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
ПО ДИСЦИПЛИНЕ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ»
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 Микропроцессорные информационно-управляющие системы в железнодорожной автоматике и телемеханике	МТиИУС	Согласовано	
2 Системы управления базами данных	МТиИУС	Согласовано	