МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 июня 2019 г.

Кафедра «Управление и защита информации»

Автор Клепцов Михаил Яковлевич, д.т.н., профессор

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Комплексные системы защиты информации объектов информатизации железнодорожного транспорта

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2019

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 25 июня 2019 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 21 24 июня 2019 г. Заведующий кафедрой  Л.А. Баранов

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Комплексные системы защиты информации на объектах железнодорожного транспорта» реализует требования федерального государственного образовательного стандарта по направлению 10.05.01 «Компьютерная безопасность».

Целью преподавания дисциплины «Комплексные системы защиты информации на объектах железнодорожного транспорта» является изложение студентам основных принципов построения и организации функционирования комплексных систем защиты информации компьютерных систем железнодорожного транспорта, ознакомление с современной технологией создания и внедрения комплексной системы защиты на объектах информатизации железнодорожного транспорта.

Данная дисциплина призвана содействовать системному подходу к процессу разработки и организации функционирования защищенных компьютерных систем. Во всех разделах дисциплины большое внимание уделяется практической направленности рассматриваемых методов и средств защиты.

Задачами дисциплины являются:

- четкое осознание необходимости и важности системного подхода к процессу разработки защищенных КС и соблюдение разумного компромисса между различными механизмами защиты;
- ознакомление с основными нормативно-правовыми и регламентными документами РФ в области защиты информации;
- умение разрабатывать концепцию и политики безопасности комплексной системы защиты информации КС;
- умение применять эффективные методы управления информационной безопасности, обеспечивающие требуемый уровень защищенности;
- умение выполнять работы по организации архитектуры комплексной системы защиты объектов информатизации.

Таким образом, дисциплина «Комплексные системы защиты информации на объектах ж.д. транспорта» является неотъемлемой составной часть. профессиональной подготовки по направлению 10.05.01 «Компьютерная безопасность». Вместе с другими дисциплинами цикла профессиональных дисциплин изучение данной дисциплины призвано формировать специалиста по защите информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Комплексные системы защиты информации объектов информатизации железнодорожного транспорта" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Основы информационной безопасности :

Знания: сущности и понятия информации, информационной безопасности и характеристику ее составляющих

Умения: Владения профессиональной терминологией в области информационной безопасности

Навыки: применения методов формирования требований к защите информации

2.1.2. Основы построения защищенных баз данных:

Знания: методик использования средств защиты, представленные средствами управления базами данных, а также основные принципы построения системы защиты баз данных

Умения: использование средств защиты, представленные средствами управления базами данных, а также основные принципы построения системы защиты баз данных

Навыки: владение методиками использования средств защиты, представленные средствами управления базами данных, а также основные принципы построения системы защиты баз данных

2.1.3. Основы построения защищенных компьютерных сетей:

Знания: механизмов реализации атак в сетях и средства обеспечения сетевой безопасности, включая средства и методы обнаружения вторжений для защиты информации в сетях

Умения: применение механизмов реализации атак в сетях и средства обеспечения сетевой безопасности

Навыки: применения механизмов реализации атак в сетях и средства обеспечения сетевой безопасности, включая средства и методы обнаружения вторжений для защиты информации в сетях

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Научно-исследовательская работа

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПКР-10 Способен проводить тестирование систем защиты информации автоматизированных систем	ПКР-10.1 Проводит индивидуальное тестирование систем защиты информации в блоке автоматизированных систем.
2	ПКР-7 Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	ПКР-7.1 Разрабатывает математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.2 Анализирует математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.3 Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
3	ПКС-2 Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации	ПКС-2.1 Знать основные процессы проектирования систем обеспечения информационной безопасности. ПКС-2.2 Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.
4	ПКС-3 Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации	ПКС-3.1 Знать основные методы и подходы к анализу защищенности компьютерных систем. ПКС-3.2 Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации. ПКС-3.3 Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.
5	ПКС-4 Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем	ПКС-4.1 Знать основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении. ПКС-4.2 Уметь создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации. ПКС-4.3 Владеть навыками создания систем обеспечения информационной безопасности.
6	ПКС-5 Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации	ПКС-5.1 Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации. ПКС-5.2 Уметь разрабатывать нормативно правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования. ПКС-5.3 Владеть навыками разработки нормативной

№ п/п	Код и название компетенции	Ожидаемые результаты
		правовой документации.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

5 зачетных единиц (180 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 10
Контактная работа	72	72,15
Аудиторные занятия (всего):	72	72
В том числе:		
лекции (Л)	54	54
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	108	108
ОБЩАЯ трудоемкость дисциплины, часы:	180	180
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	5.0	5.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КП (1), ПК1, ПК2	КП (1), ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	10	Раздел 1 Вводная лекция	2					2	
2	10	Тема 1.1 Цели и задачи обучения по программе «Комплексные системы защиты информации» / Проблемы защиты информации на современном этапе обработки информации в системах и сетях	2					2	
3	10	Раздел 2 Система нормативных и регламентных документов.	4				14	18	
4	10	Тема 2.1 Концептуальные нормативные документы.	2				6	8	
5	10	Тема 2.2 Процедурные нормативные документы. Инструкции, определяющие порядок действия должностных лиц при функционировании систем защиты информации. Журналы учета	2				8	10	
6	10	Раздел 3 Основные нормативно-правовые документы РФ в области защиты информации	4				20	24	
7	10	Тема 3.1 Доктрина информационной безопасности РФ	2				10	12	
8	10	Тема 3.2 Закон «Об информации, информационных технологиях и защите информации».	2				10	12	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Основные положения международного стандарта безопасности ISO 17799 и типовая политик безопасности, основанная на данном стандарте и стандарте ISO 27001							
9	10	Раздел 4 Стратегия построения комплексной системы защиты информации (КСЗИ).	6		5		28	39	
10	10	Тема 4.1 Разработка комплексной системы защиты информации. / Политика информационной безопасности. Оценка уязвимости и рисков информации	2		2		8	12	
11	10	Тема 4.2 Разработка методологии оценки риска. / Общие требования к комплексной системе защиты информации. Организационные требования.	2		2		10	14	
12	10	Тема 4.3 Требования к подсистемам защиты информации. Требования к среде защиты. Выбор средств защиты информации и их характиристик. Внедрение средств защиты и их тестирование	2				10	12	
13	10	Раздел 5 Основные принципы построения и функции комплексной системы защиты информации	6		4		8	18	
14	10	Тема 5.1 Принцип комплексности. Принцип эшелонирования.	2		2		8	12	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Принцип прочности. Принцип разумной достаточности. Принцип непрерывности.							
15	10	Тема 5.2 Обнаружение и отражение угроз. Этапы построения КСЗИ	4		2			6	
16	10	Раздел 6 Средства и методы в комплексной системе защиты информации.	8				10	18	
17	10	Тема 6.1 Меры защиты. / Организационно - правовые. Инженерно-технические. Информационно-технологические.	4				10	14	
18	10	Тема 6.2 Оперативно технологические меры защиты	4					4	
19	10	Раздел 7 Технология внедрения комплексной системы защиты информации.	8				10	18	
20	10	Тема 7.1 Объектовые исследования технических средств системы на побочные электромагнитные излучения и наводки с целью определения соответствия установленной категории. / Реализация разрешительной системы доступа пользователей и эксплуатационного персонала ИС к обрабатываемой информации.	4				10	14	
21	10	Тема 7.2 Включение и настройка комплекса программных средств защиты информации в общую программную	4					4	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		среду системы. Отработка рабочей документации и должностных инструкций по эксплуатации комплексной системы защиты информации							
22	10	Раздел 8 Аудит и сертификация ИС и ее компонентов по требованиям информационной безопасности	4		3		8	15	
23	10	Тема 8.1 Цели и задачи аудита. Этапы проведения аудита. / Отчетные документы. Что такое сертификация и аттестация. Порядок сертификации. Показатели защищенности и классы защищенности ИС.	4		2		8	14	
24	10	Раздел 9 Архитектура и построение системы защиты информации на объекте информации	4		2		10	16	
25	10	Тема 9.1 Методы, средства и мероприятия системы защиты. / Основные методологические принципы построения КСЗИ. Ядро КСЗИ, семирубежная модель защиты. Управление механизмами защиты	4		2		10	16	
26	10	Раздел 10 Основные принципы защиты информации при хранении и использовании электронных и иных документов	8		4			12	
27	10	Тема 10.1 Организация работы со служебными документами.	4		2			6	
28	10	Тема 10.2	4		2			6	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Обслуживание и модификация технического и программного обеспечения ИС. Обеспечение и контроль физической целостности. Основные принципы защиты информации от несанкционированного доступа							
29	10	Раздел 11 Курсовой проект						0	КП
30	10	Раздел 12 Дифференцированный зачет						0	ЗаО
31		Всего:	54		18		108	180	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	10	РАЗДЕЛ 4 Стратегия построения комплексной системы защиты информации (КСЗИ). Тема: Разработка комплексной системы защиты информации. / Политика информационной безопасности. Оценка уязвимости и рисков информации	ПЗ 1 Разработка политики ИБ конкретного объекта информатизации	2
2	10	РАЗДЕЛ 4 Стратегия построения комплексной системы защиты информации (КСЗИ). Тема: Разработка методологии оценки риска. / Общие требования к комплексной системе защиты информации. Организационные требования.	ПЗ 2 Разработка политики ИБ конкретного объекта информатизации	2
3	10	РАЗДЕЛ 4 Стратегия построения комплексной системы защиты информации (КСЗИ).	ПК 1 Текущий контроль РИТМ	1
4	10	РАЗДЕЛ 5 Основные принципы построения и функции комплексной системы защиты информации Тема: Принцип комплексности. Принцип эшелонирования. Принцип прочности. Принцип разумной достаточности. Принцип непрерывности.	ПЗ 3 Разработка политики ИБ конкретного объекта информатизации	2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
5	10	РАЗДЕЛ 5 Основные принципы построения и функции комплексной системы защиты информации Тема: Обнаружение и отражение угроз. Этапы построения КСЗИ	ПЗ 4 Разработка политики ИБ конкретного объекта информатизации	2
6	10	РАЗДЕЛ 8 Аудит и сертификация ИС и ее компонентов по требованиям информационной безопасности Тема: Цели и задачи аудита. Этапы проведения аудита. / Отчетные документы. Что такое сертификация и аттестация. Порядок сертификации. Показатели защищенности и классы защищенности ИС.	ПЗ 5 Практика организации аудита информационной безопасности на конкретном объекте информатизации	2
7	10	РАЗДЕЛ 8 Аудит и сертификация ИС и ее компонентов по требованиям информационной безопасности	ПК 2 Текущий контроль РИТМ	1
8	10	РАЗДЕЛ 9 Архитектура и построение системы защиты информации на объекте информации Тема: Методы, средства и мероприятия системы защиты. / Основные методологические принципы построения КСЗИ. Ядро КСЗИ, семирубежная модель защиты. Управление механизмами защиты	ПЗ 6 Разработка семирубежной модели защиты для конкретного объекта информатизации	2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
9	10	РАЗДЕЛ 10 Основные принципы защиты информации при хранении и использовании электронных и иных документов Тема: Организация работы со служебными документами.	ПЗ 7 Разработка регламентной документации по ИБ конкретных объектов информатизации	2
10	10	РАЗДЕЛ 10 Основные принципы защиты информации при хранении и использовании электронных и иных документов Тема: Обслуживание и модификация технического и программного обеспечения ИС. Обеспечение и контроль физической целостности. Основные принципы защиты информации от несанкционированного доступа	ПЗ 8 Разработка регламентной документации по ИБ конкретных объектов информатизации	2
			ВСЕГО:	18 / 0

4.5. Примерная тематика курсовых проектов (работ)

Курсовой проект является заключительным этапом в изучении дисциплины Комплексные системы защиты информации объектов информатизации на железнодорожном транспорте и защищается в 10 семестре.

Целью курсового проекта по дисциплине КЗСИ является изучение и освоение основных принципов разработки КСЗИ и ее основных подсистем. Исходя из цели курсового проекта, можно выделить следующие:

1) Основные принципы построения и организации функционирования КЗСИ КС ж/д транспорта.
2) Анализ объектов защиты информации при создании КСЗИ.
3) Разработка эффективных политик безопасности при при проектировании КСЗИ.
4) Анализ и определение требований для создания КСЗИ.
5) Характеристика и анализ основных подсистем комплексной системы защиты информации

Для реализации цели и задач курсового проекта сформированы следующие темы курсового проектирования.

1) Основные факторы и принципы создания КСЗИ
2) Обеспечение ИБ сети компании на основе средств антивирусной защиты
3) Защита серверов на основе внедрения системы SAFE RDP
4) Защита в мобильных устройствах
5) Анализ рисков и угрозы КС
6) Системы централизованного управления КС
7) Модернизация сетевой безопасности предприятия на основе впн решений
8) Обеспечение целостности и сохранности данных при администрировании сети
9) Подсистема антивирусной защиты
10) Подсистема резервного копирования
11) Подсистема обнаружения атак
12) Подсистема управления ИБ централизованного мониторинга и аудита событий
13) Подсистема защиты каналов передачи данных
14) Подсистема идентификации и аутентификации пользователей
15) Подсистема регистрации и учета
16) Подсистема обеспечения целостности
17) Подсистема защиты информации в филиалах и дочерних организациях
18) Подсистема электронной почты
19) Системы виртуальных ловушек
20) Защита передачи голосовых данных в IP-сети
21) Организация защита периметра сети
22) Моделирование КЗСИ
23) Обеспечение информационной безопасности Web-приложений
24) Защита персональных данных и коммерческой тайны в АСУТР
25) Информационная безопасность хранилищ данных аналитических информационных систем

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Комплексные системы защиты информации объектов информатизации железнодорожного транспорта» осуществляется в форме лекций, лабораторных работ и практических занятий.
В соответствии с требованиями ФГОС ВПО по направлению 10.05.01 «Компьютерная безопасность» с целью формирования и развития профессиональных навыков студентов предусмотрено использовать и проводить разбор презентаций лучших дипломных проектов по данной специализации. Кроме того, предусмотрены мастер-классы специалистов из:
- академии ФСБ
- компании «Информзащита»
- лаборатории Касперского
- РОСАТОМА

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	10	РАЗДЕЛ 2 Система нормативных и регламентных документов. Тема 1: Концептуальные нормативные документы.	СР 1	6
2	10	РАЗДЕЛ 2 Система нормативных и регламентных документов. Тема 2: Процедурные нормативные документы. Инструкции, определяющие порядок действия должностных лиц при функционировании систем защиты информации. Журналы учета	СР 2	8
3	10	РАЗДЕЛ 3 Основные нормативно-правовые документы РФ в области защиты информации Тема 1: Доктрина информационной безопасности РФ	СР 3	10
4	10	РАЗДЕЛ 3 Основные нормативно-правовые документы РФ в области защиты информации Тема 2: Закон «Об информации, информационных технологиях и защите информации». Основные положения международного стандарта безопасности ISO 17799 и типовая политик безопасности, основанная на данном стандарте и	СР 4	10

		стандарте ISO 27001		
5	10	РАЗДЕЛ 4 Стратегия построения комплексной системы защиты информации (КСЗИ). Тема 1: Разработка комплексной системы защиты информации. / Политика информационной безопасности. Оценка уязвимости и рисков информации	СР 5 Препроектное обследование объекта информатизации. Определить основные этапы и виды работ при проведении предпроектного обследования	8
6	10	РАЗДЕЛ 4 Стратегия построения комплексной системы защиты информации (КСЗИ). Тема 2: Разработка методологии оценки риска. / Общие требования к комплексной системе защиты информации. Организационные требования.	СР 6 Препроектное обследование объекта информатизации. Определить основные этапы и виды работ при проведении предпроектного обследования	10
7	10	РАЗДЕЛ 4 Стратегия построения комплексной системы защиты информации (КСЗИ). Тема 3: Требования к подсистемам защиты информации. Требования к среде защиты. Выбор средств защиты информации и их характиристик. Внедрение средств защиты и их тестирование	СР 7 Препроектное обследование объекта информатизации. Определить основные этапы и виды работ при проведении предпроектного обследования	10
8	10	РАЗДЕЛ 5 Основные принципы построения и функции комплексной системы защиты информации Тема 1: Принцип комплексности. Принцип эшелонирования. Принцип прочности. Принцип разумной достаточности. Принцип	СР 8 Подготовка документации. Разработать регламент в части защиты для компьютерной системы "Защита от несанкционированного доступа" для службы эксплуатации	8

		непрерывности.		
9	10	РАЗДЕЛ 6 Средства и методы в комплексной системе защиты информации. Тема 1: Меры защиты. / Организационно - правовые. Инженерно-технические. Информационно-технологические.	СР 9	10
10	10	РАЗДЕЛ 7 Технология внедрения комплексной системы защиты информации. Тема 1: Объектовые исследования технических средств системы на побочные электромагнитные излучения и наводки с целью определения соответствия установленной категории. / Реализация разрешительной системы доступа пользователей и эксплуатационного персонала ИС к обрабатываемой информации.	СР 10 Разработка моделей. Разработать модель злоумышленника в соответсвии с требованиями к обеспечению информационной безопасности	10
11	10	РАЗДЕЛ 8 Аудит и сертификация ИС и ее компонентов по требованиям информационной безопасности Тема 1: Цели и задачи аудита. Этапы проведения аудита. / Отчетные документы. Что такое сертификация и аттестация. Порядок сертификации. Показатели защищенности и классы защищенности ИС.	СР 11 Применение стандартов. Разработать основные положения и порядок проведения аудита для оценки соединения защищенности КС.	8
12	10	РАЗДЕЛ 9 Архитектура и построение системы защиты информации на объекте информации	СР 12 Внедрение КСЗИ. Раскрыть принципы построения системы защиты на конкретном объекте информатизации	10

		Тема 1: Методы, средства и мероприятия системы защиты. / Основные методологические принципы построения КСЗИ. Ядро КСЗИ, семирубежная модель защиты. Управление механизмами защиты		
			ВСЕГО:	108

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Информационная безопасность и защита информации	В.П. Мельников, С.А. Клейменов, А.М. Петраков	Издательский центр "Академия", 2011 ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)	Все разделы
2	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта	В.В. Яковлев, А.А. Корниенко	УМК МПС России, 2002 НТБ (уч.4); НТБ (фб.); НТБ (чз.1)	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	«Анализ тенденций развития теории практики компьютерной безопасности». Сборник трудов X1 пленума УМО вузов РФ по образовазованию в области ИБ	Лось В.П.,Черемушкин А.В.	Самара: Изд-во «Универс-Групп», , 2007	Все разделы
4	«Комплексная защита информации на предприятии»	Грибунин В. Г., Чудовский В. В	Издательский центр «Академия», М., , 2009	Все разделы
5	«Введение в защиту информации в автоматизированных системах». Учебное пособие	Малюк А.А.	2008	Все разделы
6	«Служба защиты информации: организация и управление»	Аверченков В.И.,Рытов М.Ю.	Изд-во БГТУ, , 2005	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

- Вузовские электронно-библиотечные системы учебной литературы
- База научно-технической информации ВИНИТИ РАН
- Интернет-ресурсы:

http://www.fstec.ru - сервер ФСТЭК (Федеральная служба по техническому и экспортному контролю
http://www.itsec.ru - информационная безопасность
http://www.security.lab.ru - информационный портал в области защиты информации
http://www.fstec.ru – материалы сайта фирмы «Лаборатория Касперского»
Электронно-библиотечная система должна обеспечивать возможность индивидуального

доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Не требуются

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Организация рабочего места студента в университете контролируется администрацией учебного заведения. Для лекций и семинаров имеется компьютерный класс (локальная сеть, состоящая из 20 рабочих мест (компьютеров), сервера, компьютера преподавателя, проектора, электронная доска).

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для освоения дисциплины «Комплексные системы защиты информации объектов информатизации ж.д. транспорта» рекомендуется к самостоятельному изучению следующие средства обеспечения ИБ:
- программные решения Safen Soft;
- Safen Soft Dip Guard Workstation – для защиты информации от утечки;
- Safen Soft Enterpise Suite – комплексная защита рабочих станций от всех видов вредоносного ПО и хакерских атак;
- Safen Soft WebServer – система безопасности для защиты корпоративных сайтов и web-серверов;
- Safen Soft Enterpise Suite Server - комплексная система защиты корпоративных серверов;
- система анализа угроз и рисков КСЗИ «Гриф»;
- система управления политикой ИБ «Кондор»