МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Комплексные системы защиты информации объектов информатизации железнодорожного транспорта

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

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. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-19 - Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

ПК-22 - Способен проводить тестирование систем защиты информации автоматизированных систем;

ПК-25 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-26 - Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-27 - Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем;

ПК-28 - 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.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Владеть:

Разрабатывает математические модели процессов, возникающих при работе программно- аппаратных средств защиты информации.

Уметь:

Разрабатывает математические модели процессов, возникающих при работе программно- аппаратных средств защиты информации.

Уметь:

Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.

Уметь:

Проводит индивидуальное тестирование систем защиты информации в блоке автоматизированных систем.

Знать:

Знать основные процессы проектирования систем обеспечения информационной безопасности.

Уметь:

Уметь разрабатывать и реализовывать технологию проведения аудита

информационной безопасности на объектах информатизации.

Уметь:

Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации.

Владеть:

Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.

Знать:

Знать основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении.

Уметь:

Уметь создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

Владеть:

Владеть навыками создания систем обеспечения информационной безопасности.

Знать:

Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации.

Уметь:

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.

Владеть:

Владеть навыками разработки нормативной правовой документации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144

академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №10
Контактная работа при проведении учебных занятий (всего):	72	72
В том числе:		
Занятия лекционного типа	36	36
Занятия семинарского типа	36	36

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 72 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Вводная лекция
2	Цели и задачи обучения по программе «Комплексные системы защиты информации» / Проблемы защиты информации на современном этапе обработки информации в системах и сетях
3	Система нормативных и регламентных документов

№ п/п	Тематика лекционных занятий / краткое содержание
4	Концептуальные нормативные документы.
5	Процедурные нормативные документы. Инструкции, определяющие порядок действия должностных лиц при функционировании систем защиты информации. Журналы учета
6	Основные нормативно-правовые документы РФ в области защиты информации
7	Доктрина информационной безопасности РФ
8	Закон «Об информации, информационных технологиях и защите информации».Основные положения международного стандарта безопасности ISO 17799 и типовая политик безопасности, основанная на данном стандарте и стандарте ISO 27001
9	Стратегия построения комплексной системы защиты информации (КСЗИ).
10	Разработка комплексной системы защиты информации. / Политика информационной безопасности. Оценка уязвимости и рисков информации
11	Разработка методологии оценки риска. / Общие требования к комплексной системе защиты информации. Организационные требования.
12	Требования к подсистемам защиты информации. Требования к среде защиты. Выбор средств защиты информации и их характиристик. Внедрение средств защиты и их тестирование
13	Основные принципы построения и функции комплексной системы защиты информации
14	Принцип комплексности. Принцип эшелонирования.Принцип прочности. Принцип разумной достаточности. Принцип непрерывности.
15	Обнаружение и отражение угроз. Этапы построения КСЗИ
16	Средства и методы в комплексной системе защиты информации.
17	Меры защиты. / Организационно - правовые. Инженерно-технические. Информационно-технологические.
18	Оперативно технологические меры защиты
19	Технология внедрения комплексной системы защиты информации.
20	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.
21	Включение и настройка комплекса программных средств защиты информации в общую программную среду системы. Отработка рабочей документации и должностных инструкций по эксплуатации комплексной системы защиты информации
22	Аудит и сертификация ИС и ее компонентов по требованиям информационной безопасности
23	Цели и задачи аудита. Этапы проведения аудита. / Отчетные документы. Что такое сертификация и аттестация. Порядок сертификации. Показатели защищенности и классы защищенности ИС.

№ п/п	Тематика лекционных занятий / краткое содержание
24	Архитектура и построение системы защиты информации на объекте информации
25	Методы, средства и мероприятия системы защиты. / Основные методологические принципы построения КСЗИ. Ядро КСЗИ, семирубежная модель защиты. Управление механизмами защиты
26	Основные принципы защиты информации при хранении и использовании электронных и иных документов
27	Организация работы со служебными документами.
28	Обслуживание и модификация технического и программного обеспечения ИС. Обеспечение и контроль физической целостности. Основные принципы защиты информации от несанкционированного доступа

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ1 Разработка политики ИБ конкретного объекта информатизации
2	ПЗ2 Разработка политики ИБ конкретного объекта информатизации
3	ПЗ3 Разработка политики ИБ конкретного объекта информатизации
4	ПЗ4 Разработка политики ИБ конкретного объекта информатизации
5	ПЗ5 Практика организации аудита информационной безопасности на конкретном объекте информатизации
6	ПЗ6 Разработка семирубежной модели защиты для конкретного объекта информатизации
7	ПЗ7 Разработка регламентной документации по ИБ конкретных объектов информатизации
8	ПЗ8 Разработка регламентной документации по ИБ конкретных объектов информатизации

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Концептуальные нормативные документы.
2	СР2 Процедурные нормативные документы. Инструкции, определяющие порядок действия должностных лиц при функционировании систем защиты информации. Журналы учета
3	СР3 Доктрина информационной безопасности РФ
4	СР4

№ п/п	Вид самостоятельной работы
	Закон «Об информации, информационных технологиях и защите информации». Основные положения международного стандарта безопасности ISO 17799 и типовая политик безопасности, основанная на данном стандарте и стандарте ISO 27001
5	СР5 Препроектное обследование объекта информатизации. Определить основные этапы и виды работ при проведении предпроектного обследования
6	СР6 Препроектное обследование объекта информатизации. Определить основные этапы и виды работ при проведении предпроектного обследования
7	СР7 Препроектное обследование объекта информатизации. Определить основные этапы и виды работ при проведении предпроектного обследования
8	СР8 Подготовка документации. Разработать регламент в части защиты для компьютерной системы "Защита от несанкционированного доступа" для службы эксплуатации
9	СР9 Меры защиты. / Организационно - правовые. Инженерно-технические. Информационно-технологические.
10	СР10 Разработка моделей. Разработать модель злоумышленника в соответсвии с требованиями к обеспечению информационной безопасности
11	СР11 Применение стандартов. Разработать основные положения и порядок проведения аудита для оценки соединения защищенности КС.
12	СР12 Внедрение КСЗИ. Раскрыть принципы построения системы защиты на конкретном объекте информатизации
13	Выполнение курсового проекта.
14	Подготовка к промежуточной аттестации.
15	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

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. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2011	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
2	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В. Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
1	«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	
2	«Комплексная защита информации на предприятии» Грибунин В. Г., Чудовский В. В Издательский центр «Академия», М. , 2009	
3	«Введение в защиту информации в автоматизированных системах». Учебное пособие Малюк А.А. 2008	
4	«Служба защиты информации: организация и управление» Аверченков В.И.,Рытов М.Ю. Изд-во БГТУ , 2005	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении 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.

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Не требуются

8. 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).

9. Форма промежуточной аттестации:

Зачет в 10 семестре.
Курсовой проект в 10 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы

Профессор, профессор, д.н. кафедры «Управление и защита информации»	Клепцов Михаил Яковлевич

Лист согласования

Заведующий кафедрой УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	С.В. Володин