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).

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:

Знать:

- Методологию разработки, анализа и обоснования адекватности математических моделей процессов работы программно-аппаратных средств защиты информации.
- Методики и инструментальные средства тестирования систем защиты информации автоматизированных систем.
- Структуру и содержание плана мероприятий по защите информации в объектах информатизации, включая этапы проектирования, создания и модернизации.
- Критерии и методики проведения анализа эффективности систем защиты информации в объектах информатизации.
- Принципы организации и этапы создания системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем.
- Требования к разработке проектов нормативных правовых актов, руководящих и методических документов, регламентирующих деятельность по защите информации.

Уметь:

- Разрабатывать математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации, и оценивать их адекватность.

- Проводить тестирование систем защиты информации автоматизированных систем с использованием соответствующих методик и инструментов.

- Разрабатывать и реализовывать план мероприятий по защите информации на объектах информатизации.

- Применять инструментальные средства анализа защищенности компьютерных систем для оценки эффективности систем защиты.

- Участвовать в создании системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

- Разрабатывать проекты нормативных правовых актов, руководящих и методических документов в области защиты информации.

Владеть:

- Навыками разработки и анализа математических моделей для оценки защищенности информации.

- Навыками проведения тестирования и оценки эффективности систем защиты информации.

- Навыками разработки документации по планированию мероприятий по защите информации на объектах информатизации.

- Навыками создания и сопровождения систем обеспечения информационной безопасности на объектах информатизации.

- Навыками разработки нормативной правовой и методической документации в области защиты информации.

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	Семестр №10
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32

Занятия семинарского типа	32	32

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 80 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 Рассматриваемые вопросы: - Цели и задачи обучения по программе «Комплексные системы защиты информации» - Проблемы защиты информации на современном этапе обработки информации в системах и сетях
2	Система нормативных и регламентных документов. Рассматриваемые вопросы: - Концептуальные нормативные документы.
3	Процедурные нормативные документы. Рассматриваемые вопросы: - Инструкции, определяющие порядок действия должностных лиц при функционировании систем защиты информации. - Журналы учета
4	Основные нормативно-правовые документы РФ в области защиты информации Рассматриваемые вопросы: - Основные нормативно-правовые документы РФ в области защиты информации - Доктрина информационной безопасности РФ - 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	Стратегия построения комплексной системы защиты информации (КСЗИ). Рассматриваемые вопросы: - Разработка комплексной системы защиты информации. - Политика информационной безопасности. - Оценка уязвимости и рисков информации

№ п/п	Тематика лекционных занятий / краткое содержание
	- Разработка методологии оценки риска. - Общие требования к комплексной системе защиты информации. - Организационные требования.
6	Требования к подсистемам защиты информации. Рассматриваемые вопросы: - Требования к среде защиты. - Выбор средств защиты информации и их характиристик. - Внедрение средств защиты и их тестирование
7	Основные принципы построения и функции комплексной системы защиты информации Рассматриваемые вопросы: - Принцип комплексности. - Принцип эшелонирования. - Принцип прочности. - Принцип разумной достаточности. - Принцип непрерывности.
8	Обнаружение и отражение угроз. Рассматриваемые вопросы: - особенности обнаружение и отражение угроз. - Этапы построения КСЗИ
9	Средства и методы в комплексной системе защиты информации. Рассматриваемые вопросы: - Меры защиты. - Организационно - правовые. - Инженерно-технические. - Информационно-технологические. - Оперативно технологические меры защиты
10	Технология внедрения комплексной системы защиты информации. Рассматриваемые вопросы: - 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.
11	Комплексные системы защиты информации. Рассматриваемые вопросы: - 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
12	Аудит и сертификация ИС и ее компонентов по требованиям информационной безопасности Рассматриваемые вопросы: - Цели и задачи аудита. - Этапы проведения аудита. - Отчетные документы. - Что такое сертификация и аттестация. - Порядок сертификации. - Показатели защищенности и классы защищенности ИС.
13	Архитектура и построение системы защиты информации на объекте информации Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Методы, средства и мероприятия системы защиты. - Основные методологические принципы построения КСЗИ. - Ядро КСЗИ, семирубежная модель защиты. - Управление механизмами защиты
14	Принципы защиты информации Рассматриваемые вопросы: - Основные принципы защиты информации при хранении и использовании электронных и иных документов
15	Работа со служебными документами. Рассматриваемые вопросы: - Организация работы со служебными документами.
16	Техническое и программное обеспечение ИС. Рассматриваемые вопросы: - 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	Анализ нормативно-правовой базы в области защиты информации В результате выполнения практического задания студент изучает основные нормативно-правовые документы РФ (Доктрина ИБ, закон «Об информации...», стандарты ISO 17799, 27001) и их применение при построении КСЗИ.
2	Разработка политики информационной безопасности для объекта информатизации В результате работы студент получает навык разработки политики ИБ для конкретного объекта информатизации (на примере предприятия ж.д. транспорта).
3	Оценка уязвимостей и рисков информации В результате выполнения практического задания студент осваивает методологию оценки рисков, учится выявлять уязвимости и определять критичность информационных активов.
4	Формирование требований к подсистемам защиты и выбор средств защиты В результате работы студент учится формулировать требования к среде защиты и выбирать соответствующие средства защиты информации на основе анализа рисков.
5	Разработка архитектуры КСЗИ В результате выполнения практического задания студент получает навык разработки многорубежной модели защиты для конкретного объекта информатизации.
6	Организация и проведение аудита информационной безопасности В результате работы студент изучает этапы проведения аудита ИБ на объекте, осваивает составление отчетных документов по результатам аудита.
7	Планирование мероприятий по защите информации В результате работы студент разрабатывает план мероприятий по защите информации для объекта информатизации, включая этапы внедрения, контроля и модернизации.
8	Разработка организационно-распорядительной документации В результате выполнения практического задания студент получает навык разработки инструкций, регламентов и приказов, регламентирующих работу с КСЗИ и служебными документами.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсового проекта.
4	Подготовка к промежуточной аттестации.
5	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	Защита информации в компьютерных информационных системах Пугин В.В., Голубничая Е.Ю., Лабада С.А. Учебное пособие Самара: ПГУТИ, - 119 с. , 2018	https://reader.lanbook.com/book/182299#2
2	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства Фомин Д.В. Методические указания Благовещенск: Амурский гос.ун-т, - 240 с. , 2017	https://reader.lanbook.com/book/156494#2

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

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

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» М.Я. Клепцов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин