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 бакалавриата
по направлению подготовки
27.03.04 Управление в технических системах,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Обеспечение информационной безопасности АСУ ТП

Направление подготовки: 27.03.04 Управление в технических системах

Направленность (профиль): Системы, методы и средства цифровизации и управления

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2024

1. Общие сведения о дисциплине (модуле).

Цель: Формирование у обучающихся комплекса теоретических знаний и практических навыков по обеспечению кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) на всех этапах их жизненного цикла для гарантированного обеспечения бесперебойности производственных процессов.

Задачи: Формирование комплекса знаний и навыков, необходимых для анализа уязвимостей промышленных сетей, применения нормативных требований и технических средств защиты АСУ ТП с целью обеспечения доступности и целостности технологических процессов, а также для проведения аудита и расследования инцидентов.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-6 - Способен осуществлять сбор и анализ исходных данных для формулирования задач разработки, расчета и проектирования систем и средств автоматизации и управления;

ПК-8 - Способен производить расчеты и проектирование отдельных блоков, компонент и устройств систем автоматизации и управления и выбирать стандартные средства автоматики, измерительной и вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием.

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

Знать:

- основные разработки, расчета и проектирования систем и средств автоматизации и управления
- номенклатуру и характеристики стандартных средств автоматики, измерительной и вычислительной техники, а также средств защиты информации для проектирования защищенных АСУ ТП.

Уметь:

- Разрабатывать и формулировать техническое задание для проектирования автоматизированной системы управления и (или) её составляющих.

- Выполнять документирование и моделирование бизнес-процессов и технологических процессов объекта автоматизации.

Владеть:

- навыками анализа существующих разработок систем и средств автоматизации и управления; формулирует критерии качества; обобщает выводы.

- навыками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта.

- навыками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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 №7
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 60 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	Введение Рассматриваемые вопросы: - Правовые основы обеспечения защиты информации.
2	Утечка информации по техническим каналам Рассматриваемые вопросы: - Технические каналы утечки информации. - Технические средства минимизации ущерба от инцидентов.
3	Информационные технологии. Рассматриваемые вопросы: - Угрозы безопасности информационных технологий. - Виды мер и основные принципы обеспечения безопасности информационных технологий. - Правовые основы обеспечения безопасности информационных технологий. - Государственная система защиты информации.
4	Меры и средства защиты информации. Рассматриваемые вопросы: - Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. - Организационная структура системы обеспечения безопасности информационных технологий. - Распределение функций. - Система нормативно-методических и организационно-распорядительных документов организации по обеспечению безопасности информационных технологий.
5	Аппаратно-программные средства защиты информации от несанкционированного доступа. Рассматриваемые вопросы: - Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа.
6	Безопасность в компьютерных системах и сетях Рассматриваемые вопросы: - Проблемы обеспечения безопасности в компьютерных системах и сетях. - Назначение, возможности, и основные защитные механизмы межсетевых экранов. - Виртуальные частные сети. - Обнаружение и устранение уязвимостей. - Возможности сканеров безопасности. - Анализ содержимого почтового и WEB-трафика (CONTENT SECURITY).
7	Аудит информационной безопасности Рассматриваемые вопросы: - События безопасности, аудит. - Мониторинг событий безопасности. - Стандартны и критерии проведения аудита информационной безопасности. 3. - Методология аудита информационной безопасности. Организация процесса аудита.

№ п/п	Тематика лекционных занятий / краткое содержание
8	Техническая защита информации Рассматриваемые вопросы: - Основные приборы и оборудование, применяемое для выявления технических каналов утечки информации. - Основы организации и обеспечения работ по технической защите информации. - Технические средства защиты информации и организация работ по защите информации.
9	Компьютерные инциденты Рассматриваемые вопросы: - Понятие о компьютерных инцидентах. - Минимизация ущерба, наносимого инцидентом. - Юридические предпосылки для расследования инцидентов и минимизации ущерба. - Расследование инцидентов в Российской Федерации и за рубежом. - Некоторые средства контроля коммуникаций и средств ЭВТ. - Действия в случае возникновения инцидента. - Изъятие и исследование компьютерной техники и носителей информации.
10	Методы аудирования. Рассматриваемые вопросы: - Основные понятия в области безопасности информационных технологий. - Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях. - Ответственность за нарушения. - Порядок работы с носителями ключевой информации. - Инструкции по организации паролей и антивирусной защиты. - Аудит информационной безопасности компаний: общие понятия и определения.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Технические каналы утечки информации в АСУ ТП Изучение классификации технических каналов утечки информации (электромагнитные, акустические, виброакустические, оптические). Анализ факторов, влияющих на возможность реализации угрозы по каждому из каналов. Разработка мероприятий по минимизации рисков для заданного типа объекта.
2	Угрозы безопасности информационных технологий в АСУ ТП и правовые основы защиты Анализ актуальных угроз для АСУ ТП (сетевые атаки, вредоносное ПО, инсайдеры). Изучение основных принципов обеспечения безопасности (законодательные, организационные, технические меры). Обзор ключевых нормативных документов (ФЗ-187, Приказы ФСТЭК).
3	Аппаратно-программные средства защиты от несанкционированного доступа Изучение состава и функций систем разграничения доступа. Анализ возможностей штатных средств защиты операционных систем и дополнительных средств (СКЗИ, замки доверенной загрузки). Практическая работа по настройке прав доступа в ОС семейства Windows/Linux.
4	Сетевые средства защиты: межсетевые экраны и виртуальные частные сети (VPN) Изучение принципов фильтрации трафика. Настройка политик межсетевого экрана (на примере встроенного firewall ОС или эмулятора). Принципы построения VPN для обеспечения защищенного удаленного доступа к сегменту АСУ ТП.

№ п/п	Тематика практических занятий/краткое содержание
5	Обнаружение и анализ уязвимостей АСУ ТП Изучение принципов работы сканеров безопасности (например, XSpider, OpenVAS). Проведение сканирования тестовой сети. Анализ отчета об уязвимостях. Разработка рекомендаций по устранению критических уязвимостей.
6	Аудит информационной безопасности и мониторинг событий Изучение методологии проведения аудита ИБ. Анализ стандартов аудита (ISO 27001). Настройка сбора и анализа событий безопасности в ОС Windows (журналы событий). Разработка плана аудита для гипотетического сегмента АСУ ТП.
7	Технические средства защиты информации и выявление каналов утечки Обзор приборов и оборудования для выявления каналов утечки (частотомеры, спектроанализаторы, детекторы поля). Изучение основ организации работ по технической защите информации на объекте. Разбор кейса по локализации ПЭМИН.
8	Компьютерные инциденты и порядок действий при их возникновении Классификация компьютерных инцидентов. Изучение процедуры расследования инцидентов (сбор доказательств, chain of custody). Разработка памятки (инструкции) для оператора АСУ ТП при обнаружении признаков вторжения. Разбор практических ситуаций.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

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", - 330 с., ISBN 978-5-7695-9222-5 , 2012	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, - 328 с., ISBN 5-89035-059-5 , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
3	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут, - 256 с., ISBN 5-89035-383-7 , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.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.

MathCAD 14.0 или другая система моделирования.

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 7 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» В.Г. Сидоренко

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин