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
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Комплексное обеспечение защиты объекта информатизации

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

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: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 12.06.2024

1. Общие сведения о дисциплине (модуле).

Цели и задачи изучения дисциплины «Комплексное обеспечение защиты объекта информатизации» соотносятся с общими целями ГОС ВПО по специальности/направлению подготовки. Слушатель получает систематизированные теоретические и практические знания в области информационной безопасности. Целью изучения дисциплины является формирование у студентов целостных представлений о всестороннем обеспечении защиты различных объектов информатизации.

Задачами освоения дисциплины являются:

• формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ состояния комплексной информационной безопасности на предприятии;

• изучение основ построения и реализации комплексной системы защиты информации объекта информатизации;

• изучение принципов и общих методов обеспечения информационной безопасности;

• изучение механизмов решения типовых задач программно-аппаратной защиты информации;

• формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ состояния комплексной информационной безопасности на предприятии.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1.4 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;

ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ;

ПК-4 - способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ;

ПК-7 - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной

безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ;

ПК-11 - способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

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

Знать:

- современные комплексы мер по обеспечению информационной безопасности;
- основные средства защиты информации, способы защиты информации от НСД;
- основные направления обеспечения информационной безопасности.

Уметь:

- разрабатывать предложения по совершенствованию системы защиты объектов информатизации от НСД;
- организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности;
- выявлять потенциальные каналы утечки информации;
- определять виды информации подверженные атакам потенциального злоумышленника;
- разрабатывать и реализовывать комплексные меры, обеспечивающие эффективность системы защиты информации.

Владеть:

- методологией выбора информационных ресурсов, подлежащий защите;
- разработкой предложения по совершенствованию системы защиты объектов информатизации;
- способностью обоснования критериев эффективности функционирования защищенных автоматизированных систем.

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 №8
Контактная работа при проведении учебных занятий (всего):	60	60
В том числе:		
Занятия лекционного типа	30	30
Занятия семинарского типа	30	30

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 84 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	Основы информационной безопасности Краткое содержание: Введение в предмет "Комплексное обеспечение защиты объекта информатизации". Рассмотрение основных понятий и принципов информационной безопасности. Определение целей и задач обеспечения безопасности объекта информатизации.
2	Угрозы информационной безопасности Краткое содержание: Изучение различных видов угроз информационной безопасности, таких как вирусы, хакерские атаки, фишинг и др. Анализ методов их распространения и последствий для объекта информатизации.
3	Анализ уязвимостей информационных систем Краткое содержание: Изучение методов анализа уязвимостей информационных систем. Определение основных уязвимых мест и слабых точек в объекте информатизации. Разработка плана мер по устранению уязвимостей.

№ п/п	Тематика лекционных занятий / краткое содержание
4	Физическая защита объекта информатизации Краткое содержание: Рассмотрение методов физической защиты объекта информатизации, таких как контроль доступа, видеонаблюдение, охранная сигнализация и др. Определение требований к физической безопасности.
5	Защита информационных систем Краткое содержание: Изучение методов защиты информационных систем объекта информатизации, включая аутентификацию, авторизацию, шифрование, бэкапы и др. Разработка плана мер по усилению защиты информационных систем.
6	Управление доступом и идентификацией Управление доступом и идентификацией
7	Управление рисками информационной безопасности Краткое содержание: Изучение методов управления рисками информационной безопасности. Определение потенциальных угроз и вероятности их реализации. Разработка плана мер по минимизации рисков.
8	Управление инцидентами информационной безопасности Краткое содержание: Рассмотрение методов управления инцидентами информационной безопасности. Анализ типичных инцидентов и разработка плана реагирования на них.
9	Обеспечение конфиденциальности информации Краткое содержание: Изучение методов обеспечения конфиденциальности информации в объекте информатизации. Разработка плана мер по защите конфиденциальных данных.
10	Обеспечение целостности информации Краткое содержание: Рассмотрение методов обеспечения целостности информации в объекте информатизации. Определение требований к контролю целостности данных.
11	Обеспечение доступности информации Краткое содержание: Изучение методов обеспечения доступности информации в объекте информатизации. Определение требований к отказоустойчивости и восстановлению после сбоев.
12	Обучение и осведомленность пользователей Краткое содержание: Разработка программы обучения пользователей в области информационной безопасности. Создание обучающих материалов и проведение тренингов.
13	Аудит информационной безопасности Краткое содержание: Изучение методов проведения аудита информационной безопасности в объекте информатизации. Анализ соответствия системы безопасности требованиям и стандартам.
14	Мониторинг и анализ безопасности информационных систем Краткое содержание: Рассмотрение методов мониторинга и анализа безопасности информационных систем объекта информатизации. Определение потенциальных угроз и разработка плана мер по их предотвращению.
15	Этические аспекты информационной безопасности Краткое содержание: Обсуждение этических аспектов информационной безопасности, включая вопросы конфиденциальности, неприкосновенности частной жизни, этики использования информации и др.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Анализ угроз информационной безопасности Краткое содержание: Студенты проводят анализ угроз информационной безопасности для конкретного объекта информатизации. Они изучают различные виды угроз, их распространение и последствия. В результате работы студенты получают навыки анализа угроз и определения их влияния на объект информатизации.
2	Анализ уязвимостей информационных систем Краткое содержание: Студенты проводят анализ уязвимостей информационных систем объекта информатизации. Они определяют основные уязвимые места и слабые точки в системе. В результате работы студенты получают навыки выявления уязвимостей и разработки плана мер по их устранению.
3	Разработка плана мер по обеспечению физической безопасности 2Краткое содержание: Студенты разрабатывают план мер по обеспечению физической безопасности объекта информатизации. Они изучают методы контроля доступа, видеонаблюдения, охранной сигнализации и другие методы физической защиты. В результате работы студенты получают навыки разработки плана мер по обеспечению физической безопасности.
4	Разработка плана мер по защите информационных систем Краткое содержание: Студенты разрабатывают план мер по защите информационных систем объекта информатизации. Они изучают методы аутентификации, авторизации, шифрования и другие методы защиты информационных систем. В результате работы студенты получают навыки разработки плана мер по усилению защиты информационных систем.
5	Разработка политики управления доступом и идентификацией Краткое содержание: Студенты разрабатывают политику управления доступом и идентификацией пользователей в информационных системах объекта информатизации. Они определяют требования к аутентификации и авторизации. В результате работы студенты получают навыки разработки политики управления доступом и идентификацией.
6	Разработка плана мер по минимизации рисков информационной безопасности Краткое содержание: Студенты разрабатывают план мер по минимизации рисков информационной безопасности. Они определяют потенциальные угрозы и вероятность их реализации. В результате работы студенты получают навыки разработки плана мер по минимизации рисков.
7	Разработка плана реагирования на инциденты информационной безопасности Краткое содержание: Студенты разрабатывают план реагирования на инциденты информационной безопасности. Они анализируют типичные инциденты и разрабатывают план действий для их предотвращения и устранения. В результате работы студенты получают навыки разработки плана реагирования на инциденты информационной безопасности.
8	Разработка плана мер по защите конфиденциальных данных Краткое содержание: Студенты разрабатывают план мер по защите конфиденциальных данных в объекте информатизации. Они изучают методы обеспечения конфиденциальности информации и разрабатывают план действий для их применения. В результате работы студенты получают навыки разработки плана мер по защите конфиденциальных данных.
9	Разработка плана мер по контролю целостности данных Краткое содержание: Студенты разрабатывают план мер по контролю целостности данных в объекте информатизации. Они определяют требования к контролю целостности данных и разрабатывают план действий для их обеспечения. В результате работы студенты получают навыки разработки плана мер по контролю целостности данных.

№ п/п	Тематика практических занятий/краткое содержание
10	Разработка плана мер по обеспечению доступности информации Краткое содержание: Студенты разрабатывают план мер по обеспечению доступности информации в объекте информатизации. Они изучают методы обеспечения отказоустойчивости и восстановления после сбоев и разрабатывают план действий для их применения. В результате работы студенты получают навыки разработки плана мер по обеспечению доступности информации.
11	Разработка программы обучения пользователей в области информационной безопасности Краткое содержание: Студенты разрабатывают программу обучения пользователей в области информационной безопасности. Они создают обучающие материалы и проводят тренинги для повышения осведомленности пользователей. В результате работы студенты получают навыки разработки программы обучения и проведения тренингов.
12	Проведение аудита информационной безопасности Краткое содержание: Студенты проводят аудит информационной безопасности в объекте информатизации. Они анализируют соответствие системы безопасности требованиям и стандартам и разрабатывают рекомендации по ее улучшению. В результате работы студенты получают навыки проведения аудита информационной безопасности.
13	Мониторинг и анализ безопасности информационных систем Краткое содержание: Студенты проводят мониторинг и анализ безопасности информационных систем объекта информатизации. Они определяют потенциальные угрозы и разрабатывают план мер по их предотвращению. В результате работы студенты получают навыки мониторинга и анализа безопасности информационных систем.
14	Разработка этических правил использования информации Краткое содержание: Студенты разрабатывают этические правила использования информации в объекте информатизации. Они обсуждают вопросы конфиденциальности, неприкосновенности частной жизни и этики использования информации. В результате работы студенты получают навыки разработки этических правил использования информации.
15	Практическое занятие по решению кейсов Краткое содержание: Студенты решают практические кейсы, связанные с комплексным обеспечением защиты объекта информатизации. Они применяют полученные знания и навыки для анализа ситуаций и разработки планов мер по обеспечению информационной безопасности. В результате работы студенты углубляют свои практические навыки в области комплексного обеспечения защиты объекта информатизации.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
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. Методологические основы организации комплексной системы защиты информации

2. Система управления информационной безопасностью предприятия.

3. Классификация информации по видам тайны и степеням конфиденциальности

4. Порядок внедрения Перечня сведений, составляющих коммерческой тайны, внесение в него изменений и дополнений

5. Этапы разработки комплексной системы защиты информации

6. Проектирование системы защиты информации для существующей АС

7. Технологическое и организационное построение комплексной системы защиты информации

8. Назначение, структура и содержание управления комплексной системы защиты информации

9. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

10. Факторы, определяющие необходимость защиты периметра и здания предприятия

11. Особенности помещений как объектов защиты для работы по защите информации

12. Факторы, создающие угрозу информационной безопасности

13. Угрозы безопасности информации

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

№ п/п	Библиографическое описание	Место доступа
1	Ларина Т. Б., Сетевые средства операционных систем : учебное пособие / Т. Б. Ларина. — Москва : РУТ (МИИТ), 2021. — 106 с. — Текст : электронный // Лань : электронно-библиотечная система	URL: https://e.lanbook.com/book/269561 (дата обращения: 01.03.2024). — Режим доступа: для авториз. пользователей.
2	Шелухин О.И., Системы обнаружения вторжений в компьютерные сети : учебное пособие / Шелухин О.И., Руднев А.Н., Савелов А.В.. — Москва : Московский технический университет связи и информатики, 2013. — 88 с. — Текст : электронный // Цифровой	URL: https://www.iprbookshop.ru/63360.html (дата обращения: 01.03.2024). — Режим доступа: для авторизир. пользователей

	образовательный ресурс IPR SMART : [сайт]	
3	Башлы П.Н., Информационная безопасность и защита информации : учебное пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К.. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/10677.html (дата обращения: 01.03.2024). — Режим доступа: для авторизир. пользователей

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

Современные профессиональные базы данных и информационные справочные системы не требуются.

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

Для проведения занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:

• Foxit Reader/Acrobat Reader

• Microsoft Office (Power Point)

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

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

Для проведения аудиторных занятий требуется специализированная лекционная аудитория с мультимедиа аппаратурой.

Для проведения практических работ: компьютеры с предустановленным Microsoft Windows не ниже Windows XP и процессором не ниже Pentium 4.

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

9. Форма промежуточной аттестации:

Курсовой проект в 8 семестре.
Экзамен в 8 семестре.

10. Оценочные материалы.

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

Авторы:

С.В. Антошкин

Согласовано:

Заведующий кафедрой ВССиИБ	Б.В. Желенков
Председатель учебно-методической комиссии	Н.А. Андриянова