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
02.03.02 Фундаментальная информатика и
информационные технологии,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы управления информационной безопасностью

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

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: 24.10.2024

1. Общие сведения о дисциплине (модуле).

Цели и задачи изучения дисциплины «Основы управления информационной безопасностью» 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 компетенций по основам управления информационной безопасностью (ИБ) на предприятии или в организации;
- изучение необходимых средств и методов;
- получение навыков по участию в работах по разработке, реализации политики информационной безопасности;
- примененииюе комплексного подхода к обеспечению информационной безопасности объекта защиты и совершенствованию систем управления информационной безопасностью (СУИБ)

Задачами освоения дисциплины являются:

- ознакомление с основными принципами построения информационной безопасности объекта защиты;
- формирование навыков по определению информационных ресурсов, подлежащих защите;
- изучение и определение возможных источников и видов угроз безопасности информации;
- получение навыков по реализации СУИБ на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
- изучение методов управления СУИБ на предприятии;
- получение знаний об основных методах контроля обеспечения информационной безопасности в организации
- формирование навыков построения политики информационной безопасности организации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-5 - Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности;

ПК-8 - Способность участвовать в работах по реализации политики

информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты и принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.

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

Знать:

- принципы формирования политики информационной безопасности в автоматизированных системах;
- основных угроз безопасности информации, порядка организации инженерно-технической защиты информации;
- основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия.

Уметь:

- оценивать информационные риски в автоматизированных системах;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- оценивать область применения элементов информационной безопасности; контролировать эффективность мер защиты;
- выявлять угрозы и технические каналы утечки информации.

Владеть:

- профессиональной терминологией в области информационной безопасности;
- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;
- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
- методами оценки работы элементов ИБ как отдельно, так и в системе.

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 в управление информационной безопасностью Краткое содержание: - введение в основы управления информационной безопасностью; - обзор основных понятий и принципов; - роль информационной безопасности в современных организациях.
2	Законодательные и нормативные основы информационной безопасности Краткое содержание: - обзор законодательных и нормативных актов, регулирующих область информационной безопасности; - анализ требований и стандартов.
3	Угрозы информационной безопасности Краткое содержание: - изучение различных типов угроз информационной безопасности;

№ п/п	Тематика лекционных занятий / краткое содержание
	- анализ методов их классификации и оценки рисков.
4	Анализ и управление рисками информационной безопасности Краткое содержание: - основы анализа и оценки рисков информационной безопасности; - методы управления рисками, выбор и применение контрмер.
5	Планирование и организация информационной безопасности Краткое содержание: - прроцесс планирования и организации информационной безопасности; - разработка политики и стратегии безопасности.
6	Управление доступом и идентификацией Краткое содержание: - основы управления доступом к информационным ресурса; - методы аутентификации и авторизации; - управление идентификацией пользователей
7	Защита информационных систем Краткое содержание: - обзор методов и средств защиты информационных систем; - принципы построения защищенных архитектур.
8	Управление инцидентами информационной безопасности Краткое содержание: - организация процесса управления инцидентами информационной безопасности; - реагирование на инциденты; - восстановление после инцидентов.
9	Правовые и этические аспекты информационной безопасности Краткое содержание: - рассмотрение правовых и этических вопросов в области информационной безопасности; - требования к этическому поведению специалистов.
10	Обучение и осведомленность пользователей Краткое содержание: - разработка и проведение программ обучения и осведомленности пользователей в области информационной безопасности.
11	Аудит информационной безопасности Краткое содержание: - роль и значение аудита в области информационной безопасности; - методы и процедуры проведения аудита.
12	Мониторинг и анализ безопасности информационных систем Краткое содержание: - основы мониторинга и анализа безопасности информационных систем; - выбор и применение инструментов мониторинга.
13	Управление уязвимостями информационной безопасности Краткое содержание: - идентификация и управление уязвимостями информационных систем; - методы и средства обнаружения и устранения уязвимостей.
14	Бизнес-планирование информационной безопасности Краткое содержание:

№ п/п	Тематика лекционных занятий / краткое содержание
	- разработка бизнес-планов в области информационной безопасности; - анализ эффективности инвестиций.
15	Управление изменениями в информационной безопасности Краткое содержание: - организация процесса управления изменениями в области информационной безопасности; - анализ рисков при внедрении изменений.
16	Контроль и улучшение процессов информационной безопасности Краткое содержание: - оценка и улучшение эффективности процессов информационной безопасности; - выбор и применение методов контроля и анализа.

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 конкретной организации, определяют потенциальные уязвимости и разрабатывают план мер по их устранению. В результате работы студенты получают навыки анализа угроз и разработки мер по обеспечению информационной безопасности.
2	Разработка политики информационной безопасности Краткое содержание: Студенты разрабатывают политику информационной безопасности для организации, определяют основные принципы и правила, которые должны соблюдаться сотрудниками. В результате работы студенты получают навыки разработки политики информационной безопасности.
3	Управление доступом и идентификацией Краткое содержание: Студенты проводят анализ системы управления доступом в организации, определяют требования к аутентификации и авторизации пользователей, разрабатывают рекомендации по улучшению системы. В результате работы студенты получают навыки управления доступом и идентификацией.
4	Защита информационных систем Краткое содержание: Студенты анализируют защиту информационных систем организации, определяют уязвимые места и разрабатывают план мер по усилению защиты. В результате работы студенты получают навыки анализа и улучшения защиты информационных систем.
5	Управление инцидентами информационной безопасности Краткое содержание: Студенты проводят симуляцию инцидента информационной безопасности, разрабатывают план реагирования на инцидент и восстановления после него. В результате работы студенты получают навыки управления инцидентами информационной безопасности.
6	Обучение и осведомленность пользователей

№ п/п	Тематика практических занятий/краткое содержание
	Краткое содержание: Студенты разрабатывают программу обучения пользователей в области информационной безопасности, создают обучающие материалы и проводят тренинги. В результате работы студенты получают навыки разработки и проведения программ обучения пользователей.
7	Аудит информационной безопасности Краткое содержание: Студенты проводят аудит информационной безопасности в организации, анализируют соответствие системы безопасности требованиям и стандартам, разрабатывают рекомендации по улучшению. В результате работы студенты получают навыки проведения аудита информационной безопасности.
8	Мониторинг и анализ безопасности информационных систем Краткое содержание: Студенты проводят мониторинг и анализ безопасности информационных систем организации, определяют потенциальные угрозы и разрабатывают план мер по их предотвращению. В результате работы студенты получают навыки мониторинга и анализа безопасности информационных систем.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом .
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	Управление организацией (предприятием) : учебное пособие для бакалавров и специалистов. / Под ред. И.М. Лаврова. – 2-е изд., перераб. и доп. – М.: РУТ (МИИТ), 2024. – 177 с.	https://library.miit.ru/bookscatalog/2024/ypravlenie_org.pdf
2	Соединение данных из множества таблиц.: Учебно-методическое пособие для бакалавров по направлению «Управление в технических системах» профиля	https://library.miit.ru/bookscatalog/upos/DC-1627.pdf

	«Управление и информатика в технических системах», а также специалистов по специальности «Компьютерная безопасность» специализации «Информационная безопасность объектов информатизации на базе компьютерных систем» / М. А. Васильева, Н. А. Ракинцев; Кафедра «Управление и защита информации». - М.: РУТ (МИИТ), 2023. - 60 с. - Б. ц.	
3	Фильтрация набора данных. Рекомендации по выполнению работы и перечень типовых заданий. : Учебно - методическое пособие для бакалавров по направлению Управление в технических системах, а также специалистов по специальности Компьютерная безопасность специализации Информационная безопасность объектов информатизации на базе компьютерных систем / М. А. Васильева , Д. О. Хобта; РУТ(МИИТ). Кафедра Управление и защита инофрмации . - - 122 с. - Б. ц.	https://library.miit.ru/bookscatalog/upos/DC-1625.pdf
4	Фильтрация набора данных: учебно-метод. пособие для бакалавров по напр. Управление в технических системах профиля Управление и информатика в технических системах, а также специалистов по спец. Компьютерная безопасность специализации Информационная безопасность объектов информатизации на базе компьютерных систем / М. А. Васильева, О. А. Тимофеева, К. М. Филипченко; МИИТ.	https://library.miit.ru/bookscatalog/metod/DC-1196.pdf

	Каф. Управление и защита информации. - Москва: РУТ (МИИТ), 2020. - 31 с. - Б. ц.	

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/
• Образовательная платформа «Юрайт» https://urait.ru/
• ЭБС ibooks.ru http://ibooks.ru/
• ЭБС "Лань" https://e.lanbook.com/book/

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

ОС Windows
Microsoft Office
Foxit Reader/Acrobat Reader
Интернет-браузер (Yandex и др.)

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий):

- компьютер преподавателя, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Экзамен в 7 семестре.

10. Оценочные материалы.

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

Авторы:

заведующий кафедрой, доцент, к.н.
кафедры «Вычислительные системы,
сети и информационная
безопасность» Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова