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 магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Управление информационной безопасностью

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Управление информационной безопасностью» являются формирование компетенций по основным разделам теоретических и практических основ создания, внедрения и развития систем управления информационной безопасностью и систем обеспечения информационной безопасности в организации, а также формирование практических навыков управления процессами обеспения информационной безопасности организации.

Основными задачами дисциплины являются:

• анализ и изучение положений нормативных правовых актов Российской Федерации, методологических документов, национальных и зарубежных стандартов в области обеспечения безопасности бизнес-процессов, информации и объектов информатизации.

• изучение основных понятий, относящиеся к управлению информационной безопасностью

• изучение подходов к формализации и внедрению процессов управления в организации

• рассмотрение особенностей создания систем управления и обеспечения информационной безопасности транспортных организаций как субъектов критической информационной инфраструктуры Российской Федерации

• рассмотрение основных методик и подходов в управлении ИТ-услугами (ITIL/ITSM/COBIT) в организации, в том числе вопроса интеграции процессов управления и обеспечения информационной безопасности

с процессами управления информационными технологиями

• рассмотрение методологии разработки общих и частных политик информационной безопасности организации.

• рассмотрение подходов к формированию системы организационно-распорядительных документов в организации, обеспечивающих функционирование систем управления и обеспечения информационной безопасности

• рассмотрение вопросов формирования стратегий развития систем управления и обеспечения информационной безопасности, с учетом тенденций и динамики развития информационных технологий.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

ПК-5 - Способность организовать управление информационной безопасностью;

ПК-6 - Способность организовать работу по созданию, модернизации и сертификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий ;

УК-4 - Способен применять современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для академического и профессионального взаимодействия.

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

Знать:

- общие принципы создания, внедрения и развития систем управления и обеспечения информационной безопасности организации;
- правовые нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России;
- методологию разработки системы организационно-распорядительной документации по информационной безопасности.
- методы организации системного подхода и выработке стратегии действий при организации управления информационной безопасностью
- методы последовательного, пошагового, разработанного на научной основе решения по обеспечению управления информационной безопасностью.

Уметь:

- разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;
- применять актуальную нормативную документацию в области защиты информации;
- управлять рисками информационной безопасности в деятельности организаци;
- проводить оценку и контроль эффективности функционирования процессов управления и обеспечения информационной безопасности;

- применять современные коммуникативные технологии в процессах управления информационными технологиями и информационной безопасностью.

Владеть:

навыками:

- разработки организационно-штатной структуры подразделений информационной безопасности организации политик информационной безопасности;

- графического описания процессов обеспечения информационной безопасности, планов развития, регламентов в области деятельности подразделений информационной безопасности организации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.

- организации управления информационной безопасностью;

- применения современных коммуникативных технологий, в том числе на иностранном (ых) языке (ах), для академического и профессионального взаимодействия.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 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 №3
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 152 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	БАЗОВЫЕ ВОПРОСЫ УПРАВЛЕНИЯ ИБ Рассматриваемые вопросы: - Термины и основные понятия. -Важность и актуальность дисциплины. - Ее взаимосвязь с другими дисциплинами специальности.
2	ПРИНЦИПЫ, ПОДХОДЫ И ВИДЫ УПРАВЛЕНИЯ. Рассматриваемые вопросы: - Цели и задачи управления ИБ. - Юридические аспекты создания систем управлени
3	СТАНДАРТИЗАЦИЯ В ОБЛАСТИ ИБ Рассматриваемые вопросы: - Общие сведения о стандартах. - ГОСТ Р ИСО/МЭК 27001. - Структура стандартов в области управления ИБ.
4	СОЗДАНИЕ СИСТЕМ УПРАВЛЕНИЯ ИБ НА ОСНОВЕ ТРЕБОВАНИЙ СТАНДАРТОВ Рассматриваемые вопросы: - Цикл Шухарта Деминга (Модель PDCA). - Основные факторы создания СУИБ. - Планирование.
5	ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ Рассматриваемые вопросы: Требования ФСТЭК Росии по безопасности информации
6	ОБЪЕКТЫ КИИ Рассматриваемые вопросы: обеспечение безопасности значимых объектов критической информационной инфраструктуры
7	ЗАЩИТА ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГИС. Рассматриваемые вопросы: - Требования о защите информации, содержащейся в ГИС: - Управлене информационной безопасностью в ГИС

№ п/п	Тематика лекционных занятий / краткое содержание
8	СЕРТИФИКАЦИЯ СИСТЕМ УПРАВЛЕНИЯ ИБ Рассматриваемые вопросы: - Системы сертификации. - Цели проведения сертификации. - Порядок проведения сертификации.
9	ПРОЦЕССНЫЙ ПОДХОД И ФОРМАЛИЗАЦИЯ ПРОЦЕССОВ Рассматриваемые вопросы: - Общие принципы. - Нотации описания процессов. - Методология разработки и внедрения процессов. - Ресурсное обеспечение процессов. - Оценка и развитие процессов.
10	ПОЛИТИКА ИБ Рассматриваемые вопросы: - Виды и области применения ПолИБ. - Содержание и основные положения ПолИБ.
11	ЖИЗНЕННЫЙ ЦИКЛ ПОЛИБ Рассматриваемые вопросы: - Стадии жизненного цикла. - Методология формирования требований ПолИБ.
12	ПОДХОДЫ УПРАВЛЕНИЕ ИТ-УСЛУГАМИ. Рассматриваемые вопросы: - Методики и практики управления ИТ-услугами. - Методики управление рисками и инцилентами ITIL.
13	ТИПОВЫЕ СТРУКТУРЫ СУИБ ТРАНСПОРТНЫХ ОРГАНИЗАЦИЙ Рассматриваемые вопросы: - Требования законодательства в области ИБ к трансопртным организациям. - Осбобенности управления и обеспечения ИБ транспортрых организаций.
14	ТИПОВЫЕ СТРУКТУРЫ СУИБ ТРАНСПОРТНЫХ ОРГАНИЗАЦИЙ (ПРОДОЛЖЕНИЕ) Рассматриваемые вопросы: - Рассмотрения структуры организаций управления ИБ в ключевых организациях транспортной отрасли.
15	СТРАТЕГИЧЕСКОЕ ПЛАНИРОВАНИЕ РАЗВИТИЯ СУИБ и СОИБ Рассматриваемые вопросы: - Тенденции развития информационных технологий. - Проблемные вопросы в области информационной безопасности.
16	СТРАТЕГИЧЕСКОЕ ПЛАНИРОВАНИЕ РАЗВИТИЯ СУИБ и СОИБ (продолжение) Рассматриваемые вопросы: - Организация и проведение оценки зрелости процессов. - Методология управления рисками при планировании. - Текущие тенденции развития в области Информационной безопасности.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Управление ИБ В процессе выполнения работы обучаемый получит практические навыки по разработке юридического обоснования создания СУИБ.
2	Определение категории объекта КИИ В процессе выполнения работы обучаемый получит практические навыки по выполнению процедуры категоризации объекта КИИ
3	Безопасность ИС В процессе выполнения работы обучаемый получит практические навыки по разработке требований по информационной безопасности в различных ИС
4	Разработка плана создания и внедрения СУИБ В процессе выполнения работы обучаемый получит практические навыки по планированию процедур СУИБ для предприятия
5	Разработка карты процессов обеспечения информационной безопасности организации В процессе выполнения работы обучаемый получит практические навыки по составлению карты верхнеуровневых процессов СОИБ.
6	Составление карты верхнеуровневых процессов СОИБ В процессе выполнения работы обучаемый получит практические навыки по внедрению СУИБ.
7	Доработка карты процессов ОИБ с учетом интеграций с процессами эксплуатации объектов информатизации В процессе выполнения работы обучаемый получит практические навыки и теоретические знания по вопросам интеграции процессов ОИБ в процессами управления ИТ-услугами
8	Разработка карты одного из процессов ОИБ с учетом требований нормативных правовых актов Российской Федерации В процессе выполнения работы обучаемый получит практические навыки графического составления карты процессов ОИБ.
9	Разработка общей Политики информационной безопасности организации с учетом требований законодательства Российской Федерации В процессе выполнения работы обучаемый получит практические навыки по разработке Политики ИБ организации.
10	Разработка регламентирующего документа по одного из процессов СОИБ В процессе выполнения работы обучаемый получит практические навыки по разработке организационно-распорядительной документации организации по реализации мер по защите информации.
11	Разработка перечня ключевых показателей эффективности функционирования процессов СОИБ В процессе выполнения работы обучаемый получит практические навыки по организации контроля над эффективностью процессов СОИБ.
12	Мониторинг и оценка эффективности процессов СОИБ В процессе выполнения работы обучаемый получит практические навыки по мониторингу и анализу процедур СУИБ для предприятия.
13	Разработка планов развития процессов СУИБ и СОИБ. В процессе выполнения работы обучаемый получит практические навыки по вопросам планирования развития и совершенствования СУИБ и СОИБ.

№ п/п	Тематика практических занятий/краткое содержание
14	Автоматизация процесса управления уязвимостями в организации В процессе выполнения работы обучаемый получит практические навыки по автоматизации процессов ОИБ.
15	Автоматизация контроля защищенности объектов информатизации организации В процессе выполнения работы обучаемый получит практические навыки по автоматизации процессов ОИБ
16	Составление карты рисков организации В процессе выполнения работы обучаемый получит практические навыки по практическому применению риск-ориентированного подхода при планировании деятельности СУИБ.

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. Разработка системы управления информационной безопасностью сети интернет магазинов.
2. Разработка системы управления информационной безопасностью аэропорта.
3. Разработка системы управления информационной безопасностью ж/д вокзала.
4. Разработка системы управления информационной безопасностью строительной компании.
5. Разработка системы управления информационной безопасностью автотранспортного предприятия пассажирских перевозок.
6. Разработка системы управления информационной безопасностью автотранспортного предприятия грузовых перевозок.
7. Разработка системы управления информационной безопасностью больницы.
8. Разработка системы управления информационной безопасностью школы.
9. Разработка системы управления информационной безопасностью детского сада

10. Разработка системы управления информационной безопасностью университета.

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

№ п/п	Библиографическое описание	Место доступа
1	Голиков А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 284 с. // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/110336 (дата обращения 29.04.2025)
2	Мэйволд Эрик. Безопасность сетей: курс лекций Москва :Интуит НОУ, 2016. — 572 с. — ISBN 978-5-9570-0046-9.	https://book.ru/book/917577 (дата обращения 29.04.2025)
3	Поздняк И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/255569 (дата обращения 29.04.2025)
4	Капгер И. В. Управление информационной безопасностью:учебное пособие / И. В. Капгер,А.С. Шабуров. — Пермь:ПНИПУ,2023.— 91 с.—ISBN 978-5-398-02866-9.Текст : электронный // Лань : электронно-библиотечная система	https://e.lanbook.com/book/328889 (дата обращения 29.04.2025)

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

- Научно-техническая библиотека РУТ(МИИТ) http://library.miit.ru/
- Нормативные правовые акты и другие документы в области защиты информации опубликованные ФСТЭК России https://fstec.ru
- Форум специалистов по информационным технологиям http://citforum.ru/
- Интернет-университет информационных технологий http://www.intuit.ru/

- Тематический форум по информационным технологиям http://habrahabr.ru/

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

- ОС Windows
- Microsoft Office
- 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, рабочие станции студентов, мультимедийное оборудование, доска.
- Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Курсовой проект в 3 семестре.
Экзамен в 3 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