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

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: 19.10.2022

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Управление информационной безопасностью» являются формирование компетенций по основным разделам теоретических и практических основ использования методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

Основными задачами дисциплины являются:

• изучение принципов анализа направлений развития информационно-коммуникационных технологий объекта защиты;

• изучение методов прогнозирования эффективности функционирования систем информационной безопасности;

• рассмотрение оценок затрат и рисков;

• формирование стратегии создания систем информационной безопасности в соответствии со стратегией развития организации;

• анализ угроз информационной безопасности объектов и разработка методов противодействия им.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность

• участие в фундаментальных и прикладных исследованиях в области профессиональной деятельности;

• разработка планов, программ и методик проведения исследований объектов профессиональной деятельности;

• подготовка по результатам научных исследований отчетов;

• научное руководство научно-исследовательскими и опытно-конструкторскими разработками в области информационной безопасности.

Проектная деятельность

• Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;

• Разработка, проектирование и модернизация систем безопасности компьютерных сетей и информационных систем;

• Разработка систем управления безопасностью компьютерных систем и сетей.

Организационно-управленческая деятельность

• организация управления информационной безопасностью;

• организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

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;

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

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

Знать:

- знать методы поиска и систематизации информации для анализа проблемных ситуаций;
- знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
- знать основные меры по защите информации в автоматизированных системах;
- знать организационные меры по защите информации;
- знать криптографические методы защиты информации;
- знать национальные, межгосударственные и международные стандарты в области защиты информации;
- знать нормативные правовые акты в области защиты информации;
- знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- знать организационные меры по защите информации.

Уметь:

- уметь анализировать проблемную ситуацию и применять системный подход к ее решению, прогнозировать и оценивать последствия принятых решений;
- уметь анализировать основные характеристики и возможности

телекоммуникационных систем по передаче информации;

- уметь анализировать основные узлы и устройства современных автоматизированных систем;

- уметь восстанавливать (заменять) отказавшие технические средства защиты информации;

- уметь анализировать компьютерную систему с целью определения уровня защищенности и доверия;

- уметь прогнозировать возможные пути развития действий нарушителя информационной безопасности;

- уметь производить анализ политики безопасности на предмет адекватности;

- уметь проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;

- уметь составлять и оформлять аналитический отчет по результатам проведенного анализа;

- уметь разрабатывать предложения по устранению выявленных уязвимостей.

Владеть:

- владеть навыками разработки алгоритмов решения проблемной ситуации и проведения выбора рационального решения из множества альтернативных;

- владеть проведением анализа структурных и функциональных схем, защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;

- владеть определением уровня защищенности и доверия в компьютерных системах;

- владеть оценкой рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем;

- владеть оценкой соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам;

- владеть подготовкой аналитического отчета по результатам проведенного анализа;

- владеть формулированием предложений по устранению выявленных уязвимостей.

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	Сем. №4
Контактная работа при проведении учебных занятий (всего):	24	24
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	8	8

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 120 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	Тема 1 Базовые вопросы управления ИБ. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	-Стандартизация в области управления ИБ. -Важность и актуальность дисциплины. - Ее взаимосвязь с другими дисциплинами специальности. - Содержание дисциплины. -Виды контроля знаний. -Сущность и функции управления. -Наука управления. -Принципы, подходы и виды управления. - Цели и задачи управления ИБ. - Понятие системы управления. -Стандартизация в области построения систем управления. Тема 2. Системы управления ИБ Рассматриваемые вопросы: -Процессный подход. - Понятие процесса. -Методы формализации процессов. -Область деятельности СУИБ. - Понятие области деятельности СУИБ. -Механизм выбора области деятельности. -Ролевая структура СУИБ. - Понятие роли. - Использование ролевого принципа в рамках СУИБ. -Политика СУИБ. - Понятие Политики СУИБ. -Цели Политики СУИБ. -Структура и содержание Политики СУИБ. И -сточники информации для разработки . -Политики СУИБ. Тема 3. Основы управления рисками ИБ Рассматриваемые вопросы: -Рискология ИБ. - Основные определения и положения рискологии. -Цель процесса анализа рисков ИБ. -Этапы и участники процесса анализа рисков ИБ. -Анализ рисков ИБ. - Методики анализа рисков ИБ. -Инвентаризация активов. -Понятие актива. -Типы активов. -Источники информации об активах организации. -Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Тема 4. Процессы управления ИБ. Рассматриваемые вопросы: -Основные процессы СУИБ. -Обязательная документация СУИБ. - Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). -Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия»,

№ п/п	Тематика лекционных занятий / краткое содержание
	«Предупреждающие действия»). - Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). - Понятие «Зрелость процесса». «Анализ со стороны высшего руководства». -Процесс «Обучение и обеспечение осведомленности». Тема 5. Внедрение разработанных процессов. Рассматриваемые вопросы: -Документ «Положение о применимости». -Этапы внедрения процессов и их последовательность. -Обучение сотрудников, как один из этапов внедрения. -Сложности, возникающие при внедрении процессов управления ИБ и способы их решения. - Контроль над внедрением процессов. -Документирование процесса внедрения разработанных процессов. -Типовой документ «Положение о применимости». -Цель документа. -Структура и содержание документа. -Процесс разработки документа, решение спорных ситуаций при разработке документа. -Внедрение мер (контрольных процедур) по обеспечению ИБ Категории контрольных процедур. -Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками. - Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик. Тема 6. Процесс «Управление инцидентами ИБ» Рассматриваемые вопросы: -Процесс «Управление инцидентами ИБ». - Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. - Входные/выходные данные процесса. -Участники процесса. -Обязательные этапы процесса. -Связи с другими процессами СУИБ. -Процесс «Обеспечение непрерывности ведения бизнеса». - Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». -Входные/выходные данные процесса. -Участники процесса. -Обязательные этапы процесса. -Связи с другими процессами СУИБ. Тема 7. Эксплуатация и независимый аудит СУИБ Рассматриваемые вопросы: -Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. -Внешние аудиты ИБ на соответствие требованиям нормативных документов. - Этапы проведения аудита ИБ. - Результаты аудита ИБ и их интерпретация. -Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. -Законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). -Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Практическое занятие №1. Планирование процедур СУИБ для предприятия. В процессе выполнения работы обучаемый получит практические навыки по планированию процедур СУИБ для предприятия. Практическое занятие №2 Внедрение процедур СУИБ для предприятия. В процессе выполнения работы обучаемый получит практические навыки по порядку внедрения процедур СУИБ на предприятия. Практическое занятие №3. Мониторинг и анализ процедур СУИБ для предприятия. В процессе выполнения работы обучаемый получит практические навыки по мониторингу и анализу процедур СУИБ для предприятия. Практическое занятие №4. Совершенствование СУИБ для предприятия. В процессе выполнения работы обучаемый получит практические навыки по совершенствование СУИБ для предприятия.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

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.	URL: https://e.lanbook.com/book/110336 (дата обращения: 04.10.2022). — Режим доступа: для авториз. пользователей.
2	Мэйволд Эрик. Безопасность сетей: курс лекций Москва :Интуит НОУ, 2016. — 572 с. — ISBN 978-5-9570-0046-9.	URL: https://book.ru/book/917577 (дата обращения: 04.10.2022). Текст : электронный.
3	Голдовский Я.М., Желенков Б.В.,Сафонова И.Е.Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ.,	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf.(дата обращения 04.10.2022)Текст : непосредственный.004 Г60

	обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. : МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р.	
4	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. —// Образовательная платформа Юрайт [сайт].	URL: https://urait.ru/bcode/490277 (дата обращения: 09.10.2022). Текст : электронный

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/

Официальный сайт по поддержке решений Cisco https://www.cisco.com/

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).

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

Microsoft Windows

Microsoft Office

Для проведения практических занятий необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

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

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.

Учебная аудитория для проведения практических занятий, лабораторных работ.

10 персональных компьютеров, 10 мониторов.

Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ

Рабочие станции для студентов 17шт, коммутатор CISCO – 9шт, маршрутизатор CISCO – 9шт, межсетевой экран Cisco, сетевое оборудование, рабочая станция преподавателя, проектор, экран..

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.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Курсовая работа в 4 семестре.

Экзамен в 4 семестре.

10. Оценочные материалы.

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

Авторы

Борискин Сергей
Михайлович

Лист согласования

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