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)

Основы информационной безопасности

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Дисциплина "Основы информационной безопасности" посвящена изучению основ информационной безопасности. В дисциплине предусмотрено изучение пяти учебных тем, объединенных единым замыслом. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. На основе единого подхода рассматриваются девять исторически сложившихся направлений информационной защиты. Излагаются разработанные или модифицированные автором качественные модели информационной защиты. Завершается изучение дисциплины двумя темами, посвященными двум наиболее существенным угрозам информационной безопасности – информационным преступлениям и информационным войнам. В рамках, указанных тем приводится классификация информационных и компьютерных преступлений, объясняются их причины, дается уголовно-правовая характеристика некоторых преступных деяний, рассматриваются основные стратегии информационных войн и виды информационного оружия.

Целью дисциплины «Основы информационной безопасности» является формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты. Приобретенные знания позволят студентам правильно ориентироваться в категориях защищаемых информационных ценностей и приобрести минимально необходимый кругозор в проблемах информационной безопасности. На основе данной дисциплины предполагается более подробно изучать различные направления защиты компьютерной безопасности.

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

Проектно-технологическая деятельность

-Разработка методов и средств технической защиты информации;

-Разработка технологических решений для обеспечения информационной безопасности в различных сферах.

Организационно-управленческая деятельность

-Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;

-Разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;

-Организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.

Экспериментально-техническая деятельность

-Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;

-Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации;

-Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации.

Эксплуатационная деятельность:

-установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

-администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных системю.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства ;

ОПК-10 - Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ;

ОПК-12 - Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для

технико-экономического обоснования соответствующих проектных решений .

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

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности.

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Владеть:

- профессиональной терминологией;
- навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и объектов информатизации;
- методами защиты информации.

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 №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 44 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 информационную безопасность Содержание учебного материала: - Понятие информации и информационной безопасности. - Информация, сообщения, информационные процессы как объекты информационной безопасности. - Обзор защищаемых объектов и систем.
2	Основные понятия теории информационной безопасности Содержание учебного материала: - История становления теории информационной безопасности. - Предметная область теории информационной безопасности. - Систематизация понятий в области защиты информации.
3	Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации»

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: - Основные принципы построения систем защиты. - Концепция комплексной защиты информации. - Задачи защиты информации. - Средства реализации комплексной защиты информации.
4	Информация как объект защиты Содержание учебного материала: - Понятие об информации как объекте защиты. - Уровни представления информации. Основные свойства защищаемой информации. - Виды и формы представления информации.
5	Информационные ресурсы и их защита Содержание учебного материала: - Информационные ресурсы. - Структура и шкала ценности информации. - Классификация информационных ресурсов. - Правовой режим информационных ресурсов.
6	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности Содержание учебного материала: - Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. - Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
7	Угрозы информационной безопасности Содержание учебного материала: - Анализ уязвимостей системы. - Классификация угроз информационной безопасности. - Основные направления и методы реализации угроз. - Неформальная модель нарушителя. - Оценка уязвимости системы.
8	Построение систем защиты от угрозы нарушения конфиденциальности Содержание учебного материала: - Определение и основные способы несанкционированного доступа. - Методы защиты от НСД. - Организационные методы защиты от НСД. - Инженерно-технические методы защиты от НСД. - Построение систем защиты от угрозы утечки по техническим каналам.
9	Методы контроля доступа к информации Содержание учебного материала: - Идентификация и аутентификация. - Основные направления и цели использования криптографических методов. - Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
10	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа Содержание учебного материала: - Защита целостности информации при хранении. - Защита целостности информации при обработке. Защита целостности информации при транспортировке. - Защита от угрозы нарушения целостности информации на уровне содержания.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Построение систем защиты от угрозы отказа доступа к информации. - Защита семантического анализа и актуальности информации.
11	Политика и модели безопасности Содержание учебного материала: - Политика безопасности. - Субъектно-объектные модели разграничения доступа. - Аксиомы политики безопасности. - Политика и модели дискреционного доступа. - Парольные системы разграничения доступа. - Политика и модели мандатного доступа. - Теоретико-информационные модели. - Политика и модели тематического разграничения доступа. - Ролевая модель безопасности.
12	Обзор международных стандартов информационной безопасности Содержание учебного материала: - Роль стандартов информационной безопасности. - Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. - Европейские критерии безопасности информационных технологий (ITSEC). - Федеральные критерии безопасности информационных технологий США. - Единые критерии безопасности информационных технологий. - Группа международных стандартов 270000.
13	Информационные войны и информационное противоборство Содержание учебного материала: - Определение и основные виды информационных войн. - Информационно-техническая война. - Информационно-психологическая война.
14	Нормативно правовое регулирование защиты информации Содержание учебного материала: - Организационная структура системы защиты информации. - Законодательные акты в области защиты информации. - Российские и международные стандарты, определяющие требования к защите информации. - Система сертификации РФ в области защиты информации. - Основные правила и документы системы сертификации РФ в области защиты информации.
15	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации Содержание учебного материала: - Основные механизмы защиты информации. - Система защиты информации. - Меры защиты информации, реализуемые в автоматизированных (информационных) системах. - Программные и программно-аппаратные средства защиты информации. - Инженерная защита и техническая охрана объектов информатизации. - Организационно-распорядительная защита информации. - Работа с кадрами и внутри объектовый режим. - Принципы построения организационно-распорядительной системы.
16	Управление информационной безопасностью предприятия Содержание учебного материала: - Объекты защиты информации на предприятии. - Классификация видов, способов, методов и средств защиты информации на предприятии. - Назначение и структура систем защиты информации.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Комплексная система защиты информации на предприятии.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Определение объектов защиты на типовом объекте информатизации. Основные признаки присутствия на компьютере вредоносных программ В результате выполнения лабораторной работы студент получит навыки классификации информационных активов по видам угроз и классам защищенности, а также навыки обнаружения вредоносного программного кода на персональном компьютере.
2	Обнаружение сетевой активности В результате выполнения лабораторной работы студент получит навыки обнаружения сетевой активности в защищаемой системе.
3	Справочно-правовые системы В результате выполнения лабораторной работы студент получит навыки работы в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.
4	Защита информации для автоматизированных рабочих мест. Управление правами пользователей в Windows В результате выполнения лабораторной работы студент получает навыки базовой настройки компонентов АРМ для обеспечения ИБ.
5	Криптографический алгоритм «Одноалфавитная подстановка» Криптографический алгоритм «Одноалфавитная подстановка».
6	Криптографический алгоритм «Многоалфавитная одноконтурная обыкновенная подстановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Многоалфавитная одноконтурная обыкновенная подстановка».
7	Криптографический алгоритм «Многоалфавитная одноконтурная монофоническая подстановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Многоалфавитная одноконтурная монофоническая обыкновенная подстановка»
8	Криптографический алгоритм «Многоалфавитная многоконтурная подстановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Многоалфавитная многоконтурная монофоническая обыкновенная подстановка».
9	Криптографический алгоритм «Простая перестановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Простая перестановка».
10	Криптографический алгоритм «Перестановка, усложненная по таблице» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Перестановка, усложненная по таблице».

№ п/п	Наименование лабораторных работ / краткое содержание
11	Криптографический алгоритм «Перестановка, усложненная по маршрутам» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Перестановка, усложненная по маршрутам».
12	Криптографический алгоритм «Гаммирование» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Гаммирование».
13	Криптографический алгоритм основанный на аналитических преобразованиях В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом аналитических преобразований на основе обработки прямой и транспонированной матриц.
14	Криптографический алгоритм символьного кодирования В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом символьного кодирования по кодовому алфавиту.
15	Комбинированный криптографический алгоритм «Подстановка + перестановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Подстановка + перестановка».
16	Комбинированный криптографический алгоритм «Перестановка + гаммирование» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифррования методом «Перестановка + гаммирование».

4.3. Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем курсовых работ

1. Формы психологической защиты человека от информационной перегрузки.

2. Социально вредная информация в СМИ.

3. Вредная и опасная информация в Интернет

4. Формы обмана и мошенничества в Интернет.

5. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.

6. Модель информационной защиты каналов связи.

7. Стратегия обмана и ее использование в сфере информационной

защиты.

8. Вопросы информационной безопасности в политике и дипломатии.

9. Организационно-распорядительные меры информационной защиты.

10. Традиционные направления информационной защиты и пути их интеграции.

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

№ п/п	Библиографическое описание	Место доступа
1	Кодирование и защита информации в документообороте: метод. указ. к практ. и лаб. раб. для студ. спец. Прикладная информатика (в экономике) по дисц. Информационная безопасность / В.И. Морозова, К.Э. Врублевский; МИИТ. Каф. Экономическая информатика. - М.: МИИТ, 2010. - 56 с.	URL: 03_19830.pdf (miit.ru). (дата обращения 03.03.2024) Текст : непосредственный.004.056.57 М 80
2	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с.	URL: 04-46051.pdf (miit.ru). (дата обращения 03.03.2024) Текст : непосредственный.004 К 72
3	Криптографическая защита компьютерной информации: метод. указ. к лаб. раб. по дисц. Теоретические основы компьютерной безопасности для студ., обуч. по напр. Информационная безопасность / Я. М. Голдовский, Б. В. Желенков, И. Е. Сафонова; МИИТ. Каф. Вычислительные системы и сети. - М.: МГУПС(МИИТ), 2013. - 36 с.	URL: 03-42764.pdf (miit.ru). (дата обращения 03.03.2024) Текст : непосредственный.004 Г60
4	Информационная безопасность персональных компьютеров: учеб. пособие для студ. спец. САПР и строительных спец. по курсу Методы и средства защиты компьютерной информации. Ч.2 / В.Ю. Смирнов, О.В. Смирнова; МИИТ. Каф. САПР транспортных конструкций и сооружений.М.: МИИТ, 2010. - 88 с.	URL: 10-2256.pdf (miit.ru). (дата обращения 03.03.2024) Текст : непосредственный.681.3.066 С 50
5	Разработка мер защиты информационных ресурсов в корпоративной сети с выходом в интернет: учебно-метод. пособие по курс. работе для специалистов напр. Компьютерная безопасность / В. М. Алексеев; МИИТ.	URL: DC-435.pdf (miit.ru). (дата обращения 03.03.2024) Текст : непосредственный.004 А-47

	Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2017. - 9 с.	

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

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

-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».

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

Для проведения аудиторных занятий и самостоятельной работы требуются:

- Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET.

- Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

-Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения практических занятий:

-компьютерный класс; кондиционер; компьютеры.

-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:

Зачет в 3 семестре.

Курсовая работа в 3 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова