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
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Программное обеспечение средств вычислительной техники и автоматизированных систем

Форма обучения: Очно-заочная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Основы информационной безопасности» являются изучение студентами основных понятий информационной безопасности, изучение основных видов угроз информационной безопасности; получение представления об организации и принципах обеспечения информационной безопасности; знакомство с

основами методов криптографического закрытия данных; получение навыков разработки политики безопасности предприятия, методами нарушения конфиденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

Основными задачами дисциплины являются:

• освоение методов оценки степени угрозы информационной безопасности;

• изучение использования соответствующих методов защиты.;

• рассмотрение методов организации комплексной системы защиты информации;

• изучение студентами основных угроз информационной безопасности и методов защиты

от них.

• процесса сбора, передачи, накопления и обработки информации;

• установление структуры угроз защищаемой информации;

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности).

Производственно-технологическая деятельность

• Контроль соблюдения регламентов по обеспечению безопасности на уровне БД;

• Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным;

• Установка специальных средств управления безопасностью администрируемой ИС.

Проектная деятельность

• Проектирование программного обеспечения;

• Проектирование и дизайн ИС;

• Планирование восстановления сетевой инфокоммуникационной системы;

Организационно-управленческая

• Контроль использования цифровых устройств и программного

обеспечения;

• Разработка политики информационной безопасности на уровне БД;

• Разработка регламентов и аудит системы безопасности данных на уровне БД;

• Подготовка отчетов о состоянии и эффективности системы безопасности на уровне БД;

• Администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов).

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-5 - Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем

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, источники угроз информационной безопасности и меры по их предотвращению, жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи, современные средства и способы обеспечения информационной безопасности.

Уметь

классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, применять основные правила и документы системы сертификации Российской Федерации, классифицировать основные угрозы безопасности информации;

Владеть

навыками подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности, инструментами и методами защиты информации, механизмами реакции на инциденты, навыком

распознавания заражений и точечных атак, навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 зачетных единиц (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. №7
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
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 112 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: ОСНОВНЫЕ ПОНЯТИЯ. ВВЕДЕНИЕ. Информация. и защита данных. Конфиденциальность информации. Целостность информации. Доступность информации. Служебная информация. Личные данные. ТЕМА 2: ЗАКОНОДАТЕЛЬСТВО РФ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Государственные структуры, отвечающие за защиту данных. Определение служебной тайны. Информационная безопасность коммерческой структуры. Типовой набор должностей, связанных с защитой данных на предприятии. ТЕМА 3: СТАНДАРТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Международные стандартизирующие организации. Стандарты РФ в области информационной безопасности. ТЕМА 4: ПРИРОДА ВОЗНИКНОВЕНИЯ УГРОЗ. Классификация угроз по преднамеренности проявления. Классификация по источнику угрозы. Классификация по степени воздействия на информационную систему. По способам доступа к ресурсам информационной системы ТЕМА 5: УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТЕМА 6: СТРУКТУРА ПОЛИТИКИ БЕЗОПАСНОСТИ ТЕМА 7: БАЗОВАЯ ПОЛИТИКА БЕЗОПАСНОСТИ ТЕМА 8: СПЕЦИАЛИЗИРОВАННЫЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ТЕМА 9: КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ. Основные определения. Назначение шифрования. Принципы криптографического закрытия информации. Простые методы шифрования. Таблица Вижинера. Шифрование с открытым и закрытым ключами. Основные виды атак на криптоалгоритмы ТЕМА 10: СИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ. БЛОЧНЫЕ И ПОТОКОВЫЕ КРИПТОАЛГОРИТМЫ. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования. ТЕМА 11: АСИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения ТЕМА 12: АУТЕНТИФИКАЦИЯ, АВТОРИЗАЦИЯ И АДМИНИСТРИРОВАНИЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ТЕМА 13: ФИЛЬТРАЦИЯ ТРАФИКА. СПИСКИ ДОСТУПА. ИНСПЕКЦИЯ ТРАФИКА. ТРАДИЦИОННЫЙ МЕЖСЕТЕВОЙ ЭКРАН

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Лабораторная работа № 1. Одноалфавитная подстановка. Лабораторная работа № 2 Многоалфавитная подстановка. Таблица Виженера. Лабораторная работа № 3 Многоалфавитная одноконтурная монофоническая подстановка. Лабораторная работа № 4. Многоалфавитная многоконтурная подстановка. Лабораторная работа № 5. Простая перестановка. Лабораторная работа №6. Перестановка, усложненная по таблице. Лабораторная работа № 7. Гаммирование.

Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем

Примерный перечень тем курсовых работ

Примерный перечень тем курсовых работ

1. Формы психологической защиты человека от информационной перегрузки.

2. Формы обмана и мошенничества в Интернет.

3. Атаки на информационные системы путем перегрузки каналов связи и входных буферов памяти.

4. Способы подделки компьютерной информации и программный инструментарий.

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

6. Формы и методы диверсионно-террористической деятельности с использованием современных информационных технологий.

7. Доктрина информационной безопасности России и реальности ее осуществления.

8. Государственная система защиты граждан и общества от опасной информации (законодательная практика).

9. Вопросы информационной безопасности в теории военного искусства.

10. Вопросы информационной безопасности в политике и дипломатии.

11. Стратегия пассивной информационной защиты.

12. Стратегия уничтожения источника угроз в сфере информационной защиты.

13. Модель комплексной информационной защиты и ее элементы.

14. Модель информационной защиты каналов связи.

15. Угрозы скрытого информационного воздействия на пользователей Интернет.

16. Информация как ценность и объект преступных посягательств.

17. Угрозы конфиденциальности и формы их реализации.

18. Модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа.

19. Задачи информационной защиты в финансовой сфере.

20. Задачи информационной защиты в сфере предоставления услуг связи.

21. Организационно-распорядительные меры информационной защиты.

22. 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	Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.:	URL: http://www.bwbooks.net/books/obrazovanie/yarochkin-vi

	Академический Проект; Гаудеамус, 4-е изд.— 2014. — 544 с.	
2	Вострецова, Е.В. В78 Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с	URL: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

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/

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

Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

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

Microsoft Windows

Microsoft Office

Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

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.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций №1329

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

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 7 семестре.

Курсовая работа в 7 семестре.

10. Оценочные материалы.

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

Авторы

Цыганова Наталия Алексеевна

Лист согласования

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