МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное автономное образовательное учреждение высшего образования**
**«Национальный исследовательский технологический университет «МИСИС»**
**Новотроицкий филиал**

Рабочая программа дисциплины (модуля)

# Информационная безопасность

Закреплена за подразделением — Кафедра математики и естествознания (Новотроицкий филиал)

Направление подготовки — 09.03.03 Прикладная информатика

Профиль — Прикладная информатика в технических системах

Квалификация **Бакалавр**
Форма обучения **заочная**
Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 24
самостоятельная работа 111
часов на контроль 9

Формы контроля на курсах:
экзамен 5

**Распределение часов дисциплины по курсам**

| Курс | 5 | | Итого | |
|---|---|---|---|---|
| Вид занятий | УП | РП | | |
| Лекции | 8 | 8 | 8 | 8 |
| Лабораторные | 10 | 10 | 10 | 10 |
| Практические | 6 | 6 | 6 | 6 |
| Итого ауд. | 24 | 24 | 24 | 24 |
| Контактная работа | 24 | 24 | 24 | 24 |
| Сам. работа | 111 | 111 | 111 | 111 |
| В том числе сам. работа в рамках ФОС | | | | |
| Часы на контроль | 9 | 9 | 9 | 9 |
| Итого | 144 | 144 | 144 | 144 |

Программу составил(и):

*к.т.н, доцент, Леднов А.В.*

Рабочая программа

**Информационная безопасность**

Разработана в соответствии с ОС ВО:

Самостоятельно устанавливаемый образовательный стандарт высшего образования - бакалавриат Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСИС» по направлению подготовки 09.03.03 Прикладная информатика (приказ от 05.03.2020 г. № 95 о.в.)

Составлена на основании учебного плана:

09.03.03 Прикладная информатика, 09.03.03_22_Прикладная информатика_ПрПИвТС_заоч.plx Прикладная информатика в технических системах, утвержденного Ученым советом ФГАОУ ВО НИТУ "МИСиС" в составе соответствующей ОПОП ВО 30.11.2021, протокол № 35

Утверждена в составе ОПОП ВО:

09.03.03 Прикладная информатика, Прикладная информатика в технических системах, утвержденной Ученым советом ФГАОУ ВО НИТУ "МИСиС" 30.11.2021, протокол № 35

Рабочая программа одобрена на заседании

**Кафедра математики и естествознания (Новотроицкий филиал)**

Протокол от 12.03.2025 г., №3

Руководитель подразделения доцент, к.п.н. Швалева А.В.

| 1. ЦЕЛИ ОСВОЕНИЯ | |
|---|---|
| 1.1 | Цели освоения дисциплины: формирование у обучающихся системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации. |
| 1.2 | |
| 1.3 | Задачи: |
| 1.4 | - систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования; |
| 1.5 | - изучить основы защиты информации, а также методы, средства и инструменты шифрования, применяемых в сфере информационных технологий и бизнеса; |
| 1.6 | - получить навыки работы с методами шифрования и криптоанализа. |

| 2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ | | |
|---|---|---|
| | Блок ОП: | Б1.В |
| **2.1** | **Требования к предварительной подготовке обучающегося:** | |
| 2.1.1 | Интеллектуальные технологии в металлургии | |
| 2.1.2 | Интеллектуальные технологии в энергетике | |
| 2.1.3 | Моделирование металлургических процессов с использованием современных программных продуктов | |
| 2.1.4 | Управление техническими системами | |
| 2.1.5 | Электротехника, электроника и схемотехника | |
| 2.1.6 | Вычислительные системы, сети и телекоммуникации | |
| 2.1.7 | Компьютерная графика | |
| 2.1.8 | Языки программирования | |
| 2.1.9 | Архитектура ЭВМ и систем | |
| 2.1.10 | Информатика | |
| **2.2** | **Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:** | |

| 3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ |
|---|
| **ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности** |
| **Знать:** |
| ОПК-2-З1 принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности |
| **ПК-1: Способен выполнять работы по критическому анализу функционирования технических систем, выявлять объекты информатизации и осуществлять работу по созданию или совершенствованию информационной системы** |
| **Знать:** |
| ПК-1-З1 принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности |
| **ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности** |
| **Уметь:** |
| ОПК-2-У1 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности |
| **ПК-1: Способен выполнять работы по критическому анализу функционирования технических систем, выявлять объекты информатизации и осуществлять работу по созданию или совершенствованию информационной системы** |
| **Уметь:** |
| ПК-1-У1 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности |
| **ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности** |
| **Владеть:** |

ОПК-2-В1 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публи-каций, и библиографии по научноисследовательской работе с учетом требований информацион-ной безопасности

**4. СТРУКТУРА И СОДЕРЖАНИЕ**

| Код занятия | Наименование разделов и тем /вид занятия/ | Семестр / Курс | Часов | Формируемые индикаторы компетенций | Литература и эл. ресурсы | Примечание | КМ | Выполняемые работы |
|---|---|---|---|---|---|---|---|---|
| | **Раздел 1. Введение, основы информационной безопасности** | | | | | | | |
| 1.1 | Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. /Лек/ | 5 | 4 | ПК-1-З1 ПК-1-У1 ОПК-2-У1 ОПК-2-В1 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э3 Э4 | | | |
| 1.2 | Самостоятельное изучение учебного материала в электронном курсе: Информация. Её виды и свойства. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность. /Ср/ | 5 | 20 | ОПК-2-В1 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э3 Э4 | | | |
| 1.3 | Методы и средства организационно-правовой защиты информации. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. /Лаб/ | 5 | 2 | | Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4 | | | Р1 |
| | **Раздел 2. Экономическая безопасность предприятия** | | | | | | | |
| 2.1 | Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. /Лек/ | 5 | 1 | | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э3 Э4 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2 | Самостоятельное изучение учебного материала в электронном курсе: Коммерческая тайна. Персональные данные. Служебная тайна. Профессиональная тайна. Угрозы информационной безопасности. Классификация угроз. Каналы утечки информации. Модель нарушителя информационной безопасности. Классификация средств защиты информации. /Ср/ | 5 | 26 | ОПК-2-З1 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э4 | | | |
| 2.3 | Составление плана и основных положений политики безопасности для учреждения. /Лаб/ | 5 | 2 | | Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4 | | | Р2 |
| 2.4 | Анализ возможных каналов утечки информации. Защита документооборота в вычислительных системах. /Пр/ | 5 | 2 | ОПК-2-В1 | Л1.2Л2.3 Э2 Э4 | | | Р5 |
| | **Раздел 3. Криптографические методы защиты информации** | | | | | | | |
| 3.1 | Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы. /Лек/ | 5 | 1 | ПК-1-З1 ОПК-2-У1 | Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 | | | |
| 3.2 | Самостоятельное изучение учебного материала в электронном курсе: Основные этапы развития криптологии. Основные понятия и определения. Криптостойкость. Методы криптографического преобразования данных. Кодирование. /Ср/ | 5 | 22 | | Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3.3 | Асимметричные системы шифрования RSA. Надежность использования криптосистем. Перспективы развития криптографических методов защиты информации. /Пр/ | 5 | 2 | | | | | Р6 |
| 3.4 | Шифрование текста по ключу методами замены. Шифрование текста по ключу методами перестановки. Методы шифрования текста при помощи аналитических преобразований. Шифрование текста по ключу аддитивными методами (гаммированием). Шифры с открытым ключом. Алгоритм RSA. /Лаб/ | 5 | 2 | | Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 | | | Р3 |
| | **Раздел 4. Методы и средства защиты информации** | | | | | | | |
| 4.1 | Методы парольной защиты. Использование простого пароля. Использование динамически изменяющегося пароля. Методы идентификации и аутентификации пользователей. Идентификация, аутентификация с помощью биометрических данных. Использование средств стеганографии для защиты файлов. Создание защищенного канала связи средствами виртуальной частной сети. Антивирусные средства защиты информации. /Лек/ | 5 | 2 | | Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 | | | |
| 4.2 | Самостоятельное изучение учебного материала в электронном курсе: Классификация существующих типов систем обнаружения атак (СОА). Общие понятия антивирусной защиты. Методы защиты от вредоносных программ. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/ | 5 | 34 | | Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э2 Э3 Э4 | | | |
| 4.3 | Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. /Пр/ | 5 | 1 | | Л1.1Л2.1 Э2 Э4 | | | Р7 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4.4 | Основы работы антивирусных программ. Пароли как средство защиты информации. Системы и средства генерации паролей и их недостатки. /Пр/ | 5 | 1 | | Л1.1Л2.2 Э2 Э4 | | | Р8 |
| 4.5 | Методы парольной защиты. Разработка программной парольной защиты. Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требуемой стойкостью к взлому. Генератор паролей, обладающий требованиями к парольным генераторам. Диагностика антивирусной программы и создание тестовых вирусов. /Лаб/ | 5 | 4 | | Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 | | | Р4 |
| 4.6 | Проведение экзамена /Ср/ | 5 | 9 | | Э1 Э2 Э3 Э4 | | КМ1 | |
| | **Раздел 5. Подготовка к контрольным мероприятиям и выполняемым работам** | | | | | | | |
| 5.1 | Объем часов самостоятельной работы на подготовку к КМ /Ср/ | 5 | 0 | | | | | |
| 5.2 | Объем часов самостоятельной работы на подготовку к ВР /Ср/ | 5 | 0 | | | | | |

## 5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

### 5.1. Контрольные мероприятия (контрольная работа, тест, коллоквиум, экзамен и т.п), вопросы для самостоятельной подготовки

| Код КМ | Контрольное мероприятие | Проверяемые индикаторы компетенций | Вопросы для подготовки |
|---|---|---|---|
| КМ1 | Экзамен | ОПК-2-З1;ПК-1-З1 | Причины возникновения угроз безопасности информации.<br>2. Проблемы информационной безопасности. Причина кризиса информационной безопасности.<br>3. Проблема потери электронной информации. Человеческий фактор.<br>4. Носители информации. Что такое сигналы, знаки, символы. Информационные процессы и их взаимосвязь. Роль защиты данных в информационных процессах.<br>5. Основные пути утечки информации. Проблема потери электронных данных.<br>6. Классификация вирусов и других вредоносных программ по степени опасности, по заражаемым объектам, по методу заражения, по методу скрытия своего наличия в системе, по среде создания.<br>7. Особенности алгоритмов работы вирусов и основные методы определения их в системе.<br>8. Антивирусные программы, их классификация, источники компьютерных вирусов.<br>9. Задачи безопасности и существующие угрозы. Злоумышленники и их классификация.<br>10. Внутренние угрозы корпоративной безопасности и меры противодействия им.<br>11. Компьютерные преступления. Преступления в сфере компьютерной информации в УК РФ.<br>12. Криптографические методы защиты информации. |

| | | | |
|---|---|---|---|
| | | | История криптографии. Задачи криптографии и криптоанализа.<br>13. Основные понятия криптографии: шифр, ключ, шифрование, дешифрование, криптостойкость. Что называют абсолютно стойким шифром?<br>14. Принципы кодирования информации. Алфавит и длина кода. Цифровая и дискретная информация.<br>15. Потоковые шифры. Аппаратные и программные скремблеры.<br>16. Алгоритм шифрования кодом Цезаря. Алгоритм взлома кода Цезаря и других алгоритмов замены.<br>17. Алгоритм шифрования кодом Виженера. Алгоритм взлома кода Виженера при известной длине ключа.<br>18. Алгоритмы генерации псевдослучайных чисел. Алгоритмы аддитивного конгруэнтного генератора псевдослучайной последовательности. Генераторы случайных чисел и их использование.<br>19. Потоковые шифры. Скремблеры. Алгоритм шифрования в режиме гаммирования, схема гаммирования с обратной связью.<br>20. Принципы построения симметричных блочных шифров (рассеивание и перемешивание). Сеть Фейстеля и ее ветви.<br>21. Схема абсолютно стойкого шифра, ее основные проблемы.<br>22. Основные характеристики и применение систем с секретным ключом DES, FEAL, IDEA, ГОСТ 28147-89, RC5.<br>23. Системы криптографической защиты данных с открытым ключом, их достоинства и недостатки.<br>24. Алгоритм RSA и его использование в современном ПО.<br>25. Алгоритм Эль-Гамаля и его использование в современном ПО.<br>26. Сравнение симметричных и несимметричных алгоритмов шифрования. Достоинства и недостатки асимметричных алгоритмов. Цифровой конверт.<br>27. Сертификаты открытых ключей. Назначение удостоверяющих центров (бюро сертификации).<br>28. Функция хеширования и ее свойства. Однонаправленные хэш-функции.<br>29. Электронная цифровая подпись с использованием симметричных алгоритмов. Достоинства и недостатки.<br>30. Электронная цифровая подпись с использованием асимметричных алгоритмов. Классическая схема.<br>31. Сжатие данных без потерь. Алгоритм Хаффмана.<br>32. Сжатие данных без потерь. Алгоритм Лемпеля-Зива.<br>33. Стеганография как способ сокрытия секретных данных. Понятия: контейнер, стеганографический канал, стегоключ.<br>34. Ограничение стеганографических методов. Принципы построения тайных каналов. Защита музыки, видеофильмов посредством скрытых «водяных знаков».<br>35. Аутентификация пользователей с применением паролей. Почему взломщикам удается проникать в систему защищенную паролями?<br>36. Совершенствование безопасности паролей, схема аутентификации «отклик-отзыв». Распространенные методы взлома информационной системы.<br>37. Необратимые функции. Одноразовые пароли Лампорта.<br>38. Аутентификация пользователей с использованием физического объекта, виды карт: пластиковые, магнитные, смарт-карты и пр.<br>39. Аутентификация пользователей с использованием биометрических данных. |

**5.2. Перечень работ, выполняемых по дисциплине (Курсовая работа, Курсовой проект, РГР, Реферат, ЛР, ПР и т.п.)**

| Код работы | Название работы | Проверяемые индикаторы компетенций | Содержание работы |
|---|---|---|---|
| Р1 | Лабораторная работа №1 | ОПК-2-У1;ОПК-2-В1;ПК-1-У1 | Методы и средства организационно-правовой защиты информации. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. |

| | | | |
|---|---|---|---|
| Р2 | Лабораторная работа №2 | ОПК-2-У1;ОПК-2-В1;ПК-1-У1 | Составление плана и основных положений политики безопасности для учреждения. |
| Р3 | Лабораторная работа №3 | ПК-1-У1;ОПК-2-В1;ОПК-2-У1 | Шифрование текста по ключу методами замены. Шифрование текста по ключу методами перестановки. Методы шифрования текста при помощи аналитических преобразований. Шифрование текста по ключу аддитивными методами (гаммированием). Шифры с открытым ключом. Алгоритм RSA. |
| Р4 | Лабораторная работа №4 | ОПК-2-У1;ОПК-2-В1;ПК-1-У1 | Методы парольной защиты. Разработка программной парольной защиты. Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требуемой стойкостью к взлому. Генератор паролей, обладающий требованиями к парольным генераторам. Диагностика антивирусной программы и создание тестовых вирусов. |
| Р5 | Практическая работа №1 | ОПК-2-У1;ОПК-2-В1;ПК-1-У1 | Анализ возможных каналов утечки информации. Защита документооборота в вычислительных системах. |
| Р6 | Практическая работа №2 | ПК-1-У1;ОПК-2-В1;ОПК-2-У1 | Асимметричные системы шифрования RSA. Надежность использования криптосистем. Перспективы развития криптографических методов защиты информации. |
| Р7 | Практическая работа №3 | ОПК-2-У1;ОПК-2-В1;ПК-1-У1 | Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. |
| Р8 | Практическая работа №4 | ОПК-2-У1;ОПК-2-В1;ПК-1-У1 | Основы работы антивирусных программ. Пароли как средство защиты информации. Системы и средства генерации паролей и их недостатки. |

**5.3. Оценочные материалы, используемые для экзамена (описание билетов, тестов и т.п.)**

Формой промежуточной аттестации по дисциплине является экзамен.
Ниже представлен образец билета для экзамена, проводимого в устной форме.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
НОВОТРОИЦКИЙ ФИЛИАЛ
Федеральное государственное автономное образовательное учреждение высшего образования
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
«МИСИС»

Кафедра Математики и естествознания
Экзаменационный билет № 0

Дисциплина: Информационная безопасность
Направление: 09.03.03 Прикладная информатика
Форма обучения: заочная
Форма проведения: устная

1. Причины возникновения угроз безопасности информации.
2. Алгоритм шифрования кодом Цезаря. Алгоритм взлома кода Цезаря и других алгоритмов замены.
3. Совершенствование безопасности паролей, схема аутентификации «отклик-отзыв». Распространенные методы взлома информационной системы.

Составил: доцент кафедры МиЕ _____ И.М. Ячиков
(подпись)
Зав. кафедрой МиЕ _____ А.В. Швалева
(подпись)
«____» _____ 20__ г.

**5.4. Методика оценки освоения дисциплины (модуля, практики. НИР)**

Критерии оценки:
– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;
– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.
– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;
– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

Критерии оценки защиты лабораторных работ:
При оценке результатов защиты отчетов по лабораторным работам используется бинарная система, которая предусматривает следующие результаты и критерии оценивания:
- "Зачтено" Выполнены все задания лабораторной работы, студент ответил на все контрольные вопросы;
- "Не зачтено" Студент не выполнил или выполнил неправильно задания лабораторной работы, студент ответил на контрольные вопросы с ошибками или не ответил на контрольные вопросы.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

### 6.1. Рекомендуемая литература

#### 6.1.1. Основная литература

| | Авторы, составители | Заглавие | Библиотека | Издательство, год, эл. адрес |
|---|---|---|---|---|
| Л1.1 | Ярочкин В.И. | Информационная безопасность: Учебник | | М.: Академ.проект, 2006, |
| Л1.2 | Б.И. Филиппов, О.Г. Шерстнева | Информационная безопасность. Основы надежности средств связи: учебник | | Москва ; Берлин : Директ-Медиа, 2019, http://biblioclub.ru/index.php?page=book&id=499170 |
| Л1.3 | Артемов А.В. | Информационная безопасность: курс лекций | | Орел : МАБИВ, 2014, http://biblioclub.ru/index.php?page=book&id=428605 |

#### 6.1.2. Дополнительная литература

| | Авторы, составители | Заглавие | Библиотека | Издательство, год, эл. адрес |
|---|---|---|---|---|
| Л2.1 | Ю.С.Уфимцев и др. | Информационная безопасность России | | М.: Экзамен, 2003, |
| Л2.2 | Под ред. С.Я. Казанцева | Правовое обеспечение информационной безопасности: Учеб.пособие | | М.: Академия, 2007, |
| Л2.3 | А.А.Садердинов, В.А.Трайнёв, А.А.Федулов | Информационная безопасность предприятия: Учеб.пособие | | М.: Дашков и К, 2007, |
| Л2.4 | Галатенко В.А. | Основы информационной безопасности. Курс лекций: Учеб.пособие | | М.: ИНТУИТ.РУ, 2004, |
| Л2.5 | А.А.Малюк, С.В.Пазизин, Н.С.Погожин | Введение в защиту информации в автоматизированных системах: Учеб.пособие | | М.: Горячая линия-Телеком, 2005, |
| Л2.6 | Нестеров С.А. | Основы информационной безопасности: учебное пособие | | Санкт-Петербург : Издательство Политехнического университета, 2014, http://biblioclub.ru/index.php?page=book&id=363040 |

#### 6.1.3. Методические разработки

| | Авторы, составители | Заглавие | Библиотека | Издательство, год, эл. адрес |
|---|---|---|---|---|

| | Авторы, составители | Заглавие | Библиотека | Издательство, год, эл. адрес |
|---|---|---|---|---|
| Л3.1 | М.А. Лапина, Д.М. Марков, Т.А. Гиш, М.В. Песков | Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум | | Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016, http://biblioclub.ru/index.php?page=book&id=458012 |

**6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

| | | |
|---|---|---|
| Э1 | Научная электронная библиотека eLIBRARY | https://www.elibrary.ru/ |
| Э2 | LMS Canvas | https://lms.misis.ru |
| Э3 | НФ НИТУ МИСиС | http://nf.misis.ru/ |
| Э4 | Университетская библиотека ONLINE | https://biblioclub.ru/ |

**6.3 Перечень программного обеспечения**

**6.4. Перечень информационных справочных систем и профессиональных баз данных**

| | |
|---|---|
| И.1 | https://lib.itsec.ru/articles2/allpubliks - Журнал Информационная безопасность |
| И.2 | http://www.kaspersky.ru/ - Лаборатория Касперского |
| И.3 | http://www.intuit.ru/ - Национальный Открытый Университет "ИНТУИТ" |
| И.4 | https://elbib.ru/ - Научная электронная библиотека |

## 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

| Ауд. | Назначение | Оснащение |
|---|---|---|
| 113 | Учебная лаборатория (компьютерный класс) | Комплект учебной мебели на 12 мест для обучающихся, 12 стационарных компьютеров для студентов, 1 стационарный компьютер для преподавателя (у всех выход в интернет), проектор, экран настенный, коммутатор, доска аудиторная меловая, веб камера Logitech, доступ к ЭИОС Университета МИСИС через личный кабинет на платформе LMS Canvas и Moodle, лицензионные программы MS Office, MS Teams, антивирус Dr.Web. |
| 127 | Учебная лаборатория (компьютерный класс) | Комплект учебной мебели на 24 мест для обучающихся, 12 стационарных компьютеров для студентов, 1 стационарный компьютер для преподавателя (у всех выход в интернет), проектор, интерактивная доска, доска аудиторная меловая, коммутатор, веб камера, документ-камера, доступ к ЭИОС Университета МИСИС через личный кабинет на платформе LMS Canvas и Moodle, лицензионные программы MS Office, MS Teams, антивирус Dr.Web. |

## 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Освоение дисциплины предполагает как проведение традиционных аудиторных занятий, так и работу в электронной информационно-образовательной среде (ЭИОС), в электронном курсе по дисциплине. Электронный курс позволяет использовать специальный контент и элементы электронного обучения и дистанционных образовательных технологий. используется преимущественно для асинхронного взаимодействия между участниками образовательного процесса посредством сети "Интернет".

Чтобы эффективно использовать возможности ЭИОС, а соответственно и успешно освоить дисциплину, нужно:

1) зарегистрироваться на курс;

2) ознакомиться с содержанием курса, вопросами для самостоятельной подготовки, условиями допуска к аттестации, формой промежуточной аттестации (зачет/экзамен), критериями оценивания и др.;

3) изучать учебные материалы, размещенные преподавателем. В т.ч. пользоваться литературой, рекомендованной преподавателем, переходя по ссылкам;

4) пользоваться библиотекой , в т.ч. для выполнения письменных работ (контрольные работы);

5) ознакомиться с содержанием задания к письменной работе, сроками сдачи, критериями оценки. В установленные сроки выполнить работу(ы), подгрузить файл работы для проверки. Рекомендуется называть файл работы следующим образом (название предмета (сокращенно), группа, ФИО, дата актуализации (при повторном размещении).

Например,Информационная безопасность _Иванов_И.И._БМТ-19з_20.04.2020. Если работа содержит рисунки, формулы, то с целью сохранения форматирования ее нужно подгружать в pdf формате.

Работа, размещаемая в электронном курсе для проверки, должна:

- содержать все структурные элементы: титульный лист, введение, основную часть, заключение, список источников, приложения (при необходимости);
- быть оформлена в соответствии с требованиями.

Преподаватель в течение установленного срока (не более десяти дней) проверяет работу и размещает в комментариях к заданию рецензию. В ней он указывает как положительные стороны работы, так замечания. При наличии в рецензии

замечаний и рекомендаций, нужно внести поправки в работу, подгрузить ее заново для повторной проверки. При этом важно следить за сроками, в течение которых должно быть выполнено задание. При нарушении сроков, указанных преподавателем возможность подгрузить работу остается, но система выводит сообщение о нарушении сроков. По окончании семестра загрузить работу не получится;
6) пройти тестовые задания, освоив рекомендуемые учебные материалы;
7) отслеживать свою успеваемость;
8) читать объявления, размещаемые преподавателем, давать обратную связь;
9) создавать обсуждения и участвовать в них (обсуждаются общие моменты, вызывающие вопросы у большинства группы). Данная рубрика также может быть использована для взаимной проверки;
10) проявлять регулярную активность на курсе.
Преимущественно для синхронного взаимодействия между участниками образовательного процесса посредством сети «Интернет» используется Microsoft Teams (MS Teams). Чтобы полноценно использовать его возможности нужно установить приложение MS Teams на персональный компьютер и телефон. Старостам нужно создать группу в MS Teams. Участие в группе позволяет:
- слушать лекции;
- работать на практических занятиях;
- быть на связи с преподавателем, задавая ему вопросы или отвечая на его вопросы в общем чате группы в рабочее время с 9.00 до 17.00;
- осуществлять совместную работу над документами (вкладка «Файлы).
При проведении занятий в дистанционном синхронном формате нужно всегда работать с включенной камерой. Исключение – если преподаватель попросит отключить камеры и микрофоны в связи с большими помехами. На аватарках должны быть исключительно деловые фото.
При проведении лекционно-практических занятий ведется запись. Это дает возможность просмотра занятия в случае невозможности присутствия на нем или при необходимости вновь обратится к материалу и заново его просмотреть.