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)

Защита информации

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 **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 18
самостоятельная работа 158
часов на контроль 4

Формы контроля на курсах:
зачет с оценкой 4

Распределение часов дисциплины по курсам

Курс	4		Итого	
Вид занятий	УП	РП		
Лекции	6	34	6	34
Практические	12	17	12	17
Итого ауд.	18	68	18	68
Контактная работа	18	68	18	68
Сам. работа	158	108	158	108
Часы на контроль	4	4	4	4
Итого	180	180	180	180

Программу составил(и):

к.т.н, доцент, Леднов А.В.

Рабочая программа

Защита информации

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 24.06.2021 г., №11

Руководитель подразделения доцент, к.ф.м.н. Гюнтер Д.А.

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Цели освоения дисциплины: понимание моделей и стандартов информационной безопасности, усвоение методов защиты информационных систем, приобретение теоретических знаний и практических навыков по использованию современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.
1.2	
1.3	Задачи:
1.4	- изучить основные теоретические положения защиты информации, причины нарушений безопасности;
1.5	- получить практические навыки работы с современными сетевыми фильтрами и средствами криптографического преобразования информации.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Блок ОП:	Б1.В.ДВ.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	CASE-технологии
2.1.2	Программная инженерия
2.1.3	Информационные системы и технологии
2.1.4	Учебная практика по получению первичных профессиональных умений
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.2	Преддипломная практика
2.2.3	Разработка интернет-приложений на клиентской стороне
2.2.4	Управление IT-структурами предприятий
2.2.5	Управление проектами
2.2.6	Языки и среды разработки интернет-приложений

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
ПК-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС
Знать:
ПК-2-З1 информационное обеспечение и принципы построения информационных систем управления технологическими процессами
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
Знать:
ОПК-3-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-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС
Уметь:
ПК-2-У1 использовать методы системного моделирования технологических процессов
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
Уметь:
ОПК-3-У1 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
ПК-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС
Владеть:

ПК-2-В1 современными компьютерными методами математического моделирования технологических процессов
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
Владеть:
ОПК-3-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. Основы информационной безопасности и защиты информации							
1.1	Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Обзор и сравнительный анализ стандартов информационной безопасности. Исследование причин нарушений безопасности. Понятие политики безопасности. Реализация и гарантирование политики безопасности. Принципы организации системы защиты, направления, способы и методы защиты. /Лек/	4	8		Л1.3 Л1.4Л2.1 Л2.3 Л2.4 Э1 Э2 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в LMS Canvas: Основные понятия и определения. Современное состояние и перспективы развития защиты информации. Общая проблема информационной безопасности информационных систем. /Ср/	4	26		Л1.3 Л1.4Л2.1 Л2.3 Л2.4 Э1 Э2 Э3 Э4			
1.3	Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Состав и назначение должностных инструкций. /Пр/	4	5		Л1.1Л2.1 Э2 Э4			

1.4	Исследование и изучение структуры средств безопасности операционных систем и использование их для конфиденциального доступа к информации. Разработка и реализация алгоритма функционирования системы безопасности объектов. /Лаб/	4	4		Л1.3 Л1.4Л2.1 Л2.3 Л2.4Л3.1 Э1 Э2 Э3 Э4			
	Раздел 2. Модели безопасности в компьютерных системах							
2.1	Модели безопасного субъектного взаимодействия в компьютерной системе. Процедура идентификации и аутентификации. Сопряжение защитных механизмов. Архитектура защищенных операционных систем. Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе. /Лек/	4	8		Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
2.2	Самостоятельное изучение учебного материала в LMS Canvas: Аутентификация пользователей. Формализация задачи сопряжения. Методы сопряжения. Типизация данных, необходимых для обеспечения работы средств сопряжения. Понятие внешнего разделяемого сервиса безопасности. Постановка задачи. Понятие и свойства модуля реализации защитных функций. /Ср/	4	20		Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
2.3	Разработка и реализация алгоритма функционирования системы безопасности субъектов. Проектирование модуля реализации защитных функций в среде гарантирования политики безопасности. Методика проверки попарной корректности субъектов при проектировании механизмов обеспечения безопасности с учетом передачи параметров. /Лаб/	4	5		Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
	Раздел 3. Защита информации в компьютерных сетях							

3.1	Особенности обеспечения информационной безопасности в компьютерных сетях. Специфика средств защиты в компьютерных сетях. Сетевые модели передачи данных. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP. Модель взаимодействия открытых систем OSI/ISO. Современные средства построения защищенных виртуальных сетей. /Лек/	4	10		Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Э1 Э2 Э3 Э4			
3.2	Самостоятельное изучение учебного материала в LMS Canvas: Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO. Адресация в глобальных сетях. Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. /Ср/	4	20		Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Э1 Э2 Э3 Э4			
3.3	Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. /Пр/	4	6		Л1.1Л2.1			
3.4	Разработка и реализация алгоритма сетевого фильтра. Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. /Лаб/	4	4		Л1.3 Л1.4Л2.1 Л2.2 Л2.4Л3.1 Э1 Э2 Э3 Э4			
	Раздел 4. Методы и системы защиты информации							

4.1	Защита информации от несанкционированного доступа. Каналы утечки информации. Системы анализа защищённости и обнаружения вторжений. Модели и источники каналов утечки информации. Способы несанкционированного доступа к информации. Компьютерные средства реализации защиты в информационных системах. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись. /Лек/	4	8		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
4.2	Самостоятельное изучение учебного материала в LMS Canvas: Причины нарушения целостности информации. Функции непосредственной защиты информации. Задачи защиты информации. Методы и системы защиты информации. Аппаратные средства защиты. Программные средства защиты. Криптографические средства защиты. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/	4	42		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
4.3	Программные средства защиты. Криптографические средства защиты. /Пр/	4	6		Л1.1Л2.1 Э2 Э4			
4.4	Разработка и реализация алгоритма криптографического преобразования. Источники и защита от несанкционированного доступа. /Лаб/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
4.5	Проведение зачета с оценкой /ЗачётСОц/	4	4		Э1 Э2 Э3 Э4			

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

5.1. Вопросы для самостоятельной подготовки к экзамену (зачёту с оценкой)

Вопросы к зачету с оценкой (ОПК-3-З1, ОПК-3-У1, ПК-2-З1, ПК-2-У1, УК-3-З1, УК-3-У1, УК-6-З1, УК-6-З2, УК-6-У1, УК-6-У2):

1. Основные концептуальные положения системы защиты информации.
2. Концептуальная модель информационной безопасности.
3. Обзор и сравнительный анализ стандартов информационной безопасности.
4. Причины нарушений безопасности.
5. Понятие политики безопасности.
6. Реализация и гарантирование политики безопасности.
7. Принципы организации системы защиты, направления, способы и методы защиты.
8. Состав и назначение должностных инструкций.
9. Модели безопасного субъектного взаимодействия в компьютерной системе.
10. Процедура идентификации и аутентификации.
11. Сопряжение защитных механизмов.
12. Архитектура защищенных операционных систем.
13. Модели сетевых сред.
14. Создание механизмов безопасности в распределенной компьютерной системе.
15. Аутентификация пользователей.
16. Формализация задачи сопряжения. Методы сопряжения.
17. Типизация данных, необходимых для обеспечения работы средств сопряжения.
18. Понятие внешнего разделяемого сервиса безопасности.
19. Понятие и свойства модуля реализации защитных функций.
20. Особенности обеспечения информационной безопасности в компьютерных сетях.
21. Специфика средств защиты в компьютерных сетях.
22. Сетевые модели передачи данных.
23. Транспортный протокол TCP и модель TCP/IP.
24. Модель взаимодействия открытых систем OSI/ISO.
25. Современные средства построения защищенных виртуальных сетей.
26. Принципы защиты распределенных вычислительных сетей.
27. Разработка и реализация алгоритма сетевого фильтра.
28. Построение защищенных виртуальных сетей.
29. Безопасность удаленного доступа к локальной сети.
30. Защита информации от несанкционированного доступа.
31. Каналы утечки информации.
32. Системы анализа защищённости и обнаружения вторжений.
33. Модели и источники каналов утечки информации.
34. Способы несанкционированного доступа к информации.
35. Компьютерные средства реализации защиты в информационных системах.
36. Классическая криптография и алгоритмы блочного шифрования.
37. Цифровая электронная подпись.

5.2. Перечень работ, выполняемых по дисциплине (модулю, практике, НИР) - эссе, рефераты, практические и расчетно-графические работы, курсовые работы, проекты и др.

Контрольная работа включает в себя выполнение расчетно-графической работы на тему: "Вычисление хэш-функции и подпись сообщения цифровой сигнатурой" (ОПК-3-В1, ПК-2-В1, УК-3-В1, УК-6-В1, УК-6-В2).

Цель расчетно-графической работы: изучение процедуры хэширования сообщения и подтверждения ее электронной цифровой подписью.

Исходные данные: общее задание для расчетно-графической работы, текст сообщения выбирается студентом самостоятельно.

Задание:

1. Выбрать сообщение M длиной 5 букв.
2. Получить хэш-код m для сообщения M при помощи хэш-функции H, взятой из рекомендаций МККТТ X.509. Вектор инициализации H0 выбрать равным нулю.
3. Вычислить цифровую подпись методом RSA под электронным документом M, используя рассчитанный хэш-код m и секретный ключ d.
4. Представить схему цифровой подписи с подробным описанием ее функционирования.

Объем расчетно-графической работы – 15-20 стр.

Расчетно-пояснительная записка должна содержать следующие основные структурные элементы:

1. Титульный лист
2. Задание
3. Содержание
4. Введение
5. Основную часть, которая включает в себя: исходное сообщение и его двоичный код, хэшируемые блоки, итерационную процедуру вычисления хэш-значения, вычисленную цифровую подпись, результат проверки достоверности ЭЦП.
6. Заключение
7. Список использованных источников
8. Приложения (при необходимости)

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

Экзамен по дисциплине не предусмотрен.
Формой промежуточной аттестации является зачет с оценкой. Дифференцированная оценка по дисциплине рассчитывается как среднее арифметическое по результатам выполнения контрольной работы и проверочных заданий по итогам каждого раздела дисциплины.

Дистанционно зачет с оценкой проводится в LMS Canvas. Тест содержит 30 заданий. На решение отводится 30 минут. Разрешенные попытки - две. Зачитывается наилучший результат.

Образец заданий для экзамена, проводимого дистанционно в LMS Canvas:

1. Критерии фильтрации пакетов для фильтрующего маршрутизатора
а) IP-адрес отправителя
б) IP-адрес получателя
в) тип протокола (TCP, UDP, ICMP)
г) e-mail-адрес отправителя (SMTP)
д) порт отправителя (TCP, UDP)
е) порт получателя (TCP, UDP)
ж) тип сообщения (ICMP)

2. Выяснить открытые сетевые порты можно с помощью программы
а) PING
б) IPCONFIG
в) NETSTAT
г) NET
д) DIR

3. Выяснить настройки IP-адреса можно с помощью программы
а) PING
б) IPCONFIG
в) NET
г) DIR

4. Построение карты сети возможно на основе сетевых протоколов
а) ICMP
б) ARP
в) HTTP
г) SNMP
д) SMTP
е) CDP

5. Утилита PING предназначена для
а) настройки таблицы маршрутизации
б) тестирования достижимости узлов
в) обеспечения безопасности работы
г) задания маски подсети

6. Основными источниками угроз информационной безопасности являются все указанное в списке:

а) Хищение жестких дисков, подключение к сети, инсайдерство
б) Перехват данных, хищение данных, изменение архитектуры системы
в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

7. К основным типам средств воздействия на компьютерную сеть относится:

а) Компьютерный сбой
б) Логические закладки («мины»)
в) Аварийное отключение питания

8. Наиболее распространены угрозы информационной безопасности корпоративной системы:
а) Покупка нелицензионного ПО
б) Ошибки эксплуатации и неумышленного изменения режима работы системы
в) Сознательного внедрения сетевых вирусов

9. Наиболее распространены угрозы информационной безопасности сети:
а) Распределенный доступ клиент, отказ оборудования
б) Моральный износ сети, инсайдерство
в) Сбой (отказ) оборудования, нелегальное копирование данных

10. Утечкой информации в системе называется ситуация, характеризуемая:
а) Потерей данных в системе
б) Изменением формы информации
в) Изменением содержания информации

11. Угроза информационной системе (компьютерной сети) – это:
а) Вероятное событие
б) Детерминированное (всегда определенное) событие
в) Событие, происходящее периодически

12. Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:
а) Программные, технические, организационные, технологические
б) Серверные, клиентские, спутниковые, наземные
в) Личные, корпоративные, социальные, национальные

13. Наиболее распространены средства воздействия на сеть офиса:
а) Слабый трафик, информационный обман, вирусы в интернет
б) Вирусы в сети, логические мины (закладки), информационный перехват
в) Компьютерные сбои, изменение администрирования, топологии

14. Виды информационной безопасности:
а) Персональная, корпоративная, государственная
б) Клиентская, серверная, сетевая
в) Локальная, глобальная, смешанная

15. Цели информационной безопасности – своевременное обнаружение, предупреждение:
а) несанкционированного доступа, воздействия в сети
б) инсайдерства в организации
в) чрезвычайных ситуаций

16. Основные объекты информационной безопасности:
а) Компьютерные сети, базы данных
б) Информационные системы, психологическое состояние пользователей
в) Бизнес-ориентированные, коммерческие системы

17. Основными рисками информационной безопасности являются:
а) Искажение, уменьшение объема, перекодировка информации
б) Техническое вмешательство, выведение из строя оборудования сети
в) Потеря, искажение, утечка информации

18. К основным функциям системы безопасности можно отнести все перечисленное:
а) Установление регламента, аудит системы, выявление рисков
б) Установка новых офисных приложений, смена хостинг-компании
в) Внедрение аутентификации, проверки контактных данных пользователей

19. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:
а) Идентификация
б) Аутентификация
в) Авторизация
г) Экспертиза
д) Шифрование

20. Для безопасной передачи данных по каналам интернет используется технология:
а) WWW
б) DICOM
в) VPN
г) FTP
д) XML

21. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:
а) Антивирус
б) Замок
в) Брандмауэр
г) Криптография
д) Экспертная система

22. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:
а) Токен
б) Password
в) Пароль
г) Login
д) Смарт-карта

23. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:
а) Авторизация
б) Аутентификация
в) Обезличивание
г) Деперсонализация
д) Идентификация

24. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:
а) Авторизация
б) Обезличивание
в) Деперсонализация
г) Аутентификация
д) Идентификация

25. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом
а) Авторизация
б) Идентификация
в) Аутентификация
г) Обезличивание
д) Деперсонализация

26. Для того чтобы снизить вероятность утраты информации необходимо:
а) Регулярно производить антивирусную проверку компьютера
б) Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
в) Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
г) Защитить вход на компьютер к данным паролем
д) Проводить периодическое обслуживание ПК

27. К правовым методам, обеспечивающим информационную безопасность, относятся:
а) Разработка аппаратных средств обеспечения правовых данных
б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

28. Принципом политики информационной безопасности является принцип:
а) Усиления защищенности самого незащищенного звена сети (системы)
б) Перехода в безопасное состояние работы сети, системы
в) Полного доступа пользователей ко всем ресурсам сети, системы

29. Принципом политики информационной безопасности является принцип:
а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
б) Одноуровневой защиты сети, системы
в) Совместимых, однотипных программно-технических средств сети, системы

30. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
а) Регламентированной
б) Правовой
в) Защищаемой

31. Окончательно, ответственность за защищенность данных в компьютерной сети несет:
а) Владелец сети
б) Администратор сети
в) Пользователь сети

32. Политика безопасности в системе (сети) – это комплекс:
а) Руководств, требований обеспечения необходимого уровня безопасности

б) Инструкций, алгоритмов поведения пользователя в сети
в) Нормы информационного права, соблюдаемые в сети

33. Наиболее важным при реализации защитных мер политики безопасности является:
а) Аудит, анализ затрат на проведение защитных мер
б) Аудит, анализ безопасности
в) Аудит, анализ уязвимостей, риск-ситуаций

34. К основным принципам обеспечения информационной безопасности относится:
а) Экономической эффективности системы безопасности
б) Многоплатформенной реализации системы
в) Усиления защищенности всех звеньев системы

35. Принципом информационной безопасности является принцип недопущения:
а) Неоправданных ограничений при работе в сети (системе)
б) Рисков безопасности сети, системы
в) Презумпции секретности

36. Принцип Кирхгофа:
а) Секретность ключа определена секретностью открытого сообщения
б) Секретность информации определена скоростью передачи данных
в) Секретность закрытого сообщения определяется секретностью ключа

37. Система защиты информации должна удовлетворять требованиям
а) охватывать весь технологический комплекс информационной деятельности
б) быть разнообразной по используемым средствам
в) быть открытой для изменения и дополнения мер
г) быть нестандартной, разнообразной
д) быть надежной
е) все из перечисленного
ж) ничего из перечисленного

38. В число основных принципов архитектурной безопасности входят:
а) следование признанным стандартам;
б) применение нестандартных решений, не известных злоумышленникам;
в) разнообразие защитных средств.

39. В число основных принципов архитектурной безопасности входят:
а) усиление самого слабого звена;
б) укрепление наиболее вероятного объекта атаки;
в) эшелонированность обороны.

40. Устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер, не подсоединяемые к компьютеру и имеющие собственный источник питания:
а) Токен
б) Автономный токен
в) USB-токен
г) Устройство iButton
д) Смарт-карта

41. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:
а) Статическими алгоритмами
б) Алгоритмы RMS
в) Динамическими алгоритмами

42. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:
а) Каталоги
б) Символьные файлы
в) Регулярные файлы

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

Работа оценивается на отлично, если:
- теоретические сведения изложены в достаточном объеме, четко и последовательно, исследуются и сравниваются разные подходы, методики, приводятся собственные суждения и выводы, даются ссылки на источники, текст написан грамотно, стилистически выдержан и оформлен в соответствии с требованиями.
- приведено описание всех разделов работы развернуто, в полном объеме, цифровая подпись представлена с подробным описанием ее функционирования, проведена проверка достоверности ЭЦП.

В целом по работе: расставлены ссылки на источники, текст написан грамотно, стилистически выдержан, оформлен в соответствии с требованиями.

Выполнение работы оценивается как хорошее, если она соответствует всем критериям, перечисленным выше, но отсутствует описания и сравнения разных подходов, методик и т.д. с последующим формированием собственных выводов на данный счет. Приведено описание всех разделов работы, но описание функционирования представлено кратко, отсутствуют пояснения.

В целом по работе: расставлены ссылки на источники, текст написан грамотно, стилистически выдержан, оформлен в соответствии с требованиями.

Выполнение работы оценивается как удовлетворительное, если она соответствует всем критериям, перечисленным выше, но в работе отсутствуют описания и сравнения разных подходов, методик и т.д. с последующим формированием собственных выводов на данный счет. Описание функционирования представлено кратко, отсутствуют пояснения. Отсутствует результат проверки достоверности ЭЦП.

Если расчетно-графическая работа не соответствует критериям, перечисленным выше, то оценивается неудовлетворительно.

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	Баричев С.Г.	Основы современной криптографии: Учеб. курс		М.: Горячая линия –Телеком, 2002,
Л1.2	Нечаев В.И.	Элементы криптографии: Учеб. пособие		М.: Высшая шк., 1999,
Л1.3	А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др.	Методологические основы построения защищенных автоматизированных систем: учебное пособие		Воронеж : Воронежская государственная лесотехническая академия, 2013, http://biblioclub.ru/index.php?page=book&id=255851
Л1.4	Сергеева Ю.С.	Защита информации: Конспект лекций: учебное пособие		Москва : А-Приор, 2011, http://biblioclub.ru/index.php?page=book&id=72670

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год, эл. адрес
Л2.1	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
Л2.2	Осипенко А.Л.	Борьба с преступностью в глобальных компьютерных сетях: Монография		М.: НОРМА, 2004,
Л2.3	В.И. Аверченков, М.Ю. Рытов	Служба защиты информации: организация и управление: учебное пособие для вузов		Москва : Издательство «Флинта», 2016, http://biblioclub.ru/index.php?page=book&id=93356
Л2.4	В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский	Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов		Москва : Издательство «Флинта», 2016, http://biblioclub.ru/index.php?page=book&id=93351

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	http://docs.cntd.ru/document/1200121984 - Криптографическая защита информации
И.2	
И.3	http://www.inside-zi.ru/ - Журнал «Защита информации. Инсайд»
И.4	https://lib.itsec.ru/articles2/allpubliks - Журнал Информационная безопасность
И.5	http://www.intuit.ru/ - Национальный Открытый Университет "ИНТУИТ"
И.6	https://elbib.ru/ - Научная электронная библиотека

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Освоение дисциплины предполагает как проведение традиционных аудиторных занятий, так и работу в электронной информационно-образовательной среде НИТУ «МИСиС» (ЭИОС), частью которой непосредственно предназначенной для осуществления образовательного процесса является Электронный образовательный ресурс LMS Canvas. Он доступен по URL адресу https://lms.misis.ru и позволяет использовать специальный контент и элементы электронного обучения и дистанционных образовательных технологий. LMS Canvas используется преимущественно для асинхронного взаимодействия между участниками образовательного процесса посредством сети «Интернет».
Чтобы эффективно использовать возможности LMS Canvas, а соответственно и успешно освоить дисциплину, нужно:
1) зарегистрироваться на курс. Для этого нужно перейти по ссылке … Логин и пароль совпадает с логином и паролем от личного кабинета НИТУ МИСиС;
2)в рубрике «В начало» ознакомиться с содержанием курса, вопросами для самостоятельной подготовки, условиями допуска к аттестации, формой промежуточной аттестации (зачет/экзамен), критериями оценивания и др.;
3)в рубрике «Модули», заходя в соответствующие разделы изучать учебные материалы, размещенные преподавателем. В т.ч. пользоваться литературой, рекомендованной преподавателем, переходя по ссылкам;
4)в рубрике «Библиотека» возможно подбирать для выполнения письменных работ (контрольные, домашние работы, курсовые работы/проекты) литературу, размещенную в ЭБС НИТУ «МИСиС;
5)в рубрике «Задания» нужно ознакомиться с содержанием задания к письменной работе, сроками сдачи, критериями оценки. В установленные сроки выполнить работу(ы), подгрузить здесь же для проверки. Удобно называть файл работы следующим образом (название предмета (сокращенно), группа, ФИО, дата актуализации (при повторном размещении)). Например, Экономика_Иванов_И.И._БМТ-19_20.04.2020. Если работа содержит рисунки, формулы, то с целью сохранения форматирования ее нужно подгружать в pdf формате.
Работа, подгружаемая 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 подгрузить работу не получится;
6)в рубрике «Тесты» пройти тестовые задания, освоив соответствующий материал, размещенный в рубрике «Модули»;
7)в рубрике «Оценки» отслеживать свою успеваемость;
8)в рубрике «Объявления» читать объявления, размещаемые преподавателем, давать обратную связь;
9)в рубрике «Обсуждения» 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.