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

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	6	6	6
Практические	12	12	12	12
Итого ауд.	18	18	18	18
Контактная работа	18	18	18	18
Сам. работа	158	158	158	158
Часы на контроль	4	4	4	4
Итого	180	180	180	180

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 Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСиС» по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата) (приказ от 05.03.2020 г. № № 95 о.в.)

Составлена на основании учебного плана:

Направление подготовки 09.03.03 Прикладная информатика Профиль. Прикладная информатика в технических системах, 09.03.03_21_ Прикладная информатика_ПрПИвТС_заоч_2020.plx , утвержденного Ученым советом ФГАОУ ВО НИТУ "МИСиС" в составе соответствующей ОПОП ВО 21.04.2021, протокол № 30

Утверждена в составе ОПОП ВО:

Направление подготовки 09.03.03 Прикладная информатика Профиль. Прикладная информатика в технических системах, , утвержденной Ученым советом ФГАОУ ВО НИТУ "МИСиС" 21.04.2021, протокол № 30

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: 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.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
ПК-2-З2 методологические основы моделирования, принципы математического моделирования технологических процессов в системах управления
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. Введение, основы информационной безопасности							
1.1	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. /Лек/	4	1		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э2 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в LMS Canvas: Информация. Её виды и свойства. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. /Ср/	4	34		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э2 Э3 Э4			
1.3	Методы и средства организационно-правовой защиты информации. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. /Пр/	4	2		Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	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/	4	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 LMS Canvas: 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/	4	40		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э3 Э4			
2.3	Анализ возможных каналов утечки информации. Защита документооборота в вычислительных системах. /Пр/	4	2		Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	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/	4	2		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			

3.2	Самостоятельное изучение учебного материала в LMS Canvas: Основные этапы развития криптологии. Основные понятия и определения. Криптостойкость. Методы криптографического преобразования данных. Кодирование. Асимметричные системы шифрования RSA. Надежность использования криптосистем. Перспективы развития криптографических методов защиты информации. /Ср/	4	30		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
3.3	Шифрование текста по ключу методами замены, перестановки, аддитивными методами (гаммированием). Методы шифрования текста при помощи аналитических преобразований. /Пр/	4	4		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	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/	4	2		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			

4.2	Самостоятельное изучение учебного материала в LMS Canvas: Классификация существующих типов систем обнаружения атак (СОА). Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ. Пароли как средство защиты информации. Системы и средства генерации паролей и их недостатки. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/	4	54		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
4.3	Разработка программной парольной защиты. Количественная оценка стойкости парольной защиты. Диагностика антивирусной программы и создание тестовых вирусов. /Пр/	4	4		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			
4.4	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-З2, УК-3-У1, УК-6-З1, УК-6-У1):

1. Понятие информации, ее свойства.
2. Основные понятия защиты информации.
3. Основные нормативно-правовые акты в области информационной безопасности.
4. Государственная тайна.
5. Основные стандарты в области обеспечения информационной безопасности.
6. Политика безопасности.
7. Составляющие информационной безопасности.
8. Безопасность в информационной среде.
9. Экономическая безопасность предприятия.
10. Классификация средств защиты.
11. Каналы утечки информации.
12. Основные виды сетевых и компьютерных угроз.
13. Результат и способы реализации угроз.
14. Инженерно-технические методы и средства защиты информации.
15. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
16. Классификация криптографических методов защиты информации.
17. Простейшие шифры с симметричным ключом.
18. Шифрование методами замены. Шифр «Атбаш». Шифр Playfair.
19. Шифрование методами замены. Шифр «Полибианский квадрат».
20. Шифрование методами замены. Шифр Трисимуса. Шифр «Юлия Цезаря».
21. Шифрование методами перестановки. Перестановка по таблице.
22. Шифрование методами перестановки. Шифр «Магический квадрат».
23. Шифрование аддитивными методами (гаммирование).
24. Шифрование с симметричными ключами при помощи аналитических преобразований.
25. Комбинированные методы шифрования.
26. Криптографические системы DES.
27. Асимметричные шифры.
28. Системы с открытыми ключами.
29. Электронно-цифровая подпись.
30. Криптографические протоколы: аутентификации, обмена ключами. Специфические протоколы.
31. Оценка криптостойкости шифров. Элементы криптоанализа.
32. Компьютерная стеганография и ее применение.
33. Туннелирование.
34. Основы биометрической идентификации.
35. Статические методы аутентификации.
36. Динамические методы аутентификации.
37. Парольная защита. Способы атаки на пароль. Обеспечение безопасности пароля.
38. Количественная оценка стойкости парольной защиты. Основные требования при выборе пароля пользователя.
39. Аутентификация пользователей на основе паролей.
40. Варианты атак на систему и пароль.
41. Антивирусные средства защиты информации.
42. Потенциальные угрозы и характер проявления компьютерных вирусов.

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: "Обеспечение информационной безопасности предприятия" (ОПК-3-В1, ПК-2-В1, УК-3-В1, УК-3-В2, УК-6-В1, УК-6-В2).
Цель расчетно-графической работы: закрепить теоретические знания и получить навыки обеспечения информационной безопасности предприятия.
В расчетно-графической работе требуется обеспечить информационную безопасность заданного объекта по нескольким ключевым позициям.
Исходные данные: индивидуальные варианты заданий с описанием объектов.
Для выполнения работы необходимо: обеспечить контроль над физическим доступом к информации, обеспечить безопасность информации в пределах сети и локальной системы, определить наиболее уязвимые места локальных машин, обеспечить безопасность каналов передачи данных.
Объем расчетно-графической работы - 20-25 стр.
Пояснительная записка к расчетно-графической работе должна содержать:
1) Титульный лист
2) Задание
3) Содержание
4) Введение
5) Описание объекта
6) Описание работы и устройство каждого из выбранных способов контроля над физическим доступом к информации
7) Сводная таблица характеристик четырех продуктов выбранного ПО для обеспечения безопасности
8) Описание причин проникновения, точки вторжения и симптомы заражения вредоносным ПО, способы противодействия
9) Описание выбранного протокола передачи данных, отличие от других протоколов из списка, обоснование использования протокола в коммуникациях объекта
10) Заключение
11) Список использованных источников
12) 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. Информация – это ...
а) содержание упорядоченной последовательности сообщений, отражающих умения и навыки.
б) содержание упорядоченной последовательности сообщений, передающих умения и навыки.
в) содержание упорядоченной последовательности сообщений, увеличивающих знания, умения и навыки.
г) содержание упорядоченной последовательности сообщений (в некотором алфавите), отражающих, передающих, увеличивающих знания, умения и навыки.

2. Интерпретация информации – это
а) переход к семантическому смыслу.
б) переход к синтаксическому смыслу.
в) расшифровка информации
г) искажение информации

3. Информация по доступу к ней бывает:
а) открытая (общедоступная) и закрытая (конфиденциальная)
б) избыточная, достаточная и недостаточная
в) исходная, промежуточная и результирующая
г) постоянная, переменная и смешанная

4. Что такое защита информации?
а) защита от несанкционированного доступа к информации;
б) выпуск бронированных коробочек для дискет;
в) комплекс мероприятий, направленных на обеспечение информационной безопасности.

5. К какой группе мер по защите информации относится шифрование информации?
а) организационным;
б) техническим;

в) аппаратным;
г) программным.

6. Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?
а) Уголовный кодекс РФ
б) Гражданский кодекс РФ
в) Доктрина информационной безопасности РФ
г) Постановления Правительства
д) Указ Президента РФ

7. Информация в праве рассматривается как ...
а) объект собственности и как интеллектуальная собственность.
б) объект собственности
в) интеллектуальная собственность.
г) предмет собственности

8. Информационное право составляет:
а) нормативную базу информационного общества
б) государственную политику
в) нормативную базу аграрного общества
г) нормативную базу доиндустриального общества

9. Политика безопасности:
а) строится на основе общих представлений об информационной системе организации;
б) строится на основе изучения политик родственных организаций;
в) строится на основе анализа рисков;
г) фиксирует правила разграничения доступа;
д) отражает подход организации к защите своих информационных активов;
е) описывает способы защиты руководства организации.

10. Правовое обеспечение безопасности информации делится:
а) международно-правовые нормы
б) национально-правовые нормы
в) все ответы правильные

11. Внешние техногенные угрозы информационной безопасности обусловлены:
а) средствами связи и помехами от них;
б) близко расположенными опасными производствами;
в) некачественными программными средствами;
г) взаимодействием технических средств.

12. К какой группе угроз информационной безопасности относятся ошибки программного обеспечения?
а) стихийные;
б) техногенные;
в) антропогенные

13. Естественные угрозы безопасности информации вызваны:
а) деятельностью человека;
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
г) корыстными устремлениями злоумышленников;
д) ошибками при действиях персонала.

14. К основным непреднамеренным искусственным угрозам АСОИ относится:
а) физическое разрушение системы путем взрыва, поджога и т.п.;
б) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
д) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи

15. Укажите принципы создания комплексной системы защиты информации:
а) неизменности;
б) прозрачности;
в) модульности;
г) рациональности;

д) доступности

16. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?
а) организационное;
б) организационно-техническое;
в) техническо-организационное;
г) техническое.

17. Какие пункты относятся к активным методам защиты речевой информации?
а) создание маскирующих акустических и вибрационных помех;
б) выявление факта несанкционированного подключения к линии;
в) создание прицельных электромагнитных помех акустическим закладным устройствам;
г) выявление излучений акустических закладных устройств;
д) уничтожение средств несанкционированного подключения к телефонной линии.

18. В число основных принципов построения системы безопасности, с точки зрения её архитектуры, входят:
а) следование признанным стандартам;
б) применение нестандартных решений, не известных злоумышленникам;
в) разнообразие защитных средств.

19. Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией о методах использования уязвимостей?
а) да, поскольку знание таких методов помогает ликвидировать уязвимости;
б) нет, поскольку это плодит новых злоумышленников;
в) не имеет значения, поскольку если информация об использовании уязвимостей понадобится, ее легко найти

20. В число принципов физической защиты входят:
а) беспощадный отпор;
б) непрерывность защиты в пространстве и времени;
в) минимизация защитных средств.

21. Меры информационной безопасности направлены на защиту от:
а) нанесения неприемлемого ущерба;
б) нанесения любого ущерба;
в) подглядывания в замочную скважину

21. Из принципа разнообразия защитных средств следует, что:
а) в разных точках подключения корпоративной сети к Internet необходимо устанавливать разные межсетевые экраны;
б) каждую точку подключения корпоративной сети к Internet необходимо защищать несколькими видами средств безопасности;
в) защитные средства нужно менять как можно чаще.

22. В чем заключается метод защиты информации - разграничение доступа?
а) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
б) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
в) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

23. В чем заключается метод защиты информации - разделение доступа (привилегий)
а) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
б) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
в) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

24. В чем заключается криптографическое преобразование информации?
а) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду
б) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого

доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
в) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
г) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

25. Программные средства – это…
а) А) специальные программы и системы защиты информации в информационных системах различного назначения
б) Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
в) В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

26. Криптографические средства – это…
а) А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
б) Б) специальные программы и системы защиты информации в информационных системах различного назначения
в) В) механизм, позволяющий получить новый класс на основе существующего

27. Характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа, называется
а) Криптографность
б) Криптоанализ
в) Криптостойкость
г) Симметричность
д) Кодировка

28. Алгоритм шифрования с двумя ключами (с открытым ключом)
а) Симметричный
б) Несимметричный
в) Открытый
г) Ключевой

29. Алгоритм шифрования с одним колючем (с секретным ключом)
а) Симметричный
б) Несимметричный
в) Асимметричный
г) Секретный

30. Присвоение какому-либо объекту или субъекту, реализующему доступ к системе, уникального имени (логина), образа или числового значения
а) Аутентификация
б) Электронно-цифровая подпись
в) Идентификация
г) Шифрация

31. Установление подлинности, проверка, является ли данный объект (субъект) в самом деле тем, за кого себя выдает
а) Электронно-цифровая подпись
б) Аутентификация
в) Идентификация
г) Дешифрация

32. Исследованием возможностей расшифрования информации без знания ключей занимается
а) криптография
б) криптоанализ
в) математика
г) математическая статистика

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

Критерии оценки ответов на зачете с оценкой, проводимом в дистанционной форме в LMS Canvas
90 ≤ Процент верных ответов ≤ 100 - отлично
75 ≤ Процент верных ответов < 90 - хорошо
60 ≤ Процент верных ответов < 75 – удовлетворительно

Критерии оценки выполнения расчетно-графической работы:
1. Теоретические сведения изложены в достаточном объеме, четко и последовательно
2. Исследуются и сравниваются разные подходы, методики, приводятся собственные суждения и выводы
3. Приведено описание объекта
4. Приведено описание работы и устройство каждого из выбранных способов контроля над физическим доступом к информации
5. Составлена сводная таблица характеристик четырех продуктов выбранного ПО для обеспечения безопасности
6. Приведено описание причин проникновения, точки вторжения и симптомы заражения вредоносным ПО, способы противодействия
7. Приведено Описание выбранного протокола передачи данных, отличие от других протоколов из списка, обоснование использования протокола в коммуникациях объекта
8. Расставлены ссылки на источники
9. Текст написан грамотно, стилистически выдержан
10. Текст оформлен в соответствии с требованиями

Работа оценивается на отлично, если:
- теоретические сведения изложены в достаточном объеме, четко и последовательно, использованы выводы (позиции, мнения и др.) известных ученых, профессионалов, исследуются и сравниваются разные подходы, методики, приводятся собственные суждения и выводы, имеются примеры, даются ссылки на источники, текст написан грамотно, стилистически выдержан и оформлен в соответствии с требованиями.
- приведено описание всех разделов работы развернуто, в полном объеме, составлена сводная таблица характеристик четырех продуктов выбранного ПО для обеспечения безопасности.
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 некоторые из них описаны кратко, не в полном объеме, 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 первой главе работы отсутствуют описания и сравнения разных подходов, методик и т.д. с последующим формированием собственных выводов на данный счет. Отсутствует описание некоторых разделов работы, отсутствует сводная таблица характеристик четырех продуктов выбранного ПО для обеспечения безопасности.
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	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,

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

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.