Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ
Проректор по учебной и научной работе
Лейфа А.В. Лейфа
« 2 » марта 2024 г.

РАБОЧАЯ ПРОГРАММА
МДК
МДК.02.02 Криптографическая защита информации

Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Квалификация выпускника – Техник по защите информации

Год набора – 2024

Курс 3,4 Семестр 6,7

Дифференцированный зачет 6,7 сем

Общая трудоемкость МДК 154.0 (академ. час)

Составитель Л.В. Никифорова, доцент, канд. техн. наук

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

2024

Рабочая программа составлена на основании Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерство просвещения Российской Федерации от 09.12.2016 № 1551

Рабочая программа обсуждена на заседании кафедры информационной безопасности

01.02.2024 г. , протокол № 8

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО
Зам. декана по учебной работе
Кирилюк Н.В. Кирилюк
« 2 » марта 2024 г.

СОГЛАСОВАНО
Выпускающая кафедра
Казакова Т.А. Казакова
« 2 » марта 2024 г.

СОГЛАСОВАНО
Научная библиотека
Петрович О.В. Петрович
« 2 » марта 2024 г.

СОГЛАСОВАНО
Центр цифровой трансформации и технического обеспечения
Тодосейчук А.А. Тодосейчук
« 2 » марта 2024 г.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Дисциплина «Криптографическая защита информации» относится к дисциплинам профессионального цикла и является частью образовательной программы в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных системах.

2. МЕСТО МДК В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Для успешного освоения данной дисциплины необходимы знания, полученные при изучении дисциплины «Информатика», «Математика», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

На компетенциях, формируемых на профессиональном модуле базируется прохождение производственной практики и производственной практики (преддипломной), а также подготовка и защита дипломного проекта(работы).

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ МДК И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1. Профессиональные компетенции и индикаторы их достижения

Категория (группа) профессиональных компетенций	Код и наименование профессиональных компетенции	Минимальные требования
ПК 2.1.	ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	ИД-1ПК 2.1 имеет практический опыт: установки, настройки, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС; ИД-2ПК 2.1 умеет: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; ИД-3 ПК 2.1 знает: способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовые программные и программно-аппаратные средства защиты информации в ИТКС;

		криптографические средства защиты информации конфиденциального характера, которые применяются в ИТКС.
ПК 2.2.	ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	ИД-1ПК 2.2 имеет практический опыт: поддержания бесперебойной работы программных и программно- аппаратных (в том числе криптографических) средств защиты информации в ИТКС; ИД-2ПК 2.2 умеет: выявлять и оценивать угрозы безопасности информации в ИТКС; проводить контроль показателей и процесса функционирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации; проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить техническое обслуживание и ремонт программно- аппаратных (в том числе криптографических) средств защиты информации; ИД-3ПК 2.2 знает: возможные угрозы безопасности информации в ИТКС; способов защиты информации от НСД и специальных воздействий на нее; порядок тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; организацию и содержание технического обслуживания и ремонта программно- аппаратных (в том числе криптографических) средств защиты информации; порядок и правила ведения эксплуатационной документации на программные и программно- аппаратные (в том числе криптографические) средства защиты информации.
ПК 2.3.	ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных	ИД-1ПК 2.3 имеет практический опыт: защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно- аппаратных (в том

	воздействий в информационно–телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	числе криптографических) средств защиты в соответствии с предъявляемыми требованиями; ИД-2ПК 2.3 умеет: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; ИД-3ПК 2.3 знает: возможные угрозы безопасности информации в ИТКС; способов защиты информации НСД и специальных воздействий на нее; типовые программные и программно- аппаратные средства защиты информации в ИТКС; криптографические средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации

4. СТРУКТУРА МДК

Общая трудоемкость МДК составляет 4.28 зачетных единицы, 154.0 академических часов.

1 – № п/п

2 – Тема (раздел) МДК, курсовая работа (проект), промежуточная аттестация

3 – Семестр

4 – Виды контактной работы и трудоемкость (в академических часах)

4.1 – Л (Лекции)

4.2 – Лекции в виде практической подготовки

4.3 – ПЗ (Практические занятия)

4.4 – Практические занятия в виде практической подготовки

4.5 – ЛР (Лабораторные работы)

4.6 – Лабораторные работы в виде практической подготовки

4.7 – ИКР (Иная контактная работа)

4.8 – КТО (Контроль теоретического обучения)

4.9 – КЭ (Контроль на экзамене)

5 – Контроль (в академических часах)

6 – Самостоятельная работа (в академических часах)

7 – Формы текущего контроля успеваемости

4.10 – У (Уроки)

4.11 – С (Семинарские занятия)

1	2	3	4											5	6	7
			4.1	4.2	4.3	4.4	4.5	4.6	4.10	4.11	4.7	4.8	4.9			
1	Введение в криптографию	6	4				4									Опрос.
2	Шифры замены и перестановки	6	4				4								2	Опрос. Подготовка к лабораторной работе. Выполнение и защита лабораторной работы.
3	Криптоанализ шифров замены и перестановки	6	4				8								2	Опрос. Подготовка к лабораторной работе. Выполнение и защита лабораторной работы.
4	Современные блочные шифры и их криптоанализ	6	28				24								6	Опрос. Подготовка к лабораторной работе. Выполнение и защита лабораторной работы.
5	Дифференцированный зачет	6														Тестирование
6	Арифметика целых чисел	7	2		2										1	Опрос. Подготовка к практической

																работе.
7	Криптография с ассиметричным ключом	7	18		18										1	Опрос. Подготовка к практической работе.
8	Целостность, установление подлинности и управление ключами	7	4		4										1	Опрос. Подготовка к практической работе.
9	Безопасность сети	7	6		6										1	Опрос. Подготовка к практической работе.
10	Дифференцированный зачет	7														
	Итого		70.0		30.0		40.0		0.0	0.0	0.0	0.0	0.0	0.0	14.0	

5. СОДЕРЖАНИЕ МДК

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Введение в криптографию	Триада и гексада Паркера. Основные понятия криптографических методов защиты информации: шифрование, расшифрование, дешифрование, криптография, криптоанализ, хеширование, электронная подпись. Классификация криптосистем. Математическая модель шифра.
2	Шифры замены и перестановки	Шифры замены: простой и многоалфавитной, усложненный шифр Цезаря, афинный шифр; перестановки: простой одинарной перестановки; блочной одинарной перестановки; табличной маршрутной перестановки; вертикальной перестановки; поворотной решетки; магический квадрат; множественной перестановки.
3	Криптоанализ шифров замены и перестановки	Криптоанализ шифров простой замены, шифра Виженера, шифров одинарной и двойной перестановки.
4	Современные блочные шифры и их криптоанализ	DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, имитовставка, AES. Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Атаки на симметричные шифры. Слайдовая атака.

5	Арифметика целых чисел	Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль- Гамаля. Криптосистема Рабина. Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3. Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012.
6	Криптография с ассиметричным ключом	Целостность сообщения и установление подлинности сообщения. Установление подлинности объекта. Управление ключами. Сертификаты открытого ключа.
7	Целостность, установление подлинности и управление ключами	Безопасность на прикладном уровне:PGP И S/ MIME. Безопасность на транспортном уровне: SSL И TLS. Безопасность на сетевом уровне: IP SEC.
8	Безопасность сети	

5.2. Практические занятия

Наименование темы	Содержание темы
Криптография с ассиметричным ключом	Протокол Диффи- Хеллмана. Шифр Шамира. Криптосистема RSA. Криптосистема Эль- Гамаля. Криптосистема Рабина. Генерация случайных чисел. Генератор Блм- Блюм- Шуба Криптографические хеш- функции. Электронная подпись RSA. Электронная подпись Эль- Гамаля. Электронная подпись ГОСТ Р 34.10-2012.
Целостность, установление подлинности и управление ключами	Установление подлинности сообщения. Установление подлинности объекта.
Безопасность сети	Изучение протоколов SSL, TLS, IPSec

5.3. Лабораторные занятия

Наименование темы	Содержание темы
Шифры замены и перестановки	Изучение классических шифров замены. Шифр Цезаря. Изучение классических шифров замены. Шифр Виженера. Шифры перестановки.
Криптоанализ шифров замены и перестановки	Криптоанализ шифров табличной перестановки. Криптоанализ шифра Виженера.
Современные блочные шифры и их криптоанализ	Исследование процесса шифрования и расшифрования сообщений с помощью S-DES. Слайдовая атака.

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в

			академических часах
1	Шифры замены и перестановки	Проработка лекции. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	2
2	Криптоанализ шифров замены и перестановки	Проработка лекции. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	2
3	Современные блочные шифры и их криптоанализ	Проработка лекции. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	6
4	Арифметика целых чисел	Проработка лекции. Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	1
5	Криптография с ассиметричным ключом	Проработка лекции. Изучение учебной литературы. Подготовка к практической работе.	1
6	Целостность, установление подлинности и управление ключами	Проработка лекции. Изучение учебной литературы. Подготовка к практической работе.	1
7	Безопасность сети	Проработка лекции. Изучение учебной литературы. Подготовка к практической работе.	1

Образовательный процесс по дисциплине строится на основе комбинации следующих образовательных технологий. Интегральную модель образовательного процесса по дисциплине формируют технологии методологического уровня: модульно-рейтинговое обучение, технология поэтапного формирования умственных действий, технология развивающего обучения, элементы технологии развития критического мышления.

Реализация данной модели предполагает использование следующих технологий стратегического уровня (задающих организационные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур:

– лекционные (вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция);

– лабораторные (углубление знаний, полученных на теоретических занятиях, решение задач);

– практические (формирование определенных умений и навыков, формирование алгоритмического мышления);

– активизации познавательной деятельности (приемы технологии развития критического мышления через чтение и письмо, работа с литературой, подготовка презентаций по темам домашних работ);

– самоуправления (самостоятельная работа студентов, самостоятельное изучение материала).

Информационные технологии используются при организации коммуникации со студентами для представления информации, выдачи рекомендаций и

консультирования по оперативным вопросам, использование мультимедиа- средств при проведении лекционных и практических занятий.

В качестве образовательных технологий при изучении дисциплины используются, мультимедийные лекции, на лабораторных занятиях используются современные пакеты программных продуктов. С целью текущего контроля знаний студентов на лабораторных работах проводится контроль выполнения работы. Студентам предлагается обсудить поученные результаты и высказать свое мнение по применению возможных приемов для улучшения показателей либо результатов работы.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма промежуточной аттестации 6 семестр: дифференцированный зачет.

Вопросы 6 семестр:

1. Способы защиты информации.
2. Триада CIA.
3. Гексада Паркера
4. Основные определения криптографии.
5. Шифр Цезаря.
6. Шифр Виженера.
7. Шифр простой одинарной перестановки.
8. Шифр блочной одинарной перестановки.
9. Шифр табличной маршрутной перестановки.
10. Шифр вертикальной перестановки.
11. Шифр множественной перестановки.
12. Простейшие исторические шифры и их анализ. Диск Энея
13. Простейшие исторические шифры и их анализ. Квадрат Полибия
14. Простейшие исторические шифры и их анализ. Магические квадраты.
15. Простейшие исторические шифры и их анализ. Таблица Тритемия
16. Простейшие исторические шифры и их анализ. Шифр Бэкона
17. Простейшие исторические шифры и их анализ. Шифровальный диск Альберти
18. Простейшие исторические шифры и их анализ. Шифры Порта
19. Простейшие исторические шифры и их анализ. Шифр Кардано и Решелье
20. Простейшие исторические шифры и их анализ. Шифр Фальконера
21. Классификация ключей.
22. Классификация криптографических алгоритмов.
23. Свойства криптосистем. Имитостойкость.
24. Свойства криптосистем. Криптографическая стойкость.
25. Основные задачи современной криптографии.
26. Общие требования к криптосистемам.
27. Алгебраическая модель шифра.
28. Вероятностная модель шифра.
29. Обобщенная модель шифра.
30. Результаты теории информации для криптографии
31. Схема Фейстеля.
32. Алгоритм шифрования DES. Общая схема алгоритма.
33. Алгоритм шифрования DES. Перестановка с расширением.
34. Алгоритм шифрования DES. Подстановка с помощью S-блоков.
35. Алгоритм шифрования DES. Процедура расширения ключа.
36. Безопасность DES.
37. Режимы работы блочных шифров
38. Схема алгоритма ГОСТ 28147-89.
39. Режимы работы алгоритма ГОСТ 28147-89 простой замены и выработки имитовставки.
40. Режимы работы алгоритма ГОСТ 28147-89 гаммирования и гаммирования с обратной связью.
41. Шифр «Магма» (ГОСТ Р 34.12-2015).
42 Вычислительная стойкость криптоалгоритмов.

43 Атаки на алгоритмы шифрования.
44 Метод грубой силы.
45 Потеря стойкости и попытки усиления существующих шифров.
46 Слайдовая атака.
47 Алгоритм AES.
48. Шифр «Кузнечик» (ГОСТ Р 34.12-2015).
49. Процедура расширения ключа алгоритма «Кузнечик».
50. Режимы шифра (ГОСТ Р 34.13-2015).
51.Имитостойкость и помехоустойчивость шифров.
52.Генерация ключей.
53.Генератор Блюм - Блюм – Шуба.
54. Стандарт ANSI X9.17.
55. Хранение и распределение ключей.

Форма промежуточной аттестации 7 семестр: дифференцированный зачет.
Вопросы 7 семестр.
1. Симметричные и асимметричные шифры.
2.Система Диффи – Хеллмана.
3. Понятие сравнения. Свойства сравнений.
4. Функция Эйлера. Малая теорема Ферма. Теорема Эйлера.
5. Вычисление числа, обратного по модулю заданному. Расширенный алгоритм Евклида.
6.Шифр Шамира
7.Шифр Эль-Гамаля.
8. Шифр RSA.
9. Метод бесключевого чтения.
10. Требования к криптографическим хэш-функциям.
11. Бесключевые хэш-функции.
12. Одноключевые хэш-функции.
13 Код аутентификации HMAC
14. Свойства цифровой подписи
15. Электронная цифровая подпись на основе RSA.
16. ЭЦП на основе схемы Эль-Гамаля
17. Стандарты на электронную цифровую подпись
18. Виды ЭЦП.
19. Цифровые сертификаты открытого ключа.
20.Целостность сообщения.
21.Установление подлинности сообщения.
22.Установление подлинности объекта.
23.Управление ключами.
24.Электронная почта.
25.Почтовая безопасность.
26.Безопасность на прикладном уровне:PGP.
27.Сценарии.
28.Кольца ключей.
29.PGP-сертификаты.
30.Аннулирование ключей.
31.PGP-пакеты.
32.PGP-сообщения.
33.MIME.
34.S/MIME.
35. Безопасность на прикладном уровне: S/MIME.
36.SSL-архитектура.
37.Алгоритмы шифрования/дешифрования.

38.Набор шифров.
39.Генерирование криптографических параметров.
40.Сеансы и соединение.
41.Четыре протокола.
42.Форматы сообщения SSL.
43.Безопасность на транспортном уровне: SSL.
44. Безопасность на транспортном уровне: TLS.
45.Безопасность на сетевом уровне: IP SEC.

Результаты (освоенные профессиональные компетенции)	Формы и методы контроля и оценки
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно- аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	Экспертная оценка выполнения практической работы по установке программного обеспечения
ПК 2.2. Поддерживать бесперебойную работу программных и программно- аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения
ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно–телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	Текущий контроль в форме: - защиты практических занятий; - защиты лабораторных работ; - контрольных работ по темам дисциплины.

8. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ МДК

а) литература

1.Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/bcode/543873

2.Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие для СПО / Б. А. Фороузан ; под редакцией А. Н. Берлина. — Саратов : Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/102192.html

Дополнительная литература:

1.Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА- М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: https:// doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https:// znanium.com/ catalog/ product/1860126

2.Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://

www.iprbookshop.ru/102207.html
3.Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3- е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340
4.Мэйволд, Э. Безопасность сетей : учебное пособие для СПО / Э. Мэйволд. — Саратов : Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102183.html

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	https://urait.ru/	Образовательная платформа Юрайт – образовательный ресурс, электронная библиотека и интернет-магазин, где читают и покупают электронные и печатные учебники авторов – преподавателей ведущих университетов для всех уровней профессионального образования, а также пользуются видео- и аудиоматериалами, тестированием и сервисами для преподавателей
2	https://e.lanbook.com/	ЭБС «Лань» – это крупнейшая политематическая база данных, включающая в себя контент сотен издательств научной, учебной литературы и научной периодики.
3	http://www.iprbooks.ru/	Электронная библиотечная система «IPRbooks» специализируется на учебных материалах по гуманитарным, естественным и точным наукам

в) профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	http://www.informika.ru	Сайт «Информика». Обеспечивает информационную поддержку всестороннего развития и продвижения новых информационных технологий в сферах образования и науки России
2	https://bdu.fstec.ru/ubi/	Банк данных угроз безопасности информации, созданный и поддерживаемый Федеральной службой по техническому и экспортному контролю и Государственным научно- исследовательским испытательным институтом проблем технической защиты информации
3	https://fstec.ru/	Сайт ФСТЭК России, содержащий актуальную и архивную информацию о действующих нормативно-правовых актах в области защиты информации, реестр сертифицированных средств защиты информации, перечень обязательных требований, соблюдение которых оценивается при проведении мероприятий по контролю при осуществлении деятельности в области информационной безопасности, Реестр лицензий СЗКИ, Реестр лицензий ТЗКИ и др. важную информацию.
4	https://standartgost.ru/	Открытая база ГОСТов
5	https://attack.mitre.org/	База знаний о тактике и методах противника, основанная на реальных наблюдениях.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ МДК

Занятия по дисциплине проводятся в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Все помещения, в которых проводятся занятия, соответствуют действующим противопожарным правилам и нормам. Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам и к электронной информационно- образовательной среде университета. Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду университета.

При изучении дисциплины «Криптографическая защита информации» используются: лекционная аудитория, оборудованная мультимедийными средствами; лаборатории, оборудованные рабочими местами пользователей ЭВМ