Аннотация к рабочей программе дисциплины «Криптографические методы защиты информации»

Цель преподавания дисциплины

Освоение студентами основных принципов и методов, применяемых при защите компьютерных систем, используя криптографические методы защиты информации.

Задачи изучения дисциплины

- ознакомить студентов сосновными положения криптографии;
- ознакомить студентов с математическими основами криптологии для наилучшего понимания построения криптографических систем;
- ознакомить студентов с наиболее известными криптоалгоритмами симметричным и асимметричным ключом, и их применением;
- ознакомить студентов с функциями хеширования и их использования в криптографии;
- обучить студентов основным методам криптографической защиты при передаче информации по незащищенному каналу;
- обучить студентов универсальным методам криптоанализа и условиям их применения.

Компетенции, формируемые в результате освоения дисциплины

Способностью применять соответствующий математический аппарат для решения профессиональных задач(ОПК-2); способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов(ПК-2);

Способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем(ПСК-10.2);

Способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи(ПСК-10.5).

Разделы дисциплины

Введение криптологию. Классификация криптоалгоритмов. Потоковыешифраторы. Блочные криптоалгоритмы. Ассиметричные криптоалгоритмы. Алгоритмы обмена ключами. Применение программных систем шифрования. Стеганография. Криптоанализ и криптостойкость.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«01» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы защиты информации

направление подготовки (специальность) *10.05.02*
(шифр согласно ФГОС
Информационная безопасность телекоммуникационных систем
и наименование направление подготовки (специальности)

Защита информации в системах связи и управления
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» и на основании учебного плана специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» (профиль «Защита информации в системах связи и управления»), одобренного Учёным советом университета, протокол 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения студентов по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» на заседании кафедры информационной безопасности.

«1» февраля 2017г. Протокол № 9

И.о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Ефремов М.А.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 1 «28» 08 2017 г. на заседании кафедры ИБ Таныгин М.О.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры ИБ протокол №: 12 от 29.06.18г
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № __ «___» _____ 20___ г. на заседании кафедры информационной безопасности, 21.06.2019, №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н. доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №4 «30» 01 2017 г. на заседании кафедры информационной безопасности протокол №1 от 31.08.2020г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №9 «26» 03 2018 г. на заседании кафедры информационной безопасности протокол №11 от 28.06.2021г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности протокол №11 от 30.06.22 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности протокол №1 от 30.08.2023г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

---

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами образовательной программы

1.1 Цель дисциплины

Освоение студентами основных принципов и методов, применяемых при защите компьютерных систем, используя криптографические методы защиты информации.

1.2 Задачи дисциплины

- ознакомить студентов с основными положения криптографии;
- ознакомить студентов с математическими основами криптологии для наилучшего понимания построения криптографических систем;
- ознакомить студентов с наиболее известными криптоалгоритмами с симметричным и асимметричным ключом, и их применением;
- ознакомить студентов с функциями хеширования и их использования в криптографии;
- обучить студентов основным методам криптографической защиты при передаче информации по незащищенному каналу;
- обучить студентов универсальным методам криптоанализа и условиям их применения.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

- механизмы решения типовых задач по криптографической защите информации;
- принципы построения алгоритмов цифровой подписи на основе асимметричных систем шифрования;
- полный перечень данных, нужных при проектировании подсистем и средств обеспечения криптографической безопасности информации;
- принципы работы программных, программно-аппаратных криптографических средств и технических средств зашиты информации;
- принципы работы программных средств системного, прикладного и специального назначения, знать языки и системы программирования для решения профессиональных задач по криптографической защите информации;
- теоретико-информационные оценки стойкости криптографических систем;
- возможные действия противника, направленные на нарушение работы криптографических средств защиты информации;
- наиболее уязвимые для атак противника элементы компьютерных систем;
- методы анализа и синтеза криптоалгоритмов;
- достаточные средства эффективной криптографической защиты информационных ресурсов компьютерных сетей и систем беспроводной связи.

уметь:

- проводить исследования с использованием наиболее подходящих математических аппаратов;
- формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование криптографической защиты объектов и процессов телекоммуникационных систем;
- оценивать техническое задание и находить оптимальное решение поставленной задачи;
- проводить комплексный анализ всех исходных данных для построения криптографических систем защиты информации;
- квалифицированно оценивать область применения конкретных механизмов криптографической защиты для построения защищенных информационных систем;
- строить и изучать математические модели криптоалгоритмов;
- применять полученные знания при решении разного рода задач по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- разрабатывать алгоритмы применения криптографических программных средств системного, прикладного и специального назначения;
- анализировать возможные уязвимости криптографических систем защиты информации.

владеть:

- навыками применения соответствующего математического аппарата для решения задач по криптографической защите информационно-телекоммуникационных систем;
- навыками применения криптографических программных средств системного, прикладного и специального назначения для решения задач по построению систем информационной безопасности телекоммуникационных систем;
- навыками, разработки средств криптографической защиты информационно-телекоммуникационных систем;
- основными навыками, необходимыми для определения степени выполнения требований применения средств криптографической защиты информационных ресурсов.

У обучающихся формируются следующие компетенции:

способностью применять соответствующий математический аппарат для решения профессиональных задач(ОПК-2);

способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов(ПК-2);

способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем(ПСК-10.2);

способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи(ПСК-10.5).

2Указание места дисциплины в структуре образовательной программы

«Криптографические методы защиты информации» представляет дисциплину с индексом Б1.Б.33 базовой части учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, изучаемую на4 курсе в7 семестре.

3Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы (з.е.),144 академических часов.

Таблица 3 –Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	72,15
в том числе:	
лекции	18
лабораторные занятия	36
практические занятия	18
экзамен	0,15
зачет	не предусмотрен
курсовая работа (проект)	не предусмотрена
расчетно-графическая (контрольная) работа	не предусмотрена
Аудиторная работа (всего):	72
в том числе:	
лекции	18
лабораторные занятия	36
практические занятия	18
Самостоятельная работа обучающихся (всего)	35,85
Контроль/экзамен (подготовка к экзамену)	36

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Введение в криптологию.	Задачи и программа курса. Введение в криптологию. Основные термины и определения. История развития науки. Криптография и криптоанализ. Исторические шифры.
2	Классификация криптоалгоритмов.	Классификация криптоалгоритмов. Математические основысистем шифрования. Симметричное и асимметричное шифрование, достоинства и недостатки систем шифрования.
3	Потоковые шифраторы.	Современные поточные шифры. Регистр сдвига с линейной обратной связью. Ассоциированный многочлен. Поточные шифры. Комбинирование РСЛОС. Наиболее распространенные поточные шифры.
4	Блочные криптоалгоритмы.	Блочные криптоалгоритмы. Блочное шифрование. Режимы блочного шифрования. Обзор наиболее распространенных блочных шифров. Алгоритмы многократного кодирования. Сеть Фейштеля. Шифр DES.
5	Ассиметричные криптоалгоритмы.	Ассиметричные криптоалгоритмы. Математические основы шифрования с открытым ключом. Открытый ключ. Секретный ключ. Системы распределения ключей. Достоинства и недостатки систем с открытым ключом. Хэш функции. Свойства криптографических хэш функций. Схемы цифровой подписи. Схема подписи с приложением. Схема с цифровой подписью с восстановлением сообщения.
6	Алгоритмы обмена ключами.	Система управления симметричными ключами с предварительной частичной установкой. Система управления симметричными ключами без предварительной частичной установки. Схема Диффи-Хеллмана. Схема Шамира. Протокол Диффи-Хеллмана распределения ключей с тремя и более участниками. Система управления ассиметричными ключами. Цифровые сертификаты. Центры сертификации. Депонирование ключей. EncryptedFileSystem (EFS). Схема Шамира разделения секрета.
7	Применение программных систем шифрования.	Применение программных криптосистем шифрования. Обзор основных программных продуктов на базе симметричных систем шифрования. Обзор основных программных продуктов на базе асимметричных систем шифрования. Программный продукт PGP.

8	Стеганография.	Стеганография. Тайнопись. Основные понятия. Классическая стеганография. Практическое использование. Обзор основных методов использования классической стеганографии. Компьютерная стеганография. Использование избыточности цифровой информации изображений, звука, видео. Использование компьютерных форматов данных. Применение компьютерной стеганографии.
9	Криптоанализ и криптостойкость.	Криптоанализ и криптостойкость. Основные методы криптоанализа. Оценка предельных мощностей взлома. Понятие стойкости шифров. Линейный криптоанализ. Дифференциальный криптоанализ. Безопасность криптографических протоколов. Доказуемая стойкость. Теоретико-информационные оценки стойкости криптосистем.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел учебной дисциплины	Виды учебной деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек.	№ лаб.	№ пр.			
1	Введение в криптологию.	2	1	1	О-1,2 Д-6,8 МУ-1,12	С, КО 2	ОПК-2
2	Классификация криптоалгоритмов.	2	2	2	О-1,2 Д-1-3 МУ-2,13	С, КО 4	ОПК-2 ПК-2
3	Потоковые шифраторы.	2	3	3	О-1,2 Д-3,6-8 МУ-3,14	С, КО 6	ОПК–2
4	Блочные криптоалгоритмы.	2	4	4	О-1,2 Д-3,6-8 МУ-4,15	С, КО 8	ПК-2
5	Ассиметричные криптоалгоритмы.	2	5	5	О-2,3 Д-4,6 МУ-5,16	С, КО 10	ОПК-2
6	Алгоритмы обмена ключами.	2	6	6	О-1,2 Д-1-3 МУ-6,17	С, КО 12	ПК-2
7	Применение программных систем шифрования.	2	7	7	О-2 Д-6 МУ-7-9,18	С, КО 14	ПСК – 10.2,
8	Стеганография.	2	8	8	О-1,2 Д-3-8 МУ-10,18	С, КО 16	ОПК-2

9	Криптоанализ и криптостойкость.	2	9	8	О-1,2 Д-1,2,4 МУ-11,19	С, КО 18	ПСК – 10.5

С – собеседование, КО – контрольный опрос.

4.2Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	2	3
1	Шифрование и анализ метода многопетлевой полиалфавитной подстановки	2
2	Программная реализация модели потокового шифратора	2
3	Построение и анализ аддитивных двоичных шифров	2
4	Построение и анализ блочных алгоритмов шифрования	2
5	Алгоритмы цифровой подписи	2
6	Алгоритмы обмена ключами. Разделение секрета.	2
7	Применение программных криптосистем шифрования. Изучение программного продукта Kremlin.Изучение программного продукта FoxSecret. Изучение программного продукта PGP	2
8	Стеганографическое закрытие данных. Изучение программных продуктов masker и s-tools	2
9	Основные методы криптоанализа. Криптоанализ методом вероятных слов	2
Итого		18

4.2.2Практическиеработы

Таблица 4.2.2–Практические занятия

№	Наименование практической работы	Объем, час.
1	2	3
1	Простые и составные числа. Нахождение НОД и НОК чисел. Алгоритм Евклида нахождения НОД двух чисел.	2

2	Расширенный алгоритм Евклида. Нахождение мультипликативно обратных элементов.	2
3	Функция Эйлера, её свойства. Мультипликативные функции. Вывод формулы для вычисления функции Эйлера.	2
4	Сравнения первой степени. Способ подбора и способ Эйлера решения сравнений первой степени.	2
5	Системы сравнений первой степени. Китайская теорема об остатках.	2
6	Первообразные корни по модулю натурального числа и их свойства. Теорема Гаусса.	2
7	Индексы (дискретные логарифмы). Теорема о степени первообразного корня. Свойства индексов.	2
8	Цепные и подходящие дроби.	4
Итого		18

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Введение в криптологию.	2 неделя	3,85
2.	Классификация криптоалгоритмов.	4 неделя	4
3.	Потоковые шифраторы.	6 неделя	4
4.	Блочные криптоалгоритмы.	8 неделя	4
5.	Ассиметричные криптоалгоритмы.	10 неделя	4
6.	Алгоритмы обмена ключами.	12 неделя	4
7.	Применение программных систем шифрования.	14 неделя	4
8.	Стеганография.	16 неделя	4
9.	Криптоанализ и криптостойкость.	18 неделя	4
Итого			35,85

5 Учебно-методическое обеспечение самостоятельной работы

Студенты могут при самостоятельном изучении отдельных тем и вопросов пользоваться учебно-наглядными пособиями, учебным оборудованием и

методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине, организуется:

библиотекой университета:

• библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

• имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

• путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

• путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.

• путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы аспирантов;

- заданий для самостоятельной работы;

- вопросов к зачетам;

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;

-удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии

В соответствии с требования ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017г. №301 по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 16,7 процента от аудиторных занятий согласно УП.

Таблица 6.1 – Образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.

1.	Выполнение лабораторной работы «Построение и анализ аддитивных двоичных шифров»	Выполнение студентом интерактивных заданий по криптоанализу аддитивных двоичных шифров	2
2.	Выполнение лабораторной работы «Построение и анализ блочных алгоритмов шифрования»	Исследование возможности передачи шифрованных сообщений блочными криптографическими средствами	2
3.	Выполнение лабораторной работы «Разделение секрета»	Выполнение студентом интерактивных заданий по реализации схем разделения секрета	2
4.	Выполнение лабораторной работы «Применение программных криптосистем шифрования.Изучение программного продукта PGP»	Выполнение студентом интерактивных заданий по настройке и применению программных криптосистем шифрования	2
5.	Выполнение лабораторной работы «Системы электронной подписи»	Выполнение студентом интерактивных заданий пососставлению и исследованию модели электронной подписи	2
6.	Выполнение работы по исследованию компьютерной стеганографии	Выполнение студентом интерактивных заданий по стеганографическому закрытию информации	2
	Итого		12

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 Этапы формирования компетенции

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способностью применять соответствующий математический аппарат для решения профессиональных задач	Математический анализ Алгебра и геометрия Теория вероятностей и математическая	Теория информации и кодирования Математические методы теории сигналов и систем	Криптографические методы защиты информации Теория

(ОПК-2)	статистика Дискретная математика Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности	Квантовая и оптическая электроника Моделирование систем и сетей телекоммуникаций Основы криптографии Основы теории чисел Учебно-лабораторный практикум	массового обслуживания Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов (ПК-2)		Математические методы теории сигналов и систем Цифровая обработка сигналов Моделирование систем и сетей телекоммуникаций Научно-исследовательская работа	Криптографические методы защиты информации Теория массового обслуживания Основы геоинформатики Инфокоммуникационные системы навигации и диспетчеризации и их защита Методы и средства мониторинга территорий и объектов Экспериментально-исследовательская практика Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем (ПСК-10.2)	Практика по получению профессиональных умений и опыта профессиональной деятельности		Криптографические методы защиты информации Программно-аппаратные средства обеспечения информационной безопасности Проектирование защищённых телекоммуникационных систем Основы многоканальных систем передачи Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-10.5)	Практика по получению профессиональных умений и опыта профессиональной деятельности	Безопасность операционных систем	Криптографические методы защиты информации Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 Показатели и критерии определения уровня сформированности компетенций (частей компетенций)

Код компетенции/этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ОПК-2/ начальный, основной, завершающий	*1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД* *2. Качество освоенных обучающимся знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	Знать: -основы теории информации построения криптографических систем. Уметь: -использовать математический аппарат для построения простейших криптографических систем Владеть: -навыками сбора необходимой информации для построения моделей криптографической защиты телекоммуникационных систем.	Знать: - основы теории информации и классификацию криптографических систем зашиты информации Уметь: - использовать математический аппарат и анализ полученных данных для построения криптографических систем Владеть: -навыками подбора наилучшего математического метода решения задачи по криптографической защите телекоммуникационных систем.	Знать: -принципы работы математических, программных, программно – аппаратных средств и технических средств криптографической зашиты информации телекоммуникационных систем Уметь: -применять все полученные знания при решении разного рода задач по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации Владеть: -навыками сбора и анализа информации для решения возникающих проблем профессионального характера по криптографической защите телекоммуникационных систем.
ПК-2 / начальный,	*1. Доля освоенных*	Знать: базовые принципы	Знать: современные	Знать: принципы формулирования

основной, завершающий	*обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД* *2. Качество освоенных обучающимся знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	формулирования задачи процессов телекоммуникационных систем Уметь: строить задачи, планировать исследования телекоммуникационных систем Владеть: навыками, позволяющими оценить объекты, явления и процессы телекоммуникационных систем	принципы формулирования задачи процессов телекоммуникационных систем Уметь: строить задачи, планировать и проводить исследования телекоммуникационных систем я Владеть: навыками, позволяющими оценить технические объекты, явления и процессы телекоммуникационных систем	задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование процессов телекоммуникационных систем Уметь: формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, Владеть: навыками, позволяющими формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов
ПСК-10.2 / начальный, основной, завершающий	*1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН,*	Знать: базовые знания формирования технического задания Уметь: работать с программными	Знать: необходимые знания формирования технического задания Уметь: работать	Знать: достаточными знаниями формирования технического задания Уметь оценивать

	установленных в п.1.3 РПД *2. Качество освоенных обучающимся знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	средствами защиты информационной безопасности Владеть: навыками, позволяющими оценить техническое задание средств защиты информационно-телекоммуникационных систем	с аппаратными и программными средствами защиты информационной безопасности Владеть: навыками, разработки средств защиты информационно-телекоммуникационных систем	техническое задание и находить оптимальное решение поставленной задачи Владеть: навыками, позволяющими формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем
ПСК-10.5 / начальный, основной, завершающий	*1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД* *2. Качество освоенных обучающимся знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	Знать: минимальные средства защиты информационных ресурсов компьютерных сетей и систем беспроводной связи Уметь: оценивать степень защищенности информационных ресурсов компьютерных сетей Владеть: навыками, необходимыми для определения степени выполнения требований применения средств защиты информационных ресурсов	Знать: необходимые средства защиты информационных ресурсов компьютерных сетей и систем беспроводной связи Уметь: оценивать степень защищенности и обеспечения эффективного применения средств защиты информационных ресурсов компьютерных сетей Владеть: основными навыками, необходимыми для определения степени выполнения требований применения средств защиты информационны	Знать: достаточные средства эффективной защиты информационных ресурсов компьютерных сетей и систем беспроводной связи Уметь: оценивать степень защищенности и обеспечения эффективного применения средств защиты информационных ресурсов компьютерных сетей Владеть: основными навыками, необходимыми для проведения оценки уровня защищенности и обеспечивать эффективное применение средств защиты информационных

			х ресурсов	ресурсов компьютерных сетей и систем беспроводной связи

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средствдля текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Введение в криптологию	ОПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	1-3	Согласно табл.7.2
				контрольные вопросы к лб. №1	1-6	
				контрольные вопросы к пр. №1	1-4	
2	Классификация криптоалгоритмов.	ОПК-2, ПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	4-7	Согласно табл.7.2
				контрольные вопросы к лб. №2	1-4	
				контрольные вопросы к пр. №2	1-6	
3	Потоковые шифраторы	ОПК-2	Лекция, СРС,	собеседование	8-12	Согласно табл.7.2

			лабораторное занятие, практическое занятие	контрольные вопросы к лб. №3	1-6	
				контрольные вопросы к пр. №3	1-5	
4	Блочные криптоалгоритмы.	ПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	13-17	Согласно табл.7.2
				контрольные вопросы к лб. №4	1-8	
				контрольные вопросы к пр. №4	1-10	
5	Ассиметричные криптоалгоритмы.	ОПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	18-22	Согласно табл.7.2
				контрольные вопросы к лб. №5	1-5	
				контрольные вопросы к пр. №5	1-5	
6	Алгоритмы обмена ключами.	ПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	23-26	Согласно табл.7.2
				контрольные вопросы к лб. №6	1-7	
				контрольные вопросы к пр. №6	1-5	
7	Применение программных систем шифрования.	ПСК-10.2	Лекция, СРС, лабораторное занятие, практическ	собеседование	27-31	Согласно табл.7.2
				контрольныевo-	1-5	

			ое занятие	просы к пр. №7		
				кон-троль-ные во-просы к пр. №7	1-6	
8	Стеганография.	ОПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	32-39	Согласно табл.7.2
				кон-троль-ные во-просы к лб. №8	1-6	
				кон-троль-ные во-просы к пр. №8	1-4	
9	Криптоанализ и криптостойкость.	ПСК-10.5	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	40-45	Согласно табл.7.2
				кон-троль-ные во-просы к лб. №9	1-5	
				кон-троль-ные во-просы к пр. №8	5-8	

Примеры типовых контрольных заданий для текущего контроля

Контрольные вопросы к лабораторной работе по разделу (теме) 1. «Шифрование и анализ метода многопетлевойполиалфавитной подстановки»

1. Какие подстановочные шифры вам известны,назовите их?
2. Какими методами возможно определение периода шифра?
3. В чем особенности применения метода Метод Ф. Казиски?
4. Как узнать длину первичных ключей?
5. Какую длину имеют первичные ключи, если длинна составного ключа равна 48, 60?

В чем отличие шифра Виженера от многопетлевых подстановок, какой метод более криптостойкий?

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Положение П 02.016–2018 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица**7.**4– Рейтинговый контроль изучения дисциплины

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы «Шифрование и анализ метода многопетлевойполиалфавитной подстановки»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Программная реализация модели потокового шифратора»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Построение и анализ аддитивных двоичных шифров»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Построение и анализ блочных алгоритмов шифрования»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Алгоритмы цифровой подписи»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Алгоритмы обмена ключами. Разделение секрета»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Применение программных криптосистем шифрования»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»

Выполнение лабораторной работы «Стеганографическое закрытие данных. Изучение программных продуктов masker и s-tools»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Основные методы криптоанализа. Криптоанализ методом вероятных слов»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
СРС	6		12	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Применко, Э. А. Алгебраические основы криптографии [Текст] : учебное пособие / Э. А. Применко. - Москва :Либроком, 2013. - 288 с. - (Основы защиты информации). - ISBN 978-5-382-014 55-5 : 470.00 р.

2. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В. Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. : ил., табл., схем. - ISBN 978-5-4332-0020-3 // Режим доступа - http://biblioclub.ru/

8.2 Дополнительная учебная литература

1. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. - 2-е изд., перераб. и доп. - М. : Радио и связь, 2001. - 376 с. : ил. - ISBN 5-256-01518-4 : 89.70 р.

2. Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с. : ил. - Б. ц.

3. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты [Текст] / А. А. Петров. - М. : ДМК, 2000. - 448 с. : ил. - ISBN 5-89818-064-8 : Б. ц.

4. Левин, М. PGP. Кодирование и шифрование информации с открытым ключом [Текст] / М. Левин. - М. : Майор, 2001. - 176 с. - ISBN 5-901321-05-7 : 41.80 р.

5. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / М. А.

Иванов, И. Чугунков. - Москва : МИФИ, 2012. - 400 с. - ISBN 978-5-7262-1676-8 : Б. ц.

6. Алферов, А. П. Основы криптографии [Текст] : учеб.пособие / А. П. Алферов [и др.]. - М. : Гелиос АРВ, 2001. - 480 с. : ил. - ISBN 5-85438-019-6 : 150.00 р.

7. Галатенко, В. А. Основы информационной безопасности. Курс лекций [Текст] : учебное пособие для студентов вузов / Под ред. В. Б. Бетелина. - 2-е изд., испр. - М. : ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004. - 264 с. - (Основы информационных технологий). - ISBN 5-9556-0015-9 : 184.00 р.

8. Смарт, Н. Криптография [Текст] / перевод с англ. С. А. Кулешова, под ред. С. К. Ландо. - М. :Техносфера, 2006. - 528 с. - (Мир программирования). - ISBN 5-94836-043-1 : 217.26 р.

9. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Текст] / О. Н. Василенко ; Институт проблем информационной безопасности МГУ. - М. : МЦНМО, 2003. - 328 с. - (Информационная безопасность : криптография). - ISBN 5-94057-103-4 : 75.00 р.

10. Логачев, О. А. Булевы функции в теории кодирования и криптологии [Текст] / О. А. Логачев, А. А. Сальников, В. В. Ященко. - М. : МЦНМО, 2004. - 470 с. - ISBN 5-94057-117-4 : 85.00 р.

8.3 Переченьметодическихуказаний

1. Ефремов, М. А. Криптоанализ шифра многопетлевойполиалфавитной подстановки [Электронный ресурс] : методические указания по выполнению лабораторной работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (537 КБ). - Курск : ЮЗГУ, 2015. - 15 с. : ил., табл. - Библиогр.: с. 15. - Б. ц.

2. Ефремов, М. А. Программная реализация модели потокового шифратора [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, А. Л. Ханис. - Электрон.текстовые дан. (456 КБ). - Курск : ЮЗГУ, 2015. - 20 с. : ил., табл. - Библиогр.: с. 20. - Б. ц.

3. Ефремов, М. А. Криптоанализ аддитивный двоичных шифров [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптоанализ» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, Р. А. Приходько. - Электрон.текстовые дан. (926 КБ). - Курск : ЮЗГУ, 2015. - 43 с. : ил., табл. - Библиогр.: с. 43. - Б. ц.

4. Ефремов, М. А. Криптоанализ блочных шифров [Электронный ресурс] : методические указания по выполнению лабораторной работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А.

Ефремов. - Электрон.текстовые дан. (353 КБ). - Курск : ЮЗГУ, 2015. - 13 с. : ил., табл. - Б. ц.

5. Ефремов, М. А. Алгоритмы цифровой подписи [Электронный ресурс] : методические указания по выполнению курсовой работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (782 КБ). - Курск : ЮЗГУ, 2016. - 31 с. - Библиогр.: с. 31. - Б. ц.

6. Ефремов, М. А. Разделение секрета [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (552 КБ). - Курск : ЮЗГУ, 2016. - 13 с. - Библиогр.: с. 13. - Б. ц.

7. Ефремов, М. А. Применение программных криптосистем шифрования. Изучение программного продукта Kremlin [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, А. Л. Ханис. - Электрон.текстовые дан. (650 КБ). - Курск : ЮЗГУ, 2015. - 20 с. : ил. - Б. ц.

8. Ефремов, М. А. Применение программных криптосистем шифрования. Изучение программного продукта FoxSecret [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, А. Л. Ханис. - Электрон.текстовые дан. (666 КБ). - Курск : ЮЗГУ, 2015. - 20 с. : ил. - Б. ц.

9. Ефремов, М. А. Применение программных криптосистем шифрования. Изучение программного продукта PGP [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, А. Л. Ханис. - Электрон.текстовые дан. (552 КБ). - Курск : ЮЗГУ, 2015. - 19 с. : ил. - Б. ц.

10. Ефремов, М. А. Стеганографические системы скрытия данных. Изучение программных продуктов masker и s-tools [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, А. Л. Ханис. - Электрон.текстовые дан. (642 КБ). - Курск : ЮЗГУ, 2015. - 18 с. : ил. - Библиогр.: с. 18. - Б. ц.

11. Ефремов, М. А. Криптоанализ методом вероятных слов [Электронный ресурс] : методические указания по выполнению лабораторной работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (365 КБ). - Курск : ЮЗГУ, 2015. - 13 с. : ил., табл. - Библиогр.: с. 13. - Б. ц.

12. Ефремов, М. А. Нахождение НОД и НОК чисел [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (511 КБ). - Курск : ЮЗГУ, 2016. - 15 с. - Библиогр.: с. 15. - Б. ц.

13. Ефремов, М. А. Расширенный алгоритм Евклида [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (327 КБ). - Курск : ЮЗГУ, 2016. - 10 с. - Библиогр.: с. 10. - Б. ц.

14. Ефремов, М. А. Функция Эйлера [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (305 КБ). - Курск : ЮЗГУ, 2016. - 8 с. - Библиогр.: с. 8. - Б. ц.

15. Ефремов, М. А. Сравнения [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (546 КБ). - Курск : ЮЗГУ, 2016. - 15 с. - Библиогр.: с. 15. - Б. ц.

16. Ефремов, М. А. Системы сравнений [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (550 КБ). - Курск : ЮЗГУ, 2016. - 16 с. - Библиогр.: с. 16. - Б. ц.

17. Ефремов, М. А. Первообразные корни [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (393 КБ). - Курск : ЮЗГУ, 2016. - 15 с. - Библиогр.: с. 15. - Б. ц.

18. Ефремов, М. А. Дискретные логарифмы [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (410 КБ). - Курск : ЮЗГУ, 2016. - 14 с. - Библиогр.: с. 14. - Б. ц.

19. Ефремов, М. А. Цепные и подходящие дроби [Электронный ресурс] : методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон.текстовые дан. (628 КБ). - Курск : ЮЗГУ, 2016. - 13 с. - Библиогр.: с. 13. - Б. ц.

8.4 Другие учебно-методические материалы

9 Перечень ресурсов информационно-телекоммуникационной сети

«Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru-Электронно-библиотечная система «Университетская библиотека онлайн».
2. www.elibrary.ru/defaultx.asp - научная электронная библиотека.
3. www.edu.ru - федеральный портал «Российское образование».
4. www.consultant.ru-Официальный сайткомпании «Консультант Плюс».
5. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/.
6. Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Криптографические методы защиты информации» являются лекции, лабораторные и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Криптографические методы защиты информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т.п.

В процессе обучения преподаватели используют активные формы работы со

студентами: чтение лекций, привлечение студентов к творческому процессу на практических занятиях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Криптографические методы защиты информации» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Криптографические методы защиты информации» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практическиенавыкисамостоятельногоанализаособенностейдисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включаяпереченьпрограммногообеспеченияиинформационныхсправочныхсистем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/) система шифрования OpenPGP (свободное ПО https://www.openpgp.org/ GNU Privacy Guard) , система стеганографического сокрытия данных S-Tools (свободное ПО https://myfreesoft.ru/s-tools.html) систем стеганографического сокрытия данных Masker (свободное ПО www.softportal.com/get-7599-masker.html) система шифрования Kremlin v3.0 (свободное ПО http://soft.sibnet.ru/soft/1089-kremlin-v3-0/) система шифрования Fox Secret 1.0 (свободное ПО www.softportal.com/software-4962-fox-secret.html)

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

13. Листдополненийи изменений,внесенныхврабочуюпрограмму дисциплины

Номер изменения	Номерастраниц				Всего страниц	Дата	Основаниедля измененияи подпись лица, проводившего изменения
	изменённых	заме-нённых	анну-лирован-ных	новых			
1	2,5,9,19				4	30.08.18	Протокол 12 от 29.06.2018