Аннотация к рабочей программе дисциплины «Криптографические методы защиты информации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Методы и средства криптографической защиты информации» является освоение студентами основных принципов и методов, применяемых при защите компьютерных систем, используя криптографические методы защиты информации.

Задачи изучения 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.

Компетенции, формируемые в результате освоения дисциплины

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

способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы

программирования для решения профессиональных задач (ПК-2);

способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).

Разделы дисциплины

Введение в криптологию. Классификация криптоалгоритмов. Потоковые шифраторы. Блочные криптоалгоритмы. Сеть Фейштеля. Ассиметричные криптоалгоритмы. Системы электронной цифровой подписи. Алгоритмы обмена ключами. Разделение секрета. Применение программных симметричных систем шифрования. Применение программных асимметричных систем шифрования. Стеганография. Основные понятия. Компьютерная стеганография. Криптоанализ и криптостойкость. Основные методы криптоанализа. Анализ безопасности криптографических протоколов. Способы применения криптосистем для решения специальных задач.

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) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
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 образования направления подготовки 10.03.01 – «Информационная безопасность» и на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность» (профиль «Безопасность автоматизированных систем»), одобренного Учёным советом университета, протокол 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения студентов по направлению подготовки 10.03.01 – «Информационная безопасность» на заседании кафедры информационной безопасности.

«1» февраля 2017 г. 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 направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол №1 «28» 08 2017 г. на заседании кафедры ИБ

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол №5 «01» 30 2017 г. на заседании кафедры ИБ

29.06.2018 № 12

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 – «Информационная безопасность», одобренного Ученым советом университета протокол №5 «30» 08 2017 г. на заседании кафедры

информационной безопасности 27.06.2019 № 11

(наименование кафедры, дата, номер протокола)

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

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения 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 изучения 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;
- принципы построения доказуемо стойких криптографических систем.

уметь:

- 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 криптографических программных средств системного, прикладного и специального назначения для решения задач по построению систем информационной безопасности;
- навыками подбора наилучшего метода решения поставленной задачи;
- основными методами криптоанализа для наилучшего понимания способов построения доказуемо стойких криптографических систем;
- навыками проектирования подсистем и средств обеспечения криптографической безопасности информации и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- навыками выявления уязвимостей в эксплуатируемых средствах криптографической защиты компьютерной информации.

У обучающихся формируются следующие компетенции:

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

способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).

2. Указание места дисциплины в структуре образовательной программы

«Криптографические методы защиты информации» представляет дисциплину с индексом Б1.Б.16 базовой части учебного плана направления подготовки 10.03.01 Информационная безопасность, изучаемую на 3 курсе в 6 семестре.

3. Объем 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 обучающихся

Общая трудоемкость (объем) дисциплины составляет 6 зачетных единиц (з.е.), 216 академических часов.

Таблица 3 – Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	216
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	91,15
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	18
экзамен	0,15
зачет	не предусмотрен
курсовая работа (проект)	1
расчетно-графическая (контрольная) работа	не предусмотрена
Аудиторная работа (всего):	90
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	18

Объём дисциплины	Всего, часов
Самостоятельная работа обучающихся (всего)	88,85
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. Классификация систем шифрования. Симметричное и асимметричное шифрование, достоинства и недостатки систем шифрования относительно друг друга.
3	Симметричные криптоалгоритмы.	Симметричные криптоалгоритмы. Основы симметричного шифрования. Блочные и поточные системы шифрования. Достоинства и недостатки симметричного шифрования.
4	Потоковые шифраторы.	Современные поточные шифры. Регистр сдвига с линейной обратной связью. Ассоциированный многочлен. Поточные шифры. Комбинирование РСЛОС. Наиболее распространенные поточные шифры.
5	Блочные криптоалгоритмы.	Блочные криптоалгоритмы. Блочное шифрование. Режимы блочного шифрования. Обзор наиболее распространенных блочных шифров.
6	Сеть Фейштеля.	Алгоритмы многократного кодирования. Раунды шифрования. Сеть Фейштеля. Шифр DES.
7	Ассиметричные криптоалгоритмы.	Ассиметричные криптоалгоритмы. Математические основы шифрования с открытым ключом. Открытый ключ. Секретный ключ. Системы распределения ключей. Достоинства и недостатки систем с открытым ключом.
8	Системы электронной цифровой подписи.	Хэш функции. Свойства криптографических хэш функций. Схемы цифровой подписи. Схема подписи с приложением. Схема с цифровой подписью с восстановлением сообщения.

9	Алгоритмы обмена ключами. Разделение секрета.	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. Encrypted File System (EFS). Схема Шамира разделения секрета.
10	Применение программных симметричных систем шифрования.	Применение программных криптосистем шифрования. Программная реализация симметричные системы шифрования. Обзор основных программных продуктов на базе симметричных систем шифрования.
11	Применение программных асимметричных систем шифрования.	Программная реализация асимметричные системы шифрования. Обзор основных программных продуктов на базе асимметричных систем шифрования. Программный продукт PGP.
12	Стеганография. Основные понятия.	Стеганография. Тайнопись. Основные понятия. Классическая стеганография. Практическое использование. Обзор основных методов использования классической стеганографии.
13	Компьютерная стеганография.	Компьютерная стеганография. Использование избыточности цифровой информации изображений, звука, видео. Использование компьютерных форматов данных. Применение компьютерной стеганографии.
14	Криптоанализ и криптостойкость. Основные методы криптоанализа.	Криптоанализ и криптостойкость. Основные методы криптоанализа. Оценка предельных мощностей взлома. Понятие стойкости шифров. Линейный криптоанализ. Дифференциальный криптоанализ.
15	Анализ безопасности криптографических протоколов.	Безопасность криптографических протоколов. Доказуемая стойкость. Теоретико-информационные оценки стойкости криптосистем.
16	Способы применения криптосистем для решения специальных задач.	Обзор способов применения криптосистем для решения специальных задач. Аутентификация. Удаленная идентификация пользователей. Контроль целостности сообщений. Невозможность отказа от авторства.

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. час	№ лаб.	№ пр.			
1	Введение в криптологию.	2	1	1	О-1,2 Д-6,8 МУ-1,15	С, КО2	ПК-7

2	Классификация криптоалгоритмов.	2	2	2	О-1,2 Д-1-3 МУ-2,16	С, КО 3	ПК-2
3	Симметричные криптоалгоритмы.	2	3	3	О-1,2 Д-3,6-8 МУ-3,17	С, КО 4	ПК-2
4	Потоковые шифраторы.	2	4,5	4	О-1,2 Д-3,6-8 МУ- 4,5,18	С, КО 5	ОПК-2 ПК-1
5	Блочные криптоалгоритмы.	2	6	5	О-2,3 Д-1-3,6 МУ-6,19	С, КО 6	ПК-1 ПК-2
6	Сеть Фейштеля. Алгоритмы многократного кодирования.	2	7	6	О-1,2 Д-1-3 МУ-7,20	С, КО 7	ПК-2
7	Ассиметричные криптоалгоритмы.	2		7	О-1,2 Д-2,4,6 МУ-21	С 8	ОПК-2 ПК-1 ПК-2
8	Системы электронной цифровой подписи.	4	8	8	О-1,2 Д-3-8 МУ-8,21	С, КО 10	ПК-1 ПК-7
9	Алгоритмы обмена ключами. Разделение секрета.	2	9		О-1,2 Д-1,2,4 МУ-9,22	С, КО 11	ПК-1 ПК-2
10	Применение программных криптосистем шифрования. Симметричные системы шифрования.	2	10, 11		О-1,2 Д- 8,9 МУ- 10,11	С, КО 12	ПК-2
11	Применение программных криптосистем шифрования. Асимметричные системы шифрования.	2	12		О-1,2 Д-8,9 МУ-12	С, КО 13	ПК-7
12	Стеганография. Основные понятия. Практическое использование.	2			О-1,2 Д-6,8	С 14	ПК-2
13	Компьютерная стеганография. Использование избыточности цифровой информации.	2	13		О-1,2 Д-6,8 МУ-13	С, КО 15	ПК-1 ПК-7
14	Криптоанализ и криптостойкость. Основные методы криптоанализа.	4	14		О-2 Д-6-8 МУ-14	С, КО 16	ПК-7
15	Анализ безопасности криптографических протоколов.	2			О-1,2 Д-6,8	С 17	ПК-2
16	Обзор способов применения криптосистем для решения специальных задач.	2			О-1,2 Д-2,4,6	С 18	ПК-7

С – собеседование, КО – контрольный опрос.

4.2 Лабораторные работы и (или) практические занятия

4.2.1Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	2	4
1	Шифрование и анализ метода моноалфавитной подстановки	2
2	Шифрование и анализ метода полиалфавитной подстановки	2
3	Шифрование и анализ метода многопетлевой полиалфавитной подстановки	2
4	Программная реализация модели потокового шифратора	2
5	Построение и анализ аддитивных двоичных шифров	2
6	Построение и анализ блочных алгоритмов шифрования	4
7	Криптоанализ шифра табличной перестановки	2
8	Алгоритмы цифровой подписи	4
9	Алгоритмы обмена ключами. Разделение секрета.	2
10	Применение программных криптосистем шифрования. Симметричные системы шифрования. Изучение программного продукта Kremlin.	2
11	Применение программных криптосистем шифрования. Изучение программного продукта FoxSecret.	2
12	Применение программных криптосистем шифрования. Асимметричные системы шифрования. Изучение программного продукта PGP.	2
13	Стеганографические системы скрытия данных. Изучение программных продуктов masker и s-tools	4
14	Основные методы криптоанализа. Криптоанализ методом вероятных слов	4
Итого		36

4.2.2 Практические занятия

Таблица 4.2 – Практические занятия

№	Наименование практического занятия	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	2

	обратных элементов.	
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	2
2.	Классификация криптоалгоритмов.	3 неделя	2
3.	Симметричные криптоалгоритмы.	4 неделя	2
4.	Потоковые шифраторы.	5 неделя	2
5.	Блочные криптоалгоритмы.	6 неделя	2
6.	Сеть Фейштеля. Алгоритмы многократного кодирования.	7 неделя	2
7.	Ассиметричные криптоалгоритмы.	8 неделя	4
8.	Системы электронной цифровой подписи.	10 неделя	4
9.	Алгоритмы обмена ключами. Разделение секрета.	11 неделя	4
10.	Применение программных криптосистем шифрования. Симметричные системы шифрования.	12 неделя	2
11.	Применение программных криптосистем шифрования. Асимметричные системы шифрования. Системы электронной подписи	13 неделя	2
12.	Стеганография. Основные понятия. Практическое использование	14 неделя	2
13.	Компьютерная стеганография. Использование избыточности цифровой информации.	15 неделя	2
14.	Криптоанализ и криптостойкость. Основные методы криптоанализа.	16 неделя	2
15.	Анализ безопасности криптографических протоколов.	17 неделя	2
16.	Обзор способов применения криптосистем для решения специальных задач.	18 неделя	2
17.	Курсовая работа.	19 неделя	14,85
Итого			88,85

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин 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;

– тем рефератов и докладов;

– вопросов к экзаменам и зачетам;

–методических указаний к выполнению лабораторных и практических работ и т.д.

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 направлению подготовки 10.03.01 «Информационная безопасность» 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 24,8 процента от аудиторных занятий согласно УП.

Таблица 6.1 – Интерактивные 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 «Шифрование и анализ метода моноалфавитной подстановки»	Выполнение студентом интерактивных заданий по криптоанализу шифра моноалфавитной подстановки	2
2.	Выполнение лабораторной работы «Шифрование и анализ метода полиалфавитной подстановки»	Выполнение студентом интерактивных заданий по криптоанализу шифра полиалфавитной подстановки	1
3.	Выполнение лабораторной работы «Шифрование и анализ метода многопетлевой полиалфавитной подстановки»	Выполнение студентом интерактивных заданий по криптоанализу шифра многопетлевой полиалфавитной подстановки	2
4.	Выполнение работы «Программная реализация модели потокового шифратора»	Выполнение студентом интерактивных заданий по реализации потокового шифрования	2
5.	Выполнение лабораторной работы «Построение и анализ аддитивных двоичных шифров»	Выполнение студентом интерактивных заданий по криптоанализу аддитивных двоичных шифров	2
6.	Выполнение лабораторной работы «Построение и анализ блочных алгоритмов шифрования»	Исследование возможности передачи шифрованных сообщений блочными криптографическими средствами	2
7.	Выполнение лабораторной работы «Криптоанализ шифра табличной перестановки»	Выполнение студентом интерактивных заданий по криптоанализу	2
8.	Выполнение лабораторной работы «Алгоритмы цифровой подписи»	Составление и исследование студентами модели электронной подписи	2
9.	Выполнение лабораторной работы «Алгоритмы обмена ключами. Разделение секрета»	Выполнение студентом интерактивных заданий по реализации схем разделения секрета	2
10.	Выполнение лабораторной работы «Симметричные системы шифрования. Изучение программного продукта Kremlin»	Выполнение студентом интерактивных заданий по настройке и применению программных криптосистем шифрования	1
11.	Выполнение лабораторной работы «Применение программных криптосистем шифрования. Изучение программного продукта FoxSecret»	Выполнение студентом интерактивных заданий по настройке и применению программных криптосистем шифрования	1
12.	Выполнение лабораторной работы «Асимметричные системы шифрования. Изучение программного продукта PGP»	Выполнение студентом интерактивных заданий по настройке и применению программных	1

		криптосистем шифрования	
13.	Выполнение лабораторной работы «Стеганографические системы скрытия данных. Изучение программных продуктов masker и s-tools»	Выполнение студентом интерактивных заданий по стеганографическому закрытию информации	2
14.	Выполнение лабораторной работы «Основные методы криптоанализа. Криптоанализ методом вероятных слов»	Выполнение студентом интерактивных заданий по криптоанализу методом вероятных слов	2
Итого			24

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
ОПК-2 - Способностью применять соответствующий математический аппарат для решения профессиональных задач	Математика Теория вероятностей и математическая статистика Дискретная математика Высшая математика (спецглавы) Математическая логика и теория алгоритмов Элементы алгебры и теории чисел Теория графов Ознакомительная практика	Криптографические методы защиты информации Методы оптимизации Вычислительные методы	Теория информации Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-1 - Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Ознакомительная практика	Введение в криптографию; Аппаратные средства вычислительной техники; Криптографические методы защиты информации;	Программно-аппаратные средства защиты информации; Инженерно-техническая защита информации; Эксплуатацион

		Безопасность сетей ЭВМ; Технические средства охраны; Системы контроля доступа и видеонаблюдения; Технологическая практика	ная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-2 - способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Языки программирования; Технологии и методы программирования; Информационные технологии; Ознакомительная практика	Введение в криптографию; Криптографические методы защиты информации; Методы защиты программного обеспечения; Основы риверсинжиниринга программных средств	Эксплуатационная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-7 - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Патентоведение	Введение в криптографию; Криптографические методы защиты информации; Экология; Технологическая практика; Проектно-технологическая практика	Инженерно-техническая защита 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, описания кал оценивания

Код компетенции/этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («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: -основные математические функции и алгоритмы прикладного и специального назначения. Уметь: - применять соответствующий математический аппарат для решения профессиональных задач Владеть: -минимальными навыками математического моделирования и программирования	Знать: -принципы работы программных средств системного, прикладного и специального назначения криптографической защиты информации Уметь: -разрабатывать алгоритмы применения программных средств системного, прикладного и специального назначения Владеть: -навыками программирования для решения поставленных профессиональных задач по криптографической защите информации	Знать: -принципы работы программных средств системного, прикладного и специального назначения, знать языки и системы программирования для решения задач криптографической защиты информации Уметь: -разрабатывать алгоритмы применения программных средств системного, прикладного и специального назначения, инструментальные средства Владеть: -навыками применения программных средств системного, прикладного и специального назначения, программирования для решения поставленных профессиональных задач
ПК-1/ 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*	Знать: -простейшие методы работы с программным обеспечением. Уметь: -выполнять работы по установке и настройке программного обеспечения Владеть: -навыками сбора необходимой информации по	Знать: -принципы работы программных, программно – аппаратных средств и технических средств зашиты информации Уметь: -проводить анализ полученных исходных данных Владеть: -навыками подбора наилучший метода	Знать: -принципы работы программных, программно – аппаратных средств и технических средств криптографической зашиты информации Уметь: -применять все полученные знания при решении разного рода задач по установке, настройке и обслуживанию

Код компетенции/этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	работе с программных, программно – аппаратных средств.	решения поставленной задачи.	программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации Владеть: -достаточным количеством информации для решения возникающих проблем профессионального характера.
ПК-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: -основные характеристики программных и технических средств прикладного и специального назначения. Уметь: -разбираться в технической документации к программным средствам Владеть: -минимальными навыками программирования	Знать: -принципы работы программных средств системного, прикладного и специального назначения криптографической защиты информации Уметь: -разрабатывать алгоритмы применения программных средств системного, прикладного и специального назначения Владеть: -навыками программирования для решения поставленных профессиональных задач по	Знать: -принципы работы программных средств системного, прикладного и специального назначения, знать языки и системы программирования для решения задач криптографической защиты информации Уметь: -разрабатывать алгоритмы применения программных средств системного, прикладного и специального назначения, инструментальные средства Владеть: -навыками применения программных средств системного,

Код компетенции/этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
			криптографической защите информации	прикладного и специального назначения, программирования для решения поставленных профессиональных задач
ПК-7/ 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: -минимальный перечень данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности Уметь: -обосновать правильность и необходимость собранных данных Владеть: -базовыми методами сбора данных	Знать: -достаточный перечень данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности Уметь: -проводить анализ исходных данных для построения криптографических систем Владеть: -навыками сбора и обработки исходных данных для построения криптографических систем	Знать: -полный перечень данных, нужных при проектировании подсистем и средств обеспечения криптографической защиты информационных систем Уметь: -проводить комплексный анализ всех исходных данных для построения криптографических систем защиты данных Владеть: - навыками проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

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 средств

№ 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	ПК-7	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	1-8	Согласно табл.7.2
				контрольные вопросы к лб. №1	1-6	
				контрольные вопросы к пр. №1	1-4	
2	Классификация криптоалгоритмов.	ПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	1-5	Согласно табл.7.2
				контрольные вопросы к лб. №2	1-4	
				контрольные вопросы к пр. №2	1-6	
3	Симметричные криптоалгоритмы.	ПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	1-5	Согласно табл.7.2
				контрольные вопросы к лб. №3	1-6	
				контрольные вопросы к пр. №3	1-5	
4	Потоковые шифраторы	ОПК-2 ПК-1	Лекция, СРС,	собеседование	1-7	Согласно табл.7.2

			лабораторные занятия, практическое занятие	контрольные вопросы к лб. №4,5	1-8	
				контрольные вопросы к пр. №4	1-10	
5	Блочные криптоалгоритмы.	ПК-1	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	1-4	Согласно табл.7.2
				контрольные вопросы к лб. №6	1-5	
				контрольные вопросы к пр. №5	1-5	
6	Сеть Фейштеля. Алгоритмы многократного кодирования.	ПК-2	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	1-4	Согласно табл.7.2
				контрольные вопросы к лб. №7	1-7	
				контрольные вопросы к пр. №6	1-5	
7	Ассиметричные криптоалгоритмы.	ОПК-2 ПК-1 ПК-2	Лекция, СРС, практическое занятие	собеседование	1-7	Согласно табл.7.2
				контрольные вопросы к пр. №7	1-5	
8	Системы электронной цифровой подписи.	ПК-1 ПК-7	Лекция, СРС, лабораторное занятие, практическое занятие	собеседование	1-5	Согласно табл.7.2
				контрольные вопросы к лб. №8	1-6	
				контрольные во-	1-5	

				просы к пр. №8		
9	Алгоритмы обмена ключами. Разделение секрета.	ПК-1 ПК-2	Лекция, СРС, лабораторное занятие	собеседование	1-10	Согласно табл.7.2
				контрольные вопросы к лб. №9	1-5	
10	Применение программных криптосистем шифрования. Симметричные системы шифрования.	ПК-2	Лекция, СРС, лабораторное занятие	собеседование	1-4	Согласно табл.7.2
				контрольные вопросы к лб. №10	1-8	
				контрольные вопросы к лб. №11	1-12	
11	Применение программных криптосистем шифрования. Асимметричные системы шифрования.	ПК-7	Лекция, СРС, лабораторное занятие	собеседование	1-4	Согласно табл.7.2
				контрольные вопросы к лб. №12	1-12	
12	Стеганография. Основные понятия. Практическое использование.	ПК-2	Лекция, СРС	собеседование	1-6	Согласно табл.7.2
13	Компьютерная стеганография. Использование избыточности цифровой информации.	ПК-1 ПК-7	Лекция, СРС, лабораторное занятие	собеседование	1-6	Согласно табл.7.2
				контрольные вопросы к лб. №13	1-8	
14	Криптоанализ и криптостойкость. Основные методы криптоанализа.	ПК-7	Лекция, СРС	собеседование	1-7	Согласно табл.7.2
				контрольные во-	1-7	

				просы к лб. №14		
15	Анализ безопасности криптографических протоколов.	ПК-2	Лекция, СРС	собеседование	1-3	Согласно табл.7.2
16	Обзор способов применения криптосистем для решения специальных задач.	ПК-7	Лекция, СРС	собеседование	1-5	Согласно табл.7.2

Примеры типовых контрольных заданий для текущего контроля

Вопросы собеседования по разделу (теме) 1. «Введение в криптологию»

1. Назовите основные этапы истории развития криптологии как науки.
2. Каковы основные задачи криптологии как науки.
3. Назовите основные термины используемые в криптографии.
4. Исторические сведения о системах и способах составления шифрованных писем.
5. Как были устроены первые криптосистемы.
6. Что такое криптоанализ.
7. Чем криптография отличается от криптоанализа.
8. Какое понятие шире криптография или криптология.

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

1. Что понимается под моноалфавитными подстановками?
2. Приведите примеры моноалфавитных подстановок.
3. Что такое коэффициент сдвига?
4. Что такое мощность алфавита?
5. Что такое частотные характеристики символов?
6. Какова криптостойкость шифра моноалфавитной подстановки?

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

оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

- методические указания, используемые в образовательном процессе, указан- ные 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 моноалфавитной подстановки»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы «Шифрование и анализ метода полиалфавитной подстановки»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы «Шифрование и анализ метода многопетлевой полиалфавитной подстановки»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение работы «Программная реализация модели потокового шифратора»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Построение и анализ аддитивный 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 «Криптоанализ шифра табличной перестановки»	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 «Симметричные системы шифрования. Изучение программного продукта Kremlin»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы «Применение программных криптосистем шифрования. Изучение программного продукта FoxSecret»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы «Асимметричные системы шифрования. Изучение программного продукта PGP»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Стеганографические системы скрытия данных. Изучение программных продуктов masker и s-tools»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Криптоанализ методом вероятных слов»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
СРС	0		0	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

При итоговом контроле (экзамене) в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговое количество правильных ответов (максимум 15) переводят в баллы на зачёте (максимум 36) путём умножения на 2,4 и округления до целого значения.

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

8.1 Основная учебная литература

1. Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание / Н. В. Майстренко, А. В. Майстренко. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 13.09.2021). – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Текст : электронный.

2. Усенко, О. А. Приложения теории информации и криптографии в радиотехнических системах : учебное пособие / О. А. Усенко ; Южный

федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 171 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500141 (дата обращения: 13.09.2021). – Библиогр. в кн. – ISBN 978-5-9275-2569-0. – Текст : электронный.

3. Фороузан, Б. А. Математика криптографии и теория шифрования : учебное пособие : [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с. : ил., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428998 (дата обращения: 13.09.2021). – Библиогр. в кн. – ISBN 978-5-9963-0242-0. – Текст : электронный.

4. Кнауб, Л. В. Теоретико-численные методы в криптографии : учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2011. – 160 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=229582 (дата обращения: 13.09.2021). – ISBN 978-5-7638-2113-7. – Текст : электронный.

8.2 Дополнительная учебная литература

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

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

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

4. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. - М. : КУДИЦ-ОБРАЗ, 2001. - 368 с. - ISBN 5-93378-021-9 : 165.60 р. - Текст : непосредственный.

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

6. Галатенко, В. А. Основы информационной безопасности. Курс лекций : 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. - Текст : непосредственный.

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

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

8.3Перечень методических указаний

1. 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.

2. 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.

3. 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. 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. 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.

6. Криптоанализ шифра многопетлевой полиалфавитной 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.

7. Криптоанализ шифра моноалфавитной 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. (631 КБ). - Курск : ЮЗГУ, 2015. - 14 с. : ил., табл. - Библиогр.: с. 14. - Б. ц.

8. Криптоанализ шифра полиалфавитной 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. (429 КБ). - Курск : ЮЗГУ, 2015. - 18 с. : ил., табл. - Библиогр.: с. 18. - Б. ц.

9. Криптоанализ шифра табличной перестановки : [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. (662 КБ). - Курск : ЮЗГУ, 2015. - 12 с. : ил., табл. - Библиогр.: с. 12. - Б. ц.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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 сайт компании «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 лабораторные 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 практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (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. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего
	изменённых	заме-нённых	анну-лирован-ных	новых			
1	2, 5,10, 20				4	30.08.18	Протокол 12 от 29.06.2018