Аннотация к рабочей программе дисциплины «Методы и средства криптографической 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

Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности; (ОПК-10).

Разделы дисциплины

Введение в криптологию. Классификация криптоалгоритмов. Потоковые шифраторы. Блочные криптоалгоритмы. Ассиметричные криптоалгоритмы.

Алгоритмы обмена ключами. Применение программных систем шифрования. Стеганография. Криптоанализ и криптостойкость.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

М.О. Таныгин
(подпись, инициалы, фамилия)
«31» 08 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации
(наименование дисциплины)

ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем
шифр и наименование направление подготовки (специальности)

Управление безопасностью телекоммуникационных систем и сетей
наименование направленности (профиля, специализации)

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

Курск – 2021

Рабочая программа дисциплины «Методы и средства криптографической защиты информации» составлена в соответствии с ФГОС ВО – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета (протокол № 6 «22» 02 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей» на заседании кафедры информационной безопасности №1 «30» 08 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Ефремов М.А.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины «Методы и средства криптографической защиты информации» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №6 «26» 02 2021 г., на заседании кафедры ИБ, протокол № 11 от 30.06.2022 г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой М.О. Таныгин

Рабочая программа дисциплины «Методы и средства криптографической защиты информации» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «27» 02 2023 г., на заседании кафедры ИБ протокол №1 от 30.08.2023
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «27» 03 2024 г., на заседании кафедры *информационной безопасности*, протокол №12 от «24» 06 2024 г.

Зав. кафедрой ____________ Марухленко А.П.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «31» 03 2025 г., на заседании кафедры *информационной безопасности*, протокол № 12 от «24» 06 2025 г.

Зав. кафедрой ____________ Паньшин М.О.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___«__»______20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»________202__ г.

Зав. кафедрой ____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___«__»______20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»________202__ г.

Зав. кафедрой ____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___«__»______20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»________202__ г.

Зав. кафедрой ____

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

1.1 Цель 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.

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 основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ОПК – 10	Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК – 10.1 использует средства криптографической защиты информации в автоматизированных системах	***Знать:*** - механизмы решения типовых задач по криптографической защите информации; - полный перечень данных, нужных при проектировании подсистем и средств обеспечения криптографической безопасности информации; - принципы работы программных, программно-аппаратных

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			криптографических средств и технических средств зашиты информации; - возможные действия противника, направленные на нарушение работы криптографических средств защиты информации. ***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. ***Владеть (****или* ***Иметь опыт деятельности):*** **-** 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;
		ОПК – 10.2. решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических про-	***Знать:*** - принципы построения алгоритмов цифровой подписи на основе асимметричных систем шифрования; - наиболее уязвимые для атак противника элементы компьютерных систем; - методы анализа и синтеза криптоалгоритмов. ***Уметь:*** - строить и изучать ма-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		токолов	тематические 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. ***Владеть (****или* ***Иметь опыт деятельности):*** - основными методами криптоанализа для наилучшего понимания способов построения доказуемо стойких криптографических систем.
		ОПК – 10.3 рассчитывает сложность типовых криптографических алгоритмов	***Знать:*** - 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; - принципы построения доказуемо стойких криптографических систем. ***Уметь:*** - разрабатывать алгоритмы применения криптографических программных средств системного, прикладного и специального назначения; - анализировать возможные уязвимости криптографических систем защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками про-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			ектирования 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.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Методы и средства криптографической защиты информации» входит в обязательную часть блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная безопасность телекоммуникационных систем специализация «Управление безопасностью телекоммуникационных сетей и систем». Дисциплина изучается на 3 курсе в 5 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 3 зачетные единицы (з.е.), 108 академических часов.

Таблица 3 - Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54.1
в том числе:	
лекции	18
лабораторные занятия	36
практические занятия	0

Виды учебной работы	Всего, часов
Самостоятельная работа обучающихся (всего)	53.9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всегоАттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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 основы систем 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-1-3 МУ-1,12	С, КО 2	ОПК-10.1
2	Классификация криптоалгоритмов.	2	2	2	О-1,2 Д-1-3 МУ-2	С, КО 4	ОПК-10.1
3	Потоковые шифраторы.	2	3	3	О-1,2 Д-3,5 МУ-3,14	С, КО 6	ОПК–10.2
4	Блочные криптоалгоритмы.	2	4	4	О-1,2 Д-3,4 МУ-4,15	С, КО 8	ОПК-10.2 ОПК-10.3

5	Ассиметричные криптоалгоритмы.	2	5	5	О-2,3 Д-4,5 МУ-5,16	С, КО 10	ОПК-10.2
6	Алгоритмы обмена ключами.	2	6	6	О-1,2 Д-1-3 МУ-6,17	С, КО 12	ОПК-10.2 ОПК-10.3
7	Применение программных систем шифрования.	2	7	7	О-2 Д-5 МУ-7-9,18	С, КО 14	ОПК-10.1 ОПК-10.2 ОПК-10.3
8	Стеганография.	2	8	8	О-1,2 Д-3 МУ-13	С, КО 16	ОПК-10.1
9	Криптоанализ и криптостойкость.	2	9	9	О-1,2 Д-1,2,4 МУ-11,19	С, КО 18	ОПК-10.3

С – собеседование, Т – тест, Р – реферат, КО – контрольный опрос.

4.2 Лабораторные 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	4
2	Программная реализация модели потокового шифратора	4
3	Построение и анализ аддитивных двоичных шифров	4
4	Построение и анализ блочных алгоритмов шифрования	4
5	Алгоритмы цифровой подписи	4
6	Алгоритмы обмена ключами. Разделение секрета.	4
7	Применение программных криптосистем шифрования. Изучение программного продукта Kremlin.Изучение программного продукта FoxSecret. Изучение программного продукта PGP	4
8	Стеганографическое закрытие данных. Изучение программных продуктов masker и s-tools	4
9	Основные методы криптоанализа. Криптоанализ методом вероятных слов	4
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельнаяработа студентов

№	Наименование раздела (темы) дисциплины	Срок вы-	Время, затрачива-

раздела (темы)		полнения	емое на выполнение СРС, час
1	2	3	4
1.	Введение в криптологию.	2 неделя	6
2.	Классификация криптоалгоритмов.	4 неделя	6
3.	Потоковые шифраторы.	6 неделя	6
4.	Блочные криптоалгоритмы.	8 неделя	6
5.	Ассиметричные криптоалгоритмы.	10 неделя	6
6.	Алгоритмы обмена ключами.	12 неделя	6
7.	Применение программных систем шифрования.	14 неделя	6
8.	Стеганография.	16 неделя	6
9.	Криптоанализ и криптостойкость.	18 неделя	5,9
Итого			53,9

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 студентов;

– тем рефератов;

– вопросов к зачету;

–методических указаний к выполнению лабораторных 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. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе лабораторных практикоориентированных заданий.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	2	3	4
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
Итого:			8

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества.

Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся. Реализация воспитательного потенциала дисциплины подразумевает:

- целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых, их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

- применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций);

- личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры. Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды.

Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули)и практики, при изучении/ прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК – 10.1 использует средства криптографической защиты информации в автоматизированных системах	Методы и средства криптографической защиты информации		Производственная эксплуатационная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ОПК – 10.2 решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и крипто-	Методы и средства криптографической защиты информации		Подготовка к процедуре защиты и защита выпускной квалификационной работы

графических протоколов		
ОПК – 10.3 рассчитывает сложность типовых криптографических алгоритмов	Методы и средства криптографической защиты информации Учебная практика (учебно-лабораторный практикум)	Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ОПК-10 основной	ОПК – 10.1 использует средства криптографической защиты информации в автоматизированных системах	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, при-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				кладного и специального назначения, программирования для решения поставленных профессиональных задач
	ОПК – 10.2 решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов	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 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 ре-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				шения поставленных профессиональных задач
	ОПК – 10.3 рассчитывает сложность типовых криптографических алгоритмов	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

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				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 основной профессиональной образовательной программы

Таблица 7.3 - Паспорт комплекта оценочных средств для текущего контроля-успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Введение в криптологию	ОПК-10.1	Лекция, СРС, лабораторное занятие	собеседование	1-3	Согласно табл.7.2
				контрольные вопросы к лб. №1	1-6	
2	Классификация криптоалгоритмов	ОПК-10.1	Лекция, СРС, лабораторное занятие	собеседование	4-7	Согласно табл.7.2
				контрольные вопросы к лб. №2	1-4	
3	Потоковые	ОПК-10.2	Лекция,	собеседо-	8-12	Согласно табл.7.2

	шифраторы		СРС, лабораторное занятие	вание		
				контрольные вопросы к лб. №3	1-6	
4	Блочные криптоалгоритмы	ОПК-10.2 ОПК-10.3	Лекция, СРС, лабораторное занятие	собеседование	13-17	Согласно табл.7.2
				контрольные вопросы к лб. №4	1-10	
5	Ассиметричные криптоалгоритмы	ОПК-10.2	Лекция, СРС, лабораторное занятие	собеседование	18-22	Согласно табл.7.2
				контрольные вопросы к лб. №5	1-5	
6	Алгоритмы обмена ключами	ОПК-10.2 ОПК-10.3	Лекция, СРС, лабораторное занятие	собеседование	23-26	Согласно табл.7.2
				контрольные вопросы к лб. №6	1-7	
7	Применение программных систем шифрования	ОПК-10.1 ОПК-10.2 ОПК-10.3	Лекция, СРС, лабораторное занятие	собеседование	27-31	Согласно табл.7.2
				контрольные вопросы к лб. №7	1-6	
8	Стеганография	ОПК-10.1	Лекция, СРС, лабораторное занятие	собеседование	32-39	Согласно табл.7.2
				контрольные вопросы к лб. №8	1-6	
9	Криптоанализ и криптостойкость	ОПК-10.3	Лекция, СРС, лабораторное занятие	собеседование	40-45	Согласно табл.7.2
				контрольные вопросы к лб. №9	1-5	

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для 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 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?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являют-

ся многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Для частотного анализа необходимо сопоставить _____ появления символов шифра с вероятностями появления букв используемого алфавита.

Задание в открытой форме:

Система криптографии и криптоанализа образуют новую науку:

- криптология;
- общая криптография;
- статистика;
- шифрование.

Задание на установление правильной последовательности:

Процесс стеганографии:

1) Выбор информационного файла;
2) Кодирование файла;
3) Отправление сокрытого сообщения по электронной почте и его декодирование;
4) Выбор стеганографической программы;
5) Выбор файла-контейнера.

Задание на установление соответствия:

1) Криптосистема;
2) Криптоанализ;
3) Криптография

А) раздел прикладной математики, изучающий модели, методы, алгоритмы,

программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст;

Б) система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации;

В) раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования.

Компетентностно-ориентированная задача:

Методом моноалфавитной подстановки дешифровать криптограмму: КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАС БДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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, указанные в списке литературы.

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Выполнение лабораторной работы «Шифрование и анализ метода многопетлевойполиал-	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
фавитной подстановки»				
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	8		24	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме –2балла,

– задание в открытой форме – 2 балла,

– задание на установление правильной последовательности – 2 балла,
– задание на установление соответствия – 2 балла,
– решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

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. 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.

3. 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.

4. 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.

5. 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.

5.3 Перечень 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. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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. 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.

12. 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.

13. 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.

14. 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. - Биб-

лиогр.: с. 20. - Б. ц.

15. 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.

16. 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.

17. 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. 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.

19. 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.

20. 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.

21. 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.

22. 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.

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 «Методы и средства криптографической защиты информации» являются лекции и лабораторные 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.

Лабораторному 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 лабораторным работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Методы и средства криптографической 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 лекциях, отработку студентами пропущенных лекций, 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 закрепления 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 освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность жизнедеятельности» с целью освоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Методы и средства криптографической 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 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций;тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а такжесурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменноотвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			