Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таныгин Максим Олегович
Должность: и.о. декана факультета фундаментальной информатики и информационных технологий
Дата подписания: 06.10.2022 12:34:24
Уникальный программный ключ:
65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе дисциплины «Основы криптографии»

Цель преподавания дисциплины

Формирование у студентов основных представлений об одной из наиболее важных областей современной прикладной математики – криптографии, а также создание предпосылок для использования полученных знаний в дальнейшем образовательном процессе на старших курсах.

Задачи изучения дисциплины

- ознакомить студентов с методами теории информации, применяемыми в криптографии;
- обучить студентов универсальным методами шифрования и условиями их применения;
-научить студентов дешифровать криптограммы, зашифрованные простейшими классическими шифрами.

Компетенции, формируемые в результате освоения дисциплины

Способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК–2)

Способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации (ОПК–4)способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК–1)

Разделы дисциплины

История криптографии. Первые криптосистемы. Криптография как наука. Основные понятия и определения криптографии. Неопределенность сообщения. Совершенные и несовершенные шифры .Источники дискретных сообщений и их вероятностные модели. Шенноновские модели криптосистем. Классификация систем шифрования. Основы симметричного шифрования. Криптостойкость. Теоретико-информационные оценки стойкости симметричных криптосистем. Математические основы шифрования с открытым ключом.

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

Основы криптографии

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

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

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

Курск 2017

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

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения студентов по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» на заседании кафедры информационной безопасности.
«1» февраля 2017г. Протокол № 9

И.о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Ефремов М.А.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

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

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 5 «30» 01 2018г. на заседании кафедры ИБ, протокол № 12 от 29.06.18г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № __ «__» _____ 20___г. на заседании кафедры информационной безопасности 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 *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_1_ от «_31_» _08_ 20_20_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_28_» _06_ 20_21_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_30_» _06_ 20_22_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 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 *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1 Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы.

1.1 Цель преподавания дисциплины

Формирование у студентов основных представлений об одной из наиболее важных областей современной прикладной математики – криптографии, а также создание предпосылок для использования полученных знаний в дальнейшем образовательном процессе на старших курсах.

1.2 Задачи изучения дисциплины.

- ознакомить студентов с методами теории информации, применяемыми в криптографии;
- обучить студентов универсальным методами шифрования и условиями их применения;
- научить студентов дешифровать криптограммы зашифрованные простейшими классическими шифрами.

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

Обучающиеся должны **знать:**

- историю развития криптографии как науки;
- основные исторические сведения о системах и способах составления шифрованных писем;
- основные понятия и определения криптографии;
- основы теории информации;
- меру неопределенности сообщения;
- условие абсолютной стойкости шифров;
- принцип построения надежных шифров;
- классификацию основных систем шифрования;
- основы симметричного шифрования;
- шенноновские модели криптосистем;
- источники дискретных сообщений и их вероятностные модели;
- теоретико-информационные оценки стойкости криптографических систем;
- математические основы шифрования с открытым ключом.

уметь:

- применять полученные знания к исследованию простейших систем шифрования;

- 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;

- анализировать возможные уязвимости криптографических систем защиты информации.

владеть:

- навыками построения моделей простейших систем шифрования;

- навыками подбора наилучшего метода решения поставленной задачи;

- навыками дешифрования криптограмм зашифрованных с использованием простейших систем шифрования;

- основными методами криптоанализа для наилучшего понимания способов построения 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 понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации (ОПК–4)

способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК–1)

2 Указание места дисциплины в структуре образовательной программы

Дисциплина «Основы криптографии» (Б1.В.ДВ.3.1) относится к вариативной части, блоку дисциплин по выбору, 3 курс, 6 семестр изучения.

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 часов.

Таблица 3 – Объём дисциплины

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	72,1
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	0
экзамен	не предусмотрен
зачет	0,1
курсовая работа (проект)	не предусмотрена
расчетно-графическая (контрольная) работа	не предусмотрена
Аудиторная работа (всего):	72
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	0
Самостоятельная работа обучающихся (всего)	35,9
Контроль/экзамен (подготовка к экзамену)	0

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	История криптографии. Первые криптосистемы.	Задачи и программа курса. История криптографии. Первые криптосистемы. Исторические сведения о системах и способах составления шифрованных писем. Сциталла. Шифр Цезаря. Квадрат Полибия.

2	Криптография как наука. Основные понятия и определения криптографии.	Понятие криптографии как науки. Основные понятия, определения и термины используемые в криптографии. Шифрование. Расшифровка. Шифротекст. Ключ. Криптосистема. Дешифрование сообщений. Криптоанализ. Криптостойкость.
3	Неопределенность сообщения. Совершенные и несовершенные шифры.	Мера неопределенности сообщения. Априорная неопределенность Апостериорная условная неопределенность. Количество информации об исходном тексте. Условие абсолютной стойкости шифров. Принцип Керкгоффса построения надежных шифров. Функция ненадежности ключа. Расстояние единственности шифра.
4	Источники дискретных сообщений и их вероятностные модели.	Источники дискретных сообщений и их вероятностные модели. Функционал энтропии и его свойства. Определение условной энтропии. Определение удельной энтропии стационарной символьной последовательности. Удельная энтропия для произвольного источника дискретных сообщений.
5	Шенноновские модели криптосистем.	Количество информации по Шеннону и его свойства. Собственная информация о сообщении. Шенноновские модели криптосистем. Подстановка символов алфавита.
6	Классификация систем шифрования.	Классификация систем шифрования. Симметричное и асимметричное шифрование, достоинства и недостатки систем шифрования относительно друг друга.
7	Основы симметричного шифрования.	Основы симметричного шифрования. Блочное шифрование. Режимы блочного шифрования. Поточное шифрование.
8	Криптостойкость. Теоретико-информационные оценки стойкости симметричных криптосистем.	Понятие стойкости шифров. Криптостойкость. Доказуемая стойкость. Совершенные и несовершенные шифры. Теоретико-информационные оценки стойкости симметричных криптосистем.
9	Математические основы шифрования с открытым ключом.	Математические основы шифрования с открытым ключом. Открытый ключ. Секретный ключ. Системы распределения ключей. Сложность алгоритмов. Достоинства и недостатки систем с открытым ключом.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды учебной деятельности (в часах)			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ практ.			
1	История криптографии. Первые криптосистемы.	4	1		О-1,2 Д-1-4,10 МУ-1	С, КО 2	ОПК-2 ОПК-4

2	Криптография как наука. Основные понятия и определения криптографии.	4	2		О-1,2 Д-4, 8, 10 МУ-2	С, КО 4	ОПК-4 ПК-1
3	Неопределенность сообщения. Совершенные и несовершенные шифры.	4	3		О-1,2 Д-8,10 МУ-3	С, КО 6	ПК-1
4	Источники дискретных сообщений и их вероятностные модели.	4	4		О-1,2 Д-4,6-8 МУ-4	С, КО 8	ОПК-2, ОПК-4
5	Шенноновские модели криптосистем.	4	5		О-1,2 Д-4,8 МУ-5	С, КО 10	ПК-1
6	Классификация систем шифрования.	4	6		О-2 Д-8,10 МУ-6	С, КО 12	ПК-1
7	Основы симметричного шифрования.	4	7		О-1,2 Д-8,10 МУ-7	С, КО 14	ОПК-2, ПК-1
8	Криптостойкость. Теоретико-информационные оценки стойкости симметричных криптосистем.	4	8		О-1,2 Д-2,4,6 МУ-8	С, КО 16	ПК-1
9	Математические основы шифрования с открытым ключом.	4	9		О-1,2 Д-3-8 МУ-9	С, КО 18	ОПК-4 ПК-1

С – собеседование, 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	Шифр «Литорея»	4
2	Шифрование методом прямой замены	4
3	Криптоанализ шифра моноалфавитной подстановки	4
4	Шифрование методом полиалфавитной замены	4
5	Криптоанализ шифра полиалфавитной подстановки	4
6	Шифрование методом перестановок	4
7	Криптоанализ шифра табличной перестановки	4
8	Шифрование аналитическими методами	4
9	Шифрование с открытым ключом	4
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	История криптографии. Первые криптосистемы.	2 неделя	3,9
2.	Криптография как наука. Основные понятия и определения криптографии.	4 неделя	4
3.	Неопределенность сообщения. Совершенные и несовершенные шифры.	6 неделя	4
4.	Источники дискретных сообщений и их вероятностные модели.	8 неделя	4
5.	Шенноновские модели криптосистем.	10 неделя	4
6.	Классификация систем шифрования.	12 неделя	4
7.	Основы симметричного шифрования.	14 неделя	4
8.	Криптостойкость. Теоретико-информационные оценки стойкости симметричных криптосистем.	16 неделя	4
9.	Математические основы шифрования с открытым ключом.	18 неделя	4
Итого:			35,9

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 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. 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 профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение практикоориентированных заданий в ходе лабораторных занятий.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение лабораторной работы «Шифрование методом простой замены»	Выполнение студентом интерактивных заданий по реализации шифрования методом простой замены	2
2.	Выполнение лабораторной работы «Шифрование методом полиалфавитной замены»	Выполнение студентом интерактивных заданий по реализации шифрования методом полиалфавитной замены	4
3.	Выполнение лабораторной работы «Шифрование методом перестановок»	Выполнение студентом интерактивных заданий по реализации шифрования методом перестановок	4
4.	Выполнение лабораторной работы «Шифрование аналитическими методами (методами матричной алгебры)»	Анализ и исследование студентами аналитических методов шифрования	4
5.	Выполнение лабораторной работы «Шифрование с открытым ключом»	Выполнение студентом интерактивных заданий по реализации шифрования с открытым ключом	4

	Итого	18

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, 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 (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), 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 образовательной программы

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	Математический анализ Алгебра и геометрия Теория вероятностей и математическая статистика Дискретная математика Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности	Теория информации и кодирования Математические методы теории сигналов и систем Квантовая и оптическая электроника Моделирование систем и сетей телекоммуникаций Основы криптографии Основы теории чисел Учебно-лабораторный практикум	Криптографические методы защиты информации Теория массового обслуживания Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ОПК-4 - Способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации	Информатика Языки программирования	Информационные технологии Основы криптографии Основы теории чисел	Ознакомительная практика Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

ПК–1 - Способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем	Русский язык и культура речи Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Учебно-лабораторный практикум	Информационная безопасность телекоммуникационных систем Основы информационной безопасности Основы криптографии Основы теории чисел Научно-исследовательская работа	Планирование и управление информационной безопасностью Основы многоканальных систем передачи Системы и сети радиосвязи Системы и сети мобильной связи Ознакомительная практика Практика по получению профессиональных умений и опыта профессиональной деятельности Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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

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/ основной	*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: -основы теории информации построения криптографических систем. Уметь: -использовать математический аппарат для построения простейших криптографических систем Владеть:	Знать: - основы теории информации и классификацию криптографических систем зашиты информации Уметь: - использовать математический аппарат и анализ полученных данных для построения криптографических	Знать: -принципы работы математических, программных, программно – аппаратных средств и технических средств криптографической зашиты информации телекоммуникационных систем Уметь: -применять все полученные знания при решении разного

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	-навыками сбора необходимой информации для построения моделей криптографической защиты телекоммуникационных систем.	систем Владеть: -навыками подбора наилучшего математического метода решения задачи по криптографической защите телекоммуникационных систем.	рода задач по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации Владеть: -навыками сбора и анализа информации для решения возникающих проблем профессионального характера по криптографической защите телекоммуникационных систем.
ОПК-4/ основной	*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: принципы развития современного общества Уметь: находить рациональные достижения информационных технологий Владеть: способностью понимать значение информации в развитии современного общества	Знать: принципы развития и роль криптографии в современном обществе Уметь: эффективно применять достижения информационных технологий для построения криптографических систем Владеть: способностью применять достижения информационных технологий для поиска и обработки информации по криптографической защите	Знать: принципы развитии современного общества Уметь: находить рациональные и наиболее эффективно применять достижения информационных технологий Владеть: способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации с целью

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
			телекоммуникационных систем	построения защищенных криптографических систем
ПК-1/ основной	*1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД* *2. Качество освоенных обучающимся знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	Знать: основы анализа научно-технической информации Уметь: анализировать научно-техническую информацию для решения возникающих задач Владеть: навыками анализа научно-технической информации	Знать: анализ научно-технической информации, нормативных и методических материалов Уметь: анализировать научно-техническую информацию для решения возникающих задач информационной безопасности телекоммуникационных систем Владеть: навыками анализа научно-технической информации при решении задач информационной безопасности телекоммуникационных систем	Знать: анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем Уметь: анализировать научно-техническую информацию для решения возникающих задач информационной безопасности телекоммуникационных систем Владеть: навыками осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем

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 для текущего контроля

№	Раздел (тема)	Код	Технология	Оценочные	Описание шкал

п/п	дисциплины	контролируемой компетенции (или её части)	формирования	средства		оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	История криптографии. Первые криптосистемы.	ОПК-2 ОПК-4	Лекция, СРС, лабораторное занятие	собеседование	1-9	Согласно табл.7.2
				контрольные вопросы к лб. №1	1-5	
2	Криптография как наука. Основные понятия и определения криптографии.	ОПК-4, ПК-1	Лекция, СРС, лабораторное занятие	собеседование	1-10	Согласно табл.7.2
				контрольные вопросы к лб. №2	1-4	
3	Неопределенность сообщения. Совершенные и несовершенные шифры.	ПК-1	Лекция, СРС, лабораторное занятие	собеседование	1-8	Согласно табл.7.2
				контрольные вопросы к лб. №3	1-6	
4	Источники дискретных сообщений и их вероятностные модели.	ОПК-2 ОПК-4	Лекция, СРС, лабораторное занятие	собеседование	1-5	Согласно табл.7.2
				контрольные вопросы к лб. №4	1-4	
5	Шенноновские модели криптосистем.	ПК-1	Лекция, СРС, лабораторное занятие	собеседование	1-5	Согласно табл.7.2
				контрольные вопросы к лб. №5	1-5	
6	Классификация систем шифрования.	ПК-1	Лекция, СРС, лабораторное занятие	собеседование	1-5	Согласно табл.7.2
				контрольные вопросы к лб. №6	1-7	

7	Основы симметричного шифрования.	ОПК-2 ПК-1	Лекция, СРС, лабораторное занятие	собеседование	1-7	Согласно табл.7.2
				контрольные вопросы к пр. №7	1-5	
8	Криптостойкость. Теоретико-информационные оценки стойкости симметричных криптосистем.	ПК-1	Лекция, СРС, лабораторное занятие	собеседование	1-6	Согласно табл.7.2
				контрольные вопросы к лб. №8	1-6	
9	Математические основы шифрования с открытым ключом.	ОПК-4 ПК-1	Лекция, СРС, лабораторное занятие	собеседование	1-6	Согласно табл.7.2
				контрольные вопросы к лб. №9	1-5	

Примеры типовых контрольных заданий для текущего контроля

Вопросы собеседования по разделу (теме) 1. «История криптографии. Первые криптосистемы»

1. Назовите основные этапы истории развития криптографии.
2. Исторические сведения о системах и способах составления шифрованных писем.
3. Как были устроены первые криптосистемы.
4. Что такое сцитала.
5. Как устроен шифр Цезаря.
6. Для чего служит квадрат Полибия.
7. Что такое открытый и закрытый текст.
8. Принципы организации криптографических систем.
9. Для чего используется шифрование и дешифровка.

Контрольные вопросы к лабораторной работе по разделу (теме) 4. «Шифрование методом полиалфавитной замены»

1. На чем основан метод полиалфавитной замены?
2. Что такое матрица Вижинера?
3. Как строится матрица Вижинера?

4. Как осуществляется шифрование сообщения данным методом?
5. Как осуществляется расшифрование сообщения?

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

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

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

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы «Шифр «Литорея»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение работы «Шифрование методом простой замены»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Криптоанализ шифра моноалфавитной подстановки»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Шифрование методом полиалфавитной замены»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Криптоанализ шифра полиалфавитной подстановки»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Защита работы «Шифрование методом перестановок»	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 «Шифрование аналитическими методами»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»

Выполнение работы по исследованию шифрования с открытым ключом	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
СРС	6		12	
Итого:	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого:	24		100	

При итоговом контроле (зачёт) в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (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. Применко, Э. А. Алгебраические основы криптографии [Текст] : учебное пособие / Э. А. Применко. - Москва : Либроком, 2013. - 288 с. - (Основы защиты информации). - ISBN 978-5-382-014 55-5 : 470.00 р.

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

8.2 Дополнительная учебная литература

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

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

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

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

5. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / М. А. Иванов, И. Чугунков. - Москва : МИФИ, 2012. - 400 с. - ISBN 978-5-7262-1676-8 : Б. ц.

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

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

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

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

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

8.3 Перечень методических указаний

1. Ефремов, М. А. Шифр «Литорея» [Электронный ресурс] : методические указания п+о выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (351 КБ). - Курск : ЮЗГУ, 2016. - 13 с. : ил., табл. - Библиогр.: с. 13. - Б. ц.

2. Ефремов, М. А. Шифрование методом прямой замены [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (240 КБ). - Курск : ЮЗГУ, 2016. - 14 с. : ил. - Библиогр.: с. 14. - Б. ц.

3. Ефремов, М. А. 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.

4. Ефремов, М. А. Шифрование методом полиалфавитной замены [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (294 КБ). - Курск : ЮЗГУ, 2016. - 9 с. : ил., табл. - Библиогр.: с. 9. - Б. ц.

5. Ефремов, М. А. 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.

6. Ефремов, М. А. Шифрование методом перестановок [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (223 КБ). - Курск : ЮЗГУ, 2016. - 9 с. : ил., табл. - Библиогр.: с. 9. - Б. ц.

7. Ефремов, М. А. 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.

8. Ефремов, М. А. Шифрование аналитическими методами [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (333 КБ). - Курск : ЮЗГУ, 2016. - 11 с. - Б. ц.

9. Ефремов, М. А. Шифрование с открытым ключом [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (315 КБ). - Курск : ЮЗГУ, 2016. - 14 с. : ил. - Библиогр.: с. 14. - 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. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/.
7. 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 «Основы криптографии» 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 готовить рефераты по отдельным темам дисциплины, выступать 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 «Основы криптографии»: 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, 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 «Основы криптографии» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Основы криптографии» - 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

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

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы. Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)

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 также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

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	заменен ных	аннулир ованных	новых			
1	2,6,9,17				4	30.08.18	Протокол 12 от 29.06.2018