Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ
Декан, председатель совета
факультета КТВТиЭ
_____ Ш. А. Юсуфов
«18» 10 2018 г.

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического совета
ДГТУ
_____ Н. С. Суракатов
«24» 10 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина С1.Б.25 Криптографические метод защиты информации
наименование дисциплины по ОПОП и код по ФГОС

Направление 10.03.01 – Информационная безопасность

Профиль Безопасность автоматизированных систем

Факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

Кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника бакалавр
бакалавр, специалист

Форма обучения очная, курс 4 семестр 7

Всего трудоемкость в зачетных единицах (часах) 6 ЗЕТ (216 ч.)

лекции 34 (час); экзамен 7 (1 ЗЕТ – 36 ч.) (семестр)

практические (семинарские) занятия ___ (час); зачет - (семестр)

лабораторные занятия 51 (час); самостоятельная работа 95 (час);

курсовой проект (работа, РГР) 7 (семестр).

Зав. кафедрой _____ Г.И. Качаева
подпись

Начальник УО _____ О.В. Магомаева
подпись

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем».

Программа одобрена на заседании выпускающей кафедры ИБ протокол № 2 от 15.10.2018г.

Зав. выпускающей кафедрой по данному направлению _____ **Г.И. Качаева**

ОДОБРЕНО
Методической комиссией по
укрупненным группам специальностей и
направлению подготовки
10.00.00- «Информационная безопасность»

Председатель МК

_____
подпись И.О. Фамилия

«15» 10 2018г.

АВТОР ПРОГРАММЫ

Качаева Г.И. к.э.н., ст.препод. кафедры ИБ
И.О. Фамилия, уч. степень, уч. звание

_____
подпись

1. Цели освоения дисциплины «Криптографические методы защиты информации»

Целью дисциплины «Криптографические методы защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

Задачами дисциплины являются:

- дать представление о криптографических методах защиты информации;
- изучить математические основы современной криптографии;
- изучить современные стандарты симметричного шифрования;
- изучить основные криптографические алгоритмы с открытым ключом;
- изучить криптографические функции хеширования;
- сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

2.Место дисциплины в структуре ООП специалитета

Дисциплина «Криптографические методы защиты информации» относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Основы информационной безопасности.

Последующими дисциплинами являются: Управление информационной безопасностью, Защита программ и данных, Обеспечение ИБ в интеллектуальных системах.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины «Криптографические методы защиты информации»

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

В результате изучения дисциплины обучающийся должен:

знать основные виды криптографических методов и алгоритмов; принципы построения криптографических алгоритмов и предъявляемые к ним требования; математические основы современной криптографии; криптографические стандарты и их использование в информационных системах; простейшие методы криптоанализа.

уметь эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять простейшие методы криптоанализа.

владеть криптографическими методами и средствами защиты информации; простейшими методами криптоанализа; методами оценки стойкости криптографических алгоритмов.

4. Структура и содержание дисциплины «Криптографические методы защиты информации»

Общая трудоемкость дисциплины составляет 6 зачетных единиц – 216 часов, в том числе: лекционных -34 часа, лабораторных - 51 часа, СРС – 95 часов, форма отчетности экзамен в 7 семестре, курсовая работа в 7 семестре.

4.1.Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего* контроля успеваемости (по срокам текущих аттестаций в семестре) Форма промежуточной аттестации (по семестрам)
				ЛК	ПЗ	ЛР	СР	
1.	Лекция №1. Тема: «Нападения и угрозы в компьютерных системах». Ретроспективный анализ развития подходов к разработке средств криптографической защиты информации. Понятия «информация», ее «источники и носители». Информация общедоступная и ограниченного доступа. Категории ценности информации. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; приводится классификация атак. Модели сетевой безопасности и безопасности информационной системы. Информация как объект защиты. Основные задачи обеспечения криптографической защиты информации. Основные методы и средства защиты информации в информационных системах. Анализ угроз информационной безопасности: классификация угроз.	8	1	2		2	6	Входная контрольная
2.	Лекция №2. Тема: «Введение в криптологию. Основные цели и задачи криптографии». Возникновение и развитие криптографии и криптоанализа. Общие методы криптографии и криптоанализа. Виды конфиденциальной информации и их защита. Способы и средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Взлом криптоалгоритмов. Виды атак на криптографические протоколы. Причины нарушения безопасности информации при ее обработке СКЗИ.		2	2		2	6	
3.	Лекция № 3. Тема «Историческая криптография» Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.		3	2		2	6	
4.	Лекция № 4. Тема: «Математические основы криптографии» Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа. Эллиптические кривые. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой		4	2		4	6	

	степени с одним неизвестным. Китайская теорема об остатках.						
5.	Лекция № 5. Тема «Симметричное шифрование. Симметричные криптоалгоритмы». Основные понятия, относящиеся к алгоритмам симметричного шифрования. Ключ шифрования. Типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа. Линейный и дифференциальный криптоанализ. Алгоритмы DES и тройной DES.	5	2		4	6	АКР №1
6.	Лекция № 6. Тема: «Симметричное шифрование. Симметричные криптоалгоритмы». Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения. Способы создания псевдослучайных чисел. Стандарт алгоритма симметричного шифрования – AES. Критерии выбора стандарта. Атаки на алгоритмы. Понятие резерва безопасности. Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура раунда алгоритмов Rijndael и RC6.	6	2		4	6	
7.	Лекция № 7. Тема: «Симметричное шифрование. Симметричные криптоалгоритмы». Блочные шифры. DES-алгоритм: история создания, строение, режимы шифрования, применение, характеристики аппаратных и программных реализаций. 3-DES.	7	2		2	6	
8.	Лекция № 8. Тема: «Симметричное шифрование. Симметричные криптоалгоритмы». Алгоритм шифрования ГОСТ-28147. Алгоритмы шифрования FEAL-N и IDEA. Использование для аутентификации открытых и шифрованных сообщений режимов шифрования, распространяющих в шифртексте искажения открытого текста. Потоковые шифры. Структура. Гаммирование. Основные критерии качества. Синхронные (СПШ) и самосинхронизирующиеся (ССПШ) потоковые шифры. Виды СПШ. Атака на СПШ с помощью вставки символа.	8	2		2	4	
9.	Лекция № 9. Тема: «Алгоритмические проблемы теории чисел». Измерение сложности теоретико-числовых алгоритмов. Полиномиальные алгоритмы. Алгоритм вычисления $a^d \bmod m$. Алгоритм Евклида. Алгоритм решения уравнения $ax + by = 1$. Простые и составные числа. Построение больших простых чисел. Разложение составных чисел на множители. Дискретное логарифмирование. Алгоритмически неразрешимые задачи в криптографии.	9	2		4	6	
10.	Лекция № 10. Тема: «Криптография с открытым ключом». Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина. Алгоритмы работы с большими числами.	10	2		4	6	АКР №2
11.	Лекция № 11. Тема: «Криптография с открытым ключом». Предпосылки появления криптографии с открытым ключом. Схемы шифрования с открытым ключом.	11	2		2	4	

	Функция Эйлера Основные понятия, относящиеся к криптографии с открытым ключом, а также способы их использования. Обмен ключами. Реализация алгоритма RSA.							
12.	Лекция № 12. Тема: «Криптография с открытым ключом». Процедуры шифрования и расшифрования в шифрсистеме Эль-Гамаля. Процедура генерации ключей шифрсистемы Эль-Гамаля. Работа в режиме подписи. Криптостойкость алгоритма. Преимущества и недостатки систем асимметричного шифрования. Взлом криптосистем с открытым ключом.		12	2		2	6	
13.	Лекция № 13. Тема: «Идентификация и аутентификация». Функции хэширования. Классификация. Функции хэширования без ключа (MDC) и с ключом (MAC). Принципы построения. Функции хэширования Ривеста: MD2, MD4, MD5. Американский стандарт функции хэширования (SHS) и его изменения. Российский стандарт функции хэширования (ГОСТ Р 34.11-94).		13	2		4	4	
14.	Лекция № 14. Тема: «Идентификация и аутентификация». Применение функции хэширования в схемах цифровой подписи и при построении криптосистем. Сильные хэш-функции SHA-1, SHA-2. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC. Контроль целостности данных. Идентификация и аутентификация. Использование для аутентификации открытых и шифрованных сообщений режимов шифрования, распространяющих в шифртексте искажения открытого текста. Шифрование, создание и проверка цифровой подписи. Использование открытых ключей. Схемы подписи RSA и Рабина. Схема цифровой подписи Эль Гамаля и ее модификации.		14	2		2	6	
15.	Лекция № 15. Тема «Хеширование» Криптографические хеш-функции. ГОСТ Р 34.11-2012. DES. AES.		15	2		4	6	АКР №3
16.	Лекция № 16. Тема: «Стойкость шифра». Определение теоретической стойкости алгоритма. Шифр Вернама для 8-битных символов. Побитный «одноразовый блокнот». Виды атак. Понятие о и практической стойкости шифра. Защита от угроз нарушения целостности информации на уровне содержания. Временная стойкость шифра.		16	2		4	6	
17.	Лекция № 17. Тема: «Электронная подпись» Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10- 2012. DSS. Инфраструктура открытого ключа.		17	2		3	5	
	Итого за 7 семестр			**34**		**51**	**95**	**Экзамен 1 ЗЕТ =36 часов**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	2	3	4	5
1	№1	Нападения и угрозы в компьютерных системах.	2	№№ 1-14
2	№2	Введение в криптологию. Основные цели и задачи криптографии.	2	№№ 1-14
3	№3	Историческая криптография.	2	№№ 1-14
4	№4	Математические основы криптографии.	4	№№ 1-14
5	№5	Симметричное шифрование. Симметричные криптоалгоритмы.	4	№№ 1-14
6	№ 6	Симметричное шифрование. Симметричные криптоалгоритмы.	4	№№ 1-14
7	№7	Симметричное шифрование. Симметричные криптоалгоритмы.	2	№№ 1-14
8	№8	Симметричное шифрование. Симметричные криптоалгоритмы.	2	№№ 1-14
9	№9	Алгоритмические проблемы теории чисел.	4	№№ 1-14
10	№10	Криптография с открытым ключом.	4	№№ 1-14
11	№11	Криптография с открытым ключом.	2	№№ 1-14
12	№12	Криптография с открытым ключом.	2	№№ 1-14
13	№13	Идентификация и аутентификация.	4	№№ 1-14
14	№14	Идентификация и аутентификация.	2	№№ 1-14
15	№15	Хеширование.	4	№№ 1-14
16	№16	Стойкость шифра.	4	№№ 1-14
17	№17	Электронная подпись.	3	№№ 1-14
Итого			51	

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля СРС
1	Нападения и угрозы в компьютерных системах.	6	№№ 1-14	Опрос, реферат, статья
2	Введение в криптологию. Основные цели и задачи криптографии.	6	№№ 1-14	Опрос, реферат, статья
3	Историческая криптография.	6	№№ 1-14	Опрос, реферат, статья
4	Математические основы	6	№№ 1-14	Опрос, реферат,

	криптографии.			статья
5	Симметричное шифрование. Симметричные криптоалгоритмы.	6	№№ 1-14	Опрос, реферат, статья
6	Симметричное шифрование. Симметричные криптоалгоритмы.	6	№№ 1-14	Опрос, реферат, статья
7	Симметричное шифрование. Симметричные криптоалгоритмы.	6	№№ 1-14	Опрос, реферат, статья
8	Симметричное шифрование. Симметричные криптоалгоритмы.	4	№№ 1-14	Опрос, реферат, статья
9	Алгоритмические проблемы теории чисел.	6	№№ 1-14	Опрос, реферат, статья
10	Криптография с открытым ключом.	6	№№ 1-14	Опрос, реферат, статья
11	Криптография с открытым ключом.	4	№№ 1-14	Опрос, реферат, статья
12	Криптография с открытым ключом.	6	№№ 1-14	Опрос, реферат, статья
13	Идентификация и аутентификация.	4	№№ 1-14	Опрос, реферат, статья
14	Идентификация и аутентификация.	6	№№ 1-14	Опрос, реферат, статья
15	Хеширование.	6	№№ 1-14	Опрос, реферат, статья
16	Стойкость шифра.	6	№№ 1-14	Опрос, реферат, статья
17	Электронная подпись.	5	№№ 1-14	Опрос, реферат, статья
	Итого:	**95**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров реализация компетентностного подхода предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий.

Аудиторная работа включает: лекции, практические занятия, мастер-классы, консультации.

В курсе лекций использованы наглядные, иллюстрированные материалы, обширная информация в табличной и графической формах, а также электронные ресурсы сети Интернет. Разработаны продвинутые лекции (с визуализацией) в формате презентаций, с использованием пакета прикладных программ MS Power Point.

Внеаудиторная работа призвана для формирования и развития профессиональных навыков обучающихся. Самостоятельная работа включает: выполнение домашних заданий, подготовка рефератов, участие в дискуссиях, работа в информационно-образовательной среде. В конце обучения проводится экзамен.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины «Криптографические методы защиты информации»

ФОНД ВОПРОСОВ (ЗАДАЧ) ДЛЯ КОНТРОЛЬНЫХ РАБОТ

Вопросы для входной контрольной работы

1. Формальное описание структуры информационной системы.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

Контрольные работы по проверке текущих знаний студентов

Аттестационная контрольная работа №1

1. Ретроспективный анализ развития подходов к разработке средств криптографической защиты информации.
2. Понятия «информация», ее «источники и носители».
3. Информация общедоступная и ограниченного доступа.
4. Категории ценности информации.
5. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; приводится классификация атак.
6. Модели сетевой безопасности и безопасности информационной системы. Информация как объект защиты.
7. Основные задачи обеспечения криптографической защиты информации.
8. Основные методы и средства защиты информации в информационных системах.
9. Анализ угроз информационной безопасности: классификация угроз.
10. Возникновение и развитие криптографии и криптоанализа.

11. Общие методы криптографии и криптоанализа.
12. Виды конфиденциальной информации и их защита.
13. Способы и средства криптографической защиты информации (СКЗИ).
14. Криптографические преобразования.
15. Шифрование и дешифрование информации. Взлом криптоалгоритмов.
16. Виды атак на криптографические протоколы.
17. Причины нарушения безопасности информации при ее обработке СКЗИ.
18. Математическая модель шифра.
19. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.
20. Алгебраические структуры. Группы. Циклические группы.
21. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа.
22. Эллиптические кривые.
23. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках.
24. Основные понятия, относящиеся к алгоритмам симметричного шифрования. Ключ шифрования.
25. Типы операций, используемые в алгоритмах симметричного шифрования.
26. Сеть Фейштеля. Основные понятия криптоанализа.
27. Линейный и дифференциальный криптоанализ.
28. Аалгоритмы DES и тройной DES.

Аттестационная контрольная работа №2

1. Предпосылки появления криптографии с открытым ключом.
2. Схемы шифрования с открытым ключом. Функция Эйлера.
3. Основные понятия, относящиеся к криптографии с открытым ключом, а также способы их использования. Обмен ключами.
4. Реализация алгоритма RSA.
5. Процедуры шифрования и расшифрования в шифрсистеме Эль-Гамаля. Процедура генерации ключей шифрсистемы Эль-Гамаля.
6. Работа в режиме подписи.
7. Криптостойкость алгоритма. Преимущества и недостатки систем асимметричного шифрования. Взлом криптосистем с открытым ключом.
8. Функции хэширования. Классификация.
9. Функции хэширования без ключа (MDC) и с ключом (MAC). Принципы построения.
10. Функции хэширования Ривеста: MD2, MD4, MD5.
11. Американский стандарт функции хэширования (SHS) и его изменения.
12. Российский стандарт функции хэширования (ГОСТ Р 34.11-94).
13. Применение функции хэширования в схемах цифровой подписи и при построении криптосистем.
14. Сильные хэш- функции SHA-1, SHA-2.
15. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.
16. Контроль целостности данных.
17. Идентификация и аутентификация. Использование для аутентификации открытых и шифрованных сообщений режимов шифрования, распространяющих в шифртексте искажения открытого текста.

18. Шифрование, создание и проверка цифровой подписи. Использование открытых ключей.
19. Схемы подписи RSA и Рабина. Схема цифровой подписи Эль Гамаля и ее модификации.
20. Криптографические хеш-функции. ГОСТ Р 34.11-2012.
21. DES. AES.

Аттестационная контрольная работа №3

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Принципы, используемые для повышения стойкости шифра?
11. Приведите схему и объясните принцип работы блочного шифра.
12. Дайте характеристику шифра DES.
13. Дайте характеристику шифра ГОСТ 28147-89.
14. Перечислите основные различия между DES и ГОСТ 28147-89.
15. Что такое – режим применения блочного шифра?
16. Чем отличается поточное и блочное шифрование.
17. Дайте характеристику шифра RC4.
18. Основные свойства криптографических хеш-функций.
19. Принципы работы хеш-функции.
20. Особенности построение хеш-функции на базе блочного шифра.
21. Опишите операцию приведения по модулю.
22. Какими свойствами обладает операция приведения по модулю?
23. Приведите определение простого числа.
24. Какие два числа называются взаимно простыми?
25. Определите понятие обратного значения по модулю.
26. Сформулируйте малую теорему Ферма.
27. Дайте определение функции Эйлера.
28. Сформулируйте теорему Эйлера.
29. Перечислите свойства простых чисел.
30. Чем отличается криптография с открытым ключом от симметричных шифров?
31. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
32. Опишите алгоритм Шамира.
33. Опишите алгоритм Эль-Гамаля.
34. .Опишите алгоритм RSA.

Перечень экзаменационных вопросов по дисциплине «Основы управления информационной безопасностью»

1. Алгебраические структуры. Свойства алгебраических структур. Группы, подгруппы.
2. Циклические группы.
3. Группы подстановок.
4. Кольца. Кольца классов вычетов.
5. Поля. Поля Галуа.
6. Эллиптические кривые над конечным полем.

7. Цели и задачи криптографии. Основные понятия.
8. Простейшие шифры: простой замены, перестановочный, аффинный.
9. Шифр Хилла.
10. Шифры гаммирования. Шифр Вернама.
11. ГОСТ Р 34.12-2015. Шифр «Магма».
12. ГОСТ Р 34.12-2015. Шифр «Кузнечик».
13. ГОСТ Р 34.13- 2015. Режимы гаммирования.
14. ГОСТ Р 34.13-2015. Режимы простой замены, режим выработки имитовставки.
15. Стандарт шифрования DES.
16. Стандарт шифрования AES.
17. Криптография с открытым ключом.
18. Криптосистема RSA.
19. Криптосистема Эль-Гамаля.
20. Протокол Диффи- Хеллмана.
21. Алгоритмы работы с большими числами.
22. Хеш-функции. Свойства хеш-функций.
23. ГОСТ Р 34.11-2012.
24. Коды аутентичности сообщений. Электронная подпись.
25. ГОСТ Р 34.10-2012.

Практические задачи:

1. Изучить свойства данной алгебраической структуры.
2. Пусть G — циклическая группа порядка n с образующим x. Найти все образующие и все подгруппы данной группы.
3. Исследовать кольцо классов вычетов по модулю n.
4. Построить поле Галуа посредством неприводимого многочлена f(x). Найти образующий элемент мультипликативной группы поля.
5. Построить группу точек эллиптической кривой над полем Галуа GF(q) для данных значений параметров a, b.
6. Записать целочисленную линейную комбинацию чисел a и b.
7. Дано сообщение M. Зашифровать его с помощью данного шифра.
8. Дано сообщение M. Сформировать электронную подпись для данного сообщения по ГОСТ Р 34.10-2012, используя данные параметры эллиптической кривой.

Вопросы для проверки остаточных знаний студентов

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Принципы, используемые для повышения стойкости шифра?
11. Приведите схему и объясните принцип работы блочного шифра.
12. Дайте характеристику шифра DES.
13. Дайте характеристику шифра ГОСТ 28147-89.
14. Перечислите основные различия между DES и ГОСТ 28147-89.
15. Что такое – режим применения блочного шифра?
16. Чем отличается поточное и блочное шифрование.

17. Дайте характеристику шифра RC4.
18. Основные свойства криптографических хеш-функций.
19. Принципы работы хеш-функции.
20. Особенности построение хеш-функции на базе блочного шифра.
21. Опишите операцию приведения по модулю.
22. Какими свойствами обладает операция приведения по модулю?
23. Приведите определение простого числа.
24. Какие два числа называются взаимно простыми?
25. Определите понятие обратного значения по модулю.
26. Сформулируйте малую теорему Ферма.
27. Дайте определение функции Эйлера.
28. Сформулируйте теорему Эйлера.
29. Перечислите свойства простых чисел.
30. Чем отличается криптография с открытым ключом от симметричных шифров?
31. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
32. Опишите алгоритм Шамира.
33. Опишите алгоритм Эль-Гамаля.
34. .Опишите алгоритм RSA.

7. Учебно-методическое и информационное обеспечение дисциплины «Криптографические методы защиты информации»

Зав. библиотекой _____

№ п/п	Виды заня-тий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Автор(ы)	Изда-тельство и год издания	Количество изданий	
					В библио-теке	На кафед ре
1	2	3	4	5	6	7
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк., пз, срс	Основы современной криптографии и стеганографии. [Электронный ресурс]	Б.Я. Рябко, А.Н. Фионов.	2-е изд. — М.: Горячая линия – Телеком, 2013. — 232 с.	http://e.lanbook.com/view/book/63244/	
2.	Лк., пз, срс	Введение в теоретико-числовые методы криптографии: учебное пособие	М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин	СПб.: Издательство «Лань», 2011. — 400 с. [Электронный ресурс].	http://e.lanbook.com/view/book/68466/	
3.	Лк., пз, срс	Методы и средства криптографической защиты данных в вычислительных системах. Часть 2 [Электронный ресурс]:	Борисова С.Н.	Пенза: ПензГТУ (Пензенский государственный технологический университет), 2013. — 107 с.	http://e.lanbook.com/books/element.php?pl1_id=62779	
4.	Лк., пз, срс	Основы защиты информации и информационные технологии: Учебное пособие в 3 частях. – Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс]: учебное пособие	Серёдкин А.Н.	Пенза: ПензГТУ (Пензенский государственный технологический университет), 2013. — 180 с.	http://e.lanbook.com/books/element.php?pl1_id=62755	
5.	Лк., пз, срс	Введение в криптографию: сборник задач и упражнений [Электронный ресурс]	Е.Г. Кукина, В.А. Романьков	Омск: ОмГУ (Омский государственный университет им. Ф.М. Достоевского), 2013. — 91 с.	http://e.lanbook.com/books/element.php?pl1_id=75394	
6.	Лк., пз, срс	Введение в криптографию [Электронный ресурс]:	В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин [и др.].	М.: МЦНМО (Московский центр непрерывного математического образования), 2012. — 348 с.	http://e.lanbook.com/books/element.php?pl1_id=71813	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
7.	Лк., пз, срс	Интеллектуальные системы защиты информации	Васильев В.И.	М.: Машиностроение, 2013. — 172 с.	http://e.lanbook.com/books/element.php?pl1_id=5792	

		[Электронный ресурс]			
8.	Лк., пз, срс	Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие.	В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин [и др.].	М.: ФЛИНТА, 2011. — 187 с.	http://e.lanbook.com/books/element.php?pl1_id=60717
9.	Лк., пз, срс	Методы и средства защиты компьютерной информации. Часть 1 [Электронный ресурс]	Борисова С.Н.	Пенза: ПензГТУ (Пензенский государственный технологический университет), 2013. — 55 с.	http://e.lanbook.com/books/element.php?pl1_id=62780
ИНТЕРНЕТ-ИСТОЧНИКИ					
10.	Лк., пз, срс	http://kmb.ufoctf.ru/index.html			
11.	Лк., пз, срс	https://habrahabr.ru/hub/crypto/			
12.	Лк., пз, срс	http://training.hackerdom.ru/			
13.	Лк., пз, срс	http://fstec.ru/			
14.	Лк., пз, срс	Виртуальная операционная система Microsoft Windows XP SP3 (VirtualBox, доступ из локальной сети каф. КИБЭВС. URL: file://cesir/vm/WinXPBasic).			

8. Материально-техническое обеспечение дисциплины «Криптографические методы защиты информации»

Материально-техническое обеспечение дисциплины «Криптографические методы защиты информации» включает:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет (лаборатории по автоматизированным информационным системам, оснащенные современной электронно-вычислительной техникой с соответствующим программным обеспечением);
- аудитории, оборудованные проекционной техникой.

Для проведения практических занятий используются компьютерные классы кафедры ИБ, оборудованные современными персональными компьютерами, характеристики которых не ниже:

Pentium 4, DDR 1 Gb, HDD – 150 GB, Video Card – 126 MB, CD/DVD, USB -2.

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

На компьютере предустанавливается ОС Windows XP/Vista/7 и программное обеспечение MS Office 2010, Borland C++ , Borland C++ Builder 6 и др. Приложение командной строки dumpasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumpasn1.rar (Windows, x86).

КриптоПро OCSPCOM (версия 1.05.0726).

КриптоПро TSPCOM (версия 1.05.0972).

8.4. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

При проведения лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

Microsoft Office (Word, Excel, PowerPoint, Access)

ЭБС http://library.mirea.ru/.

Дистрибутив КриптоПро WinLogon и КриптоПро EAP-TLS;

Дистрибутив КриптоПро JCP и КриптоПро JTLS

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем».

Рецензент рабочей программы от выпускающей кафедры по направлению 10.03.01 – «Информационная безопасность», профилю «Безопасность автоматизированных систем».

Подпись З.Р. Рахманкулова

ДОПОЛНЕНИЕ И ИЗМЕНЕНИЯ В РАБОЧЕЙ ПРОГРАММЕ НА 20___/_____ УЧЕБНЫЙ ГОД

В рабочую программу вносятся следующие изменения

Рабочая программа переосмотрена и одобрена на заседании кафедры _____20___

Заведующий кафедрой _____

Внесенные изменения утверждаю
Проректор по учебной работе (декан)__ _____

_____20___