МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ:
Декан, председатель совета факультета КТ,ВТиЭ

_____ **Юсуфов Ш.А.**
подпись Ф.И.О

«20» 08 **2018г.**

УТВЕРЖДАЮ:
Проректор по учебной работе, председатель методического совета ДГТУ

_____ **Суракатов Н.С.**
подпись Ф.И.О

«28» 08 **2018г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.В.ОД.15 ЗАЩИТА ИНФОРМАЦИИ

для направления 09.03.04 Программная инженерия

по профилю Разработка программно-информационных систем

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

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) бакалавр

Форма обучения очная ; курс 4; семестр 8 ;

Всего трудоемкость в зачетных единицах (часах) 3зет(108ч);

Лекции 16 (час); Экзамен 8-1зет (36ч);

Практические (семинарские) занятия 8 (час); Зачет - (семестр);

Лабораторные занятия 16 (час); Курсовая работа - (семестр);

Самостоятельная работа 32 (час).

Зав. кафедрой _____ **Качаева Г.И.**

Начальник учебного отдела _____ **Магомаева Э.В.**

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров 09.03.04 «Программная инженерия», профилю «Разработка программно-информационных систем».
Программа одобрена на заседании выпускающей кафедры ПОВТиАС
от 12.09.2018 г., протокол № 1

Зав. выпускающей кафедрой по направлению подготовки бакалавров 09.03.04 Программная инженерия, профилю «Разработка программно-информационных систем» _____ В.Б. Мелехин

ОДОБРЕНО:
Методической комиссией по укрупненным группам специальностей и направлений подготовки
09.00.00 –Информатика и вычислительная техника

Председатель МК
Абдулгалимов А.М.
подпись Ф.И.О.
«12» 09 2018 г.

АВТОР(Ы) ПРОГРАММЫ:

Качаева Г.И., к.э.н., ст.преп.
Ф.И.О. уч. степень, ученое звание, подпись

1. Цели освоения дисциплины

Целью дисциплины «Защита информации » является формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области.

Основные задачи, на решение которых нацелен курс:

- сформировать взгляд на криптографию и защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер;
- изучить базовые теоретические понятия, лежащие в основе процесса защиты информации, сервисы и механизмы безопасности;
- получить представление о компьютерной криптографии, включающей программную реализацию криптографических алгоритмов, проверку их качества, генерацию и распределение ключей, автоматизацию работы по анализу перехвата и раскрытию шифров;
- научиться использованию криптографических алгоритмов шифрования, электронной цифровой подписи, хэш-функций, генерации псевдослучайных последовательностей чисел и протоколов аутентификации, используемых в широко распространенных программных продуктах.

2 .Место дисциплины в структуре ООП бакалавриата

Дисциплина относится к базовой части ФГОС ВО. по направлению подготовки 09.03.04 Программная инженерия.

Освоение дисциплины предполагает знание дисциплин математического и естественно-научного цикла: Информатика, Алгебра и геометрия, Математическая логика и теория алгоритмов, Теория вероятностей и математическая статистика, Дискретная математика, а также знание Программирования, Структуры и алгоритмы обработки данных, Базы данных.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины «Защита информации»

Процесс изучения дисциплины направлен на формирование следующих *компетенций*:

профессиональных:

владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества (ПК-4);

В результате изучения дисциплины студент *должен*:

а) *знать* правовые основы защиты компьютерной информации, математические основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях,

стандарты, модели и методы шифрования, методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей, методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных);

б) *уметь* применять известные методы и средства поддержки информационной безопасности в компьютерных системах, проводить сравнительный анализ,

выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах;

в) *владеть* навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации, навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, алгоритмы простановки и проверки электронной цифровой подписи, алгоритмы хэш-функций, алгоритмы генерации псевдослучайных последовательностей чисел.

В результате изучения дисциплины студент *должен*:

а) *знать* правовые основы защиты компьютерной информации, математические основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях,

стандарты, модели и методы шифрования, методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей, методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных);

б) *уметь* применять известные методы и средства поддержки информационной безопасности в компьютерных системах, проводить сравнительный анализ,

выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах;

в) *владеть* навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации, навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, алгоритмы простановки и проверки электронной цифровой подписи, алгоритмы хэш-функций, алгоритмы генерации псевдослучайных последовательностей чисел.

4. Структура и содержание дисциплины «Защита информации»

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля (по срокам текущей аттестации)
				ЛК	ПЗ	ЛР	СРС	
1	2	3	4	5	6	7	8	9
1.	**Лекция 1. Тема: Основные понятия и определения в области информационной безопасности.** 1. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. 2. Классификация атак.	8	1	2			4	Вх.контр.
2.	**Лекция 2. Тема: Традиционное шифрование: классические методы. Криптостойкость.** 1. Основные понятия и определения. Подстановочные и перестановочные шифры. 2. Дисковые шифраторы. 3. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.		2	2	2		4	
3.	**Лекция 3. Тема: Алгоритмы генерации псевдослучайных последовательностей чисел.** 1. Различные способы создания псевдослучайных чисел.		3	2		2	4	
4.	**Лекция 4. Тема: Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411.** 1. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. 2. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. 3. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.		4	2	2	4	4	КР№1

1	2	3	4	5	6	7	8	9
5.	**Лекция 5. Тема: Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.** 1. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.	8	5	2		2	4	КР №1
6.	**Лекция 6. Тема: Блочные и поточные алгоритмы симметричного шифрования.** 1. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. 2. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. 3. Сеть Фейштеля.		6	2	2	2	4	КР №2
7.	**Лекция 7. Тема: Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.** 1. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. 2. Описание алгоритмов DES и тройного DES. 3. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения.		7	2		4	4	
8.	**Лекция 8. Тема: Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael. Асимметричные системы шифрования (системы с открытым ключом). RSA.** **1.** Стандарт криптографической защиты 21 века(AES). **2.** Алгоритмы Rijndael и RC6. 1. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра. Понятия однонаправленной функции и однонаправленной функции с лазейкой. 2. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля. 3. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.		8	2	2	2	4	
Итого				**16**	**8**	**16**	**32**	**Экзамен 1 зет-36 часов**

4.2 Содержание практических занятий

№ п/п	№ лекции из рабочей программы	Наименование практического, семинарского занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	2	3	4	5
1	1	Основные понятия и определения в области информационной безопасности.	1	1-11
2	2	Традиционное шифрование: классические методы. Криптостойкость.	1	1,2,5,10,11
3	3	Алгоритмы генерации псевдослучайных последовательностей чисел.	1	2,3,5,9,10
4	4	Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411.	1	1,3,6,7,10,11
5	5	Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.	1	2,10
6	6	Блочные и поточные алгоритмы симметричного шифрования.	1	1,3,4,7,8,10,11
7	7	Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.	1	2,4,6,8,10,11
8	8	Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael. Асимметричные системы шифрования (системы с открытым ключом). RSA.	1	1,2,5,10,11
Итого			8	

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	Шифрование информации методами традиционного шифрования. Генерация псевдослучайных последовательностей чисел в системах защиты информации.	2	№1-№8
2.	1-3	Хэш-функции и электронная цифровая подпись.	2	№ 2, 3,8
3.	1-4	Изучение американского стандарта шифрования данных DES. Изучение отечественного стандарта шифрования	4	№ 2-8

		данных (ГОСТ 28147-89).		
4.	**1-7**	Симметричный криптографический алгоритм с AES – подобной структурой Rijndael.	**4**	**№ 2, 3, 4**
5.	**1-8**	Асимметричные криптосистемы. Шифрование и электронная цифровая подпись на основе с помощью алгоритма RSA.	**2**	**№ 2, 3, 4**
6.	**1-18**	Выработка общего секретного ключа по алгоритму Диффи – Хэллмана.	**2**	**№ 2, 3**
Итого			**16**	

4.4.Тематика для самостоятельной работы студентов

№	Содержание дисциплины, самостоятельно изучаемое студентами	Кол-во Часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля (контр. работа, практич. и лаб. занятия и т.д..)
1.	Основные понятия и определения в области информационной безопасности.	2	№1,2	КР
2.	Традиционное шифрование: классические методы. Криптостойкость.	2	№1-4	Кр
3.	Алгоритмы генерации псевдослучайных последовательностей чисел.	2	№1-5	Кр
4.	Хэш-функции и аутентификация сообщений.	4	№1-8	Кр
5.	Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП.	4	№1-8	Кр
6.	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы.	4	№1-8	Кр
7.	Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.	4	№1-8	Кр
8.	Асимметричные системы шифрования	4	№1-8	Кр
9.	Криптография с использованием эллиптических кривых.	2	№1-8	Кр
10.	Безопасность современных сетевых технологий. Протоколы аутентификации.	2	№1-8	Кр
11.	Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.	2	№1-8	кр
Итого		**32**		

5. Образовательные технологии

Образовательный процесс по дисциплине строится на основе комбинации следующих образовательных технологий.

Интегральную модель образовательного процесса по дисциплине формируют технологии методологического уровня: модульно-рейтинговое обучение, контекстное обучение, технология поэтапного формирования умственных действий, технология развивающего обучения, элементы технологии развития критического мышления.

Реализация данной модели предполагает использование следующих технологий стратегического уровня (задающих организационные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур:

– лекционные (вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция);

– практические (углубление знаний, полученных на теоретических занятиях, решение задач);

– тренинговые (формирование определенных умений и навыков, формирование алгоритмического мышления);

– активизации познавательной деятельности (приемы технологии развития критического мышления через чтение и письмо, работа с литературой, подготовка презентаций по темам домашних работ);

– самоуправления (самостоятельная работа студентов, самостоятельное изучение материала).

Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и практических занятий.

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Вопросы входного контроля

1. Запишите в двоичной системе счисления заданное в десятичной системе число.
2. Что показывает кодовая таблица ЭВМ?
3. Что понимается под байтовым алфавитом?
4. В каком виде существует информация в ЭВМ?
5. По какому правилу текстовая информация превращается в цифровую для ввода в ЭВМ?

Оценочные средства для текущего контроля успеваемости

Контрольная работа №1

1. Алгоритмы шифрования последовательности блоков методами DES, ГОСТ 28147-89 во всех режимах;
2. Алгоритмы многораундового шифрования блока методами DES, ГОСТ 28147-89 во всех режимах;
3. Операции, применяемые для шифрования блока в раунде методами DES, ГОСТ 28147-89;
4. Алгоритмы шифрования блока в раунде методами DES, ГОСТ 28147-89;
5. Алгоритмы выработки ключа для шифрования блока в раунде методами DES, ГОСТ 28147-89;

Контрольная работа №2

1. Операции в конечном поле $GF(2^8)$ (умножение, сложение и т.д.);
2. Алгоритм многораундового шифрования методом Rijndael;

3. Алгоритм раундового преобразования при шифровании Rijndael;
4. Операции раундового преобразования и их реализация;
5. Алгоритм выработки раундовых ключей при шифровании Rijndael;
6. Выработка открытого ключа для шифрования алгоритмом RSA. Алгоритм шифрования и подписывания методом RSA;
7. Определение секретного ключа по открытому ключу в алгоритме RSA. Алгоритмы определения взаимной простоты чисел (e и n) и поиска обратного элемента $e^{-1} \bmod n$;
8. Алгоритм поиска примитивных элементов в поле GF(P). Алгоритм Диффи-Хэллмана выработки общего секретного ключа.

Контрольные вопросы для проверки остаточных знаний.

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности.
2. Шифры замены и перестановки.
3. Классификация методов дешифрования. Модель предполагаемого противника.
4. Совершенная секретность по Шеннону.
5. Блочные криптосистемы с секретным ключом.
6. Блочные криптосистемы с секретным ключом.
7. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы..
8. Теория сложности вычислений. Классификация алгоритмов.
9. Электронная подпись.
10. Хэш-функции и их применение. Хеш-функция MD2.
11. Однонаправленные (односторонние) функции с секретом и их применение.
12. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны.
13. Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования.
14. Сертификация ключей с помощью цифровых подписей.
15. Основы криптоанализа.
16. Криптосистемы на эллиптических кривых.

Список экзаменационных вопросов

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
2. Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.
3. Шифры замены и перестановки. Моно- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.
4. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.
5. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.
6. 6 Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.
7. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
8. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.
9. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.
10. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в

режимах гаммирования.

11. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.
12. Теория сложности вычислений. Классификация алгоритмов.
13. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.
14. Криптосистема Эль-Гамаля.
15. Электронная подпись. Варианты электронной подписи на основе алгоритмов RSA и Эль-Гамаля.
16. Хэш-функции и их применение. Хеш-функция MD2.
17. Однонаправленные (односторонние) функции с секретом и их применение.
18. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамаля.
19. Цифровая подпись на основе алгоритма RSA.
20. Стандарт цифровой подписи DSS. Генерация цифровой подписи. Проверка цифровой подписи.
21. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Протоколы аутентификации с использованием nonce и временных меток.
22. Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования. Протокол обмена сеансовыми ключами. Вскрытие "человек-в-середине". Протокол "держась за руки".
23. Сертификация ключей с помощью цифровых подписей. Разделение секрета. Метки времени. Пример протокола защиты базы данных.
24. Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Вижинера, использующей простой XOR.
25. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.
26. Криптосистемы на эллиптических кривых.

7.Учебно –методическое и информационное обеспечение дисциплины(модуля) «Защита информации»

№	Виды занятий (лк, пз, лб, срс, ирс)	Комплект необходимой учебной литературы по дисциплинам (наименование учебника, учебного пособия, конспект лекций, учебно-методической литературы)	Автор	Издат. и год издания	Кол-во пособий, учебников и прочей литературы	
					в библиотеке	на кафедре
Основная литература						
1.	ЛК,СР, КР	Информационная безопасность и защита информации. Учебное пособие для ВУЗов.	Мельников В.П., Клейменов С.А., Петраков А.М.	М.: Академия, 2007г.-336с., ил. ISBN 978-5-7695-4884-0	47	
2.	ЛК,СР, КР	Инженерно-техническая защита информации [Электронный ресурс]	Рагозин Ю. Н.	СПб.: Интермедия, 2018. — 168 c. — 978-5-4383-0161-5.	http://www.iprbookshop.ru/73641.html	
3.	ЛК,СР, КР	Организационная защита информации [Электронный ресурс]	Аверченков В. И.	Брянск: Брянский государственный технический университет, 2012. — 184 c. — 978-89838-489-0	http://www.iprbookshop.ru/7002.html	
4.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. — 95 c. — 2227-8397	http://www.iprbookshop.ru/17925.html	
5.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. — 104 c. — 2227-8397	http://www.iprbookshop.ru/17926.html	

6.	ЛК,СР, КР	Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие	Креопалов В. В.	М.: Евразийский открытый институт, 2011. — 278 с. — 978-5-374-00507-3.	http://www.iprbookshop.ru/10871.html	
7.	ЛК,СР, КР	Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие	Башлы П. Н.	М.: Евразийский открытый институт, 2012. — 311 с. — 978-5-374-00301-7.	http://www.iprbookshop.ru/10677.html	
8.	ЛК,СР, КР	Методы и средства криптографической защиты информации [Электронный ресурс] :	Алексеев В. А.	Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009. — 16 с. — 2227-8397.	http://www.iprbookshop.ru/17710.html	
Дополнительная литература						
9.	ЛК,СР, КР	Комплексная защита информации в компьютерных системах. Учебное пособие	Завгородний В.И.	М.: Логос, Пбоюл Н.А.Егоров, 2001-264с.,		
10.	ЛК,СР, КР	Методы и средства защиты информации в компьютерных системах. Учебное пособие для ВУЗов.3-е издание	Хорев П.Б.	М.: Академия, 2007-256.: ил.-(высш.проф. образ.) ISBN 978-5-7695-4157-5		
11.	ЛК,СР, КР	Организационное обеспечение информационной безопасности. Учебник для ВУЗов.	Романов О.А., Бабин С.А., Жданов С.Г.	М.: Академия, 2008-190с. ISBN 978-5-7695-4272-5		
12.	ЛК,СР, КР	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. Учебное пособие для ВУЗов	Белкин П.Б., Михальский О.О., Першаков А.С. и др.	М.: Радио и связь, 1999.-168с.		
13.	ЛК,СР, КР	Основы криптографии. Учебное пособие – 2.е издание.		М.: Гелиос АРВ; 2002.-480с., ил.		
14.	ЛК,СР, КР	Криптография: скоростные шифры	Молдовян А.А. и др.	СПб., БХВ-Петербург, 2002.-496с.		

		Интернет - источники
15.	ЛК,СР, КР	http://dstu.ru/nauka/biblioteka/ – образовательный портал университета
16.	ЛК,СР, КР	http://www.elibrary.ru – научная электронная библиотека
17.	ЛК,СР, КР	http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.

8. Материально-техническое обеспечение дисциплины

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью.

Программное обеспечение: – Far Manager – LibreOffice – Microsoft Visual Studio 2013 Professional – Microsoft Windows 7 Pro – Notepad++.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 09.03.04 – «Программная инженерия» и профилю подготовки «Разработка программно-информационных систем».

Рецензент рабочей программы от выпускающей кафедры по направлению 09.03.04 – Программная инженерия

ст. пр. каф. ПОВТиАС Шишова И.В.

Подпись должность ФИО

Дополнения и изменения в рабочей программе
на 20__/___ учебный год

В рабочую программу вносятся следующие изменения

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Рабочая программа пересмотрена и одобрена на заседании кафедры _____20

Заведующий кафедрой _____

Внесенные изменения утверждаю
Проректор
по учебной работе _____

(декан) _____