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

«18» 10 **2018г.**

УТВЕРЖДАЮ:
Проректор по учебной работе, председатель методического совета ДГТУ

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

«29» 10 **2018г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.Б.14 ЗАЩИТА ИНФОРМАЦИИ

для направления 09.03.01 Информатика и вычислительная техника

по профилю Вычислительные машины, комплексы, системы и сети

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) 2зет(72ч);

Лекции 8 (час); Экзамен - ;

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

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

Самостоятельная работа 48 (час).

Зав. кафедрой _____ **Качаева Г.И.**

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

Программа составлена в соответствии с требованиями ФГОСВОпо направлению подготовки бакалавров 09.03.01«Информатика и вычислительная техника», профилю «Вычислительные машины, комплексы, системы и сети».
Программа одобрена на заседании выпускающей кафедры УиИТСиВТ
от 17.10.2018г. г., протокол № 2

Зав. выпускающей кафедрой по направлению подготовки бакалавров «Информатика и вычислительная техника», профилю «Вычислительные машины, комплексы, системы и сети»_____ Саркаров Т.Э.

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.
«18» 10 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 учебного плана ФГОС ВОпо направлению подготовки 09.03.01Информатика и вычислительная техника.

Освоение дисциплины предполагает знание дисциплин: 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, Операционные системы.

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

Процесс изучения дисциплины направлен на формирование следующих *компетенций*:

а) *общекультурных*:

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4).

б) общепрофессиональных:

способностью инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем (ОПК-1);

способностью осваивать методики использования программных средств для решения практических задач (ОПК-2);

способностью учувствовать в настройке и накладке программно –аппаратных комплексов (ОПК-4);

в) профессиональных

способностью разрабатывать модели компонентов информационных систем, включая модели без данных и модели интерфейсов «человек- электронно – вычислительная машина» (ПК-1);

способностью разрабатывать компоненты аппаратно – программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования (ПК-2);

способностью обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности (ПК-3);

способностью сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем (ПК-5)

способностью проверять техническое состояние вычислительного оборудования и осуществлять необходимые профилактические процедуры (ПК-7).

В результате изучения дисциплины студент *должен*:

знать:

- правовые основы защиты компьютерной информации;
- организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях;
- стандарты, модели и методы шифрования;
- методы идентификации и аутентификации пользователей;
- методы передачи конфиденциальной информации по каналам связи;

уметь:

- применять известные методы и средства поддержки информационной безопасности в компьютерных системах;
- проводить сравнительный анализ, выбирать методы и средства защиты компьютерной информации;
- оценивать уровень защиты информационных ресурсов в автоматизированных системах;

владеть:

- навыками построения аппаратно-программных систем, использующих сервисы и механизмы безопасности;
- навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, а также алгоритмы простановки и проверки электронной цифровой подписи.

4.Структура и содержание дисциплины «Защита информации»

Общая трудоемкость дисциплины составляет 2 зачетные единицы – 72 часа, в том числе: лекционных -8 часов, практических -17 часов, лабораторных - 16 часов, СРС -48 часов, форма отчетности зачет в 8 семестре.

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: Правовые и организационные основы защиты информации.** 1. Понятия «организационная защита информации» и «режим защиты информации». 2. Понятие «система организационной защиты информации»; субъекты и объекты системы. 3. Анализ нормативных документов, регламентирующих основные принципы организации защиты информации. 4. Проблемы защиты информации в автоматизированных системах.	8	1,2	2		4	6	Вх.контр.
2.	**Лекция 2. Тема: Построение систем защиты информации от несанкционированного доступа.** 1. Основные понятия защиты от НСД. 2. Формальные модели защиты. 3. Системы разграничения доступа.		3,4	2		4	12	АКР№1
3.	**Лекция 3. Тема: Использование экранирования для защиты информации в автоматизированных системах.** 1. Сущность и задачи комплексной системы защиты информации (КСЗИ). 2. Средства защиты информации в автоматизированных системах 3. Экранирование для защиты информации в АС.		5,6	2		4	12	
4.	**Лекция 4. Тема: Защита информации в компьютерных сетях.** 1. Виды компьютерных сетей		7,8	2		4	18	

	определение защищенной информационной системы локальные вычислительные сети. 2. Понятие защиты информации в системах и сетях 3. Система защиты информации 4. Информационная глобальная сеть интернет							
Итого				**8**		**16**	**48**	**зачет**

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.	1	Администрирование учетных записей пользователей	4	№1-№8
2.	1-2	Управление параметрами операционной системы	4	№ 2, 3,8
3.	1-3	Дискреционный механизм разграничения доступа	4	№ 2-8
4.	1-3	Симметричный криптографический алгоритм с AES – подобной структурой Rijndael. Асимметричные криптосистемы. Шифрование и электронная цифровая подпись на основе с помощью алгоритма RSA.	4	№ 2, 3, 4
Итого			**16**	

4.3.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.	**Правовые и организационные основы защиты информации.** Понятия «организационная защита информации» и «режим защиты информации». Понятие «система организационной защиты информации»; субъекты и объекты системы. Анализ нормативных документов, регламентирующих основные	6	№1,2	КР

	принципы организации защиты информации. Проблемы защиты информации в автоматизированных системах.			
2.	**Построение систем защиты информации от несанкционированного доступа.** Основные понятия защиты от НСД. Формальные модели защиты. Системы разграничения доступа.	12	№1-4	Кр
3.	**Использование экранирования для защиты информации в автоматизированных системах.** Сущность и задачи комплексной системы защиты информации (КСЗИ). Средства защиты информации в автоматизированных системах Экранирование для защиты информации в АС.	12	№1-5	Кр
4.	**Защита информации в компьютерных сетях.** Виды компьютерных сетей определение защищенной информационной системы локальные вычислительные сети. Понятие защиты информации в системах и сетях Система защиты информации Информационная глобальная сеть интернет	18	№1-8	Кр
Итого		**48**		

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

Аттестационная 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;
6. Операции в конечном поле $GF(2^8)$ (умножение, сложение и т.д.);
7. Алгоритм многораундового шифрования методом Rijndael;
8. Алгоритм раундового преобразования при шифровании Rijndael;
9. Операции раундового преобразования и их реализация;
10. Алгоритм выработки раундовых ключей при шифровании Rijndael;
11. Выработка открытого ключа для шифрования алгоритмом RSA. Алгоритм шифрования и подписывания методом RSA;
12. Определение секретного ключа по открытому ключу в алгоритме RSA. Алгоритмы определения взаимной простоты чисел (e и n) и поиска обратного элемента $e^{-1} \bmod n$;
13. Алгоритм поиска примитивных элементов в поле GF(P). Алгоритм Диффи-Хэллмана выработки общего секретного ключа.

Список вопросов на зачет

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 временны́х 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 выбранномушифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.
26. Криптосистемы на эллиптических кривых.

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.

и.о. зав каф. библ. ЖВУ.

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 с. — 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 с. — 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 с. — 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 с. — 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 c. — 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 c. — 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 c. — 2227-8397.	
http://www.iprbookshop.ru/17710.html					
9.	ЛК,СР, КР	Комплексная защита информации в компьютерных системах. Учебное пособие	Завгородний В.И.	М.: Логос, ПбоюлН.А.Егоров, 2001-264с.,	http://www.iprbookshop.ru/16510.html
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	http://www.iprbookshop.ru/1723.html
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	http://www.iprbookshop.ru/17760.html
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.	http://www.iprbookshop.ru/17380.html
13.	ЛК,СР, КР	Основы криптографии. Учебное пособие – 2.е издание.		М.: Гелиос АРВ; 2002.-480с., ил.	http://www.iprbookshop.ru/17729.html
14.	ЛК,СР, КР	Криптография: скоростные шифры	Молдовян А.А. и др.	СПб., БХВ-Петербург, 2002.-496с.	http://www.iprbookshop.ru/17010.html

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.

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

Программа составлена в соответствии с требованиями ФГОС ВОпо направлению 09.03.01 – «Информатика и вычислительная техника» и профилю подготовки «Вычислительные машины, комплексы, системы и сети».

Рецензент рабочей программы от выпускающей кафедры по направлению

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) _____