МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
функционального анализа
и операторных уравнений

Каменский М.И.
26.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.32 Прикладная криптография

1. Шифр и наименование направления подготовки / специальности: 10.05.04 Информационно-аналитические системы безопасности
2. Профиль подготовки / специализации:
3. Квалификация (степень) выпускника: специалист
4. Форма обучения: очная
5. Кафедра, отвечающая за реализацию дисциплины:
функционального анализа и операторных уравнений
6. Составители программы:
Завгородний Михаил Григорьевич, канд. физ-мат. наук, доцент.

7. **Рекомендована:** НМС математического факультета, протокол №0500-07 от 03.07.2018
8. Учебный год: 2018-2019 **Семестр(-ы): 6**

9. Цели и задачи учебной дисциплины:

Цель курса – дать знания не только по теоретическим вопросам криптологии, но и по практическим реализациям алгоритмов криптографии и криптоанализа; научить студентов логике программирования защищенных криптосистем, дать им умения компьютерного криптоанализа; научить самостоятельному созданию программного обеспечения, содержащего криптографические алгоритмы.

10. Место учебной дисциплины в структуре ООП:

Дисциплина входит в базовую (общепрофессиональную) часть профессионального цикла. Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Алгебра, Теория вероятностей, Математическая статистика, Дискретная математика, Математическая логика и теория алгоритмов, Языки программирования, Технология и методы программирования, Основы информационной безопасности. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении курсов: Безопасность электронного документооборота, Криптографические методы защиты информации, Безопасность информационных и аналитических систем, Моделирование автоматизированных информационных систем, Принципы построения, проектирования и эксплуатации автоматизированных информационных систем, а также при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области информационной безопасности и защиты информации.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-12	способностью разрабатывать программное и иные виды обеспечения специальных ИАС.	знать: понятия шифра, ключа, расстояния единственности, криптографической системы, криптографического протокола;основные понятия симметричной и асимметричной криптографии; правила стойкости шифрсистемы; математические методы построения стойких шифров, криптографические свойства булевых функций; принципы создания безопасного канала общения и выбора кодов аутентичности сообщений; уметь: определять целесообразность применения различных криптографических систем и методов их криптоанализа;использовать существующие методы шифрования; применять статистические и алгебраические методы криптоанализа блочных и

		поточных шифров; владеть: навыками работы с криптографическими протоколами, компьютерными средствами исследования криптографических алгоритмов.
ОПК-7	способностью применять методы и средства обеспечения информационной безопасности специальных ИАС	знать: вероятностную и алгебраическую модели шифрсистемы; результаты по совершенной секретности шифра, избыточности языка открытых сообщений, об определении числа ложных ключей и расстояния единственности шифра; математические методы построения стойких шифров, криптографические свойства булевых функций; алгебраические методы криптоанализа, методы решения нелинейных систем булевых уравнений; инфраструктуры открытого ключа; процесс стандартизации и патентования; уметь: разрабатывать криптографически стойкие компоненты шифров (такие, как S-блоки и др.), исследовать криптографические свойства булевых функций; осуществлять программную реализацию современных методов криптографии и криптоанализа с использованием языка C++; выбрать на практике функции хэширования; создать безопасный канал общения; владеть: способами выбора из числа существующих средств криптографической защиты информации наиболее эффективных для решения проблемы защиты информации, обрабатываемой в автоматизированных системах или передаваемой по телекоммуникационным каналам с учетом особенностей их функционирования, а также возможных попыток несанкционированного доступа к информационным ресурсам конкретной информационной системы

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 2/72

Форма промежуточной аттестации *зачёт*

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		сем. № 6
Аудиторные занятия	*32*	*32*
в том числе: лекции	*16*	*16*
практические	*-*	*-*
лабораторные	*16*	*16*
Самостоятельная работа	*40*	*40*
форма промежуточной аттестации		*1 контрольная работа, зачет*
Итого:	*72*	*72*

13.3. Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1	Введение в криптографию	Шифрование, принцип Кирхгофа. Аутентификация. Цифровые подписи. Инфраструктура открытого ключа. Типы атак. Сложность и производительность.
2	Блочные шифры и режимы их работы	Понятие блочного шифра и его безопасности. Современные блочные шифры (DES, ГОСТ 28147-89, AES, Serpent, Twofish). Атаки с помощью решения уравнений. Выбор блочного шифра и размер ключа. Электронная шифровальная книга (ECB). Сцепление шифрованных блоков (CBC). Вектор инициализации. Обратная связь по выходу (OFB). Счетчик (CTR). Выбор режима.
3	Функции хэширования	Функция хэширования и ее безопасность. Современные функции хэширования (MD5, SHA-1, SHA-256, SHA-384 и SHA-512). Коллизии. Недостатки функций хэширования и их исправление. Практический выбор функции хэширования.
4	Безопасный канал общения и коды аутентичности сообщений	Практические проблемы создания безопасного канала общения. Порядок аутентификации и шифрования. Код аутентичности сообщения (MAC) и его безопасность. Метод CBC-MAC. Алгоритмы HMAC и UMAC. Практический выбор функции вычисления MAC. Практическое использование MAC.
5	Практические подходы к реализации криптографических систем	Качество кода: простота, модуляризация, утверждения, переполнение буфера, тестирование.
6	Согласование ключей и управление ключами	Генерация случайных и псевдослучайные чисел. Генератор. Аккумулятор. Управление файлом начального числа. Протокол согласования ключей. Срок действия ключей. Выполнение транзакций в режиме реального времени. Виды угроз (перевод и остановка часов). Создание надежных часов. Серверы ключей. Kerberos. Создание и

		обновление ключа.
7	Инфраструктуры открытого ключа (PKI)	Обзор инфраструктуры открытого ключа. Стандартная концепция и примеры (электронные платежи, ассоциация кредитных карт). Имена и доверие. Прямая и непрямая авторизация. Системы мандатов. Практические аспекты PKI. Формат сертификата. Жизненный цикл ключа.
8	Стандарты и патенты	Процесс стандартизации. SSL – протокол безопасности, используемый Web-обозревателями для безопасного подключения к Web-серверам. Стандартизация на конкурсной основе. Лицензирование. Защищающие патенты.
3. Лабораторные		
1	Введение в криптографию	Шифрование, принцип Кирхгофа. Аутентификация. Цифровые подписи. Инфраструктура открытого ключа. Типы атак. Сложность и производительность.
2	Блочные шифры и режимы их работы	Понятие блочного шифра и его безопасности. Современные блочные шифры (DES, ГОСТ 28147-89, AES, Serpent, Twofish). Атаки с помощью решения уравнений. Выбор блочного шифра и размер ключа. Электронная шифровальная книга (ECB). Сцепление шифрованных блоков (CBC). Вектор инициализации. Обратная связь по выходу (OFB). Счетчик (CTR). Выбор режима.
3	Функции хэширования	Функция хэширования и ее безопасность. Современные функции хэширования (MD5, SHA-1, SHA-256, SHA-384 и SHA-512). Коллизии. Недостатки функций хэширования и их исправление. Практический выбор функции хэширования.
4	Безопасный канал общения и коды аутентичности сообщений	Практические проблемы создания безопасного канала общения. Порядок аутентификации и шифрования. Код аутентичности сообщения (MAC) и его безопасность. Метод CBC-MAC. Алгоритмы HMAC и UMAC. Практический выбор функции вычисления MAC. Практическое использование MAC.
5	Практические подходы к реализации криптографических систем	Качество кода: простота, модуляризация, утверждения, переполнение буфера, тестирование.
6	Согласование ключей и управление ключами	Генерация случайных и псевдослучайные чисел. Генератор. Аккумулятор. Управление файлом начального числа. Протокол согласования ключей. Срок действия ключей. Выполнение транзакций в режиме реального времени. Виды угроз (перевод и остановка часов). Создание надежных часов. Серверы ключей. Kerberos. Создание и обновление ключа.
7	Инфраструктуры открытого ключа (PKI)	Обзор инфраструктуры открытого ключа. Стандартная концепция и примеры (электронные платежи, ассоциация кредитных карт). Имена и доверие. Прямая и непрямая авторизация. Системы мандатов. Практические аспекты PKI. Формат сертификата. Жизненный цикл ключа.
8	Стандарты и патенты	Процесс стандартизации. SSL – протокол безопасности, используемый Web-обозревателями для безопасного подключения к Web-серверам. Стандартизация на конкурсной основе. Лицензирование. Защищающие патенты.

13.2. Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Введение в криптографию	2	2	5	9
2	Блочные шифры и режимы их работы	2	2	5	9
3	Функции хэширования	2	2	5	9
4	Безопасный канал общения и коды аутентичности сообщений	2	2	5	9
5	Практические подходы к реализации криптографических систем	2	2	5	9
6	Согласование ключей и управление ключами	2	2	5	9
7	Инфраструктуры открытого ключа (PKI)	2	2	5	9
8	Стандарты и патенты	2	2	5	9
	Итого	16	16	40	72

14. Методические указания для обучающихся по освоению дисциплины

Аудиторные занятия, лекции и лабораторные занятия, предполагают самостоятельную работу студентов по данному курсу. Ряд тем выносятся для самостоятельного изучения, предлагаются темы для создания докладов с презентациями. Предусмотрены домашние задания и оформление отчетов выполнения лабораторных заданий, а также дополнительные задания для сильных студентов.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Аграновский, Александр Владимирович. Практическая криптография : Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил. + CD-ROM .— (Аспекты защиты) .— ISBN 5-98003-002-6 : 172.50.*
2	*Шнайер, Брюс. Прикладная криптография : Протоколы, алгоритмы, исходные тексты на языке Си : Пер. с англ. / Б. Шнайер .— М. : Триумф, 2003 .— 815 с. : ил. — (Знания и опыт экспертов) .— Библиогр.: с. 741-796 .— Парал. тит. л. англ. — ISBN 5-89392-055-4*

3	*Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.*
4	*Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-x.*

б) дополнительная литература:

№ п/п	Источник
5	*Вельшенбах, М. Криптография на Си и C++ в действии : Пер. с нем. / М. Вельшенбах .— М. : Триумф, 2004 .— 461 с. : ил + 1 CD-ROM .— (Практика программирования) .— Библиогр.: с.449-461 .— ISBN 5-89392-083-X.*
6	*Осипян, В.О. Криптография в задачах и упражнениях / В.О. Осипян, К.В. Осипян .— М. : Гелиос АРВ, 2004 .— 143 с. : ил. — Библиогр.: с.138 .— ISBN 5-85438-009-9.*

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
1	*www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .*

16. Учебно-методическое обеспечение для организации самостоятельной работы

№ п/п	Источник
1	*Аграновский, Александр Владимирович. Практическая криптография : Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил. + CD-ROM .— (Аспекты защиты) .— ISBN 5-98003-002-6 : 172.50.*
2	*Шнайер, Брюс. Прикладная криптография : Протоколы, алгоритмы, исходные тексты на языке Си : Пер. с англ. / Б. Шнайер .— М. : Триумф, 2003 .— 815 с. : ил. — (Знания и опыт экспертов) .— Библиогр.: с. 741-796 .— Парал. тит. л. англ. — ISBN 5-89392-055-4*

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Лекционная аудитория (доска, мел, маркеры), компьютерные классы для проведения лабораторных работ, мультимедийный проектор.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-7 способностью применять методы и средства обеспечения информационной безопасности специальных ИАС	знать: вероятностную и алгебраическую модели шифрсистемы; результаты по совершенной секретности шифра, избыточности языка открытых сообщений, об определении числа ложных ключей и расстояния единственности шифра; математические методы построения стойких шифров, криптографические свойства булевых функций; алгебраические методы криптоанализа, методы решения нелинейных систем булевых уравнений; инфраструктуры открытого ключа; процесс стандартизации и патентования; уметь: разрабатывать криптографически стойкие компоненты шифров (такие, как S-блоки и др.), исследовать криптографические свойства булевых функций; осуществлять программную реализацию современных методов криптографии и криптоанализа с использованием языка C++; выбрать на практике функции хэширования; создать безопасный канал общения; владеть: способами выбора из числа	Разделы 1-4: 1. Введение в криптографию 2. Блочные шифры и режимы их работы 3. Функции хэширования 4. Безопасный канал общения и коды аутентичности сообщений	Лабораторные работы и контрольная работа
			Лабораторные работы

	существующих средств криптографической защиты информации наиболее эффективных для решения проблемы защиты информации, обрабатываемой в автоматизированных системах или передаваемой по телекоммуникационным каналам с учетом особенностей их функционирования, а также возможных попыток несанкционированного доступа к информационным ресурсам конкретной информационной системы		
ПК-12 способностью разрабатывать программное и иные виды обеспечения специальных ИАС.	знать: понятия шифра, ключа, расстояния единственности, криптографической системы, криптографического протокола;основные понятия симметричной и асимметричной криптографии; правила стойкости шифрсистемы; математические методы построения стойких шифров, криптографические свойства булевых функций; принципы создания безопасного канала общения и выбора кодов аутентичности сообщений;	Разделы 5-8: 5. Практические подходы к реализации криптографических систем 6. Согласование ключей и управление ключами 7. Инфраструктуры открытого ключа (PKI) 8. Стандарты и патенты	
	уметь: определять целесообразность применения различных криптографических систем и методов их криптоанализа;использовать существующие методы шифрования; применять статистические и		

	алгебраические методы криптоанализа блочных и поточных шифров;		
	владеть: навыками работы с криптографическими протоколами, компьютерными средствами исследования криптографических алгоритмов.		
Промежуточная аттестация			Комплект КИМ

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

владение понятийным аппаратом данной области науки (теоретическими основами дисциплины), способность иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач в области информатики

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами применять теоретические знания для решения практических задач в области прикладной криптографии	*Повышенный уровень*	*Зачтено*
Обучающийся владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами, допускает ошибки при решении практических задачи или способен применять теоретические знания для решения практических задач в области информатики, но допускает неточности при применении понятийного аппарата данной области науки, но отвечает на дополнительные вопросы	*Базовый уровень*	*Зачтено*
Обучающийся владеет частично теоретическими основами	*Пороговый*	*Зачтено*

дисциплины, фрагментарно способен иллюстрировать ответ примерами, фактами, не отвечает на дополнительные вопросы *Не умеет применять теоретические знания для решения практических задач в области прикладной криптографии*	*уровень*	
Ответ на контрольно-измерительный материал не соответствует любым трем(четырем) из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	*Не зачтено*

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1
Пример контрольно-измерительного материала для зачёта

Б ВГУ 038.824-2016

УТВЕРЖДАЮ

заведующий кафедрой функционального анализа и операторных уравнений

М.И. Каменский

подпись, расшифровка подписи

Направление подготовки / специальность: 10.05.04 Информационно-аналитические системы безопасности / Информационная безопасность финансовых и экономических структур

шифр, наименование

Дисциплина Прикладная криптография

Вид контроля зачет

промежуточный контроль - экзамен, зачет; текущий контроль с указанием формы

Контрольно-измерительный материал №___

1. Сеть Файстеля.

2. Дешифруйте сообщение "17 12 26 26 24 29 25 32 19 26 29 10 05 11 07 10 05 32 29 09 05 29 05 01 05 08 32 04 26 30 26 19 17 25 32 31 00 19 19 05 03 32 13 00 31 00 23 17", зашифрованное на открытом ключе: e = 3, n = 33.

19.3.2 Перечень практических заданий

Пример лабораторного задания (вариант задания)

Лабораторная работа № ___
по дисциплине «Основы информационной безопасности»
Тема: «**Шифрование с открытым ключом методом RSA**»

Задание. Выберите текст (не менее 60 символов) для шифрования методом укладки рюкзака. Сформируйте закрытую и открытую части ключа. При этом учтите требования, предъявляемые к выбору ключа с целью повышения криптостойкости. Зашифруйте выбранный текст. Сформируйте шифрграмму. Обменяйтесь шифрграммами. Расшифруйте полученный шифртекст. Предполагается, что Вы знаете закрытую и открытую части ключа. Подготовьте отчет.

Вопросы

1. Какие криптосистемы относятся к системам шифрования с открытым ключом? В чем их особенность?
2. Сформулируйте математические основы шифрования с открытым ключом.
3. Сформулируйте математические основы шифрования методом **RSA**.

По результатам выполнения заданий подготовьте отчет.

Отчет по лабораторной работе № должен содержать:

1) Титульный лист.
2) Выбранный текст для шифрования.
3) Пояснения по выбору ключа с поверкой требований, предъявляемых к выбору ключа.
4) Пояснения по шифрованию и полученный шифртекст.
5) Шифрграмму, подготовленную Вами, с указанием открытой части ключа.
6) Шифрграмму, полученную Вами при обмене.
7) Пояснения по расшифрованию и полученный открытый текст.
8) Ответы на вопросы.
9) Ваши выводы.

19.3.4 Перечень заданий для контрольных работ

Контрольная работа
по дисциплине «Основы информационной безопасности»
Вариант №___

В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЬБТЖЩИОБ». Прочитайте этот шифртекст, если известно, что шифрующая последовательность содержит только символы А, Б и В.

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

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса (индивидуальный опрос на коллоквиуме); письменных работ (контрольные работы). Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний, или практические задания, позволяющие оценить степень сформированности умений, навыков и опыт деятельности.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.