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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа
Шабров С.А.

25.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.04.02 Криптографические протоколы и стандарты

1. Код и наименование направления подготовки/специальности: 10.05.04 Информационно-аналитические системы безопасности

2. Профиль подготовки/специализация: Информационная безопасность финансовых и экономических структур

Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра математического анализа

6. Составители программы: Шабров Сергей Александрович, доктор физико-математических наук, доцент

7. Рекомендована: Научно-методическим Советом математического факультета, протокол 25.05.2023, № 0500-06

8. Учебный год: 2027-2028 **Семестр(ы): 10**

9. Цели и задачи учебной дисциплины

Цель изучения дисциплины: изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации.

Задачи изучения дисциплины: обучить студентов принципам работы основных протоколов; привить студентам навыки реализации криптографических протоколов с использованием ЭВМ; дать студентам представление об анализе стойкости протоколов к атакам.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Криптографические протоколы и стандарты» относится к дисциплине по выбору. В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, самостоятельной работы и лабораторных работ, ориентированных на освоение студентами современных методологий проектирования, разработки и сопровождения информационно-аналитических систем, а также методов и способов их применения в профессиональной деятельности. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-2	Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа	ПК-2.1	Способен анализировать безопасность информации с помощью формальных моделей	Знать: типовые криптографические протоколы и основные требования к ним; методы аутентификации и подтверждения подлинности сообщений и пользователей; способы построения хеш-функций и основные требования к ним; основные типы электронной подписи; базовые протоколы проверки подлинности и обмена ключами; протоколы разделения секрета; основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности; Уметь: формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям; использовать схемы разделения секрета; проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов; осуществлять распределение аутентифицированных криптографических ключей в корпоративных сетях; Владеть: криптографической терминологией; простейшими подходами к анализу безопасности криптографических протоколов; навыками использования и администрирования современных средств электронной подписи; навыками самостоятельной работы с современными международными стандартами криптографических протоколов.

12. Объем дисциплины в зачетных единицах/час. — 3 / 108.

Форма промежуточной аттестации экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			10	№ семестра	…
Аудиторные занятия					
в том числе:	лекции	22	22		
	практические				
	лабораторные	22	22		
Самостоятельная работа		28	28		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*		36	36		
Итого:		108	108		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Основные понятия криптографии	Предмет и задачи. Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа, симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. История криптографии. Принцип Керкгоффса. Понятие абсолютной стойкости или теоретико-информационной стойкости.	
1.2	Симметричные криптосистемы	Потоковые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потоковым шифрам: Постулаты Голомба, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. Блоковые шифры. Определение блокового шифра. Требования к блоковым шифрам. Различие понятий PRP и PRF. Определение стойкости. Способы построение блоковых шифров: подстановки, перестановки, сети Фейстеля. Алгоритм DES. Режимы использования блочных 4 шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). Детерминированные и недерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров	
1.3	Основные алгоритмы открытым ключом.	Схема RSA. Атаки на RSA. Базовые задачи, допущение Диффи и Хелмана. Возможность реализации систем на мультипликативной группе точек эллиптических кривых. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. Схема шифрования Меркла-Хелмана. Электронная цифровая подпись. Основные понятия, требования. Определение безопасности	
1.4	Управление ключами	Попарные ключи. Использование мастер-ключей. Система Диффи и Хелмана. Человек посередине. Протоколы обмена ключами. С сервером, без сервера. Известные атаки на протоколы обмена ключами. K-надежные схемы распределения ключей. Протоколы разделения секрета. Пороговая	

		криптография.	
1.5	Протоколы цифровых денег и электронного голосования.	Протоколы электронного голосования. Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем	
1.6	Протоколы идентификации + личностная криптография.	Схема идентификации Schnorr – Shamir. Схема идентификации Feige – Fiat – Shamir. Инфраструктура открытых ключей и альтернативные подходы (ID-based распределенные системы).	
2. Практические занятия			
2.1			
2.2			
3. Лабораторные занятия			
3.1	Основные понятия криптографии	Предмет и задачи. Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа, симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. История криптографии. Принцип Керкгоффса. Понятие абсолютной стойкости или теоретико-информационной стойкости.	
3.2	Симметричные криптосистемы	Потоковые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потоковым шифрам: Постулаты Голомба, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. Блоковые шифры. Определение блокового шифра. Требования к блоковым шифрам. Различие понятий PRP и PRF. Определение стойкости. Способы построение блоковых шифров: подстановки, перестановки, сети Фейстеля. Алгоритм DES. Режимы использования блочных 4 шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). Детерминированные и недерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров	
3.3	Основные алгоритмы открытым ключом.	Схема RSA. Атаки на RSA. Базовые задачи, допущение Диффи и Хелмана. Возможность реализации систем на мультипликативной группе точек эллиптических кривых. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. Схема шифрования Меркла-Хелмана. Электронная цифровая подпись. Основные понятия, требования. Определение безопасности	
3.4	Управление ключами	Попарные ключи. Использование мастер-ключей. Система Диффи и Хелмана. Человек посередине. Протоколы обмена ключами. С сервером, без сервера. Известные атаки на протоколы обмена ключами. K-надежные схемы распределения ключей. Протоколы разделения секрета. Пороговая криптография.	
3.5	Протоколы цифровых денег и электронного голосования.	Протоколы электронного голосования. Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем	

3.6	Протоколы идентификации + личностная криптография.	Схема идентификации Schnorr – Shamir. Схема идентификации Feige – Fiat – Shamir. Инфраструктура открытых ключей и альтернативные подходы (ID-based распределенные системы).	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Основные понятия криптографии	2		2	4	8
2	Симметричные криптосистемы	4		4	4	12
3	Основные алгоритмы открытым ключом.	4		4	4	12
4	Управление ключами	4		4	4	12
5	Протоколы цифровых денег и электронного голосования.	4		4	6	14
6	Протоколы идентификации + личностная криптография.	4		4	6	14
	Итого:	22		22	28	72

14. Методические указания для обучающихся по освоению дисциплины: *(рекомендации обучающимся по освоению дисциплины: указание наиболее сложных разделов, работа с конспектами лекций, презентационным материалом, рекомендации по выполнению курсовой работы, по организации самостоятельной работы по дисциплине и др.)*

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся. На лекциях излагается теоретический материал, на лабораторных занятиях решаются задачи по теоретическому материалу, прочитанному на лекциях.

При изучении курса обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все понятия и ГОСТы. Перед следующей лекций обязательно повторить материал предыдущей лекции.

2. Перед лабораторным занятием обязательно повторить лекционный материал.

3. При подготовке к лабораторным занятиям повторить основные понятия по темам. Выполняя работу, предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить задачи.

3. Выбрать время для работы с литературой по дисциплине в библиотеке.

Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций и лабораторных занятий) и активную работу на них, но и самостоятельную учебную деятельность в семестрах, на которую отводится 48 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Анализ защищенности информационных систем» предполагает изучение рекомендуемой преподавателем литературы по вопросам лекционных и лабораторных занятий, самостоятельное освоение понятийного аппарата и подготовку к текущим аттестациям.

Вопросы лекционных и лабораторных занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и лабораторным занятиям, обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать

свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

Все выполняемые студентами самостоятельно задания (выполнение контрольной работы и лабораторных заданий) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации (10 семестр – экзамен).

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	*Авдошин, С. М. Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс] / Авдошин С. М., Набебин А. А. — Москва : ДМК Пресс, 2017 .— 352 с. — Книга из коллекции ДМК Пресс - Информатика .— ISBN 978-5-97060-408-3 .— <URL:https://e.lanbook.com/book/93575>.*

б) дополнительная литература:

№ п/п	Источник
1	*Ищукова, Е. А. Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ ; Южный федеральный университет ; Инженерно-технологическая академия .— Таганрог : Издательство Южного федерального университета, 2016 .— 80 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-9275-2066-4 .— <URL:http://biblioclub.ru/index.php?page=book&id=493059>*

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)
2	ЭБС «Университетская библиотека онлайн»
3	http://www.math.vsu.ru – официальный сайт математического факультета ВГУ

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных), курсовых работ и др.)*

№ п/п	Источник
1	*Антонов В.О. Теоретико-числовые методы в криптографии : практикум / ; авт.-сост. Ф. Б.Тебуева ; авт.-сост. В. О. Антонов ; Министерство образования и науки РФ ; Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет» .— Ставрополь : СКФУ, 2017 .— 107 с. : ил. — Библиогр. В кн.— http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=483838>*

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Осуществляется интерактивная связь с преподавателем через сеть интернет, проводятся индивидуальные онлайн консультации. Лабораторные занятия ведутся с привлечением мультимедийных технологий.

Microsoft Windows 10, Foxit Reader, 7-Zip, Mozilla Firefox

18. Материально-техническое обеспечение дисциплины:

Для проведения лекционных и лабораторных занятий используются аудитории и компьютерные лаборатории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Для самостоятельной работы используются классы с компьютерной техникой, оснащенные необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

---

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Основные понятия криптографии	**ПК-2**	ПК-2.1	Контрольная работа № 1
2.	Симметричные криптосистемы	ПК-2	ПК-2.1	Контрольная работа № 1
3.	Основные алгоритмы открытым ключом.	ПК-2	ПК-2.1	Контрольная работа № 1
4.	Управление ключами	ПК-2	ПК-2.1	Контрольная работа № 2
5.	Протоколы цифровых денег и электронного голосования.	ПК-2	ПК-2.1	Контрольная работа № 2
6.	Протоколы идентификации + личностная криптография.	ПК-2	ПК-2.1	Контрольная работа № 2
Промежуточная аттестация форма контроля – Экзамен				Вопросы к Экзамену

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контрольная работа № 1

Задача 1. Оценить теоретически количество зашифрованного текста (в символах) для успешного частотного криптоанализа и подтвердить результаты экспериментально, если известно, что открытый текст – это осмысленный текст на русском языке и была использована следующая система шифрования: 1) Шифр Цезаря; 2) Аффинный шифр; 3) Шифр Вижинера с известной длиной ключа (показать зависимость от длины ключа); 4) Шифр Вижинера с неизвестной длиной ключа (показать зависимость от длины ключа).

Задача 2. Простым перестановочным шифром зашифрован некий текст, при этом известно, что в качестве открытого текста использован палиндром, в котором все пробелы и знаки препинания опущены. В результате шифрования получен следующий текст: МТИССЛАИЛПНАОЛМУИЛОПИТУ Необходимо: 1) Расшифровать текст, 2) Оценить, насколько можно уменьшить сложность перебора, используя информацию об исходном сообщении; 3) При программной реализации минимизировать количество возвращаемых вариантов ответа. 4) Позволяет ли успешный криптоанализ данного сообщения раскрыть ключ шифрования?

Задача 3. Шифром простой замены зашифровано некоторое стихотворение, при этом сохранены все пробелы и знаки препинания, одинаковые символы заменены одинаковыми, а различные - различными. В результате шифрования получился следующий текст: Э рсдх ыъсг, фрьыя сяы тцорт срэдт Юрь нфурсау уцир нэръ, мрьыя Нрусиъ рнмясяэуцэяуц нурэрт, 6 Нурэрт оячолжяуц ьрорыя. 1) Расшифровать текст, 2) Позволяет ли успешный криптоанализ данного сообщения раскрыть ключ шифрования?

Контрольная работа № 2

Задача. Рассмотрим MAC Картера-Вегмана (Carter--Wegman MAC) ICW =(SCW,VCW), который строится на основе стойкого одноразового MAC I=(S,V) и стойкой PRF функции F(k,m). Проверочное значение tag формируется по

правилу: tag = SCW((k1, k2), m) = (r, F(k1, r) S(k2, m)), r R ← {0,1} n Построить функцию верификации для проверки сообщения VCW(m,tag).

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Вопросы к Экзамену

1. Предмет и задачи. Определение шифра, понятие стойкости.
2. Предположения об исходных условиях криптоанализа.
3. Симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы.
4. История криптографии. Криптография древности, частотный критоанализ.
5. Криптография нового времени.
6. Криптография XX века. Принцип Керкгоффса.
7. Понятие абсолютной стойкости или теоретико-информационной стойкости. Одноразовый блокнот.
8. Понятие псевдослучайности.
9. Поточные шифры. Синхронные и самосинхронизирующиеся шифры.
10. Требования к поточным шифрам: Постулаты Голомба, профиль линейной сложности.
11. Методы построения больших периодов в поточных шифрах. Регистры сдвигов с линейнойобратной связью.
12. Статистические тесты.
13. Семантическая стойкость. CPA модель атаки.
14. Требования к блочным шифрам. PRP и PRF.
15. Способы построение блочных шифров: подстановки, перестановки, сети фейстеля.
16. Примеры симметричных шифров: DES, AES. 10
17. Подходы к криптоанализу: линейный, дифференциальный, «встреча посередине».
18. Режимы использования блочных шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров).
19. Детерминированные и недерминированные алгоритмы шифрования.
20. Влияние случайности на стойкость. Слабости блочных шифров.
21. Контроль целостности. MAC. Определение, модель безопасности. Построение на базе Блоковых шифров.
22. HMAC. Хэш-функции. Требования к хэш-функциям.
23. Аутентифицированное шифрование.
24. CCA модель атаки. Примеры активных атак.
25. Понятие алгоритма с открытым ключом.
26. Схема RSA. Атаки на RSA.
27. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана.
28. Управление ключами. Групповые ключи. Попарные ключи. Использование мастер ключей.
29. Протоколы обмена ключами. С сервером, без сервера.
30. Известные атаки на протоколы обмена ключами.
31. K-надежные схемы распределения ключей.
32. Протоколы разделения секрета.
33. Пороговая криптография.
34. Протоколы цифровых денег и электронного голосования.
35. Слепая подпись.
36. Схема идентификации Schnorr – Shamir.
37. Схема идентификации Feige – Fiat – Shamir.
38. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы).
39. Понятие анонимности пользователей. Постановки задачи. PIR (протоколы конфиденциального получения информации).

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1. Контроль целостности передаваемых по сетям данных осуществляется посредством …

электронной цифровой подписи
аутентификации данных
аудита событий
межсетевого экранирования

2. Преобразовательный процесс, в ходе которого исходный текст, который носит также название открытого текста, заменяется измененным текстом, называется

шифрование
дешифрование
преобразование
искажение
кодирование
хеширование

3. Процесс, в ходе которого шифрованный текст преобразуется в исходный, называется …

шифрование
дешифрование
преобразование
искажение

4. Информация, необходимая для беспрепятственного шифрования и дешифрования текстов, называется …

ключ
шифр
код
пароль

5. Характеристика шифра, определяющая его стойкость к шифрованию без знания ключа, называется …

криптостойкостью
пароль
аудентификатор
шифратор

6. Асимметричное шифрование для шифрования и расшифровки использует …

один открытый ключ и один закрытый ключ
один открытый ключ
один закрытый ключ
один и тот же ключ
два открытых ключа
два закрытых ключа

7. Асимметричное шифрование для шифрования использует … ключ.

открытый
закрытый

8. Асимметричное шифрование для расшифровки использует … ключ.

закрытый
открытый

9. При симметричном шифровании для шифрования и расшифровки используются …

два ключа разной длины
два разных по значению ключа
один и тот же ключ
два открытых ключа
два закрытых ключа
один открытый ключ и один закрытый ключ

10. Относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом, называется …

закрытый ключ шифрования
электронная цифровая подпись

вирусная маска
открытый ключ шифрования

11. Криптосистема включает …

алгоритм шифрования
набор ключей, используемых для шифрования
систему управления ключами
антивирусное ПО
межсетевой экран

12. Механизм безопасности, который является сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки , – …

регистрация и аудит
аутентификация
идентификация
VPN
межсетевой экран

13. Задачи криптосистемы: …

обеспечение конфиденциальности
обеспечение целостности данных
аутентификация данных и их источников
межсетевое экранирование
защита от вирусов

14. Функции управления криптографическими ключами: …

генерация
хранение
распределение
изучение
уничтожение

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).