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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.46 Криптографические протоколы

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем и сетей

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Степанец Юлия Александровна, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:

НМС факультета ПММ, протокол № 5 от 22.03.2024

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

9. Цели и задачи учебной дисциплины

Целью является теоретическая и практическая подготовка специалистов к деятельности, связанной с анализом и синтезом криптографических протоколов.

Задачи освоения дисциплины: изучение основных свойств, характеризующих защищенность криптографических протоколов, и основных механизмов, применяемых для обеспечения выполнения того или иного свойства безопасности протокола; приобретение навыков поиска уязвимостей протоколов.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

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)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.7	Знает типовые криптопротоколы, используемые в сетях связи.	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.
		ОПК-10.8	Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем.	
		ОПК-10.9	Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.	
		ОПК-10.10	Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств.	
		ОПК-10.11	Владеет подходами к разработке и анализу безопасности криптографических протоколов.	
		ОПК-10.20	Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.	

12. Объем дисциплины в зачетных единицах/час - 4/144.
Форма промежуточной аттестации - экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			8			
Аудиторные занятия	56		56			
в том числе: лекции	28		28			
Практические	0		0			
Лабораторные	28		28			
Самостоятельная работа	52		52			
Контроль	36		36			
Итого:	144		144			
Форма промежуточной аттестации	Экзамен		Экзамен			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Протоколы распределения ключей	Протоколы и их классификация. Обмен ключами средствами симметричной криптографии. Протоколы открытого распределения ключей. Протоколы передачи секретного ключа по открытому каналу.	Криптографические протоколы (10.05.01)
1.2	Аутентификация	Аутентификация при входе в систему. Вручение битов на хранение. Бросание монеты по телефону. Доказательство с нулевым разглашением. Схемы аутентификации.	
1.3	Дополнительные промежуточные протоколы	Разделение секрета. Скрытый канал связи. Мысленный покер. Мысленный покер с тремя игроками.	
2. Лабораторные работы			
2.1	Работа с протоколами	Разработка модулярного калькулятора. Протоколы с нулевым разглашением. Протоколы удалённой аутентификации.	Криптографические протоколы (10.05.01)

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Распределение ключей.	10		0	16	8	34
1.2	Аутентификация.	10		0	14	8	32
1.3	Дополнительные промежуточные протоколы.	8		0	10	8	26
2.1	Работа с протоколами	0		28	12	12	52
	Итого:	28		28	52	36	144

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. – Санкт-Петербург : ПГУПС, [б. г.]. – Часть 1 – 2017. – 64 с. – ISBN 978-5-7641-1053-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111765 (дата обращения: 10.02.2020). – Режим доступа: для авториз. пользователей.
2	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. – Санкт-Петербург : ПГУПС, 2018 – Часть 2 – 2018. – 63 с. – ISBN 978-5-7641-1215-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/138103 (дата обращения: 10.02.2020). – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. – Самара : ПГУТИ, 2019. – 68 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/223319 (дата обращения: 20.01.2020). – Режим доступа: для авториз. пользователей.
4	Салий В. Н. Криптографические методы и средства защиты информации / В. Н. Салий. – 2010. (URL:http://www.sgu.ru/files/nodes/11017/V.N._Saliy._Kriptograficheskie_metody_i_sredstva_zashchity_informacii.doc) (дата обращения: 12.05.2019)

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

№ п/п	Источник
5	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
7	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа

студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

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

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Криптографические протоколы (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.
Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.
Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Распределение ключей.	ОПК-10	ОПК-10.7-10, 20	Контрольная работа
2	Аутентификация.	ОПК-10	ОПК-10.7-10, 20	Контрольная работа
3	Дополнительные промежуточные протоколы.	ОПК-10	ОПК-10.7-10, 20	Контрольная работа
4	Работа с протоколами	ОПК-10	ОПК-10.9-11, 20	Лабораторные работы
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- контрольные работы,
- лабораторные работы.

Перечень контрольных работ

1. Протоколы и их классификация.
2. Обмен ключами средствами симметричной криптографии.
3. Протоколы открытого распределения ключей.
4. Протоколы передачи секретного ключа по открытому каналу.
5. Аутентификация при входе в систему.
6. Вручение битов на хранение.
7. Бросание монеты по телефону.
8. Доказательство с нулевым разглашением.
9. Схемы аутентификации.
10. Методы разделения секрета.
11. Скрытый канал связи.
12. Мысленный покер.
13. Мысленный покер с тремя игроками.

Технология проведения

Студент выбирает вариант задания, ориентируясь на номер зачетки (последняя цифра). Студент выполняет предложенное преподавателем задание, представляет его в письменном виде, при необходимости, комментирует выполненные действия, анализирует и интерпретирует результаты. В курсе предусмотрено две контрольные работы (две темы из списка).

Критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Все задания контрольной работы выполнены, арифметических и логических ошибок нет, показано владение терминологией.	Повышенный уровень	Отлично
Все задания контрольной работы выполнены, но имеют место быть незначительные ошибки (арифметические, логические, в терминологии).	Базовый уровень	Хорошо
Не все задания контрольной работы выполнены и имеют место быть несущественные ошибки (арифметические, логические, в терминологии).	Пороговый уровень	Удовлетвори-тельно
Задания контрольной работы не выполнены или имеют место быть существенные ошибки (арифметические, логические, в терминологии).	–	Неудовлетво-рительно

Перечень лабораторных работ

1	Лабораторная работа №1 Тема: разработка модулярного калькулятора.	*Теоретические сведения* 1. Основные понятия и свойства модулярной арифметики. 2. Операции сравнения по модулю. 3. Обратные по модулю величины. 4. Возведение в степень по модулю. *Практическая часть* Реализация модулярного калькулятора на одном из языков программирования.

2	Лабораторная работа №2 Тема: Протоколы с нулевым разглашением.	*Теоретические сведения* 1. Определение и свойства протоколов с нулевым разглашением. 2. Протокол Гиллу - Кискатра. 3. Протокол Фиата - Шамира. 4. Протокол Шнорра. *Практическая часть* 1. Реализация и исследование протоколов. 2. Подготовка и защита отчёта по лабораторной работе.
3	Лабораторная работа №3 Тема: Протоколы удалённой аутентификации.	*Теоретические сведения* 1. Понятие аутентификации. 2. Механизмы аутентификации. 3. Механизмы предоставления прав. 4. Удалённая аутентификация. 5. Протоколы PAP, CHAP, S/KEY. *Практическая часть* 1. Реализация протоколов PAP, CHAP, S/KEY в виде приложения 2. Подготовка и защита отчёта по лабораторной работе.

Пример формирования задания к лабораторной работе

1. Ознакомиться с двумя протоколами открытого распределения ключей.
2. Изучить и привести описание одного из наиболее эффективных протоколов.
3. Реализовать с помощью ППП Maple или на каком либо языке программирования алгоритм Диффи-Хеллмана.
4. Разработать и реализовать алгоритм бросания монеты по телефону.
5. Ответить на контрольные вопросы.
6. Составить отчёт о проделанной работе.

Технология проведения

Все лабораторные работы обязательны для выполнение. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания и они правильные, даны пояснения);

оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к экзамену.

Перечень вопросов к экзамену (КИМ №1)

1. Перечислите режимы работы обучающей программы DES Tutorial.
2. Какова длина ключа алгоритма DES?
3. Что означает выражение "конкатенация битовых строк ассоциативна"?
4. Что представляет собой операция по модулю два?
5. Что такое криптология, криптограмма, криптография, криптоанализ?
6. В чем состоит основная идея шифрования данных?
7. В чем различие и в чем сходство шифрования и кодирования?

8. В чем различие терминов "дешифрование" и "расшифрование"?
9. Для решения каких задач используется кодирование информации?
10. Приведите алгоритм перехода от двоичной системы счисления к десятичной и наоборот.
11. Приведите алгоритм перехода от шестнадцатеричной системы счисления к десятичной и наоборот.
12. Опишите схему симметричного шифрования информации.
13. Что является аргументом функции шифрования F?
14. Приведите упрощённую схему алгоритма шифрования DES?
15. Приведите упрощённую схему алгоритма расшифрования DES?
16. Приведите схему реализации функции шифрования F.
17. Опишите алгоритм реализации "функций преобразования S(i).
18. Что означает фраза "процесс расшифрования данных является инверсным по отношению к процессу шифрования"?
19. Какие преобразования используются при реализации функции шифрования F(R,K)?
20. Какие биты ключа не влияют на шифрование? Для каких целей могут использоваться эти биты?
21. Расшифруйте сокращение "DES".
22. Почему (и какие?) программа добавляет символы к строкам, размеры которых не кратны восьми?
23. Для какой цели была разработана программа "DES Tutorial"?
24. Что такое криптостойкость? Каковы количественные характеристики криптостойкости?
25. Опишите алгоритм получения 48-битовых ключей K(i).Докажите, что таблица 2 ("конечная перестановка") является обратной поотношению к таблице 1 ("начальная перестановка").
26. Опишите упрощённую схему асимметричного шифрования.
27. Какова максимальная длина открытого текста в программе DES? Подтвердите экспериментально.
28. В чем разница между закрытой, секретной и конфиденциальной информацией?
29. Что такое цена и ценность информации?
30. Что подразумевается под эффективностью защиты информации?
31. Что такое система безопасности?
32. В чем заключаются постулаты безопасности?
33. Чем достигается обеспечение безопасности?
34. Что такое способы защиты информации?
35. Что такое пространственное, временное, структурное и энергетическое скрытие информации?
36. В чем состоят цели защиты информации?
37. Охарактеризуйте физические системы защиты информации.
38. На какие классы разделяются инженерно-технические средства защиты информации?
39. В чем проявляются угрозы информации?
40. Что такое инженерно-техническая защита информации?
41. Каким образом классифицируется инженерно-техническая защита информации?
42. Что такое информационная безопасность?
43. Что такое защита информации?
44. Перечислите возможные виды утечек информации.
45. Охарактеризуйте методы симметричного шифрования данных.
46. Что такое отношение сравнимости?

47. Что называется полным набором вычетов по модулю n (n - целое число)?
48. Сформулируйте основные законы модулярной арифметики.
49. Что представляет собой функция Эйлера?
50. В чем состоит теорема Эйлера?
51. Сформулируйте малую теорему Ферма.
52. Как найти функцию Эйлера $\varphi(\prod_{i=1}^{n} p_i^{r_i})$, где p_i - простые числа, n и r_i - натуральные числа?
53. Дайте определение величины, обратной целому числу a по модулю n.
54. Охарактеризуйте основные способы нахождения обратных по модулю величин.
55. Что такое дискретный логарифм? В чем заключается проблема дискретного логарифмирования?
56. Дайте определение криптосистемы (шифра).
57. Что такое криптосистема Эль Гамаля?

Критерии оценки ответов на вопросы экзамена

Для оценивания результатов обучения на экзамене используется - 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

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

ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

1) закрытые задания (тестовые, средний уровень сложности):

1. Отношение $a \equiv b\ (mod\ n)$ выполняется если
   a) $a = b + kn,\ \ k, a, b, n \in Z,\ \ a, b, n \neq 0$
   b) $a = log_k\ b\ ,\ \ k, a, b, n \in Z,\ \ a, b, n \neq 0$
   c) $a = b^k mod\ n,\ \ k, a, b, n \in Z,\ \ a, b, n \neq 0$
   d) $a = k^b mod\ n,\ \ k, a, b, n \in Z,\ \ a, b, n \neq 0$
2. Для функции Эйлера справедливо $\varphi(n) = (p-1)(q-1)$, если:
   a) $p^{\varphi(n)} \equiv q\ mod\ n$
   b) p и q простые множители n
   c) $\forall (x, p) = 1\ \ x^q \equiv x\ mod\ p$
   d) $\forall\ x \in GF(p),\ x \neq 0\ x^{q-1} \equiv 1\ mod\ p$
3. Дискретное логарифмирование является обратной задаче для:
   a) Факторизации
   b) Нахождения модульной экспоненты
   c) Разложения числа на простые множители
   d) Нахождения значения функции Эйлера
4. К проблемам симметричных шифров не относятся:
   a) Задача распространения ключей
   b) Обеспечение подлинности
   c) Низкая криптостойкость
   d) Рост количества ключей при росте числа абонентов
5. К ассиметричным криптосистемам относятся:
   a) AES
   b) Алгоритм Диффи-Хеллмана
   c) Алгоритм Эль-Гамаля
   d) RSA
6. Необходимым условием для использования функции в качестве односторонней является:
   a) Теоретическая необратимость
   b) Практическая необратимость
   c) Практическая и теоретическая необратимость
   d) Ни одно из перечисленных
7. Задача разложения большого целого числа на множители называется:
   a) Дискретным логарифмированием
   b) Нахождением вычетов по модулю
   c) Факторизацией
   d) Задачей Ферма
8. Функция $f: X \to Y$, удовлетворяющая условию $\exists t\ \exists g(y, t): g(y, t) = f^{-1}(y)$, где g(y,t) вычислима за полиномиальное время для t называется:
   a) Односторонней функцией с ловушкой t
   b) Теоретически необратимой функцией с открытым параметром t
   c) Односторонней функцией с ловушкой g
   d) Теоретически необратимой функцией с открытым параметром g
9. Какие из криптосистем не используются в режиме цифровой подписи?
   a) RSA
   b) Эль-Гамаля
   c) Диффи-Хеллмана
   d) SHA

10. Закрытым ключом в алгоритме RSA является:
    a) Произвольно выбранное число, взаимно простое со значением функции Эйлера
    b) Мультипликативно обратное число, вычисленное по алгоритму Евклида
11. Открытый ключ в схеме Эль-Гамаля получают при помощи:
    a) Выбора произвольного целого числа, меньшего чем открытый параметр
    b) Выбора числа, взаимно простого со значением функции Эйлера
    c) Определением образующего элемента поля
    d) Решением задачи дискретного логарифмирования
12. Алгоритм Рабина основан на алгоритме:
    a) Диффи-Хеллмана
    b) Эль-Гамаля
    c) RSA
    d) AES
13. Алгоритм Рабина-Миллера является способом:
    a) Проверки числа на простоту
    b) Разложения числа на сомножители
    c) Решения задачи дискретного логарифмирования
    d) Вычисления функции Эйлера
14. Частью стандартного протокола ЭЦП на основе ассиметричной криптосистемы не является:
    a) Шифрование значения хеш-функции
    b) Пересылка сообщения доверенному посреднику
    c) Генерация заголовка с идентификационной информацией
    d) Передача адресату документа и его зашифрованной свертки
15. От схем ассиметричного шифрования ЭЦП отличатся тем, что:
    a) Требует доверенного посредника
    b) Криптосистему формирует отправитель
    c) Не может использоваться совместно с шифрованием
    d) Не требует теоретической необратимости односторонних функций
16. К основным требованиям к хеш-функции не относятся:
    a) Низкая вероятность совпадения дайджеста разных документов
    b) Необратимость
    c) Однозначность
    d) Устойчивость к поиску коллизий
17. Отличие криптопротокола от криптосистемы по Шеннону состоят в:
    a) Недоверии участников криптообмена друг другу
    b) Возможность интерактивности
    c) Высокие требования к скорости информационного обмена
    d) Низкие требования к надежности шифрования
18. Протоколы аутентификации являются:
    a) Частным случаем интерактивных систем доказательства
    b) Развитием схемы византийского соглашения
    c) Модификацией схемы Шнорра
    d) Групповыми криптопротоколами
19. Закрытый ключ в ассиметричном шифровании является:
    a) Значением функции Эйлера для открытого ключа
    b) Модульной экспонентой открытого ключа
    c) Наибольшим вычетом по модулю открытого параметра шифрования
    d) Ловушкой односторонней функции
20. Системы с открытым ключом не используются:
    a) Для распределения закрытых ключей симметричных криптосистем
    b) Для скрытой передачи информации
    c) Для аутентификации
    d) Как самостоятельные криптосистемы
21. Теоретически односторонними преобразованиями являются:
    a) Факторизация

b) Логарифмирование в конечном поле
c) Модульная экспонента
d) Ни одно из перечисленных

22. В качестве односторонней функции в криптосистеме RSA выступает:
a) Функция Эйлера
b) Дискретное логарифмирование
c) Модульная экспонента
d) Свертка хеш-функцией

23. Обобщенная модель ассиметричного шифра определяется:
a) Алгеброй криптопреобразования A(X, K,Y,f)
b) Алгебрами прямого $A_E(X, K_E, Y, E)$ и обратного $A_D(Y, K_D, X, D)$ криптопреобразования
c) Алгебрами прямого $A_E(X, K_E, Y, E)$ и обратного $A_D(Y, K_D, X, D)$ криптопреобразования и функцией $f: K_E \to K_D$
d) Алгебрами прямого $A_E(X, K_E, Y, E)$ и обратного $A_D(Y, K_D, X, D)$ криптопреобразования и функциями $f: K_E \to K_D$ и $g: K_D \to K_E$

24. Управление ключами включает:
a) Генерацию ключей
b) Распределение ключей
c) Хранение ключей
d) Все перечисленное

25. Неравносильные ключи это:
a) Уязвимость криптосистемы DSA
b) Уязвимость всех ассиметричных криптосистем
c) Способ обеспечения разной криптостойкости для ключей различного вида
d) Способ разграничения доступа к устройству подписи сертификатов

26. Коллаборативная атака на центр сертификации реализуется посредствам:
a) Подделки истекшего сертификата
b) Получения сертификата через инсайдера
c) Изменение периодичности ресертификации
d) Перехват сертификата «человеком посередине»

27. Метод блуждающих ключей это:
a) Способ атаки на ЦРК
b) Способ подделки ЭЦП
c) Способ обновления ключей
d) Способ распределения ключей

28. Интеллектуальные карточки используются для:
a) Генерации ключей
b) Резервирования ключей
c) Распределения ключей при централизованном управлении
d) Распределения ключей при распределенном управлении

29. Сертификат открытого ключа абонента это:
a) ЭЦП владельца ключа
b) ЭЦП доверенного участника обмена
c) ЭЦП получателя сообщения
d) Временная метка ключа

30. Депонирование ключа это
a) Схема генерации сеансовых ключей
b) Схема сокрытия информации от оракула
c) Часть протокола аутентификации
d) Способ резервирования ключа

31. Основными недостатками программной реализации шифрования являются:
a) Низкая производительность
b) Отсутствие механизма экстренного уничтожения ключа
c) Вытеснение ключевой информации из ОЗУ на жесткий диск
d) Сложность распараллеливания процесса шифрования

32. Алгоритм Рабина является разновидностью схемы:
    a) Эль-Гамаля
    b) DSA
    c) RSA
    d) AES
33. Необратимость криптопреобразования RSA обеспечивается:
    a) Приведением по модулю секретного параметра при шифровании открытого текста
    b) Приведением по модулю функции Эйлера при шифровании открытого текста
    c) Приведением по модулю функции Эйлера при вычислении закрытого ключа
    d) Приведением по модулю функции Эйлера при вычислении открытого ключа
34. Функция построения ЭЦП легко вычисляется по:
    a) Отрытому ключу
    b) Закрытому ключу
    c) Функции Эйлера открытого параметра
    d) Дайджесту хеш-функции открытого текста
35. С ростом времени действия ключа потери при его компрометации:
    a) Увеличиваются
    b) Снижаются
    c) Увеличиваются для централизованного и снижаются для распределенного управления
    d) Не изменяются

2) <u>открытые задания (тестовые, средний уровень сложности):</u>

1. Какое отношение выполняется между a и b, если выполняется $a = b + kn,\ \ k, a, b, n \in Z,\ \ \ a, b, n \neq 0$ Ответ: сравнимость по модулю n
2. Назовите наибольший общий делитель для взаимнопростых чисел a и b Ответ: 1
1. Какая задача обратна односторонней функции вычисления модульной экспоненты с фиксированным основанием и модулем? Ответ: дискретное логарифмирование
2. Какая схема управления ключами реализует разделении секретного ключа на компоненты, распределенные среди легальных абонентов, такое что восстановление возможно только при объединении некоторой части этих компонент? Ответ: разделение секрета
3. Назовите алгоритм хеширования, разработанный для совместного использования с DSA Ответ SHA
4. Какой из сторон обмена формируется закрытый ключ в схемах ЭЦП? Ответ отправитель
5. Сложность решения какой математической задачи определяет стойкость алгоритма RSA? Ответ: Факторизация
6. К какому классу криптопротоколов относится схема Шнорра? Ответ: аутентификация
7. Какая процедура осуществляется посредствам следующих вычислений $R_i = E_k(E_k(T_i) \oplus V_i)$, $V_{i+1} = E_k(E_k(T_i) \oplus R_i)$ где R_i - случайное число, E_k - шифрование на специальном ключе k, V_0 - секретная 64-битная стартовая последовательность, T – метка времени? Ответ: генерация сеансового ключа
8. Какой протокол резервирования ключа реализуется посредствам его восстановления из частей, распределенных между легальными абонентами? Ответ разделение секрета
9. Какой из видов ЭЦП является частным случаем сокрытия информации от «оракула»? Ответ слепая подпись
10. Решением какой задачи производится сравнение значений параметра у различных абонентов без раскрытия этих значений при защищенных вычислениях? Ответ задача о двух миллионерах
11. Какая атака позволяет фальсифицировать ЭЦП RSA без знания закрытого ключа при определенном значении его хеш-функции? Ответ мультипликативная атака
12. Частным случаем каких протоколов являются протоколы аутентификации? Ответ Интерактивная система доказательства

13. Какой криптопротокол реализуется симметричной криптосистемой, такая что $D_k(f(E_k(x))) = f(x)$, где k – случайный секретный ключ, E_k, D_k – прямое и обратное криптопреобразование, f(x) – трудновычислимая целевая функция, x – секретный аргумент? Ответ сокрытие информации от оракула
14. Каким математическим объектом представляется «тень» в схеме Блекли разделения секрета? Ответ гиперплоскость

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