

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:

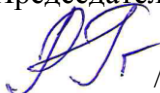
на заседании кафедры

протокол № 7 от « 18 » февраля 2022 г.

Зав. кафедрой etsef- /Исмагилова А.С.

Согласовано:

Председатель УМК института

 / Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина

Криптографические методы защиты информации

Часть, формируемая участниками образовательных отношений (Б1.В.ДВ.03.01)

программа специалитета

Специальность


10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация

«Организация и технологии защиты информации (по отраслям)»

Квалификация

специалист по защите информации

Разработчик (составитель) _____.	 / <u>Салов И.В.</u>
-------------------------------------	--

Для приема: 2022г.

Уфа 2022 г.

Составитель: Салов Игорь Владимирович

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол от « 18 »
февраля _____ 2022 г. № 7

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на
заседании
кафедры _____

протокол № _____ от « _____ » _____ 20 __ г.

Заведующий кафедрой / Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на
заседании
кафедры _____

протокол № _____ от « _____ » _____ 20 __ г.

Заведующий кафедрой _____ / Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на
заседании _____ кафедры

протокол № _____ от « _____ » _____ 20 __ г.

Заведующий кафедрой _____ / _____ Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на
заседании _____ кафедры

протокол № _____ от « _____ » _____ 20 __ г.

Заведующий кафедрой _____ / _____ Ф.И.О./

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций 4
2. Цель и место дисциплины в структуре образовательной программы 4
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся) 4
4. Фонд оценочных средств по дисциплине 5
 - 4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине. 5
 - 4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине. 10
5. Учебно-методическое и информационное обеспечение дисциплины 21
 - 5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 21
 - 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы 21
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 24

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
Организационно-управленческая	ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.	ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
		ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
		ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 4 курсе в 7 семестре.

Целью учебной дисциплины «Криптографические методы защиты информации», является формирование требований по применению криптографических методов в защите информации и политике безопасности компьютерных систем и сетей.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций индикаторов достижения компетенций с указанием соотношенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

ПК-1.Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Не знает или показывает очень слабые знания.	Знает некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей., но допускает ошибки при их применении.	Знает некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Не умеет.	Умеет применять некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Умеет применять некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.

			информации и политики безопасности компьютерных систем и сетей, но допускает при этом ошибки.	информации и политики безопасности компьютерных систем и сетей.	политики безопасности компьютерных систем и сетей.
ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Не владеет.	Владеет методикой формирования основных требований по защите информации и политики безопасности компьютерных систем и сетей, но допускает ошибки при ее использовании.	Владеет методикой формирования основных требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и	Знать основные принципы, методы и этапы формирования требования по защите информации и политики	тестирование, практическое задание; лабораторная работа

политики безопасности компьютерных систем и сетей.	безопасности компьютерных систем и сетей.	
ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	тестирование, практическое задание; лабораторная работа
ПК-1.3 Владет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	тестирование, практическое задание; лабораторная работа

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины «Криптографические методы защиты информации»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Симметричные шифры.				
Текущий контроль				
Лабораторная работа	3	5	0	15
Практическая работа	3	5	0	15
Рубежный контроль				
Тест	10	1	0	10
Всего			0	40

Модуль 2. Асимметричные шифры				
Текущий контроль				
Лабораторная работа	3	4	0	12
Практическая работа	3	4	0	12
Рубежный контроль				
Тест	6	1	0	6
Всего			0	30
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2. Публикация научной статьи	4	1	0	4
3. Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1. Экзамен	30	1	0	30

Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Экзаменационные материалы

1. Виды криптосистем.
2. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели и свойства.
4. Частотные характеристики открытых сообщений.
5. Критерии на открытый текст.
6. Особенности нетекстовых сообщений.
7. Классификация шифров.
8. Классификация шифров по области применения.
9. Кодирование.
10. Классификация шифров по особенностям алгоритма шифрования.
11. Классификация шифров по количеству символов сообщения.
12. Этапы криптографии.
13. Шифры наивной криптографии.
14. Шифр Цезаря.
15. Полибианский квадрат.
16. Шифр «Решетка».
17. Шифр Виженера.
18. Шифр Плейфера.
19. Шифр Хилла.
20. Шифр Вернама.
21. Шифр Хагелина.
22. Машина шифрования Enigma.
23. Блочные и поточные шифры.

24. Лавинный эффект.
25. Поточные шифры.
26. Избыточность информации.
27. Ненадежность шифра и расстояние единственности.
28. Модель криптоаналитика.
29. Классификация блочных шифров.
30. Режим шифрования.
31. Режим простой замены ECB.
32. Режим шифрования с зацеплением CBC.
33. Режим обратной связи по шифротексту CFB.
34. Режим шифрования с обратной связью по выходу OFB (гаммирование или внутренняя обратная связь).
35. Сцепление блоков шифротекста с распространением ошибки (PCBC).
36. Counter mode (CTR) режим счетчика.
37. Режим счетчик с аутентификацией Галуа (Galois/CounterMode GCM).
38. Аутентифицированное шифрование с присоединёнными данными (AEAD-режим блочного шифрования).
39. Ячейка Фестеля.
40. Сеть Фейстеля.
41. Алгоритм Blowfish.
42. Шифр DES.
43. ГОСТ 28147–89 Системы обработки информации.
44. Защита криптографическая.
45. Алгоритм криптографического преобразования.
46. Шифр AES.
47. Процедура расширения ключа.
48. Шифр IDEA.
49. Многократное шифрование блоков.
50. Атаки на блочные шифры.
51. Режимы использования блочных шифров.
52. Классификация поточных шифров.
53. Синхронные поточные шифры.
54. Самосинхронизирующиеся (асинхронные поточные шифры АПШ) поточные шифры.
55. Генерация случайных и псевдослучайных последовательностей.
56. Криптографически безопасные псевдослучайные последовательности.
57. Настоящие случайные последовательности.
58. Детерминированные генераторы простых случайных чисел.
59. Анализ генераторов псевдослучайных чисел.
60. Регистр сдвига с линейной обратной связью (РСЛОС, англ.
61. Linearfeedbackshiftregister, LFSR).
62. Линейная сложность.
63. Нелинейные регистры сдвига с обратной связью.
64. Нелинейная комбинация генераторов.
65. Линейное и предварительное шифрование.
66. Шифр A5.
67. Гаммирование.
68. Шифр RC 4.
69. Атаки на поточные шифры.
70. Характеристики имитостойкости.
71. Методы обеспечения имитостойкости шифров.
72. Совершенная имитостойкость.
73. Связь между имитостойкостью по Симмонсу и секретностью по Шеннону.
74. Понятие кода аутентификации и его свойства имитостойкости и секретности.

75. Назначение и конструкция кодов аутентификации и защитных контрольных сумм.
76. Требования к хэш-функциям.
77. Криптографическая стойкость хэш-функций.
78. Коллизии.
79. Применение хэш-функций.
80. Подходы к проектированию хэш-функций.
81. Алгоритмы выработки хэш-функций.
82. Хэш-функции на основе блочного шифра.
83. Ключевые хэш-функции.
84. Стандарт на хэш-функции: ГОСТ Р 34.11-94
85. Алгоритм SHA.
86. Криптография открытого ключа.
87. Понятие односторонней функции и односторонней функции с "лазейкой".
88. Проблемы факторизации целых чисел и логарифмирования в конечных полях.
89. Криптосистема Диффи-Хэллимана.
90. Криптосистемы RSA, Эль-Гамала, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер.
91. Рюкзачные шифры.
92. Классификация криптографических протоколов.
93. Классификация криптографических протоколов по характеру разрешения спорных вопросов.
94. Классификация криптографических протоколов по типу используемых криптографических примитивов.
95. Классификация криптографических протоколов по числу участников.
96. Классификация криптографических протоколов по числу передаваемых сообщений.
97. Классификация криптографических протоколов по функциональному (целевому) назначению.
98. Классификация криптографических протоколов по сложности.
99. Классификация криптографических протоколов по области применения.
100. Криптографические примитивы.
101. Криптографические примитивы с секретным ключом.
102. Криптографические примитивы с открытым ключом.
103. Управление криптографическими ключами.
104. Генерация ключей.
105. Накопление ключей.
106. Цели управления ключами.
107. Политика безопасности управления ключами.
108. Сроки действия ключей.
109. Жизненный цикл ключей.
110. Управление ключами, основанное на системах с открытым ключом.
111. Протокол обмена секретным ключом.
112. Использование сертификатов.
113. Протокол распределения ключей.
114. Временные данные.
115. Разновидности временных данных Симметричные протоколы.
116. Однопроходовой key transport.
117. Challenge Response.
118. Authenticated Key Exchange Protocol.
119. Протокол Шамира.
120. Протоколы, использующие центр сертификации (доверенный центр) или сервер.
121. Лягушка с открытым ртом.
122. Протокол Нидхем-Шрёдера на симметричных ключах.
123. Протокол Kerberos.

124. The Kerberos Ticket.
125. Протокол Отвея-Рииса.
126. Алгоритм DASS.
127. Асимметричные протоколы.
128. Протокол Нидхема-Шрёдера на асимметричных ключах.
129. Электронная подпись.
130. Алгоритм X.509.
131. Хэш функция.
132. Однонаправленные хэш-функции.
133. Алгоритм MD4.
134. Алгоритм MD5.
135. Алгоритм MD2.
136. Алгоритм безопасного хэширования (SecureHashAlgorithm, SHA).
137. Алгоритм RIPE-MD.
138. Алгоритм HAVAL.
139. Однонаправленные хэш-функции, использующие симметричные блочные алгоритмы.
140. Стандарт хэш-функций ГОСТ Р 34.11-2012.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
КАФЕДРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Криптографические методы защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Классификация шифров по области применения.
2. Асимметричные протоколы.

Зав. Кафедрой УИБ

А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме.

Необходимо выбрать один или несколько ответов из предложенных вариантов.

Тест №1

Модуль 1. Симметричные шифры.

1. Симметричный шифр, оперирующий группами бит фиксированной длины, это:

а) Блочный шифр;

б) Поточный шифр;

в) Комбинированный шифр;

г) Шифр с гаммированием;

2. Математическая или иная функция, которая для строки произвольной длины

вычисляет некоторое целое значение или некоторую другую строку фиксированной длины называется:

а) Электронной цифровой подписью;

б) Односторонней функцией;

в) Односторонней функцией с ловушкой;

г) Хеш-функцией;

3. Передача информации в реальном режиме времени более характерна для:

а) Поточного шифра;

б) Блочного шифра;

в) Шифра с симметричными ключами;

г) Шифрами с асимметричными ключами;

4. Какое свойство не относится к криптографическому генератору псевдослучайных чисел:

- а) Период последовательности должен быть очень большой;
- б) Порождаемая последовательность должна быть "почти" неотличима от

действительно случайной;

- в) Вероятности порождения различных значений должны быть в точности равны;

г) Зная первые k битов случайной последовательности, с вероятностью более 50 % мы можем предсказать $(k+1)$ -ый бит;

5. Минимальный объем шифртекста, при котором ненадежность ключа равна или близка к нулю, называется:

- а) Имитостойкостью;
- б) Расстоянием единственности;**

в) Надежностью шифра;

г) Оценкой криптостойкости;

6. Р-блоки это:

а) Блоки перестановки;

б) Блоки замены;

в) Блоки рассеивания;

г) Блоки криптостойкости;

7. Какое свойство относится к синхронным поточным шифрам:

а) Плюсом является размешивание статистики открытого текста;

б) Минусом является распространение ошибки (каждому неправильному биту шифротекста соответствуют N ошибок в открытом тексте);

в) Минусом является чувствительность к вскрытию повторной передачей;

г) Плюсом является предохранение от любых вставок и удалений шифротекста;

8. Какое свойство не относится к криптографически безопасной псевдослучайной последовательности:

а) Проходит все тесты на случайность, которые нам удалось найти;

б) Очень трудно (с точки зрения применения вычислительных мощностей) предсказать, каким будет следующий случайный бит, даже если полностью известен алгоритм или устройство, генерирующее последовательность, и все предыдущие биты потока;

в) Последовательность не может быть уверенно воспроизведена. Если вы запускаете генератор случайных чисел дважды с одним и тем же входом (по крайней мере, насколько это в человеческих силах), то вы получите две совершенно независимые случайные последовательности;

г) Последовательность может быть уверенно воспроизведена. Если вы запускаете генератор случайных чисел дважды с одним и тем же входом (по крайней мере, насколько это в человеческих силах), то вы получите две совершенно одинаковые последовательности;

9. Обратную связь по шифротексту реализует режим:

а) CBC;

б) ECB;

в) CFB;

г) OFB;

10. Для регистра сдвига с линейной обратной связью (РСЛОС, Linearfeedbackshiftregister, LFSR) характерно:

а) Состоит из двух пронумерованных ячеек, каждая из которых способна хранить бит и имеет один вход и один выход;

б) На выходе регистра оказывается один, обычно старший, значащий бит;

в) Функция обратной связи представляет собой сумму по модулю 2 (xor) некоторых битов регистра, называемых отводами;

г) Когда нужно извлечь бит, все биты регистра сдвигаются влево на одну позицию;

11. Алгоритм DES это:

- а) Симметричный алгоритм шифрования, использующий эллиптические кривые;
- б) Симметричный алгоритм шифрования, использующий сеть Фейстеля;**
- в) Симметричный алгоритм шифрования, использующий функцию с ловушкой;
- г) Симметричный алгоритм шифрования, использующий метод квантовой

неопределенности;

12. Алгоритм шифрования A5 это:

а) Поточный алгоритм шифрования, основанный на побитовом сложении по модулю два («исключающее или») генерируемой псевдослучайной последовательности и шифруемой информации. Псевдослучайная последовательность реализуется на основе трёх линейных регистров сдвига с обратной связью. Регистры имеют длины 19, 22 и 23 бита соответственно;

б) Симметричный блочный алгоритм шифрования данных в котором данные шифруются блоками по 64 бита, а ключ шифрования алгоритма имеет размер 128 битов. Блок шифруемых данных разбивается на 4 16-битных субблока, над которыми выполняется 8 раундов преобразований;

в) Блочный шифр с 256-битным ключом и 32 циклами преобразования, оперирующий 64-битными блоками;

г) Поточный алгоритм шифрования, основанный на побитовом ячеек открытого текста и генерируемой псевдослучайной. Псевдослучайная последовательность реализуется на основе трёх линейных регистров сдвига с обратной связью. Регистры имеют длины 19, 22 и 23 бита соответственно;

13. Для алгоритма RC4 характерно:

а) Основан на «наложении» гамма– последовательности на открытый текст;

б) Вместо случайной гаммы наложения используется псевдослучайная последовательность, напрямую зависящая от ключа;

в) Обычно гаммирование заключается в суммировании в каком– либо конечном поле, зачастую используются логические функции;

г) Все перечисленное;

14. ГОСТ 28147-89 это:

а) Поточный шифр с 128-битным ключом и 64 циклами преобразования, оперирующий 256-битными блоками;

б) Блочный шифр с 128-битным ключом и 64 циклами преобразования, оперирующий 256-битными блоками;

в) Блочный шифр с 256-битным ключом и 32 циклами преобразования, оперирующий 64-битными блоками;

г) Блочный шифр с 128-битным ключом и 64 циклами преобразования, оперирующий 32-битными блоками;

15. Симметричный алгоритм AES (AdvancedEncryptionStandard) принятый в качестве стандарта шифрования в США имел следующее отличие от исходного алгоритма Rijndael:

а) Использовал ключ только размером 128 бит;

б) Использовал ключ только размером 256 бит;

в) Работал только с блоками размером 128 бит;

г) Работал только с блоками размером 192 бита;

16. В какой последовательности выполняются операции в раунде алгоритма AES:

а) AddRoundKey, SubBytes, ShiftRows, MixColumns;

б) AddRoundKey, ShiftRows, MixColumns, SubBytes;

в) SubBytes, ShiftRows, MixColumns, AddRoundKey;

г) MixColumns, SubBytes, ShiftRows, AddRoundKey;

17. Алгоритм IDEA (International Data Encryption Algorithm) это:

а) Симметричный блочный алгоритм шифрования данных в котором данные шифруются блоками по 64 бита, а ключ шифрования алгоритма имеет размер 128

битов. Блок шифруемых данных разбивается на 4 16-битных субблока, над которыми выполняется 8 раундов преобразований;

б) Симметричный блочный алгоритм шифрования данных в котором данные шифруются блоками по 128 бит, а ключ шифрования алгоритма имеет размер 64 бита. Блок шифруемых данных разбивается на 16 4-битных субблоков, над которыми выполняется 64 раунда преобразований;

в) Симметричный поточный алгоритм шифрования данных с длиной ключа 64 бита;

г) Симметричный блочный алгоритм шифрования данных в котором данные шифруются блоками по 8 бит, а ключ шифрования алгоритма имеет размер 64 бита. Блок шифруемых данных разбивается на 4 64-битных субблока, над которыми выполняется 64 раунда преобразований;

18. Укажите атаку, которая характерна не только для блочных шифров:

а) Атака со связанным ключом;

б) Атака с избранным ключом;

в) Усеченный дифференциальный криптоанализ;

г) Корреляционная атака;

19. Дополнение неполного блока блочного шифра для достижения лавинообразного эффекта, целесообразней делать следующим фрагментом:

а) 000...000;

б) 111...111;

в) 000...001;

г) 111...000;

20. Наличие в алгоритме входных сообщений, дающих одинаковые хэш-коды называется:

а) Нелинейностью;

б) Ошибкой;

в) Диффузией;

г) Коллизией;

21. Ячейка Фейстеля характерна следующей логической операцией:

а) Исключающее или;

б) Или не;

в) И не;

г) Или;

22. S-блоки это:

а) Блоки перестановки;

б) Блоки замены;

в) Блоки рассеивания;

г) Блоки криптостойкости;

23. Для функции F в ячейке Фейстеля должно выполняться требования:

а) Ключ K должен совпадать для всех раундов;

б) Ключ K должен быть натуральным числом;

в) Нелинейность по отношению к операции XOR;

г) Не связанность входа и выхода;

24. В хэшировании по алгоритму ГОСТ Р 34.11-12 используется:

а) Алгоритм ГОСТ 34.10–2012 в режиме шифрования с зацеплением;

б) Используется функции сжатия, в основе которой лежат три преобразования: нелинейное биективное преобразование (обозначается S), перестановка байт (обозначается P), линейное преобразование (обозначается L);

в) Алгоритм ГОСТ 28147-89 в режиме шифрования с зацеплением;

г) Алгоритм ГОСТ 34.10–2001 в режиме простой замены;

25. Криптографический генератор псевдослучайных чисел:

а) Устройство, использующее физические процессы, для получения абсолютно случайного числа;

- б) Устройство, подбрасывающее монету;
- в) Алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются равномерному распределению;**
- г) Алгоритм, порождающий четко заданную последовательность зависимых друг от друга чисел;

Тест №2

Модуль 2. Асимметричные шифры.

1. Односторонняя функция с потайным входом (англ. trapdoorfunction) это:

а) Эффективно вычислимая функция, для обращения которой (т.е. для поиска хотя бы одного значения аргумента по заданному значению функции) имеются эффективные алгоритмы;

б) Функция, которая легко вычисляется в одном направлении, но трудно вычисляется в обратном без специальной информации (секрета), называемой «лазейкой» или «потайным входом»;

в) Функция нахождения генератора мультипликативной группы в конечном поле Галуа;

г) Воображаемая идеальная функция;

2. В качестве задач, приводящих к односторонним функциям, можно привести следующие:

а) Разложение числа на простые сомножители;

б) Все перечисленное;

в) Дискретное логарифмирование в конечном простом поле;

г) Сумма точек на эллиптических кривых;

3. Чем односторонняя функция с потайным входом (англ. trapdoorfunction) отличается от односторонней функции:

а) Разные названия одной и той же функции;

б) Одностороннюю функцию с потайным входом нельзя использовать в криптографии;

в) Одностороннюю функцию нельзя использовать в криптографии;

г) Для односторонней функции с потайным входом нет математического доказательства того, что она односторонняя;

4. Криптосистемы открытого ключа применяются в:

а) Цифровых подписях и вычислении хэш-функций;

б) Только в шифровании;

в) Шифровании и цифровых подписях;

г) Только в цифровых подписях;

5. Имеется ли в криптосистемах открытого ключа связь между приватным и открытым ключом:

а) Нет;

б) Открытый ключ получают с применением функции с потайным входом из приватного ключа;

в) Приватный ключ получают с применением функции с потайным входом из открытого ключа;

г) Нет правильного ответа;

6. Основной задачей протокола Диффи-Хелмана является:

а) Блочное шифрование сообщений с симметричным ключом;

б) Получение общего секретного ключа, используя незащищенный от прослушивания канал связи;

в) Поточное шифрование сообщений с симметричным ключом;

г) Вычисление хэш-функции сообщения;

7. К протоколу Диффи-Хелмана непосредственно относится следующая формула:

а) $K = g^{AB} \bmod p$;

б) $a=g^k \bmod p$ и $b=y^k \bmod p$;

в) $g=h^{\varphi-1/q} \bmod p$;

г) $s_i=\text{sqrt}(v_i-1) \pmod n$;

8. Криптосистема с открытым ключом, в основе которой лежит проблема трудности вычисления дискретных логарифмов в конечном поле:

а) Протокол Диффи-Хелмана;

б) Протокол ГОСТ Р 34.10-2001;

в) Протокол Эль-Гамала;

г) Протокол Фиата-Шамира;

9. В основе работы ГОСТ Р 34.10-2001 лежит:

а) Проблема трудности вычисления дискретных логарифмов в конечном поле;

б) Проблема вычисления дискретного логарифма в группе точек эллиптической кривой;

в) Проблема разложения числа на простые множители;

г) Проблема факторизации больших чисел;

10. К американскому стандарту DSS непосредственно относится следующая формула:

а) $K=g^{AB} \bmod p$;

б) $a=g^k \bmod p$ и $b=y^k \bmod p$;

в) $g=h^{\varphi-1/q} \bmod p$;

г) $s_i=\text{sqrt}(v_i-1) \pmod n$;

11. Какое отношение Уриель Фейге имеет к алгоритму Фиата-Шамира:

а) Полное название алгоритма Фейге-Фиата-Шамира;

б) Фейге позже присоединился к Фиату и Шамиру и участвовал в модификации указанного алгоритма, который затем получил название Фейге-Фиата-Шамира;

в) Фейге разработал алгоритм, который модифицировали Фиат и Шамир;

г) Фейге параллельно с Фиатом и Шамиром разработал указанный алгоритм;

12. Чем примечателен алгоритм Фейге-Фиата-Шамира:

а) Первый практический протокол идентификации, считается лучшим доказательством подлинности с нулевым разглашением;

б) Первый абсолютно стойкий протокол;

в) Первый практически стойкий протокол;

г) Да нет в нем ничего примечательного;

13. Протокол позволяющий убедить одного субъекта в том, что первый субъект обладает определенной информацией, не раскрывая её, называется:

а) Доказательство с нулевым разглашением;

б) Протокол управления цифровыми сертификатами;

в) Протокол управления ключами;

г) Криптографический протокол;

14. Алгоритм RSA примечателен тем, что:

а) Стал первым полноценным алгоритмом с открытым ключом, который может работать только в режиме шифрования данных;

б) Стал первым полноценным алгоритмом с открытым ключом, который может работать только в режиме электронной цифровой подписи;

в) Стал первым полноценным алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи;

г) Стал первым полноценным алгоритмом с открытым ключом, который использует эллиптические кривые и может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи;

15. Какие требования не предъявляются к выбору сомножителей (факторам) p и q в алгоритме RSA:

а) Числа p и q должны иметь примерно одинаковую длину;

б) Числа p и q не должны быть близкими друг другу;

в) Числа p и q должны быть больше 0, но меньше $n-1$;

г) Числа p и q не должны быть слишком малы;

16. Способ адаптировать алгоритм Меркла-Хеллмана для электронных подписей предложил:

а) Меркл;

б) Хеллман;

в) Адлеман;

г) **Шамир;**

17. Какая атака наиболее опасна для алгоритма Диффи-Хеллмана:

а) **Человек посередине;**

б) Атака на основе подобранный ключа;

в) Атака дня рождения;

г) Интерполяционная атака;

18. К видам цифровой подписи относятся:

а) Подпись без разглашения (without disclosure), подпись «слепого контроля» (blind control), хэшируемая подпись (hashed signature);

б) Подпись по соглашению (agreement signature), подпись «вслепую» (blind signature), хэшируемая подпись (hashed signature);

в) Подпись с добавкой (with appendix), подпись по соглашению (agreement signature), контролируемая подпись (undeniable signature);

г) **Подпись с добавкой (with appendix), подпись «вслепую» (blind signature), контролируемая подпись (undeniable signature);**

19. Какие криптографические примитивы относятся к примитивам без ключа:

а) Асимметричные ключи, цифровая подпись, идентификационные примитивы с открытым ключом;

б) **Генератор случайных последовательностей, однонаправленная функция, хэш-функция;**

в) Все перечисленное;

г) Генератор псевдослучайных последовательностей, электронная цифровая подпись (ЭЦП), блочные шифры, поточные шифры;

20. Какие криптографические примитивы относятся к криптографии с секретным ключом:

а) Асимметричные ключи, цифровая подпись, идентификационные примитивы с открытым ключом;

б) Генератор случайных последовательностей, однонаправленная функция, хэш-функция;

в) Все перечисленное;

г) **Генератор псевдослучайных последовательностей, электронная цифровая подпись (ЭЦП), блочные шифры, поточные шифры;**

21. Под ключевой информацией понимается:

а) Совокупность центров распределения, хранения и утилизации ключей;

б) Совокупность всех мастер-ключей ИС;

в) **Совокупность всех действующих в ИС ключей;**

г) Совокупность всех мастер-ключей и ключей шифрования ключей;

22. Целью управления ключами является:

а) **Нейтрализация угроз компрометации конфиденциальности закрытых ключей, компрометации аутентичности закрытых или открытых ключей, несанкционированного использования закрытых или открытых ключей;**

б) Нейтрализация угроз компрометации доступности закрытых ключей, компрометации конфиденциальности открытых ключей, компрометации целостности закрытых или открытых ключей;

в) Компрометация конфиденциальности закрытых ключей, компрометация аутентичности закрытых или открытых ключей, несанкционированное использование закрытых или открытых ключей;

г) Ничего из перечисленного;

23. Процесс управления ключами состоит из:

а) Кодификации ключей, нормализации ключей, реализации ключей;

б) Генерации ключей, накоплении ключей, распределении ключей;

в) Идентификации ключей, модификации ключей, нотификации ключей;

г) Воспроизводства ключей, регистрации ключей, утилизации ключей;

24. Термин «короткий срок действия» относится:

а) К промежутку времени, в течение которого ключ должен оставаться в секрете;

б) К промежутку времени, в течение которого передаются данные;

в) К сроку действия ключа;

г) К сроку жизни информационной системы;

25. Классификации по сроку действия ключей выглядит следующим образом:

а) С длительным сроком действия, со средним сроком действия и с коротким сроком действия;

б) С длительным сроком действия и с коротким сроком действия;

в) Долгожители и короткоживущие;

г) Со средним сроком действия и с коротким сроком действия;

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	
Модуль 1		0,4
Модуль 2		0,24

Лабораторные работы

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

Темы лабораторных работ

- 1) Алгоритмы наивной криптографии.
- 2) Сеть Фейстеля
- 3) Режимы шифрования.
- 4) Процедура дополнения блока.
- 5) Процедура расширения ключа.
- 6) Псевдослучайные криптографические последовательности.
- 7) Хэш-функции.
- 8) Протоколы распределения ключей
- 9) Электронная подпись.

Модуль 1. Симметричные шифры.

Тема: Алгоритмы наивной криптографии. Шифр Цезаря.

Цель: Практические навыки при шифровании и расшифровывании алгоритмами наивной криптографии.

1. **Задание:** Расшифруйте стихи А.С. Пушкина, (русский алфавит, Е и Ё считается одним символом)

Х шсхтгсхфзухщсчвщпрюьлфвь
 Кхщцйжщцчхшймамфгжль
 Пхцвщ, швфхяпихсщчълфвь,
 Пкмфпр, цзчзлхсшхйлчък,
 Пштьюзр, ихкпохичмщцщмтг

2. Защита лабораторной работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
Одно лабораторное задание	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа	0/1/3
Модуль 1	выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	0/1/3
Модуль 2		

Практические работы

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

Темы практических работ

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

- 10) Алгоритмы наивной криптографии.
- 11) Ячейка Фейстеля. Сеть Фейстеля
- 12) Режимы шифрования.
- 13) Процедура расширения ключа.
- 14) Поточные шифры.
- 15) Однонаправленные хэш-функции.
- 16) Управление криптографическими ключами. Протоколы распределения ключей
- 17) Протокол Нидхема-Шрёдера на ассиметричных ключах.
- 18) Электронная подпись.

Практическая работа № 1

Модуль 1. Симметричные шифры.

Тема: Алгоритмы наивной криптографии. Полибианский квадрат.

Цель: Практические навыки при шифровании и расшифровывании алгоритмами наивной криптографии.

Задание: Расшифруйте слово 34124142364326462463 с использованием модифицированного квадрата Полибия.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К

3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	0/1/3
Модуль 1		0/1/3
Модуль 2		

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 978-5-9963-0242-0 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=428998>.

2. Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=229582>.

Дополнительная литература

3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>.

4. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93245>.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» - <https://biblioclub.ru>

2. Электронная библиотечная система «ЭБ БашГУ» - <https://elib.bashedu.ru>
3. Электронная библиотечная система БашГУ – www.bashlib.ru
4. Электронная библиотечная система издательства «Лань» - <https://e.lanbook.com>
5. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
6. Банк нормативно-правовых актов РФ Министерства юстиции РФ - http://zakon.scli.ru/ru/legal_texts/index.php
7. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. <http://www.consultant-plus.ru>
8. Национальные стандарты РФ в области информационной безопасности: <http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii>
9. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): <https://fstec.ru/> Раздел «Национальные стандарты информационной безопасности» (<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty>)

Государственные информационно-правовые системы:

1. Научный центр правовой информации при министерстве Юстиций РФ - <http://www.scli.ru>
2. Официальный интернет-портал правовой информации - <http://pravo.gov.ru>
3. Информационно-правовая система «Законодательство России» - <http://pravo.fso.gov.ru>
4. Модуль «Документы - Президент России» - <http://www.kremlin.ru/acts>
5. Банк документов, подписанных Президентом России - <http://kremlin.ru/acts/bank>
6. База данных «Федеральные законы» - <http://graph.garant.ru:8080/SESSION/PILOT/main.htm>
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы) - <http://asozd.duma.gov.ru/>
8. База данных «Издания по общественным и гуманитарным наукам» (на платформе EastView) - Ссылка <http://www.ebiblioteka.ru>(вход из сети вуза без регистрации).
9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России - <http://alrf.consultant.ru/>
10. Банк данных "Копии правовых актов: Российская Федерация» - <http://giod.consultant.ru/>
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации - <http://duma.consultant.ru/>

Другие профессиональные базы данных и информационно-справочные системы:

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: <http://dvs.rsl.ru>
2. База данных «Вестники Московского университета» (на платформе EastView) (вход без регистрации). - Ссылка <http://www.ebiblioteka.ru/browse/udb/12>.
3. AnnualReviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: <http://www.annualreviews.org/>
4. Computers & Applied Sciences Complete (EBSCO) - доступ в сетевую базу, язык английский. - Ссылка: <http://search.ebscohost.com/>
5. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: <http://www.scopus.com/>
6. TaylorandFrancis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: <http://www.tandf>
7. WebofScience - наукометрическая, библиографическая и реферативная база данных издательской корпорации ThomsonReuters. Язык английский, вход после регистрации

- или из сети вуза. – Ссылка: <http://apps.webofknowledge.com/>
8. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: <http://onlinelibrary.wiley.com/>
 9. Сайт по информационной безопасности: <http://securitypolicy.ru/>; его раздел: «Документы, стандарты и методики по информационной безопасности»: <http://securitypolicy.ru/>
 10. Докипедия: <http://dokipedia.ru>
 11. Словари и энциклопедии On-Line- <http://www.dic.academic.ru>

Программное обеспечение

1. Windows 8 Russian Russian OLP NL Academic Edition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.

6. Материально-техническая база, необходимая для осуществления

образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
<p>1. учебная аудитория для проведения занятий лекционного типа: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).</p> <p>2. учебная аудитория для проведения лабораторных работ: компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p>3. учебная аудитория для проведения занятий семинарского типа: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус).</p> <p>4. учебная аудитория для проведения групповых и индивидуальных консультаций: аудитория</p>	<p>Лекции, лабораторные занятия, практические занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация</p>	<p style="text-align: center;">Аудитория № 403 Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный ClassicNorma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p style="text-align: center;">Аудитория № 405 Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDR3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.</p> <p style="text-align: center;">Аудитория № 413 Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p style="text-align: center;">Аудитория № 415 Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p style="text-align: center;">Аудитория № 416 Учебная мебель, доска, проектор Optoma Eх542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p style="text-align: center;">Аудитория № 418 Учебная мебель, доска, Экран настенный LumienMasterPiktore 153*203 MatteWhiteFiberClas(белый корпус) – 1 шт., Проектор</p>

<p>№ 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p>5. учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p>6. помещения для самостоятельной работы: читальный зал библиотеки аудитория № 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p>7.помещение для хранения и профилактического обслуживания учебного оборудования:аудитория № 523 (гуманитарный корпус).</p>		<p>OptomaEx542 i - 1 шт.</p> <p>Аудитория № 419 Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 515 Учебная мебель, доска, терминал видео конференц-связи LifeSizelcon 600-камера, интер-ая система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI SMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDR3 4 Gb/HDD 1TB/DVD-RW/Thermaltake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с попитром.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секционные последующих рядов с попитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 610 Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.</p> <p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные,</p>
--	--	--

		комбинированные. Аудитория № 523 Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.
--	--	---

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Криптографические методы защиты информации** на 7 семестр
_____ очная ф/о _____

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	52,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к экзамену (Контроль)	36

Форма контроля
Экзамен 7 семестр

Семестр 7

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельно й работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
1	<p>Модуль 1. Симметричные шифры.</p> <p>Тема: Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.</p> <p>Тема: Классификация шифров. Классификация шифров по области применения. Кодирование. Классификация шифров по особенностям алгоритма шифрования. Классификация шифров по количеству символов сообщения. Этапы криптографии. Шифры наивной криптографии. Шифр Цезаря. Полибианский квадрат. Шифр «Решетка». Шифр Виженера. Шифр Плейфера. Шифр Хилла. Шифр Вернама. Шифр Хагелина. Машина шифрования Enigma. Блочные и поточные шифры. Лавинный эффект. Поточные шифры.</p> <p>Тема: Классификация блочных шифров. Режим шифрования. Режим простой замены ECB. Режим шифрования с сцеплением CBC. Режим обратной связи по шифротексту CFB. Режим шифрования с</p>	2	2	2	6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	лабораторная работа, практическая работа, тест
		2	2	2	6		
		2	2	2	6		

<p>обратной связью по выходу OFB (гаммирование или внутренняя обратная связь). Сцепление блоков шифротекста с распространением ошибки (PCBC). Countermode (CTR) режим счетчика. Режим счётчик с аутентификацией Галуа (Galois/CounterMode GCM). Аутентифицированное шифрование с присоединёнными данными (AEAD-режим блочного шифрования).</p> <p>Тема: Классификация поточных шифров. Синхронные поточные шифры. Самосинхронизирующиеся (асинхронные поточные шифры АПШ) поточные шифры. Генерация случайных и псевдослучайных последовательностей. Криптографически безопасные псевдослучайные последовательности. Настоящие случайные последовательности. Детерминированные генераторы простых случайных чисел. Анализ генераторов псевдослучайных чисел. Регистр сдвига с линейной обратной связью (РСЛОС, англ. Linearfeedbackshiftregister, LFSR). Линейная сложность. Нелинейные регистры сдвига с обратной связью. Нелинейная комбинация генераторов. Линейное и предварительное шифрование. Шифр А5. Гаммирование. Шифр RC 4. Атаки на поточные шифры.</p>	2	2	2	6		
<p>Тема: Требования к хэш-функциям. Криптографическая стойкость хэш-функций. Коллизии. Применение хэш-функций. Подходы к проектированию хэш-функций. Алгоритмы выработки хэш-функций. Хэш-функции на основе блочного шифра. Ключевые хэш-функции. Стандарты на хэш-функции: ГОСТ Р 34.11-94, SHA.</p>	2	2	2	6		

2	Модуль 2. Асимметричные шифры.					Самостоятельное изучение рекомендуемой основной и дополнительной литературы	лабораторная работа, практическая работа, тест
	Тема: Криптография открытого ключа. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.	2	2	2	6		
	Тема: Классификация криптографических протоколов. Классификация криптографических протоколов по характеру разрешения спорных вопросов. Классификация криптографических протоколов по типу используемых криптографических примитивов. Классификация криптографических протоколов по числу участников. Классификация криптографических протоколов по числу передаваемых сообщений. Классификация криптографических протоколов по функциональному (целевому) назначению. Классификация криптографических протоколов по сложности. Классификация криптографических протоколов по области применения. Криптографические примитивы. Криптографические примитивы с секретным ключом. Криптографические примитивы с открытым ключом.	2	2	2	6		
	Тема: Управление криптографическими ключами. Генерация ключей. Накопление ключей. Цели управления ключами. Политика безопасности управления ключами. Сроки действия ключей. Жизненный цикл ключей.	2	2	2	6		
	Тема: Протокол распределения ключей. Временные данные. Разновидности временных данных Симметричные протоколы. Однопроходовой key transport. Challenge Response. Authenticated Key Exchange Protocol. Протокол Шамира. Протоколы, использующие центр сертификации (доверенный	2	2	2	4,8		

	центр) или сервер. Лягушка с открытым ртом. Протокол Нидхема-Шрёдера на симметричных ключах. Протокол Kerberos. TheKerberosTicket. Протокол Отвея-Рииса. Алгоритм DASS.						
Всего часов		18	18	18	52,8		

