Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по учебной работе
д.юр.н., доц. Васильева Н.В.

_____

21.06.2024г.

Рабочая программа дисциплины
Б1.О.35. Криптография и защита информации

Направление подготовки: 09.03.03 Прикладная информатика
Направленность (профиль): Системы искусственного интеллекта
Квалификация выпускника: бакалавр
Форма обучения: очная, заочная

	Очная ФО	Заочная ФО
Курс	3	3
Семестр	31	31
Лекции (час)	28	4
Практические (сем, лаб.) занятия (час)	42	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	74	130
Курсовая работа (час)		
Всего часов	144	144
Зачет (семестр)		
Экзамен (семестр)	31	31

Иркутск 2024

Программа составлена в соответствии с ФГОС ВО по направлению 09.03.03 Прикладная информатика.

Автор М.М. Бусько

Рабочая программа обсуждена и утверждена на заседании кафедры математических методов и цифровых технологий

Заведующий кафедрой А.В. Родионов

1. Цели изучения дисциплины

Цель дисциплины:

Изучение теоретических основ криптографических протоколов: терминологии, стандартов, типов протоколов и требований к ним, а также знание средств анализа безопасности протоколов; освоение теоретических основ решения задач аутентификации пользователей и информации, распределения ключей; формирование умения использования криптографических протоколов для решения задач обеспечение информационной безопасности компьютерных и телекоммуникационных систем, умения применять математические методы описания и исследования криптосистем.

Задачи дисциплины:

1. Дать представление о криптографических методах защиты информации
2. Изучить математические основы современной криптографии
3. Изучить современные стандарты симметричного шифрования.
4. Изучить основные криптографические алгоритмы с открытым ключом
5. Изучить криптографические функции хеширования
6. Сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Компетенции обучающегося, формируемые в результате освоения дисциплины

Код компетенции по ФГОС ВО	Компетенция
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-5	Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем

Структура компетенции

Компетенция	Формируемые ЗУНы
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З. Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н. Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований

	информационной безопасности
ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	З. Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У. Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем Н. Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем

3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ): Обязательная часть.

Предшествующие дисциплины (освоение которых необходимо для успешного освоения данной): "Дискретная математика", "Линейная алгебра", "Математический анализ", "Алгоритмы и структуры данных", "Системы управления данными", "Численные методы", "Интернет-технологии", "Исследование операций", "Операционные системы"

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зач. ед.,144 часов.

Вид учебной работы	Количество часов (очная ФО)	Количество часов (заочная ФО)
Контактная(аудиторная) работа		
Лекции	28	4
Практические (сем, лаб.) занятия	42	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам	74	130
Всего часов	144	144

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Содержание разделов дисциплины

Заочная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Тема 1. Основные понятия криптографии. Арифметика остатков. Элементарные шифры	31	2	0	20		
2	Тема 2. Базовые теоретико-числовые	31	0	2	18		Решение задач по теме №2

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
	алгоритмы						
3	Тема 3. Криптографические системы с секретным ключом	31	0	2	18		Решение задач по теме №3
4	Тема 4. Асимметричные криптографические протоколы и системы шифрования с открытым ключом	31	2	0	20		
5	Тема 5. Асимметричные схемы электронно-цифровой подписи	31	0	2	18		Решение задач по теме №5
6	Тема 6. Функции хэширования	31	0	2	18		Решение задач по теме №6
7	Тема 7. Эллиптические кривые над конечным полем. Управление криптографическими ключами	31	0	2	18		Решение задач по теме №7
	ИТОГО		4	10	130		

Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
1	Тема 1. Основные понятия криптографии. Арифметика остатков. Элементарные шифры	31	4	6	10		Решение задач по теме №1
2	Тема 2. Базовые теоретико-числовые алгоритмы	31	4	6	10		Решение задач по теме №2
3	Тема 3. Криптографические системы с секретным ключом	31	4	6	10		Решение задач по теме №3
4	Тема 4. Асимметричные криптографические протоколы и системы шифрования с открытым ключом	31	4	6	12		Решение задач по теме №4
5	Тема 5. Асимметричные схемы электронно-цифровой подписи	31	4	6	10		Решение задач по теме №5

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
6	Тема 6. Функции хэширования	31	4	6	12		Решение задач по теме №6
7	Тема 7. Эллиптические кривые над конечным полем. Управление криптографическими ключами	31	4	6	10		Решение задач по теме №7
	ИТОГО		28	42	74		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
01	Лекция 1	Предмет криптографии. Основные задачи криптографии. История развития криптографии. Терминология. Математические основы криптографии. Модульная арифметика. Система вычетов. Простой и расширенный алгоритм Евклида. Вычисление наибольшего общего делителя. Требования к криптографическим системам. Теория Шеннона. Абсолютная стойкость шифра. Новые направления развития криптографии
02	Лекция 2	Арифметика остатков. Элементарные шифры. Понятие шифрования. Шифры подстановки. Криптоанализ. Моноалфавитные шифры. Шифр Цезаря. Аддитивный, мультипликативные, аффинный шифры. Сведения из теории чисел. Аффинный шифр. Обобщенный алгоритм Евклида. Вскрытие аффинного шифра по двум паросочетаниям. Многоалфавитные шифры. Автоключевой шифр. Шифр Виженера
03	Лекция 3	Китайская теорема об остатках. Возведение в квадрат. Символы Лежандра и Якоби, извлечение квадратного корня
04	Лекция 4	Возведение в степень и нахождение порождающего элемента группы. Генерация простых чисел
05	Лекция 5	Основные классы симметричных криптосистем. Особенности построения блочных шифров. Рассеивание и перемешивание. Раунды. Шифр Фейстеля и DES
06	Лекция 6	Отечественный стандарт шифрования данных. Основные характеристики и структура алгоритма AES алгоритм Rijndael. Потоковые шифры
07	Лекция 7	Протокол Диффи-Хеллмана. Трехпроходный протокол Шамира. Криптосистема RSA
08	Лекция 8	Криптосистема Эль-Гамаля. Криптосистема Рабина
09	Лекция 9	Электронная цифровая подпись. Цифровая подпись RSA
10	Лекция 10	Цифровая подпись Эль-Гамаля. Генерация сильно простого числа и порождающего элемента. Цифровая подпись DSA
11	Лекция 11	Хэш-функция Шаумома, ван Хейста, Пфицмана. Хэш-функции и блочные шифры. Отечественный стандарт хэш-функции
12	Лекция 12	Семейство MD4. Семейство алгоритмов SHA. Криптография в блокчейн. Аутентификация и верификация транзакций

№ п/п	Наименование разделов и тем	Содержание
13	Лекция 13	Определение эллиптической кривой. Выбор кривой и точки. Сложение точек на эллиптических кривых. Криптосистемы на эллиптических кривых. Протокол Диффи-Хеллмана на эллиптических кривых. Цифровая подпись EC-DSA. Алгоритм Эль-Гамаля на эллиптических кривых
14	Лекция 14	Генерация ключей. Генерация сеансового ключа для симметричных криптосистем. Обычная система управления ключами. Управление ключами, основанное на системах с открытым ключом. Протокол обмена секретным ключом. Использование сертификатов. Протоколы аутентификации. Анонимное распределение ключей

5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Семинар 1. Решение задач
1	Семинар 2. Решение задач
1	Семинар 3. Решение задач
2	Семинар 4. Решение задач
2	Семинар 5. Решение задач
2	Семинар 6. Решение задач
3	Семинар 7. Решение задач
3	Семинар 8. Решение задач
3	Семинар 9. Решение задач
4	Семинар 10. Решение задач
4	Семинар 11. Решение задач
4	Семинар 12. Решение задач
5	Семинар 13. Решение задач
5	Семинар 14. Решение задач
5	Семинар 15. Решение задач
6	Семинар 16. Решение задач
6	Семинар 17. Решение задач
6	Семинар 18. Решение задач
7	Семинар 19. Решение задач
7	Семинар 20. Решение задач
7	Семинар 21. Решение задач

6. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине (полный текст приведен в приложении к рабочей программе)

6.1. Текущий контроль

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
1	1. Тема 1. Основные понятия криптографии. Арифметика остатков. Элементарные шифры	ОПК-3	З.Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У.Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н.Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Решение задач по теме №1	12-14 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 10-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 8-9 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 7 и менее баллов — студент обнаружил несостоятельность ответов (14)
2	2. Тема 2. Базовые теоретико-числовые алгоритмы	ОПК-3	З.Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и	Решение задач по теме №2	12-14 баллов — сформированные систематические знания; на высоком уровне осуществляемые

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У.Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н.Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		умения, успешно применяемые навыки; 10-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 8-9 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 7 и менее баллов — студент обнаружил несостоятельность ответов (14)
3	3. Тема 3. Криптографические системы с секретным ключом	ОПК-3	З.Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	Решение задач по теме №3	12-14 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 10-11 баллов — сформированные, но содержащие

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			основных требований информационной безопасности У.Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н.Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 8-9 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 7 и менее баллов — студент обнаружил несостоятельность ответов (14)
4	4. Тема 4. Асимметричные криптографические протоколы и системы шифрования с открытым ключом	ОПК-5	З.Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У.Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	Решение задач по теме №4	12-14 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 10-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			Н.Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем		пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 8-9 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 7 и менее баллов — студент обнаружил несостоятельность ответов (14)
5	5. Тема 5. Асимметричные схемы электронно-цифровой подписи	ОПК-5	З.Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У.Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем Н.Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Решение задач по теме №5	12-14 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 10-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 8-9 баллов — общие, но не структурированн

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
					ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 7 и менее баллов — студент обнаружил несостоятельность ответов (14)
6	6. Тема 6. Функции хэширования	ОПК-5	З.Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У.Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем Н.Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Решение задач по теме №6	12-14 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 10-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 8-9 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 7 и менее баллов — студент обнаружил несостоятельност

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
					ь ответов (14)
7	7. Тема 7. Эллиптические кривые над конечным полем. Управление криптографическими ключами	ОПК-5	З.Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У.Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем Н.Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Решение задач по теме №7	13-16 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 10-12 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 8-9 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 7 и менее баллов — студент обнаружил несостоятельность ответов (16)
				Итого	**100**

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Экзамен в семестре 31.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (30 баллов), вид вопроса: Тест/проверка знаний. Критерий: Максимальное количество баллов, которые может получить каждый студент за тест в относительных единицах равняется 30-ти. Каждый правильный ответ оценивается в 1 балл, полученный результат делится на общее количество вопросов в тесте и умножится на 30..

Компетенция: ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знание: Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Аддитивный, мультипликативные, аффинный шифры.
2. Аффинный шифр
3. Возведение в степень и нахождение порождающего элемента группы
4. Вскрытие аффинного шифра по двум паросочетаниям
5. Генерация простых чисел
6. История развития криптографии. Терминология.
7. Китайская теорема об остатках
8. Многоалфавитные шифры. Автоключевой шифр.
9. Модульная арифметика. Система вычетов.
10. Моноалфавитные шифры. Шифр Цезаря
11. Новые направления развития криптографии
12. Обобщенный алгоритм Евклида
13. Понятие шифрования. Шифры подстановки. Криптоанализ.
14. Предмет криптографии. Основные задачи криптографии.
15. Простой и расширенный алгоритм Евклида. Вычисление наибольшего общего делителя.
16. Сведения из теории чисел
17. Символы Лежандра и Якоби, извлечение квадратного корня
18. Теория Шеннона. Абсолютная стойкость шифра
19. Требования к криптографическим системам
20. Шифр Виженера.

Компетенция: ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем

Знание: Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем

21. Алгоритм Эль-Гамаля на эллиптических кривых
22. Алгоритмы рюкзака
23. Алгоритмы с открытыми ключами RSA. Общие положения криптосистем с открытым ключом.
24. Анонимное распределение ключей
25. Аутентификация и верификация транзакций
26. Выбор кривой и точки
27. Генерация ключей
28. Генерация сеансового ключа для симметричных криптосистем
29. Генерация сильно простого числа и порождающего элемента
30. Использование сертификатов
31. Криптография в блокчейн
32. Криптосистема RSA

33. Криптосистема Рабина
34. Криптосистема Эль-Гамаля
35. Криптосистемы на эллиптических кривых
36. Обычная система управления ключами
37. Определение эллиптической кривой
38. Основные классы симметричных криптосистем
39. Основные характеристики и структура алгоритма AES алгоритм Rijndael
40. Особенности построения блочных шифров
41. Отечественный стандарт хэш-функции
42. Отечественный стандарт шифрования данных
43. Потоковые шифры
44. Протокол Диффи-Хеллмана
45. Протокол Диффи-Хеллмана на эллиптических кривых
46. Протокол обмена секретным ключом
47. Протоколы аутентификации
48. Рассеивание и перемешивание. Раунды.
49. Семейство алгоритмов SHA
50. Семейство алгоритмов хеширования "MD4"
51. Сложение точек на эллиптических кривых
52. Трехпроходный протокол Шамира
53. Управление ключами, основанное на системах с открытым ключом
54. Хэш-функции и блочные шифры
55. Хэш-функция Шаумома, ван Хейста, Пфицмана
56. Цифровая подпись DSA
57. Цифровая подпись EC-DSA
58. Цифровая подпись RSA
59. Цифровая подпись Эль-Гамаля
60. Шифр Фейстеля и DES
61. Электронная цифровая подпись

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ:

2-й вопрос билета (35 баллов), вид вопроса: Задание на умение. Критерий: 32-35 баллов — заслуживает студент, выполнивший задание в соответствии с заявленной инструкцией или технологией, полностью и правильно; сделаны глубокие и детальные выводы с опорой на источники; имеются ссылки на нормативные документы, не нарушены сроки выполнения задания; 25-32 баллов — заслуживает студент, за правильное выполнение задания в соответствии с инструкцией или технологией с учетом 2-3 несущественных ошибок; выводы сформулированы корректно со ссылкой на источники и нормативные документы; сроки выполнения задания не нарушены; 14-25 — заслуживает студент за выполнение задания правильно не менее чем на половину или если допущена существенная ошибка; выводы сформулированы поверхностно, некорректно; отсутствуют ссылки на источники; сроки выполнения задания не нарушены; 13 и менее — выставляется студенту, если при выполнении задания допущены две (и более) существенные ошибки или задание не выполнено вообще; выводы сформулированы с грубыми ошибками или отсутствуют вообще; задание выполнено с нарушением сроков..

Компетенция: ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Умение: Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

коммуникационных технологий и с учетом основных требований информационной безопасности
Задача № 1. Разложить число на множители используя p-метод Полларда согласно варианту
Компетенция: ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем
Умение: Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем
Задача № 2. Реализовать вероятностный алгоритм проверки числа на простоту согласно варианту

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ:

3-й вопрос билета (35 баллов), вид вопроса: Задание на навыки. Критерий: 32-35 баллов — заслуживает студент, выполнивший задание в соответствии с заявленной инструкцией или технологией, полностью и правильно; сделаны глубокие и детальные выводы с опорой на источники; имеются ссылки на нормативные документы, не нарушены сроки выполнения задания; 25-32 баллов — заслуживает студент, за правильное выполнение задания в соответствии с инструкцией или технологией с учетом 2-3 несущественных ошибок; выводы сформулированы корректно со ссылкой на источники и нормативные документы; сроки выполнения задания не нарушены; 14-25 — заслуживает студент за выполнение задания правильно не менее чем на половину или если допущена существенная ошибка; выводы сформулированы поверхностно, некорректно; отсутствуют ссылки на источники; сроки выполнения задания не нарушены; 13 и менее — выставляется студенту, если при выполнении задания допущены две (и более) существенные ошибки или задание не выполнено вообще; выводы сформулированы с грубыми ошибками или отсутствуют вообще; задание выполнено с нарушением сроков..

Компетенция: ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Навык: Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Задание № 1. Зашифровать и расшифровать сообщение M по алгоритму RSA (выбор ключей начать с p = 3, q = 11 для четных значений числа M и с p = 5, q = 7 для нечетных значений числа M). Шифрование производить поразрядно.
Компетенция: ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем
Навык: Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем
Задание № 2. Зашифровать и расшифровать сообщение M по алгоритму Эль-Гамаля (выбор ключей начать с p = 11 и g = 3).

ОБРАЗЕЦ БИЛЕТА

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования

Направление - 09.03.03 Прикладная информатика
Профиль - Системы искусственного интеллекта

«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «БГУ»)

Кафедра математических методов и цифровых технологий
Дисциплина - Криптография и защита информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест (30 баллов).
2. Разложить число на множители используя p-метод Полларда согласно варианту (35 баллов).
3. Зашифровать и расшифровать сообщение M по алгоритму RSA (выбор ключей начать с p = 3, q = 11 для четных значений числа M и с p = 5, q = 7 для нечетных значений числа M). Шифрование производить поразрядно. (35 баллов).

Составитель _____ М.М. Бусько

Заведующий кафедрой _____ А.В. Родионов

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

а) основная литература:

1. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. допущено УМО по образованию в обл. прикладной информатики. учеб. пособие. 3-е изд., перераб. и доп./ Е. К. Баранова, А. В. Бабаш.- М.: ИНФРА-М, 2016.-321 с.
2. Гришина Н. В. Информационная безопасность предприятия. учеб. пособие для вузов. рек. УМО вузов РФ по образованию в обл. историко-архивоведения. 2-е изд., доп./ Н. В. Гришина.- М.: ИНФРА-М, 2017.-238 с.
3. Бусько М.М. Информационная безопасность и защита информации : учеб. пособие.- Иркутск: Изд-во БГУ, 2022.- 220 с.
4. Фомичев, В. М. Криптография – наука о тайнописи : учебное пособие / В. М. Фомичев. — Москва : Прометей, 2020. — 66 с. — ISBN 978-5-00172-040-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/125666.html (дата обращения: 28.05.2024). — Режим доступа: для авторизир. пользователей
5. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html (дата обращения: 28.05.2024). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

1. Астахова А. В. Информационные системы в экономике и защита информации на предприятиях-участниках ВЭД. учеб. пособие для вузов/ А. В. Астахова.- СПб.: Троицкий мост, 2014.-214 с.
2. Гугуева Т. А. Конфиденциальное делопроизводство. рек. УМО по образованию в обл. менеджмента. учеб. пособие для вузов/ Т. А. Гугуева.- М.: ИНФРА-М, 2015.-191 с.
3.
4. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — Москва : СОЛОН-Пресс, 2016. — 256 с. — ISBN 5-98003-

002-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/90248.html (дата обращения: 28.05.2024). — Режим доступа: для авторизир. пользователей
5. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю. Государственный научно-исследовательский испытательный институт проблем технической защиты информации. http://bdu.fstec.ru/ (30.08.2017)
6. Боровкова, Г. С. Анализ конечных изменений в управлении и защита информации : учебное пособие / Г. С. Боровкова. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2018. — 80 с. — ISBN 978-5-88247-923-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/92843.html (дата обращения: 28.05.2024). — Режим доступа: для авторизир. пользователей
7. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. http://fstec.ru/component/attachments/download/489
8. Перечень средств защиты информации, сертифицированных ФСБ России. http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_(010717).doc
9. Плёнкин, А. П. Однофотонные приёмники для систем квантового распределения ключей : учебное пособие / А. П. Плёнкин, К. Е. Румянцев. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 117 с. — ISBN 978-5-9275-3491-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/107965.html (дата обращения: 28.05.2024). — Режим доступа: для авторизир. пользователей

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая профессиональные базы данных и информационно-справочные системы

Для освоения дисциплины обучающемуся необходимы следующие ресурсы информационно-телекоммуникационной сети «Интернет»:

– Сайт Байкальского государственного университета, адрес доступа: http://bgu.ru/, доступ круглосуточный неограниченный из любой точки Интернет

– ИВИС - Универсальные базы данных, адрес доступа: http://www.dlib.eastview.ru/. доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ

– КиберЛенинка, адрес доступа: http://cyberleninka.ru. доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению

– Научная электронная библиотека eLIBRARY.RU, адрес доступа: http://elibrary.ru/. доступ к российским журналам, находящимся полностью или частично в открытом доступе при условии регистрации

– Национальный цифровой ресурс «Руконт», адрес доступа: http://www.rucont.ru. доступ неограниченный

– Федеральная служба безопасности Российской Федерации, адрес доступа: http://fsb.ru. доступ неограниченный

– Федеральная служба по техническому и экспортному контролю, адрес доступа: http://fstec.ru. доступ неограниченный

– Федеральный образовательный портал «Экономика, Социология, Менеджмент», адрес доступа: http://www.ecsocman.edu.ru. доступ неограниченный

– ЭБС BOOK.ru - электронно-библиотечная система от правообладателя, адрес доступа: http://www.book.ru/. доступ неограниченный

– Электронная библиотека Издательского дома "Гребенников", адрес доступа: http://www.grebennikon.ru/. доступ с компьютеров сети БГУ (по IP-адресам)

– Электронно-библиотечная система IPRbooks, адрес доступа: https://www.iprbookshop.ru. доступ неограниченный

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания в области информационных технологий.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций студенту необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические (семинарские) занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое (семинарское) занятие сообщается обучающимся до его проведения. На семинаре преподаватель организует обсуждение этой темы, выступая в качестве организатора, консультанта и эксперта учебно-познавательной деятельности обучающегося.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы студентов с участием преподавателей являются:

• текущие консультации;

• коллоквиум как форма контроля освоения теоретического содержания дисциплин: (в часы консультаций, предусмотренные учебным планом);

• прием и разбор домашних заданий (в часы практических занятий);

• прием и защита лабораторных работ (во время проведения занятий);

• выполнение курсовых работ в рамках дисциплин (руководство, консультирование и защита курсовых работ в часы, предусмотренные учебным планом) и др.

Основными видами самостоятельной работы студентов без участия преподавателей являются:

• формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

• самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;

• написание рефератов, докладов;

• подготовка к семинарам и лабораторным работам;

• выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

В учебном процессе используется следующее программное обеспечение:

– MS Office,

– КонсультантПлюс: Версия Проф - информационная справочная система,

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

В учебном процессе используется следующее оборудование:
– Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза,
– Учебные аудитории для проведения: занятий лекционного типа, занятий семинарского типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения,
– Компьютерный класс,
– Наборы демонстрационного оборудования и учебно-наглядных пособий