Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ
Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«17» 05 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические методы защиты информации

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
3	*5*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*Кафедра ИБАС – Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

к.ф.-м.н., доцент		А.Ю. Лошманов
(должность, степень, ученое звание)	(подпись)	(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС		А.Ю. Лошманов
(наименование кафедры)	(подпись)	(ФИО)

1 Общие положения

Рабочая программа дисциплины «Криптографические методы защиты информации» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации от 01.12.2016 № 1509, и образовательной программы подготовки специалистов «Информационная безопасность автоматизированных систем» (10.05.03) уровень специалитета, специализация «Обеспечение информационной безопасности распределенных информационных систем».

Задачи дисциплины	Изучение теоретических принципов криптографии; Овладение практическими навыками использования; Получение представления эффективной программной и аппаратной реализации криптографических алгоритмов Развитие аналитических мышления студентов и повышение их общей математической культуры Привить студентам умение самостоятельно изучать учебную и научную литературу.
Основные разделы / темы дисциплины	1. Симметричная криптография 2. Криптография с открытым ключом 3. Криптографические библиотеки и протоколы 4. Криптопровайдеры

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

Процесс изучения дисциплины «Криптографические методы защиты информации» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные компетенции			
Способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14)	З1(ПК-14-4) Основные задачи и понятия криптографии, виды шифров	У1(ПК-14-4) Эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах	Н1(ПК-14-4) Использования типовых криптографических алгоритмов
	З2(ПК-14-4) Модели шифров и математические методы их исследования	У2(ПК-14-4) Применять математические методы исследования моделей шифров.	Н2(ПК-14-4) Использования ЭВМ в анализе простых шифров
	З1(ПК-14-5) Типовые поточные	У1(ПК-14-5) Использовать средства	Н1(ПК-14-5) Математического моде-

	и блочные шифры	электронно-цифровой подписи	лирования в криптографии
	З2(ПК-14-5) Типовые шифры с открытыми ключами	У2(ПК-14-5) Проводить настройку криптографических средств.	Н2(ПК-14-5) Криптографической терминологией

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» изучается на 3 курсе в 5 семестре.

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

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 (объем) дисциплины составляет 4 з.е., 144 акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	Всего академических часов
Общая трудоемкость дисциплины	144
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	48
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	16
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	60
Промежуточная аттестация обучающихся – Экзамен	144

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

учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Тема 1. Симметричная криптография	4			4
Тема 2. Криптография с открытым ключом	4			4
Тема 3. Криптографические библиотеки и протоколы	4			4
Тема 4. Криптопровайдеры	4			4
Лабораторная работа 1. Расчет вероятности			5	5
Лабораторная работа 2. Симметричные криптоалгоритмы			5	5
Лабораторная работа 3. Криптосистема RSA			5	5
Лабораторная работа 4. Протокол Диффи-Хеллмана			5	5
Лабораторная работа 5. Криптосистема Эль-Гамаля			6	6
Лабораторная работа 6. Криптопровайдеры			6	6
ИТОГО по дисциплине	**16**		**32**	**48**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	16
Подготовка к занятиям семинарского типа	32
Подготовка и оформление РГР	12
	60

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 5).

Таблица 5 – Технологическая карта

	Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания**
Промежуточная аттестация в форме экзамена				
1	Лабораторная работа 1	1 – 3 недели семестра	10 баллов	10 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 6 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 4 балла - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
2	Лабораторная работа 2	3 – 5 недели семестра	10 баллов	
3	Лабораторная работа 3	5 – 7 недели семестра	10 баллов	
4	Лабораторная работа 4	7 –9 недели семестра	10 баллов	
5	Лабораторная работа 5	10 – 12 недели семестра	10 баллов	
6	Лабораторная работа 6	12 – 14 недели семестра	10 баллов	
11	РГР	14 – 16 недели семестра	40 баллов	40 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 25 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 15 баллов - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
ИТОГО Текущий контроль:		-	100 баллов	-
12	Вопросы экзамена (2 вопроса по 10 баллов)	сессия	20	0 баллов – ответ на вопрос билета отсутствует или не верен 4 балла – дан не полный ответ, допущены ошибки

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				7 баллов – дан полный ответ, допущены неточности 10 баллов – дан полный ответ, приведены примеры
ИТОГО Промежуточная аттестация (экзамен)		-	20 баллов	
Критерии оценки результатов обучения по дисциплине: 0 – 64% от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине); 65-74% от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75-84% от максимально возможной суммы баллов – «хорошо» (средний уровень); 85-100% от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

Задания для текущего контроля

Лабораторная работа № 1

Вариант 1

Задумано двузначное число. Найти вероятность того, что задуманным числом окажется случайно названное двузначное число.

Вариант 2

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна пяти, а произведение — четырем».

Вариант 3

На плоскости заданы три концентрические окружности с радиусами: 3 см, 5 см, 8 см. Точка ставится наугад в область между меньше и большей окружностями. Найти вероятность того, что она попадет в промежуток между меньшей и средней окружностями.

Вариант 4

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна восьми, а разность — четырем».

Вариант 5

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна восьми, если известно, что их разность равна четырем».

Вариант 6

Задумано двузначное число. Найти вероятность того, что задуманным числом окажется случайно названное двузначное число, цифры которого различны.

Вариант 7

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет ноль окрашенных граней.

Вариант 8

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет одну окрашенную грань.

Вариант 9

Монета брошена два раза. Найти вероятность того, что оба раза появится «герб».

Вариант 10

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет три окрашенных грани.

Вариант 11

Монета брошена два раза. Найти вероятность того, что хотя бы один раз появится «герб».

Вариант 12

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет две окрашенные грани.

Вариант 13

В коробке шесть одинаковых, занумерованных кубиков. Наудачу по одному извлекают все кубики. Найти вероятность того, что номера извлеченных кубиков появятся в возрастающем порядке.

Вариант 14

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна семи».

Вариант 15

В колоде 36 карт четырех мастей. После извлечения и возвращения одной карты колода перемешивается и снова извлекается одна карта. Определить вероятность того, что обе извлеченные карты одной масти.

Лабораторная работа № 2

Ниже используются традиционные для криптографии обозначения: ***M*** – открытый текст, ***C*** – шифротект, ***K*** – ключ.

Вариант 1

Зашифровать и дешифровать M = «абсолютная стойкость» с помощью шифра Виженера, ключ K = «окно».

Вариант 2

Зашифровать и дешифровать M = «квантовый алгоритм шора» с помощью шифра простой замены с генерацией таблицы по слову, ключ K = «решетка».

Вариант 3

Зашифровать M = «производная» с помощью шифра Хилла, ключ K = «фестиваль».

Вариант 4

Зашифровать и дешифровать M = «условная вероятность» с помощью шифра Полибианский квадрат, ключ K = «автомат».

Вариант 5

Зашифровать и дешифровать M = «квантовый алгоритм гровера» с помощью шифра Плейфера, K = «предел, группа».

Вариант 6

Зашифровать и дешифровать M = «генераторы псевдослучайных чисел используются в криптографии» с помощью шифра перестановки по столбцам, K = «651342».

Вариант 7

Зашифровать и дешифровать M = «информационная безопасность» с помощью шифра Полибианский квадрат, ключ K = «квант, кубит».

Вариант 8

Зашифровать M = «аутентификация» с помощью шифра Хилла, K = «указатель».

Вариант 9

Зашифровать и дешифровать M = «дискретная математика» с помощью шифра Виженера, ключ K = «наука».

Вариант 10

Зашифровать и дешифровать M = «обеспечение конфиденциальности является задача криптографии» с помощью шифра перестановки по столбцам K = «2157364».

Вариант 11

Зашифровать и дешифровать M = «стеганография» с помощью шифра Виженера, ключ K = «жизнь».

Вариант 12

Зашифровать и дешифровать M = «сцепление блоков» с помощью шифра простой замены с генерацией таблицы по слову, K = «протокол».

Вариант 13

Зашифровать и дешифровать M = «кодовая книга» с помощью шифра Двойной квадрат, K = «кольцо, алгебра».

Вариант 14

Зашифровать и дешифровать M = «целостность сообщений» с помощью шифра Плейфера, K = «электрон, позитрон».

Вариант 15

Зашифровать и дешифровать M = «криптографический протокол» с помощью шифра Двойной квадрат, K = «алгебра, геометрия».

Лабораторная работа № 3

Даны числа p, q, m. Вычислить недостающие параметры алгоритма, зашифровать m, затем дешифровать полученный шифротекст и сравнить.

Номер варианта	p	q	m
1	7	17	16
2	3	31	24
3	7	11	8
4	5	11	9
5	3	17	20
6	3	5	10
7	5	7	6
8	5	13	14
9	7	13	15
10	3	23	22
11	5	17	18
12	3	13	12
13	3	19	21
14	3	11	7
15	3	29	23
16	3	7	11

Лабораторная работа № 4

Даны числа p, g, a, b. Найти недостающие параметры и сформировать общий секретный ключ (как со стороны Алисы, так и со стороны Боба).

Номер варианта	p	g	a	b
1	23	5	10	7
2	17	3	15	6
3	23	7	11	12
4	23	7	7	13
5	19	10	9	10
6	23	5	8	18
7	17	3	6	16
8	23	7	12	21
9	19	2	13	17
10	17	3	12	15
11	23	7	17	20
12	19	2	18	8
13	19	2	10	5
14	23	5	16	11
15	17	3	14	9
16	19	2	17	14

Лабораторная работа № 5

Даны числа p, g, x, k, m. Сформировать недостающие параметры алгоритма Эль-Гамаля. Зашифровать m, затем дешифровать полученный шифротекст и сравнить.

Номер варианта	p	g	x	k	m
1	23	5	13	8	7
2	17	3	11	9	4
3	23	7	9	7	10
4	17	3	12	11	8
5	23	5	10	7	13
6	23	5	12	6	5
7	23	7	8	8	11
8	17	3	9	7	10
9	19	2	7	6	6
10	23	5	11	5	9
11	23	7	12	9	12
12	19	2	6	5	3
13	19	2	8	7	7
14	23	7	11	10	9
15	17	3	10	8	7
16	19	2	5	4	8

Лабораторная работа № 6

1 Установить и настроить Crypto Pro 3.6 или выше.
2 Установить считыватели в КриптоПро.
3 Установить etoket pki client
4 Установить датчики случайных чисел
5 Установить VipNet CSP
6 Установить VipNetClient для работы с деловой почтой
7 Установить КриптоПро для работы с ЭЦП в Word
8 Установить КриптоПро, описать вкладки.
9 Установить VipNet CryptoFile
10 Установить КриптоПро плагины для PDF
11 Установить КриптоПро с официального сайта последнюю версию. (сертифицированную версию).
12 Установить КриптоПро с официального сайте последнюю версию (несертифицированную).
13 Сгенерировать запрос на сертификат в КриптоПро
14 Выгрузить Сертификат ЭЦП.
15 Продемонстрировать установленные на АРМ сертификаты ЭЦП используя оснастку КриптоПро.

Пример задания на РГР

1. Реализовать алгоритм DES на любом языке программирования.
2. Реализовать алгоритм AES на любом языке программирования.

Возможные вопросы и задания для защиты работ

1. Основы теории чисел (простые числа, распределение простых чисел, малая теорема Ферма, функция Эйлера, фактори-зация и т.д.)
2. Криптосистема Эль-Гамаля (с доказательством).
3. Алгоритм Диффи-Хеллмана.
4. Односторонние функции (с примерами).
5. Электронно-цифровая подпись (с примерами).
6. Криптосистема RSA (с доказательством).
7. Криптосистема Рабина.
8. Криптографические протоколы (с примерами)
9. Инфраструктура открытых ключей
10. ЭЦП Эль-Гамаля (с доказательством)
11. Основные понятия и определения криптографии.
12. Основные понятия теории вероятностей.
13. Абсолютная криптографическая стойкость.
14. Этапы развития криптографии.
15. Поточные шифры: принципы проектирования и составные блоки.
16. Поточный шифр A5/1. Принцип работы.
17. Шифр DES, характеристики, принцип работы.
18. Российский стандарт симметричного шифрования. Характеристики, принцип работы.
19. Режимы работы блочных шифров.
20. Составные элементы и структура блочных шифров.

Экзаменационные вопросы

1. Основные понятия и определения криптографии (определения, задачи, родственные науки, области применения).
2. История криптографии (основные этапы развития криптографии, исторические шифры).
3. Криптографическая стойкость (различные подходы к определению стойкости, теоретико-информационная стойкость, абсолютная стойкость и ее смысл, шифр Вернама, вычислительная стойкость).
4. Поточные шифры (основные принципы проектирования поточных шифров, примеры поточных шифров).
5. Основные составные блоки поточных шифров и их комбинации (регистр сдвига с линейными обратными связями и т.д.)
6. Практическое применение поточных шифров (шифрование в GSM, шифры проекта eStream).
7. Блочные шифры, основные определения (рассеивание, перемешивание, псевдослучайная функция, лавинный эффект).
8. Структура блочных шифров
9. Основные компоненты блочных шифров
10. Алгоритм шифрования DES и его модификации
11. Режимы работы блочных шифров (возможность параллельной обработки, распространение ошибки)
12. Российский стандарт шифрования ГОСТ 34.12-2018.
13. Алгоритм шифрования AES.
14. Шифры-финалисты конкурса AES (Serpent, Twofish).
15. Облегченная криптография (принципы построения, примеры шифров).
16. Хэш-функции.
17. Коды аутентификации сообщений (CBC-MAC, HMAC и т.д.), стойкость MAC.
18. Аутентифицированное шифрование
19. Основы теории чисел (простые чисел, арифметика остатком, малая теорема Ферма, теорема Эйлера).
20. Основы криптографии с открытым ключом (основные определения, односторонние функции, примеры).
21. Криптосистема RSA (шифрование, дешифрование).
22. Алгоритмы быстрого возведения в степень.
23. Генерация больших простых чисел. Тест Миллера-Рабина.
24. Недостатки криптосистемы RSA. Использование RSA на практике.
25. Алгоритм Диффи-Хеллмана.
26. Криптосистема Эль-Гамаля.
27. Криптосистема Рабина.
28. Аутентификация и электронно-цифровая подпись.
29. ЭЦП на основе криптосистема RSA.
30. Инфраструктура открытых ключей.

16 Учебно-методическое и информационное обеспечение дисциплины (модуля)

16.1 Основная литература

1. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш. - 4-е изд. - Москва : Лаборатория знаний, 2020. - 482 с. - (Программисту). - ISBN 978-5-00101-700-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1201346 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Специалитет). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

16.2 Дополнительная литература

1. Бахаров, Л. Е. Информационная безопасность и защита информации : разделы криптография и стеганография : практикум / Л. Е. Бахаров. - Москва : Изд. Дом НИТУ «МИСиС», 2019. - 59 с. - ISBN 978-5-906953-94-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232734 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Международная информационная безопасность: теория и практика : в трех томах. Том 1 : учебник / под общ. ред А. В. Крутских. - 2-е изд., доп. - Москва : Издательство «Аспект Пресс», 2021. - 384 с. - ISBN 978-5-7567-1098-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1241985 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

3. Пленкин, А. П. Однофотонные приёмники для систем квантового распределения ключей : учебное пособие / А. П. Плёнкин, К. Е. Румянцев ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. - 117 с. - ISBN 978-5-9275-3491-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1308429 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

16.3 Методические указания для студентов по освоению дисциплины

1. Ожиганов А.А. Криптография [Электронный ресурс]: учебное пособие / А.А. Ожиганов. — Электрон.текстовые данные. — СПб: Университет ИТМО, 2016. — 142 с. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/67231.html, ограниченный. – Загл. с экрана.

16.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1 Электронно-библиотечная система ZNANIUM.COM. Договор ЕП 44 № 003/10 эбс ИКЗ 191272700076927030100100120016311000 от 17 апреля 2019 г.

2 Электронно-библиотечная система IPRbooks. Лицензионный договор № ЕП44 № 001/9 на предоставление доступа к электронно-библиотечной системе IPRbooks ИКЗ 191272700076927030100100090016311000 от 27 марта 2019 г.

3 Электронно-библиотечная система eLIBRARY.RU. Договор № ЕП 44 № 004/13 на оказание услуг доступа к электронным изданиям ИКЗ 912727000769270301001001500163110000 от 15 апреля 2019 г.

4 Информационно-справочные системы «Кодекс»/ «Техэксперт». Соглашение о сотрудничестве № 25/19 от 31 мая 2019 г.

16.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Криптографические методы защиты информации. // Национальный открытый университет «Интуит» [Электронный ресурс] – Режим доступа: https://www.intuit.ru/studies/courses/13837/1234/info - свободный.

16.6 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 7 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты / условия использования
Microsoft Windows Seven	Лицензионный сертификат № 46243844 от 09.12.2009
OpenOffice	Свободная лицензия, условия использования по ссылке: https://www.openoffice.org/license.html
Microsoft Visual Studio 2008/2010/2012/2013/2017	(в составе лицензии dreamspark)
КриптоПРО CSP 3.6 или выше	3636B-F0000-01760-NKN4A на 4 АРМ

17 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель может проводить инструктаж по выполнению задания. В инструктаж включается:

· цель и содержание задания;

· сроки выполнения;

· ориентировочный объем работы;

· основные требования к результатам работы и критерии оценки;

· возможные типичные ошибки при выполнении.

Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

18 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

18.1 Учебно-лабораторное оборудование

Таблица 8 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
компьютерные классы ФКТ	Учебные лаборатории «Полигон вычислительной техники» 313(5), 201(5), 202(5)	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2, Сканер ВС, Анализатор сетевого траффика Астра, Агент инвентаризации сети, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор Компьютеры с ОС Windows и Linux.

18.2 Технические и электронные средства обучения

При проведении занятий используется аудитория, оборудованная проектором (стационарным или переносным) для отображения презентаций. Кроме того, при проведении лекций и практических занятий необходим компьютер с установленным на нем браузером и программным обеспечением для демонстрации презентаций.

Для реализации дисциплины подготовлены следующие презентации:

1 Высшее образование в РФ.

2 Виды учебных занятий, виды контроля занятий.

3 Разработка интеллект-карт.

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине
Криптографические методы защиты информации

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
3	*5*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*ИБАС*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины «Криптографические методы защиты информации» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные компетенции			
Способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14)	З1(ПК-14-4) Основные задачи и понятия криптографии, виды шифров	У1(ПК-14-4) Эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах	Н1(ПК-14-4) Использования типовых криптографических алгоритмов
	З2(ПК-14-4) Модели шифров и математические методы их исследования	У2(ПК-14-4) Применять математические методы исследования моделей шифров.	Н2(ПК-14-4) Использования ЭВМ в анализе простых шифров
	З1(ПК-14-5) Типовые поточные и блочные шифры	У1(ПК-14-5) Использовать средства электронно-цифровой подписи	Н1(ПК-14-5) Математического моделирования в криптографии
	З2(ПК-14-5) Типовые шифры с открытыми ключами	У2(ПК-14-5) Проводить настройку криптографических средств.	Н2(ПК-14-5) Криптографической терминологией

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Формируемая компетенция**	**Наименование оценочного средства**	**Показатели оценки**
Все темы	ПК-14	Лабораторные работы 1-6, Контрольная работа	Знает основные задачи и понятия криптографии, виды шифров, модели шифров и математические методы их исследования, типовые поточные и блочные шифры, типовые шифры с открытыми ключами Умеет эффективно использовать криптографические методы и

			средства защиты информации в автоматизированных системах, применять математические методы исследования моделей шифров, использовать средства электронно-цифровой подписи, проводить настройку криптографических средств. Владеет навыками использования типовых криптографических алгоритмов, использования ЭВМ в анализе простых шифров, математического моделирования в криптографии, криптографической терминологией

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

	Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания**
Промежуточная аттестация в форме экзамена				
1	Лабораторная работа 1	1 – 3 недели семестра	10 баллов	10 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 6 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 4 балла - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
2	Лабораторная работа 2	3 – 5 недели семестра	10 баллов	
3	Лабораторная работа 3	5 – 7 недели семестра	10 баллов	
4	Лабораторная работа 4	7 –9 недели семестра	10 баллов	
5	Лабораторная работа 5	10 – 12 недели семестра	10 баллов	
6	Лабораторная работа 6	12 – 14 недели семестра	10 баллов	
11	РГР	14 – 16 недели семестра	40 баллов	40 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 25 баллов – студент выполнил задание с неточностями и/или не

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 15 баллов - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
ИТОГО Текущий контроль:		-	100 баллов	-
12	Вопросы экзамена (2 вопроса по 10 баллов)	сессия	20	0 баллов – ответ на вопрос билета отсутствует или не верен 4 балла – дан не полный ответ, допущены ошибки 7 баллов – дан полный ответ, допущены неточности 10 баллов – дан полный ответ, приведены примеры
ИТОГО Промежуточная аттестация (экзамен)		-	20 баллов	
Критерии оценки результатов обучения по дисциплине: 0 – 64% от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине); 65-74% от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75-84% от максимально возможной суммы баллов – «хорошо» (средний уровень); 85-100% от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

Задания для текущего контроля

Лабораторная работа № 1

Вариант 1

Задумано двузначное число. Найти вероятность того, что задуманным числом окажется случайно названное двузначное число.

Вариант 2

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна пяти, а произведение — четырем».

Вариант 3

На плоскости заданы три концентрические окружности с радиусами: 3 см, 5 см, 8 см. Точка ставится наугад в область между меньше и большей окружностями. Найти вероятность того, что она попадет в промежуток между меньшей и средней окружностями.

Вариант 4

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна восьми, а разность — четырем».

Вариант 5

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна восьми, если известно, что их разность равна четырем».

Вариант 6

Задумано двузначное число. Найти вероятность того, что задуманным числом окажется случайно названное двузначное число, цифры которого различны.

Вариант 7

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет ноль окрашенных граней.

Вариант 8

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет одну окрашенную грань.

Вариант 9

Монета брошена два раза. Найти вероятность того, что оба раза появится «герб».

Вариант 10

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет три окрашенных грани.

Вариант 11

Монета брошена два раза. Найти вероятность того, что хотя бы один раз появится «герб».

Вариант 12

Куб, все грани которого окрашены, распилен на тысячу кубиков одинакового размера, которые затем тщательно перемешаны. Найти вероятность того, что наудачу извлеченный кубик имеет две окрашенные грани.

Вариант 13

В коробке шесть одинаковых, занумерованных кубиков. Наудачу по одному извлекают все кубики. Найти вероятность того, что номера извлеченных кубиков появятся в возрастающем порядке.

Вариант 14

Брошены две игральные кости. Найти вероятность события: «сумма выпавших очков равна семи».

Вариант 15

В колоде 36 карт четырех мастей. После извлечения и возвращения одной карты колода перемешивается и снова извлекается одна карта. Определить вероятность того, что обе извлеченные карты одной масти.

Лабораторная работа № 2

Ниже используются традиционные для криптографии обозначения: ***M*** – открытый текст, ***C*** – шифротект, ***K*** – ключ.

Вариант 1

Зашифровать и дешифровать M = «абсолютная стойкость» с помощью шифра Виженера, ключ K = «окно».

Вариант 2

Зашифровать и дешифровать M = «квантовый алгоритм шора» с помощью шифра простой замены с генерацией таблицы по слову, ключ K = «решетка».

Вариант 3

Зашифровать M = «производная» с помощью шифра Хилла, ключ K = «фестиваль».

Вариант 4

Зашифровать и дешифровать М = «условная вероятность» с помощью шифра Полибианский квадрат, ключ К = «автомат».

Вариант 5

Зашифровать и дешифровать М = «квантовый алгоритм гровера» с помощью шифра Плейфера, К = «предел, группа».

Вариант 6

Зашифровать и дешифровать М = «генераторы псевдослучайных чисел используются в криптографии» с помощью шифра перестановки по столбцам, К = «651342».

Вариант 7

Зашифровать и дешифровать М = «информационная безопасность» с помощью шифра Полибианский квадрат, ключ К = «квант, кубит».

Вариант 8

Зашифровать М = «аутентификация» с помощью шифра Хилла, К = «указатель».

Вариант 9

Зашифровать и дешифровать М = «дискретная математика» с помощью шифра Виженера, ключ К = «наука».

Вариант 10

Зашифровать и дешифровать М = «обеспечение конфиденциальности является задача криптографии» с помощью шифра перестановки по столбцам К = «2157364».

Вариант 11

Зашифровать и дешифровать М = «стеганография» с помощью шифра Виженера, ключ К = «жизнь».

Вариант 12

Зашифровать и дешифровать М = «сцепление блоков» с помощью шифра простой замены с генерацией таблицы по слову, К = «протокол».

Вариант 13

Зашифровать и дешифровать М = «кодовая книга» с помощью шифра Двойной квадрат, К = «кольцо, алгебра».

Вариант 14

Зашифровать и дешифровать М = «целостность сообщений» с помощью шифра Плейфера, К = «электрон, позитрон».

Вариант 15

Зашифровать и дешифровать М = «криптографический протокол» с помощью шифра Двойной квадрат, К = «алгебра, геометрия».

Лабораторная работа № 3

Даны числа p, q, m. Вычислить недостающие параметры алгоритма, зашифровать m, затем дешифровать полученный шифротекст и сравнить.

Номер варианта	p	q	m
1	7	17	16
2	3	31	24
3	7	11	8
4	5	11	9
5	3	17	20
6	3	5	10
7	5	7	6
8	5	13	14
9	7	13	15

10	3	23	22
11	5	17	18
12	3	13	12
13	3	19	21
14	3	11	7
15	3	29	23
16	3	7	11

Лабораторная работа № 4

Даны числа p, g, a, b. Найти недостающие параметры и сформировать общий секретный ключ (как со стороны Алисы, так и со стороны Боба).

Номер варианта	p	g	a	b
1	23	5	10	7
2	17	3	15	6
3	23	7	11	12
4	23	7	7	13
5	19	10	9	10
6	23	5	8	18
7	17	3	6	16
8	23	7	12	21
9	19	2	13	17
10	17	3	12	15
11	23	7	17	20
12	19	2	18	8
13	19	2	10	5
14	23	5	16	11
15	17	3	14	9
16	19	2	17	14

Лабораторная работа № 5

Даны числа p, g, x, k, m. Сформировать недостающие параметры алгоритма Эль-Гамаля. Зашифровать m, затем дешифровать полученный шифротекст и сравнить.

Номер варианта	p	g	x	k	m
1	23	5	13	8	7
2	17	3	11	9	4
3	23	7	9	7	10
4	17	3	12	11	8
5	23	5	10	7	13
6	23	5	12	6	5

7	23	7	8	8	11
8	17	3	9	7	10
9	19	2	7	6	6
10	23	5	11	5	9
11	23	7	12	9	12
12	19	2	6	5	3
13	19	2	8	7	7
14	23	7	11	10	9
15	17	3	10	8	7
16	19	2	5	4	8

Лабораторная работа № 6

19 Установить и настроить Crypto Pro 3.6 или выше.
20 Установить считыватели в КриптоПро.
21 Установить etoket pki client
22 Установить датчики случайных чисел
23 Установить VipNet CSP
24 Установить VipNetClient для работы с деловой почтой
25 Установить КриптоПро для работы с ЭЦП в Word
26 Установить КриптоПро, описать вкладки.
27 Установить VipNet CryptoFile
28 Установить КриптоПро плагины для PDF
29 Установить КриптоПро с официального сайта последнюю версию. (сертифицированную версию).
30 Установить КриптоПро с официального сайте последнюю версию (несертифицированную).
31 Сгенерировать запрос на сертификат в КриптоПро
32 Выгрузить Сертификат ЭЦП.
33 Продемонстрировать установленные на АРМ сертификаты ЭЦП используя оснастку КриптоПро.

Пример задания на РГР

1. Реализовать алгоритм DES на любом языке программирования.
2. Реализовать алгоритм AES на любом языке программирования.

Возможные вопросы и задания для защиты работ

21. Основы теории чисел (простые числа, распределение простых чисел, малая теорема Ферма, функция Эйлера, фактори-зация и т.д.)
22. Криптосистема Эль-Гамаля (с доказательством).
23. Алгоритм Диффи-Хеллмана.
24. Односторонние функции (с примерами).
25. Электронно-цифровая подпись (с примерами).
26. Криптосистема RSA (с доказательством).
27. Криптосистема Рабина.
28. Криптографические протоколы (с примерами)
29. Инфраструктура открытых ключей
30. ЭЦП Эль-Гамаля (с доказательством)
31. Основные понятия и определения криптографии.
32. Основные понятия теории вероятностей.

33. Абсолютная криптографическая стойкость.
34. Этапы развития криптографии.
35. Поточные шифры: принципы проектирования и составные блоки.
36. Поточный шифр A5/1. Принцип работы.
37. Шифр DES, характеристики, принцип работы.
38. Российский стандарт симметричного шифрования. Характеристики, принцип работы.
39. Режимы работы блочных шифров.
40. Составные элементы и структура блочных шифров.

Экзаменационные вопросы

31. Основные понятия и определения криптографии (определения, задачи, родственные науки, области применения).
32. История криптографии (основные этапы развития криптографии, исторические шифры).
33. Криптографическая стойкость (различные подходы к определению стойкости, теоретико-информационная стойкость, абсолютная стойкость и ее смысл, шифр Вернама, вычислительная стойкость).
34. Поточные шифры (основные принципы проектирования поточных шифров, примеры поточных шифров).
35. Основные составные блоки поточных шифров и их комбинации (регистр сдвига с линейными обратными связями и т.д.)
36. Практическое применение поточных шифров (шифрование в GSM, шифры проекта eStream).
37. Блочные шифры, основные определения (рассеивание, перемешивание, псевдослучайная функция, лавинный эффект).
38. Структура блочных шифров
39. Основные компоненты блочных шифров
40. Алгоритм шифрования DES и его модификации
41. Режимы работы блочных шифров (возможность параллельной обработки, распространение ошибки)
42. Российский стандарт шифрования ГОСТ 34.12-2018.
43. Алгоритм шифрования AES.
44. Шифры-финалисты конкурса AES (Serpent, Twofish).
45. Облегченная криптография (принципы построения, примеры шифров).
46. Хэш-функции.
47. Коды аутентификации сообщений (CBC-MAC, HMAC и т.д.), стойкость MAC.
48. Аутентифицированное шифрование
49. Основы теории чисел (простые чисел, арифметика остатком, малая теорема Ферма, теорема Эйлера).
50. Основы криптографии с открытым ключом (основные определения, односторонние функции, примеры).
51. Криптосистема RSA (шифрование, дешифрование).
52. Алгоритмы быстрого возведения в степень.
53. Генерация больших простых чисел. Тест Миллера-Рабина.
54. Недостатки криптосистемы RSA. Использование RSA на практике.
55. Алгоритм Диффи-Хеллмана.
56. Криптосистема Эль-Гамаля.
57. Криптосистема Рабина.

58. Аутентификация и электронно-цифровая подпись.
59. ЭЦП на основе криптосистема RSA.
60. Инфраструктура открытых ключей.

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД
1	03.10.2022 № 2 (актуализация литературы)	1	