Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптология

(наименование дисциплины)

Направление 10.03.01 "Информационная безопасность"

Направленность "Комплексная защита объектов информатизации"

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	3/108	36		18	54	Зачет
6	3/108	36		36	36	Зачет
7	6/216	18		36	117	Экзамен (45ч), КР
Итого	12/432	90		90	207	Зачет, зачет, экзамен (36ч), КР

Владимир 2018

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Криптология» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», ознакомление студентов с основами теории двоичного кодирования, алгоритмами сжатия, помехоустойчивого кодирования. Дисциплина «Криптология» рассматривается как теоретическая и прикладная дисциплина, дающая представления об основных математических и алгоритмических подходах, применяемых для хранения, передачи, исправления информации, представленной в двоичных кодах. Дисциплина посвящена изучению основ криптографии и криптографического анализа, применяемых к защите информации в информационных системах Обучаемые знакомятся с понятием шифров, симметричной и асимметричной криптографии, электронной подписью, хешированием и другими математическими объектами криптографии. Изучаются соответствующие криптографические стандарты, применяемые сегодня в защите информации в России и за рубежом. Подробно рассматриваются: стандарты RSA, DES, GOST1989, и другие. Также уделено внимание перспективным направлениям в криптографии: криптографические протоколы с разглашением и без разглашения, теория алгоритмической сложности и односторонних функций, схемы разделения секрета и некоторые их приложения в задачах идентификации и аутентификации.

Задачами изучения дисциплины «Криптология» являются: -ознакомление с основами математической теории криптологии; - приобретение навыков в практическом использовании, постановке и решении задач шифрования информации; - понимание сути информационных процессов в криптографических системах; - применение компьютеров для решения задач шифрования и дешифрования; - разработка и использование математических и вычислительных моделей процессов шифрования информации, их оптимизация и выработка направлений совершенствования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.05). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и практических занятий.

Дисциплина изучается на 3 и 4 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Математика», «Информатика» по направленности 10.03.01 «Информационная безопасность», квалификации - бакалавр. Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Основы информационной безопасности», «Техническая защита информации», «Программно-аппаратные средства защиты информации», «Математические методы в информационной безопасности».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими общепрофессиональными компетенциями:

ОПК-2 – способностью применять соответствующий математический аппарат для решения профессиональных задач

ПК-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

ПК-2 - способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** -основные положения (основополагающие теоремы) криптологии, вытекающие из теории симметричных и ассиметричных криптографических подходов, а также

информационные критерии оценок функционирования криптографических систем (ОПК-2; ПК-1, ПК-2);

2) **Уметь:** - применять эти знания для анализа существующих и вновь проектируемых информационных криптографических систем; - разрабатывать и рассчитать характеристики криптографической защиты информационных систем в зависимости от назначения этих систем (количество информации, скорость передачи информации, пропускную способность каналов связи, требуемый объём памяти и др.); - при заданных требованиях к техническим характеристикам и показателям качества функционирования систем правильно и аргументированно выбрать (предложить) методы обеспечения этих требований и показателей; - применять современные технологии криптографии в задачах обработки информации (ОПК-2; ПК-1, ПК-2);

3) **Владеть:** -научно-технической терминологией; общими проблемы криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем (ОПК-2; ПК-1, ПК-2).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность применять основные криптологические алгоритмы для решения прикладных задач в области информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 12 зачетных единицы, 432 часа.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
1.	Введение. Основные задачи криптологии. Криптография и криптографический анализ	5	1-2	4		2		6		4/67%	
2.	Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования. Примеры щифров. Шифр Цезаря, Полибия	5	3-4	4		2		6		4/67%	
3.	Симметричные шифры. Группы подстановок и перестановок.	5	5-6	4		2		6		4/67%	Рейтинг-контроль №1
4.	Чистые шифры. Шифры Виженера и Вернама.	5	7-8	4		2		6		4/67%	
5.	Одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре.	5	9-10	4		2		6		4/67%	
6.	Принцип Керкхоффса. Проблемы симметричной криптографии.	5	11-12	4		2		6		4/67%	Рейтинг-контроль №2
7.	Хеш - функции. Хеш - функции,	5	13-14	4		2		6		4/67%	
8.	Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий. Парадокс о днях рождения	5	15-16	4		2		6		4/67%	
9.	Блочные Шифры. Стандарты DES	5	17-18	4		2		6		4/67%	Рейтинг-контроль №3
Всего по семестру 5:				36		18		54		36/ 67%	Зачет
1	Стандарт GOST1989. Поточные шифры. Стандарт A5.	6	1-2	4		4		4		4/50%	
2	Асимметричная криптография. Классы алгоритмической сложности.	6	3-4	4		4		4		4/50%	
3	Сложность математических задач. Односторонние функции	6	5-6	4		4		4		4/50%	Рейтинг-контроль №1
4	Задачи факторизации и дискретного логарифма.	6	7-8	4		4		4		4/50%	
5	Функция Эйлера. RSA.	6	9-10	4		4		4		4/50%	
6	Электронная подпись.	6	11-12	4		4		4		4/50%	Рейтинг-контроль №2

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра),* форма промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
7	Криптографические протоколы.	6	13-14	4		4		4		4/50%	
8	Протокол анонимных вычислений. Схемы разделения секрета	6	15-16	4		4		4		4/50%	
9	Криптография на эллиптических кривых	6	17-18	4		4		4		4/50%	Рейтинг-контроль №3
Всего по 6 семестру:				36		36		36		36/50%	Зачет
1	Криптографический анализ	7	1-2	2		4		13		2/33%	
2	Пассивный криптографический анализ	7	3-4	2		4		13		2/33%	
3	Частотный анализ	7	5-6	2		4		13		2/33%	Рейтинг-контроль №1
4	Дифференциальный и линейный криптографический анализ	7	7-8	2		4		13		2/33%	
5	Активный криптоанализ	7	9-10	2		4		13		2/33%	
6	Пороговые схемы разделения	7	11-12	2		4		13		2/33%	Рейтинг-контроль №2
7	Протокол анонимных вычислений	7	13-14	2		4		13		2/33%	
8	МИТМ- атака на протокол	7	15-16	2		4		13		2/33%	
9	СРС Ади Шамира	7	17-18	2		4		13		2/33%	Рейтинг-контроль №3
Всего по 7 семестру:				18		36		117	КР	18/33%	Экзамен (45ч)
ИТОГО:				90		90		216	КР	90/50%	ЭКЗАМЕН

Содержание разделов дисциплины «Криптология»

1. Введение. Симметричная криптография.
2. Основные задачи теории криптологии.
3. Криптография и криптографический анализ.
4. Краткая справка по истории возникновения и развития, и современному состоянию криптографии.
5. Основные понятия криптологии.
6. Открытый и закрытый тексты. Шифры и ключи.
7. Канал секретной связи.
8. Возможности противника в канале связи. Определение криптографической системы по Шеннону.
9. Подстановки и перестановки. Примеры шифров.
10. Шифры Цезаря и Полибия. Д
11. войственность подстановки и перестановки.

12. Теорема о сохранении энтропии открытого текста при применении подстановки и перестановки.
13. Взлом подстановок и перестановок методами частотного анализа закрытого текста.
14. Шифр Виженера. Гаммирование.
15. Шифр Вернама и одноразовый блокнот.
16. Теорема Шеннона об абсолютно стойком шифре. Практическая стойкость шифра.
17. Принцип Керкхоффса.
18. Хеш – функции и их свойства.
19. Области применения хеш-функций в криптографии.
20. Необходимые свойства хеш для использования в электронной подписи.
21. Асимметричная криптография. Алгоритмическая сложность.
22. Классы алгоритмической сложности.
23. Сложность математических задач. Односторонние функции.
24. Задачи факторизации и дискретного логарифма.
25. Функция Эйлера.
26. Криптографическая система RSA. Электронные деньги.
27. Криптографические протоколы
28. Электронная подпись.
29. Протокол Диффи- Хеллмана создания симметричного ключа.
30. МИТМ- атака на протокол.
31. Криптографические протоколы.
32. Протокол анонимных вычислений. Схемы разделения секрета.
33. СРС Ади Шамира.
34. Пороговые схемы разделения.
35. Криптография на эллиптических кривых.
36. Криптографический анализ.
37. Пассивный криптографический анализ. Частотный анализ.
38. Дифференциальный и линейный криптографический анализ.
39. Активный криптоанализ.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направленности 10.03.01 «Информационная безопасность».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

- учебную дискуссию;
- электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты);
- дистанционные (сетевые) технологии.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП специальности 10.03.01 «Информационная безопасность», особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 55 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1 для семестра 5:

- Основные задачи криптографии и криптоанализа. Понятие криптопреобразования.

Краткая справка по истории возникновения и развития, и современному криптографии.

- Понятие несимметрии математических операций и трудоемкость элементарных

математических операций.

- Понятие криптосистемы.
- Типы криптосистем.
- Криптосистемы с открытым ключом
- Понятие электронной подписи. Необходимость электронной подписи в криптосистемах с

открытым ключом.

- Математическая теория групп как основа современных криптосистем.

Вопросы рейтинг-контроля №2 для семестра 5:

- Основные математические понятия для конечного поля, характеристика поля.
- Возможность построения конечного поля с необходимым числом элементов.
- Мультипликативная группа конечного поля. Образующие. Дискретный логарифм
- Порядок многочлена над конечным полем.
- Конструкция конечного поля из pn элементов.
- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Конструкция конечного поля из pn элементов.

Вопросы рейтинг-контроля №3 для семестра 5:

- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.

Перечень вопросов к зачету 5 семестр (промежуточной аттестации по итогам освоения дисциплины):

- Основные задачи криптографии и криптоанализа. Понятие криптопреобразования. Краткая справка по истории возникновения и развития, и современному криптографии.
- Понятие несимметрии математических операций и трудоемкость элементарных математических операций.
- Понятие криптосистемы.
- Типы криптосистем.
- Криптосистемы с открытым ключом
- Понятие электронной подписи. Необходимость электронной подписи в криптосистемах с открытым ключом.
- Математическая теория групп как основа современных криптосистем.
- Основные математические понятия для конечного поля, характеристика поля.
- Возможность построения конечного поля с необходимым числом элементов.
- Мультипликативная группа конечного поля. Образующие. Дискретный логарифм
- Группы перестановок и подстановок в криптографии. Двойственность. Теорема о сохранении энтропии для шифров подстановки и перестановки.
- Определение криптографических систем по Шеннону. Примеры шифров по Шеннону.
- Шифр Вижженера (Гаммирование). Взлом Гаммирования.
- Шифр Вернама. Одноразовый блокнот. Теорема об абсолютно стойком шифре.
- Классы сложности алгоритмов и задач. Примеры.
- Одностороннии функции. Задачи-кандидаты в одностороннии функции.
- Функции Эйлера и ее свойства. Теорема Эйлера и теорема Ферма.
- Факторизация целого числа.
- Порядок многочлена над конечным полем.
- Конструкция конечного поля из pn элементов.
- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.

- Конструкция конечного поля из pn элементов.
- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.

Вопросы рейтинг-контроля №1 для семестра 6:
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Аннулирующие многочлены.

Вопросы рейтинг-контроля №2 для семестра 6:
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.

Вопросы рейтинг-контроля №3 для семестра 6::
- Дискретные отображения и признаки хаотичности числовых рядов.
- Методы криптографии на основе сортировки детерминировано-хаотических рядов.
- Методы криптографии на основе парных сравнений чисел в детерминировано-хаотических числовых рядах.
- Стеганография.
- Оценки и критерии сложности алгоритмов криптографии.
- Криптоанализ и алгоритмические неразрешимые проблемы.
- Особенности хаотических систем.

Перечень вопросов к зачету 6 семестр (промежуточной аттестации по итогам освоения дисциплины):
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Аннулирующие многочлены.
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.

- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Методы криптографии на основе сортировки детерминировано-хаотических рядов.
- Методы криптографии на основе парных сравнений чисел в детерминировано-хаотических числовых рядах.
- Стеганография.
- Оценки и критерии сложности алгоритмов криптографии.
- Криптоанализ и алгоритмические неразрешимые проблемы.
- Особенности хаотических систем.
- Дискретный логарифм в конечных полях. Протокол Диффи-Хеллмана.
- Алгоритм RSA.
- Электронная подпись в ассиметричных схемах и ее свойства. С хеш функциями и без.
- Хеш функции и их свойства. Криптографические хеш-функции.
- Криптографические протоколы.
- Интераполяция многочленами. Теорема о существовании и единственности многочлена. Схема разделения секрета Шамира.
- Электронные деньги. Неотслеживаемость. Схема Шаума-Педерсана.
- Стандарты DES и ГОСТ Блочных шифров. Архитектурный и сравнительный анализ шифров.
- Блочные шифры. Режимы работ блочных шифров.
- Потоковые шифры.
- Криптографические модели безопасности. Модель симметричного шифрования, ассиметричного и модель Долев-Яо.

Вопросы рейтинг-контроля №1 7 семестр:
- Дать определение СЗИ.
- Что такое информационная безопасность?
- Цели информационной безопасности.
- Основные требования к комплексной системе защиты информации
- Задачи системы компьютерной безопасности
- Основные принципы организации СЗИ
- В чём заключается принцип системности?
- В чём заключается принцип комплексности?
- В чём заключается принцип непрерывности защиты?
- В чём заключается принцип разумной достаточности?
- В чём заключается гибкость системы защиты?
- Принцип простоты применения средств защиты
- Этап работ по созданию СЗИ.

Вопросы рейтинг-контроля №2 7 семестр:
- Что включает в себя обследование организации?
- Факторы, влияющие на организацию СЗИ.
- Определение состава защищаемой информации
- Нормативное закрепление состава защищаемой информации
- Виды информации.
- Необходимые свойства защищаемой информации

- Категорирование защищаемой информации.
- Определение объектов защиты.
- Что называется объектом защиты.
- Основные объекты защиты.
- Основные виды угроз информационной безопасности:
- Классификация угроз безопасности
- Неформальная модель нарушителя в АС .
- Что определяются при разработке модели нарушителя.

Вопросы рейтинг-контроля №3 7 семестр:
- Причины совершения компьютерных преступлений
- Потенциальные каналы несанкционированного доступа к защищаемой информации
- Потенциальные методы несанкционированного доступа к защищаемой информации.
- Классификация каналов проникновения в систему и утечки информации
- Физические каналы.
- Электромагнитные каналы.
- Информационные каналы
- Общая модель комплексной системы защиты информации.
- Средства защиты, используемые для создания системы защиты.
- Типы моделей управления доступом.
- Организационное направление работ по созданию СЗИ.
- Технология построения СЗИ
- Кадровое обеспечение функционирования СЗИ.
- Организационная структура, основные функции службы компьютерной безопасности.
- Концепция (политика) безопасности.

Темы лабораторных работ 5 семестр:
Лабораторная работа №1. Тема: Шифр Полибия;
Лабораторная работа №2.Тема: Шифрование файлов. Четыре криптопримитива;
Лабораторная работа №3.Тема: Многораундовое шифрование;
Лабораторная работа №4.Тема: Криптографические тесты (NIST).

Темы лабораторных работ 6 семестр:
Лабораторная работа №1.Тема: Хэш-функция. Электронная подпись;
Лабораторная работа №2.Тема: Генератор псевдослучайных последовательностей;
Лабораторная работа №3.Тема: Генерация ключей;
Лабораторная работа №4. Тема: Арифметика с длинными целыми.

Темы лабораторных работ 7 семестр:
Лабораторная работа №1. Построение описания объекта информатизации. Общее описание объекта и его планировка. Построение описания объекта информатизации.
Лабораторная работа №2. Перечень и характеристики информационных ресурсов. Построение описания объекта информатизации. Список и характеристики персонала.
Лабораторная работа №3.Проектирование корпоративной сети передачи данных
Лабораторная работа №4.Проектирование корпоративной сети передачи данных.

Вопросы и задания для самостоятельной работы студентов 5 семестр:
- Какие основные модели цифровых автоматов используются в криптографии?
- Особенности функционирования и взаимодействия цифровых автоматов в криптографических системах.
- Алгоритмы, универсальные алгоритмические системы, достоинства и недостатки;
- Основные понятия и определения, эквивалентность алгоритмов.
- Временная и емкостная сложность алгоритмов.

- Особенности многоядерных процессоров.
- Сопоставительный анализ

Вопросы и задания для самостоятельной работы студентов 6 семестр:
- Одномерные и многомерные дискретные отображения, примеры;
- Методы минимизации и их сопоставительный анализ?
- Сложность алгоритмов криптографии. Критерии и оценки;
- Основные соотношения затрат памяти и времени.
- Автоматы на основе дискретного отображения Лоренца, достоинства и недостатки;
- Автоматы на основе отображений TentMap и Хенона, сопоставительный анализ.
- Сопоставительный анализ алгоритмов криптоанализа, оценки сложности;
- Перспективы криптоанализа и алгоритмически неразрешимы проблемы.

Вопросы и задания для самостоятельной работы студентов 7 семестр:
- Прокомментируйте основные направления обеспечения ИБ
- Что понимается под безопасностью информации? Что такое ЗИ?
- Дайте определение понятиям «конфиденциальность», «целостность», «доступность».
- Перечислите основные задачи системы информационной безопасности.
- В чем заключается основная цель защиты информации?
- Определите организационные проблемы информационной безопасности.
- Сформулируйте технические проблемы информационной безопасности.
- Раскройте общее содержание методологии проектирования системы ЗИ. Как понимается процесс создания оптимальной системы? Сформулируйте возможные постановки задачи оптимизации СЗИ.
- Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
- Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
- Дайте определение системы ЗИ и сформулируйте основные концептуальные требования, предъявляемые к ней.
- Приведите принятую методику построения системы ИБ предприятия

Перечень вопросов к экзамену 7 семестр (промежуточной аттестации по итогам освоения дисциплины):
1. Дать определение СЗИ.
2. Что такое информационная безопасность?
3. Цели информационной безопасности.
4. Основные требования к комплексной системе защиты информации
5. Задачи системы компьютерной безопасности
6. Основные принципы организации СЗИ
7. В чём заключается принцип системности?
8. В чём заключается принцип комплексности?
9. В чём заключается принцип непрерывности защиты?
10. В чём заключается принцип разумной достаточности?
11. В чём заключается гибкость системы защиты?
12. Принцип простоты применения средств защиты
13. Этап работ по созданию СЗИ.
14. Что включает в себя обследование организации?
15. Факторы, влияющие на организацию СЗИ.
16. Определение состава защищаемой информации
17. Нормативное закрепление состава защищаемой информации
18. Виды информации.

19. Необходимые свойства защищаемой информации
20. Категорирование защищаемой информации.
21. Определение объектов защиты.
22. Что называется объектом защиты.
23. Основные объекты защиты.

Темы курсовых работ по предмету «Криптология» 7 семестр.

1. Криптография на эллиптических кривых. Отечественный стандарт электронной подписи.
2. SMT- протоколы передачи информации и их перспективы внедрения.
3. Задача о рюкзаке и рюкзачные криптографические системы. Взлом рюкзаков Меркля.
4. Протоколы доказательства без разглашения. Протокол Фиата – Шамира.
5. Протокол Диффи – Хеллмана создания симметричного ключа. Его слабость по отношению к МИТМ- атаке. Варианты усиления DH – протокола.
6. Стандарт AES (Rijndael), его криптоанализ. Варианты атак на него.
7. Стандарт LTE и его криптографические свойства.
8. Потоковые шифры. Стандарт шифрования A5 и его вариации.
9. Стандарты связи GSM и его защитные модули.
10. Криптография разделения секрета на доли секрета. Визуальная криптография в работе с изображениями.
11. Стеганография.
12. Блочные шифры и различные режимы их работы на примерах DES и GOST1989.
13. Стандарты хеширования. Их криптоанализ. MD5, SHA.
14. Российский стандарт электронной подписи.
15. Электронные деньги. Подпись вслепую электронных купюр Чаума – Педерсена.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6, Режим доступа: http://znanium.com/catalog.php?bookinfo=474838
2. Кнауб, Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2012. - 160 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=441493
3. Каратунова, Н. Г. Защита информации. Курс лекций : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://znanium.com/catalog.php?bookinfo=503511

б) Дополнительная литература:

1. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - http://www.studentlibrary.ru/book/ISBN5980030026.html 256 с. ISBN 5-98003-002-6.
2. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М. : СОЛОН-ПРЕСС, 2009. http://www.studentlibrary.ru/book/ISBN5980030115.html 272 с.
3. Башлы, П. Н. Информационная безопасность и защита информации : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

в) Периодические издания:

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 "Информационная безопасность ", направленность «Комплексная защита объектов информатизации»

Рабочую программу составил зав. кафедрой ИЗИ д.т.н., Монахов М.Ю.

(ФИО, подпись)

Рецензент
(представитель работодателя) к.т.н. Вертилевский Н.В. РАЦ ООО «ИнфоЦентр»
Заместитель руководителя.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 30.08.18 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии по направлению 10.03.01 "Информационная безопасность ", направленность «Комплексная защита объектов информатизации»

Протокол № 1 от 30.08.18 года

Председатель комиссии д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)