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)**

Институт прикладной математики, физики и информатики
(Наименование института)

УТВЕРЖДАЮ:
Директор института
_____ Хорьков К.С.
«30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ЗАЩИТА ИНФОРМАЦИИ
(наименование дисциплины)

направление подготовки / специальность
02.03.01 «Математика и компьютерные науки»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

Математические методы в экономике и финансах
(направленность (профиль) подготовки))

г. Владимир

2021 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защита информации» является обучение студентов методологии решения проблем и задач в области информационной безопасности с использованием математического аппарата и криптографических преобразований.
Задачи:

- Овладение навыками анализа защищенности информационной системы
- Изучение принципов работы с криптографическими алгоритмами и оценкой их криптостойкости.
- Формирование навыков работы со стандартными криптографическими алгоритмами с использованием современного аппарата программирования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации» относится к относится к разделу Б1.О.30 - Обязательные дисциплины учебного плана.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора*	Результаты обучения по дисциплине	
ОПК-4. Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	ОПК-4.1. Знает базовые основы современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности. ОПК-4.2. Умеет использовать этот математический аппарат в профессиональной деятельности. ОПК-4.3. Владеет практическим опытом применения современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях	Знать: базовые основы современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности. Уметь: использовать этот математический аппарат в профессиональной деятельности. Владеть: практическим опытом применения современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях.	Контрольные вопросы
ОПК-5. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-5.1. Знает принципы работы современных информационных технологий. ОПК-5.2. Умеет использовать современные информационные технологии в профессиональной деятельности. ОПК-5.3. Владеет практическими навыками разработки ПО.	Знать: принципы работы современных информационных технологий. Уметь: использовать современные информационные технологии в профессиональной деятельности. Владеть: практическими навыками разработки ПО.	Контрольные вопросы
ОПК-6. Способен разрабатывать алгоритмы и	ОПК-6.1. Знает методы алгоритмизации, языки и технологии программирования, пригодные для практического	Знать: методы алгоритмизации, языки и технологии программирования, пригодные для практического	Контрольные вопросы

компьютерные программы, пригодные для практического применения.	применения в области информационных систем и технологий. ОПК-6.2. Умеет применять методы алгоритмизации, языки и технологии программирования при решении профессиональных задач в области информационных систем и технологий. ОПК-6.3. Владеет навыками программирования, отладки и тестирования прототипов программно-технических комплексов задач.	применения в области информационных систем и технологий. Уметь: применять методы алгоритмизации, языки и технологии программирования при решении профессиональных задач в области информационных систем и технологий. Владеть: навыками программирования, отладки и тестирования прототипов программно-технических комплексов задач.	
ПК-4. способностью публично представлять собственные и известные научные результаты	ПК-4 .1. Знает: основные понятия, методы доказательств математических утверждений, их следствия. ПК-4.2. Умеет: осуществлять поиск специальной литературы и выбирать эффективные методы изложения полученных результатов ПК-4.3. Владеет: навыками систематизации и выбора необходимой информации для изложения полученных результатов при решении поставленной задачи	Знать: основные понятия, методы доказательств математических утверждений, их следствия. Уметь: осуществлять поиск специальной литературы и выбирать эффективные методы изложения полученных результатов Владеть: навыками систематизации и выбора необходимой информации для изложения полученных результатов при решении поставленной задачи	Контрольные вопросы

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет ____5__ зачетных единиц, ___180____ часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Теоретические основы защиты информации	7	1-4	4	-	2	2	25	рейтинг-контроль №1
2	Криптографические методы защиты информации	7	5-14	28	-	12	12	25	рейтинг-контроль №2
3	Основы криптоанализа	7	15-16	2	-	2	2	24	
4	Основы стеганографии	7	17-18	2	-	2	2	25	рейтинг-контроль №3
Всего за _7__ семестр:				36		18	18	99	
Наличие в дисциплине КП/КР		-	-	-	-	-	-	-	
Итого по дисциплине		-	-	36	-	18	18	99	экзамен 27 ч.

Содержание лекционных занятий по дисциплине

Раздел 1. Теоретические основы защиты информации

Тема 1. Понятие информационной безопасности. Ключевые вопросы информационной безопасности.

Рассматриваются понятия экономической и информационной безопасности. Описывается общая структура информационной безопасности с точки зрения требований информационной

безопасности. Рассматриваются ключевые вопросы информационной безопасности: надо ли защищаться и что следует защищать? от кого надо защищаться? от чего надо защищаться? как надо защищаться? что обеспечит эффективность защиты? во что обойдется разработка, внедрение, эксплуатация, сопровождение и развитие систем защиты?

Тема 2. Виды угроз информационной безопасности

Приводятся виды угроз информационной безопасности, классификация источников угроз и защищаемой информации.

Тема 3. Основы законодательства в области обеспечения информационной безопасности

Рассматривается нормативной база для защиты информации. Законодательство США и Европы в сфере защиты информации. Законодательство РФ в сфере защиты информации.

Тема 4. Построение системы информационной безопасности

Раскрываются понятия ответственности и программы информационной безопасности. Рассматриваются модели информационной безопасности, требования и основные этапы реализации информационной безопасности. Указываются мероприятия по защите информации, применяемые в организации. Рассматривается понятие политики безопасности, проводится рассмотрение методов анализа и управления рисками при реализации информационной безопасности

Раздел 2. Криптографические методы защиты информации

Тема 1. Основные понятия криптографии. Классификация шифров.

Рассматриваются понятия криптографии, ключа, шифра, криптограммы, криптографического преобразования, шифрования, дешифрования. Приводится схем простейшей криптографической системы по Шеннону. Рассматривается классификации шифров по разным признакам.

Тема 2. Классическая криптография.

Рассматриваются исторические криптографические системы (ширф и шифровальные устройства) с древнейших времен до середины XX в.

Тема 3. Перестановочные и шифры замены.

Рассматриваются шифры перестановок и замены, моноалфавитные и полиалфавитные. В качестве примеров рассматриваются шифры Цезаря и Виженера. Указываются методы их криптоанализа.

Тема 4. Шифрование гаммированием и одноразовые блокноты (шифр Вернама).

Рассматривается алгоритм шифрования гаммированием и шифр Вернама. Показывается криптостойкость шифра Вернама.

Тема 5. Симметричные шифры. Сеть Фейстеля.

Рассматривается алгоритм шифрования с использованием сети Фейстеля, а так же основные преобразующие функции, используемые в данном алгоритме. Примеры шифрования/дешифрования. Указываются методы криптоанализа данного шифра.

Тема 5. Симметричные шифры. DES

Рассматривается алгоритм шифрования DES, режимы его работы (CBC;CFB;OFB). Примеры шифрования/дешифрования. Указываются методы криптоанализа данного шифра.

Тема 6. Симметричные шифры. Шифр ГОСТ 28147-89, шифр Blowfish.

Рассматриваются алгоритмы шифрования ГОСТ и Blowfish. Указываются преимущества по сравнению с DES.

Тема 7. Симметричные шифры. Алгоритм Rijndael, шифр AES.

Рассматриваются алгоритмы шифрования Rijndael и основанный на нем AES.

Тема 8. Симметричные шифры. Управление ключевой информацией.

Рассматривается Протокол Kerberos.

Тема 9. Потоковые шифры

Рассматривается понятие потокового шифра. Типы потоковых шифров, их отличие от блочных.

Тема 10. Потоковые шифры. Шифр RC4.

Рассматривается алгоритм RC4, его криптоанализ и примеры использования.

Тема 11.Ассиметричное шифрование.

Рассматривается понятие ассиметричного шифра. Его отличие от симметричного.

Тема 11.Ассиметричное шифрование. Распределение ключей по схеме Диффи-Хеллмана

Рассматривается алгоритм Диффи-Хеллмана, позволяющий двум абонентам, обмениваясь сообщениями по небезопасному каналу связи, распределить между собой секретный ключ шифрования.

Тема 12.Ассиметричное шифрование. Шифры RSA, Эль-Гамаля.

Рассматриваются криптографические системы на основе алгоритмов RSA и Эль-Гамаля.

Тема 13. Комбинированная криптосистема шифрования

Рассматриваются методы совместного использование симметричных и ассиметричных шифров.

Тема 14. Хэш функции. Алгоритмы SHA-1 и N-hash.

Рассматриваются понятия хэш функции, дайджетса и их особенностей. Рассматриваются реализации хэш функций и шифров на из основе по алгоритмам SHA-1 и N-hash.

Тема 15. Электронная цифровая подпись (ЭЦП). Алгоритм формирования электронно-цифровой подписи DSA.

Рассматривается понятие ЭЦП, а также ее формирование на основе алгоритма DSA.

Тема 16. Защита информации в IP сетях.

Рассматриваются основные протоколы сети Интернет, обеспечивающие защиту информации: S/MIME, SSL и TLS, IPSec, SKIP, ISAKMP и межсетевые экраны.

Тема 17. Криптоалгоритмы пространства .Net.

Рассматривается пространство имен Пространство имен Cryptography в .NET Framework.

Тема 18. XML- криптография

Рассматриваются возможности XML –криптографии, сравниваются различные типы XML –подписей

Раздел 3. Криптоанализ.

Тема 19. Криптоанализ

Рассматриваются методы криптоанализа: частотный, метод полного перебора, атака по ключам, метод "встречи посередине". Криптоанализ симметричных шифров, криптоанализ асимметричных шифров, криптоанализ хэш функций, криптоанализ по побочным каналам, квантовый криптоанализ.

Раздел 4. Основы стеганографии

Тема 20. Основы стеганографии

Понятие и виды стеганографии. Стеганография и изображения: метод LSB, стеганография и видео, стеганография и аудио. Стеганографические программные продукты.

Содержание лабораторных занятий по дисциплине

Раздел 1. Теоретические основы защиты информации

Тема 1. Понятие информационной безопасности. Ключевые вопросы информационной безопасности.

Лабораторная работа №1. «Генерация псевдослучайных последовательностей»

Изучение,программная генерация и оценка псевдослучайных последовательностей.

Лабораторная работа №2. «Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты»

Исследование парольных подсистем аутентификации пользователей. Реализация простейшего генератора паролей, обладающего требуемой стойкостью ко взлому.

Раздел 2. Криптографические методы защиты информации

Тема 1. Классическая криптография

Лабораторная работа №3. «Классическая криптография. Шифр Цезаря»

Изучение и программная реализация шифра Цезаря.

Тема 2. Симметричная криптография

Лабораторная работа №4. «Симметричная криптография. Сеть Фейстеля»

Изучение особенностей и программная реализация сети Фейстеля.

Лабораторная работа №5. «Симметричная криптография. Потоковый шифр RC4»

Реализовать простейший потоковый шифр с симметричным ключом на основе алгоритма RC4.

Тема 3. Ассиметричная криптография

Лабораторная работа №6. «Ассиметричные алгоритмы шифрования данных. Алгоритм RSA»

Изучить принцип работы асимметричных алгоритмов шифрования на примере алгоритма RSA.

Тема 4. Криптография в ОС Windows

Лабораторная работа №7. «Программирование криптографических провайдеров на платформе .NET: Алгоритмы хэширования SHA-1 и MD5»

Научиться использовать криптографические провайдеры хэш-функций в .NET Framework.

Раздел 3. Основы криптоанализа

Тема 1. Дифференциальный криптоанализ

Лабораторная работа №8. «Дифференциальный криптоанализ блочных шифров»

Изучить метод дифференциального криптоанализа применительно к многораундовым алгоритмам блочного шифрования.

Раздел 4. Основы стеганографии

Тема 1. Скрытие текстовой информации в файле изображения

Лабораторная работа №9. «Стеганография. Скрытие текстовой информации в файле изображения»

Реализовывать метод LSB, который заключается в замене последних значащих битов в контейнере изображения на биты скрываемого сообщения.

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

5.1. Текущий контроль успеваемости

Примерный перечень вопросов к рейтинг-контролю №1

Вариант 1

Развернуто ответить на вопросы.

Вопрос 1. Ключевые вопросы информационной безопасности.

Вопрос 2. Виды угроз информационной безопасности.

Вопрос 3. Алгоритм проведения анализа и оценки угроз информационной безопасности.

Вариант 2

Развернуто ответить на вопросы.

Вопрос 1. Составляющие информационной безопасности.

Вопрос 2. Модель угрозы информационной безопасности.

Вопрос 3. Основные виды защищаемой информации.

Вариант 3

Развернуто ответить на вопросы.

Вопрос 1. Виды угроз информационной безопасности.

Вопрос 2. Законодательство РФ в области зашиты информации.

Вопрос 3. Содержание модели информационной безопасности.

Вариант 4

Развернуто ответить на вопросы.

Вопрос 1. Ключевые вопросы информационной безопасности.

Вопрос 2. Виды моделей информационной безопасности.

Вопрос 3. Политика информационной безопасности.

Примерный перечень вопросов к рейтинг-контролю №2

Вариант 1

Развернуто ответить на вопросы.

Вопрос 1. Алгоритм расшифрования ГОСТ 28147-89.

Вопрос 2. Алгоритм распределения ключей по схеме Диффи-Хеллмана

Вопрос 3. Алгоритм RC4

Решить задачу.

Задача №1. Алгоритм шифрования rsa.

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

Вариант 2

Развернуто ответить на вопросы.

Вопрос 1. Алгоритм расшифрования ГОСТ 28147-89. Общая схема.

Вопрос 2. Шифр Blowfish

Вопрос 3. Протокол Kerberos

Задача №1. Алгоритм шифрования rsa.

Решить задачу.

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из второй сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

Вариант 3

Развернуто ответить на вопросы.

Вопрос 1. Какие функции могут использоваться при шифровании в сети Фейстеля?

Вопрос 2. Описать алгоритм распределения ключей по схеме Диффи-Хеллмана

Вопрос 3.Описать алгоритм RC4

Решить задачу.

Задача №1

Выполнить 3 раунда шифрования и дешифрования сетью Фейстеля сообщение «2014», где F=(L+n)mod 256 (mod – остаток от деления), n – номер варианта.

Вариант 4

Развернуто ответить на вопросы.

Вопрос 1. Какими свойствами обладают хэш функции?

Вопрос 2. Описать алгоритм шифрования Эль- Гамаля

Вопрос 3. Описать алгоритм шифрования DES

Решить задачу.

Задача №1.

Используя шифр Цезаря, зашифруйте свои Фамилию Имя Отчество. Величина сдвига равна номеру варианта.

Примерный перечень вопросов к рейтинг-контролю №3

Вариант 1

Развернуто ответить на вопросы.

Вопрос 1. Комбинированная криптосистема шифрования

Вопрос 2. Алгоритм формирования Электронно-цифровой подписи DSA

Вопрос 3. Протоколы SSL и TLS

Вопрос 4. Криптоанализ симметричных шифров

Вариант 2

Развернуто ответить на вопросы.

Вопрос 1. Хэш функции

Вопрос 2. Алгоритм SHA-1

Вопрос 3. Протокол S/MIME

Вопрос 4. Криптоанализ асимметричных шифров

Вариант 3

Развернуто ответить на вопросы.

Вопрос 1. Электронная цифровая подпись

Вопрос 2. Алгоритм SHA-1

Вопрос 3. Протокол S/MIME

Вопрос 4. Криптоанализ хеш-функций

Вариант 4.

Развернуто ответить на вопросы.

Вопрос 1. Стеганографические методы

Вопрос 2. Криптоалгоритмы пространства .Net

Вопрос 3. Частотный криптоанализ

Вопрос 4. Квантовые криптоалгоритмы.

5.2. Промежуточная аттестация по итогам освоения дисциплины (экзамен)

Примерный перечень вопросов к экзамену

1. Структура и основные составляющие информационной безопасности
2. Общие вопросы информационной безопасности.
3. Виды угроз информационной безопасности.
4. Законодательство РФ в области информационной безопасности.
5. Классическая криптография.
6. Шифр Цезаря.
7. Сеть Фейстеля.
8. Функции, используемые при шифровании в сети Фейстеля.
9. Алгоритм шифрования ГОСТ.
10. Алгоритм шифрования Blowfish.
11. Алгоритм шифрования DES.
12. Алгоритм шифрования Rijndael.
13. Алгоритм шифрования AES.
14. Потоковые шифры. Алгоритм RC4.
15. Алгоритм распределения ключей по схеме Диффи-Хеллмана.
16. Алгоритм шифрования RSA.
17. Алгоритм шифрования Эль- Гамаля
18. Алгоритм шифрования SHA-1.
19. Свойства односторонних функций.
20. Криптоалгоритмы пространства .Net.
21. Протоколы защиты информации в IP сетях.
22. Методы криптоанализа
23. Методы стеганографии.

5.3. Самостоятельная работа обучающегося.

Самостоятельная работа студентов по дисциплине «Защита информации» включает в себя следующие виды деятельности:

1) проработку учебного материала по конспектам, учебной и научной литературе, в том числе по вопросам, не рассмотренным на аудиторных занятиях;

2) подготовку к лабораторным занятиям, требующую совместного выполнения малыми группами студентов рассматриваемых на лекциях отдельных вопросов использования систем MATLAB и MS Visual Studio;

3) подготовку по всем видам контрольных мероприятий, в том числе к текущему контролю знаний и промежуточной аттестации.

Вопросы для самостоятельной работы студентов:

1.Раскройте понятия информационной и экономической безопасности.

2. Перечислите и опишите виды источников угроз информационной безопасности и их особенности.

3.Укажите основные виды защищаемой информации.

4. Опишите международное законодательство в сфере защиты информации.
5. Опишите стандарты и законодательство РФ в сфере защиты информации.
6. Укажите основные аспекты построения системы информационной безопасности.
7. Сформулируйте программу информационной безопасности.
8. Причислите модели информационной безопасности, укажите их особенности.
9. Каковы основные этапы реализации модели информационной безопасности?
10. Какие мероприятия по защите информации проводятся в организациях?
11. Каким образом формируется политика безопасности в организации?
12.Каким образом производится управление рисками в системах информационной безопасности.
13.Как оценивается эффективность и рентабельность систем информационной безопасности.
14. Какие методологии оценки безопасности информационной системы существуют и используются сегодня?
15. Что такое криптографическая защита информации?
16. Какие классификации шифров существуют на сегодняшний день?
17. Опишите ширфы и устройства классической криптографии.
18. В чем заключается суть подстановочных и перестановочных шифров?
19. Раскройте суть шифра Цезаря.
20. Опишите шифр Виженера.
21. Укажите основные принципы шифрования гаммированием.
22. Как используется шифрование методом одноразового блокнота?
23. В чем заключается суть симметричной криптографии?
24. Как формируется сеть Фейстеля?
25. Каким образом организованы шифры на основе сети Фейстеля: ГОСТ, Blowfish?
26. Опишите шифр DES.
27. Опишите принцип действия шифров Rijndael, AES.
28. Каковы особенности потокового шифрования по алгоритму RC4?
29. Укажите основные принципы ассимметричной криптографии.
30. Опишите шифр RSA.
31. Опишите математическую базу шифра Эль Гамаля.
32. Сформулируйте понятие ЭЦП.
33. Опишите DSA алгоритм формирования ЭЦП.
34. Сформулируйте понятие хэш и его основные свойства.
35. Опишите алгоритмы SHA и N-hash.
36. Опишите математическую базу алгоритмов типа MD.
37.Каким образом производится комбинирование симметричной и ассиметричной криптографии?
38. Каким образом реализуются и используются криптопровайдеры на платформе .NET?
39. С использованием каких протоколов осуществляется защита информации в IP сетях?
40. Какие основные методы криптоанализа существуют?
41. Раскройте основные методы цифровой стеганографии.

Задачи для самостоятельной работы студентов:

Задача №1.

Используя шифр Цезаря, зашифруйте свои Фамилию Имя Отчество. Величина сдвига равна номеру варианта.

Задача №2.

Зашифруйте слово АЛФАВИТ по гамме ИДФНТХ.

Задача №3.

Зашифруйте слово АЛФАВИТ шифром Виженера с ключом МИР

Задача №4.

Сообщение SOKYDIOLIGCWUUHO зашифровано шифром вертикальной перестановки

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 6 & 2 \end{pmatrix}$$

Расшифромать сообщение.

Задача №5.

Зашифруйте предложение, применив следующую перестановку слов: меняются местами первое и последнее слова, затем второе и предпоследнее и т.д.

Задача №6.

Сколько дополнительных бит надо добавить к сообщению длиной 100 символов, если кодирование одного символа требует 8бит и блочный шифр работает с блоками длиной 64бита?

Задача №7.

Выполнить 3 раунда шифрования и дешифрования сетью Фейстеля сообщение «2016», где F=(L+n)mod 256 (mod – остаток от деления), n – номер варианта.

Задача №8.

Открытый текст и его шифротекст имеют длину 4бита, длина ключа 3бита. Функция извлекает 1-ыйи 3-ий биты ключа, интерпретирует их как десятичное число, возводит его в квадрат и интерпретирует результат как 4-битовую последовательность. Найти результат зашифрования и расшифрования, если первоначальный исходный текст –0111, ключ–101.

Задача №9.

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

Задача №10.

Сколько имеется натуральных чисел, меньших N=pq и взаимно простых с N, где p и q – различные простые числа?

Основным источником информации для выполнения самостоятельной работы являются справочные подсистемы и официальные сайты программных пакетов, изучаемых в рамках дисциплины. В ходе самостоятельной работы студенты должны познакомиться с содержанием соответствующих ресурсов, имеющим отношение к рассматриваемым на лекциях вопросам, к заданиям лабораторных работ и к вопросам для самостоятельной работы. При этом рекомендуется самостоятельно проанализировать и частично реализовать примеры, данные в справочных материалах.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ Наличие в электронном каталоге ЭБС
Основная литература*		
1. А.О. Кучерик, А.Ю. Лексин, Д.Н. Бухаров, А.Ю. Шагурина Курс лекций по дисциплине «Защита информации» / Владим. гос. уни-т имени Александра Григорьевича и Николая Григорьевича Столетовых. – Владимир: Изд-во ВлГУ	2017	http://e.lib.vlsu.ru/bitstream/123456789/6466/1/00702.pdf
2. Кучерик А. О. ,Бухаров Д. Н. Новикова О. А., Самышкин В. Д. Методические указания по выполнению лабораторных работ по дисциплине «Защита информации» Владим. гос. уни-т имени Александра Григорьевича и Николая Григорьевича Столетовых; – Владимир: Изд-во ВлГУ	2017	http://e.lib.vlsu.ru/bitstream/123456789/5886/1/00678.pdf

3. Болелова Э.А., Информационный мир XXI века. Криптография - основа информационной безопасности [Электронный ресурс] / Болелова Э.А. - М. : Дашков и К	2018	http://www.studentlibrary.ru/book/ISBN9785394030314.html
Дополнительная литература		
1. Аверченков В.И., Криптографические методы защиты информации [Электронный ресурс] / Аверченков В.И. - М. : ФЛИНТА.	2017	http://www.studentlibrary.ru/book/ISBN9785976529472.html
2. Авдошин С.М., Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс] / Авдошин С. М., Набебин А. А. - М. : ДМК Пресс.	2017	http://www.studentlibrary.ru/book/ISBN9785940744083.html
3. Бирюков А.А., Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А. А. - М. : ДМК Пресс.	2017	http://www.studentlibrary.ru/book/ISBN9785970604359.html

6.2. Периодические издания

1. Журнал "Защита информации. Инсайд". - Режим доступа: http://www.inside-zi.ru/
2. Информация и безопасность. - Режим доступа: http://cchgeu.ru/science/nauchnye-izdaniya/informatsiya-i-bezopasnost/
3. Information Security. - Режим доступа: http://www.itsec.ru/

6.3. Интернет-ресурсы

1. Олег Граничин, Владимир Кияев Безопасность информационных систем. – Режим доступа: https://www.intuit.ru/studies/courses/13845/1242/info
2. Ольга Лапонина Криптографические основы безопасности. – Режим доступа: https://www.intuit.ru/studies/courses/28/28/info
3. Галина Басалова Основы криптографии. – Режим доступа: https://www.intuit.ru/studies/courses/691/547/info

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, лабораторных занятий, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Лабораторные занятия проводятся в компьютерном классе (100-3, 122б-3, 511б-3 или аналогичной аудитории в зависимости от сетки расписания).

Перечень используемого лицензионного программного обеспечения:

1) MS Word;
2) MATLAB;
3) MS Visual Studio.

Рабочую программу составил Бухаров Д.Н., стр. пр. каф. ФиПМ _____
(ФИО, должность, подпись)

Рецензент заместитель директора по развитию ООО «Баланс» А.В. Кожин _____
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ФАиП
Протокол № 1 от 30.08.2021 года
Заведующий кафедрой _____ С.М. Аракелня
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена
на заседании учебно-методической комиссии направления 02.03.01 «Математика и компьютерные науки»
Протокол № 1 от 30.08.2021 года
Председатель комиссии зав. кафедрой ФАиП В.Д. Бурков _____

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____