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)**

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«_02_» _____09_____ 20_19_г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ЗАЩИТА ИНФОРМАЦИИ »
(наименование дисциплины)

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Профиль/программа подготовки Мобильные и Интернет-технологии

Уровень высшего образования бакалавриат

Форма обучения очная (ускоренное обучение)

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточной аттестации (экзамен/зачет/зачет с оценкой)
5	5/180	36	-	18	99	Экзамен (27 часов)
Итого	5/180	36	-	18	99	Экзамен (27 часов)

Владимир 2019

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Защита информации» - 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 ВО

Дисциплина «Защита информации» относится к разделу Б1.О.23 - Обязательные дисциплины направления 02.03.02 Фундаментальная информатика и информационные технологии. Изучение дисциплины проходит в 5 семестре, предполагает наличие у студентов навыков программирования, которые могут быть получены в рамках дисциплин «Теория информации», «Объектно-ориентированное программирование».

Знания, полученные в рамках изучения данной дисциплины, могут быть применены для написания выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код формируемых компетенций	Уровень освоения компетенции[1]	Планируемые результаты обучения по дисциплине характеризующие этапы формирования компетенций (показатели освоения компетенции)
1	*2*	*3*
УК-2	*полное*	Знать: общие принципы проектного подхода к решению задач защиты информации; необходимые для осуществления защиты информации правовые нормы; методики планирования проектной работы; методики оценки ресурсоёмкости проекта, ограничений и рисков его выполнения; Уметь: формулировать позволяющие достичь цели проекта взаимосвязанные задачи; определять достижимые ожидаемые результаты решения поставленных задач защиты информации; интерпретировать и учитывать правовые нормы с учётом специфики проекта; оценивать имеющиеся материальные и нематериальные ресурсы и ограничения; Владеть: практическим опытом реализации проекта как совокупности взаимосвязанных задач защиты информации; опытом работы с правовыми информационными системами; опытом реализации проекта в условиях технических, организационных и ресурсных ограничений;
ОПК-1	*полное*	Знать: базовые знания, полученные в области математических и (или) естественных наук Уметь: использовать базовые знания из области математических и (или) естественных наук в области защиты информации Владеть: навыками выбора методов решения задач защиты информации на основе теоретических знаний
ОПК-5	*полное*	Знать: принципы и основные процедуры установки и администрирования информационных систем и баз данных; основные требования информационной безопасности; содержание Единого реестра российских программ; Уметь: осуществлять обоснованный выбор и реализацию процессов установки и технического сопровождения информационных систем и баз данных; Владеть: навыками инсталляции и настройки программных комплексов, применения основ сетевых технологий

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов

№ п/п	Наименование тем и/или разделов/тем 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, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	СРС		
1	Теоретические основы защиты информации	5	1-4	4		2	25	4/66	
2	Криптографические методы защиты информации	5	5-10	28		12	25	30/75	рейтинг-контроль №1
3	Основы криптоанализа	5	11-16	2		2	24	3/75	рейтинг-контроль №2
4	Основы стеганографии	5	17-18	2		2	25	3/75	рейтинг-контроль №3
Всего за 5 семестр:			18	36		18	99	40/73	экзамен (27 часов)
Итого по дисциплине		5	18	36		18	99	40/73	экзамен (27 часов)

Содержание лекционных занятий по дисциплине «Защита информации»

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. «Линейные конгруэнтные генераторы псевдослучайных последовательностей»

Изучение и программная реализация линейных конгруэнтных генераторов 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. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «*Защита информации*» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

- *Интерактивная лекция (тема №_1-20_);*
- *Групповая дискуссия (тема №_2_);*
- *Анализ ситуаций (тема №_4_);*
- *Применение имитационных моделей (тема №_19_);*
- *Разбор конкретных ситуаций (тема №_4_);*

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

Текущий контроль успеваемости

Контрольные вопросы рейтинг-контроля:

Рейтинг-контроль 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.

Рейтинг-контроль 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.

Рейтинг-контроль 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.

Экзаменационные вопросы по дисциплине:

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.

Задачи:

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?

Вопросы для контроля самостоятельной работы:

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.

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ	
		Количество экземпляров изданий в библиотеке ВлГУ в соответствии с ФГОС ВО	Наличие в электронной библиотеке ВлГУ
1	2	3	4
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

7.2. 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/

7.3. 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

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий *лекционного типа, занятий лабораторного типа.*

Лабораторные работы проводятся в ауд. 100-3, 106-3, 511б-3, 511г-3.

Перечень используемого лицензионного программного обеспечения: MS Visual Studio

Рабочую программу составил _____Бухаров Д.Н._____
(ФИО, подпись)

Рецензент
(представитель работодателя) Ген. директор ООО "РС Сервис" Квасов Ф.С.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры _____
Протокол № 1 от 02.09.2019 года
Заведующий кафедрой _____ С.М. Аракелян
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления _____
Протокол № 1 от 02.09.2019 года
Председатель комиссии _____ С.М. Аракелян
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

ЗАЩИТА ИНФОРМАЦИИ

образовательной программы направления подготовки *02.03.02 Фундаментальная информатика и информационные технологии*, направленность: *бакалавриат*

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Зав. кафедрой_____/_____

Подпись *ФИО*