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
«_03_» _____09_____ 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ЗАЩИТА ИНФОРМАЦИИ
(наименование дисциплины)

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Профиль/программа подготовки

Уровень высшего образования бакалавриат

Форма обучения: очная, ускоренная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	5/180	36	-	36	72	Экзамен(36)
Итого	5/180	36	-	36	72	Экзамен(36)

Владимир, 2018

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины Защита информации являются: курса является изучение основных методов и способов защиты информации; современных криптографических алгоритмов; устранение и предотвращения несанкционированного доступа в систему.

Задачами дисциплины являются:

- изучение методов шифрования информации
- изучение методов и способов защиты информации
- изучение современных криптографических алгоритмов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Данная дисциплина относится к вариативной части ОПОП раздел Б1 дисциплины по выбору. Изучение дисциплины предполагает наличие у обучающихся фундаментальных знаний по информатике, которые могут быть получены в рамках курсов «Основы программирования», «Языки программирования», «Объектно-ориентированное программирование». Также необходимо знание основ языка C++, C#..

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В результате изучения дисциплины обучающийся должен освоить следующие компетенции:

- способностью к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям (ОПК-3);
- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4);
- способностью использовать современные инструментальные и вычислительные средства (ПК-3);
- способностью эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий (ПК-6).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: основные способы кодирования и шифрования информации (ОПК -3); методы и способы защиты информации с помощью современных инструментальных и вычислительных средств (ПК-3); основные требования информационной безопасности (ОПК-4).

2) Уметь: применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач (ПК-6); использовать современные инструментальные и вычислительные средства для обеспечения безопасности информации (ПК-3).

3) Владеть: методами разработки алгоритмических и программных решений для обеспечения информационной безопасности (ОПК-3,ОПК-4).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ 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	Концептуальные основы защиты информации	5	1-7	12	-	-	-	20	-	6 /50%	Рейтинг-контроль №1
2	Основные методы и способы защиты информации	5	7-14	12	-	22	-	24	-	12/ 35%	Рейтинг-контроль№2
3	Современные криптографические алгоритмы и области их применения	5	14-18	12	-	14	-	28	-	12 / 46%	Рейтинг-контроль №3
Всего		**5**	**18**	**36**	**-**	**36**	**-**	**72**	**-**	**30 / 42%**	**экзамен (36 час.)**

Тематика лекционных занятий.

Раздел 1. Концептуальные основы защиты информации.

1. Основные понятия защиты информации. Участники информационного процесса. Процедура идентификации, аутентификации, авторизации пользователя.

Раздел 2. Основные методы и способы защиты информации.

1. Понятие кодирования и шифрования данных. Алгоритмы шифрования.
2. Симметричные и асимметричные алгоритмы. Блочные шифры.
3. Понятие криптоанализа данных: виды криптоанализа.
4. Модель уязвимой среды Долева-Яо.

Раздел 3. Современные криптографические алгоритмы и области их применения.

1. Стеганография: виды и методы. Шифр AES.
2. Квантовая криптография и криптоанализ.

Тематика лабораторных занятий.

1. Изучение методов кодирования данных. (4ч.)
2. Одноразовый блокнот (6ч.)
3. Шифр Виженера.(4ч.)
4. Алгоритм RC4 (4ч)
5. Сеть Фейстеля(6ч.).
6. Шифр AES(6ч.).
7. Стеганография (6ч.)

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В данной дисциплине применяются следующие образовательные технологии:

- лекционно-семинарская система обучения (традиционные лекционные и лабораторные занятия);

- метод проектов (разработка и реализация на лабораторных работах основных этапов жизненного цикла проекта – анализ, проектирование, разработка и реализация решения задачи);
- обучение в малых группах (выполнение лабораторных работ в группах из двух или трёх человек);
- технология развития критического мышления (прививание студентам навыков критической оценки разработанных ими алгоритмов);
- мультимедиа-технологии (проведение лекционных и лабораторных занятий с использованием проекторов и других мультимедийных устройств).
- метод (case-study) студенты получают «проблемные» задания по тематике изучаемого раздела.

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

Текущий контроль успеваемости проводится по всем видам занятий с использованием рейтинговой системы.

А. Вопросы для рейтинг-контроля.

Вопросы для рейтинг-контроля№1.

1. Понятие защиты информации.
2. Свойства информации.
3. Участники информационного процесса: их роли и функции.
4. Права и правила доступа к информации.
5. Стандарты безопасности для ИС.
6. Структура данных в ИС.
7. Стандарты информационной безопасности в России.
8. Угрозы: виды и классификация.
9. Дешифровать шифротекст с использованием шифра Цезаря: «Kphrtocvkqpeqfgkuxgtaukosngogwjqfqhxkuwcnkucvkqp»
10. Раскодировать следующую строку сообщения, используя код Цезаря: «Oljkw#vljqdo#lv#d#rqh#ri#pdqb#wbshv#ri#vljdov» (# означает пробел)
11. Дайте определение понятию «информационный объект»
12. Виды криптоанализа: характеристика.
13. Адаптивное вскрытие с открытым шифротекстом.
14. Вскрытие с использованием открытого текста.
15. Дайте определение понятию «безопасность информационного объекта».
16. Алгоритм с открытым ключом.
17. Алгоритм с закрытым ключом.
18. Симметричная криптосистема.
19. Асимметричная криптосистема.

Вопросы для рейтинг-контроля№2.

1. Понятие криптографии.
2. Шифрование и кодирование данных.
3. Классы безопасности.
4. Класс безопасности С1 и его характеристика.

5. Простые перестановочные шифры.
6. Симметричные и асимметричные алгоритмы шифрования.
7. Класс безопасности С2 и его характеристика.
8. Алгоритм шифрования с открытым ключом.
9. Пространство ключей.
10. Класс В1 и его характеристика.
11. Класс В2: характеристика.
12. Класс В3: характеристика.
13. Класс А: характреристика.
14. Криптоанализ: понятие и виды.
15. Дешифрование данных.
16. Криптостойкость алгоритма.
17. Абсолютно стойкие системы.
18. Достаточно стойкие системы.
19. Расчёт трудоёмкости алгоритма.
20. Кодирование данных с использованием шифра Цезаря.
21. Кодирование данных с использованием шифра Виженера.
22. Кодирование данных с использованием шифра ДНК.

Вопросы для рейтинг-контроля№3.

1. Понятие и виды ЭЦП.
2. Криптографические протоколы и их виды.
3. Самоутверждающийся криптографический протокол.
4. Протокол с посредником.
5. Кодирование данных с использованием шифра ДНК.
6. Самодостаточные протоколы.
7. Методы вскрытия протоколов.
8. Оценка криптостойкости систем шифрования данных.
9. Кодирование данных с частью ключа с помощью шифра Виженера.
10. Принцип Керкгоффса и его требования к алгоритму шифрования данных.
11. Виды шифротекста.
12. Дифференциальный метод криптоанализа.
13. Линейный метод криптоанализа.
14. Поточные и блочные алгоритмы шифрования данных: характеристика.
15. Классификация блочных шифров.
16. Методы защиты данных в ИС.
17. Двойное шифрование.
18. Классификация поточных шифров.
19. СПШ: понятие,характеристика.
20. АПШ:понятие, харктеристика.
21. Классификация алгоритмов ЭЦП.

Б. Вопросы к экзамену.

1. Понятие информационной системы: классификация и разновидности.
2. Защита информации: основные понятия.
3. Алгоритмы шифрования данных в ИС: симметричные и асимметричные.
4. Симметричный алгоритм шифрования данных: методика шифрования, применение в ИС.

5. Асимметричный алгоритм шифрования данных.
6. Криптоанализ: понятие, разновидности, основные методы.
7. Алгоритм RC4: методика шифрования данных.
8. Участники информационного процесса: роли и функции.
9. Угрозы безопасности информации: виды и классификация.
10. Блочные шифры:виды, методика шифрования, виды атаки.
11. Поточные шифры: методика шифрования.
12. Шифр «одноразовый» блокнот: методика шифрования данных, криптостойкость.
13. Шифр XOR: алгоритм работы, применение при кодировании данных.
14. ЭЦП: понятие, виды и применение при шифровании данных в ИС.
15. Простые перестановочные шифры: понятие, виды перестановок, применение при кодировании данных.
16. Шифр Виженера: методика шифрования и дешифрования данных.
17. Шифр Цезаря: методика шифрования и дешифрования данных.
18. Шифр AES: методика шифрования данных.
19. Правовое обеспечение защиты информации.
20. Несанкционированный доступ: понятие, виды, оценка степени угрозы безопасности данных в ИС.
21. Права и правила доступа к информации.
22. Стеганография: понятие, виды, применение при шифровании данных.
23. Квантовая криптография: понятие, методика кодирования.
24. Квантовый криптоанализ: виды атаки на данные.
25. Хзш-таблицы: применение при кодировании данных.
26. Сеть Фейстеля: методика кодирования данных.
27. Кодовые деревья: структура, виды, классификация.
28. Энтропия: понятие, методика расчёта, применение в шифровании данных.
29. Гаммирование: понятие, способы расчёта, применение в кодировании информации.
30. Использование СТЕЛС технологий в вирусных программах.
31. Вирусы:виды, классификация.
32. Вредоносные воздействия: понятие, виды, методы воздействия на информацию.
33. Криптографические протоколы: виды и классификация.
34. Система с открытым ключом Диффи-Хеллмана.
35. Простые подстановочные шифры: понятие, виды подстановок, применение при кодированиии данных.
36. Алгоритм Евклида: понятие, модификации, применение при шифровании данных.
37. Криптосистема: виды и структура.
38. Алгоритмы ГОСТ: методика шифрования и практическое использование.
39. Конфиденциальная информация: понятие, виды.
40. КИС: понятие, характеристика структурных элементов.
41. Генераторы псевдослучайных чисел.
42. Информационные системы, сети, каналы и среды.
43. Организационно-административные методы защиты информации.

В. Самостоятельная работа

Самостоятельная работа по дисциплине представлена в нескольких видах:

А) изучение теоретического материала для подготовки к рейтингу и экзамену (литературные источники);

Б) решение практических задач по определению уязвимостей информационных систем (разработка программ).

Порядок выполнения самостоятельной работы следующий: все задания вида А проверяются в процессе выполнения заданий рейтинг-контроля и сдачи экзамена; задания группы Б предусматривают несколько уровней оценки: (оптимизация программного кода, интерфейс программы (консольное или оконное приложение), уровень владения языком программирования). Все перечисленные параметры заданий группы Б учитываются в качестве бонусных баллов в итоговом рейтинге обучающегося.

Особое внимание нужно уделить следующим разделам дисциплины:**2. Основные методы и способы защиты информации, 3.Современные криптографические алгоритмы и области их применения.** Данные разделы дисциплины формируют у обучающихся практические навыки кодирования и шифрования информации и понятийный аппарат по изучаемой тематике.

Вопросы для контроля самостоятельной работы:

1. Что называется НОД и сфера его применения при шифровании данных.
2. Что называется криптостойкостью алгоритма шифрования данных.
3. В чём отличие адаптивного вскрытия от вскрытия с открытым шифротекстом.
4. В чем отличие прав доступа от правил доступа к данным.
5. Как расчитать энтропию информационной системы.
6. Методы сокрытия информации с помощью стеганографии.
7. Атаки на поточные шифры.
8. Что называется СПШ.
9. Виды атаки на блочные шифры.
10. Угрозы безопасности.
11. Что называется доступностью данных.
12. В чём отличие симметричного алгоритма от асимметричного.
13. В чем суть метода коллизий при криптоанализе данных.
14. Как определить подлинность ЭЦП.
15. Что представляет собой метод «радужных» таблиц в криптоанализе.
16. Основные свойства защищаемой информации.
17. Компоненты автоматизированной ИС.
18. В чём отличие алгоритма Виженера от алгоритма Цезаря.
19. Что называется афинной перестановкой.
20. Как осуществляется вскрытие по методу «дат» рождения.
21. Каковы основные условия для обеспечения безопасности данных в ИС.
22. В чём суть метода криптоанализа: «атака грубой силой».
23. Что называется однофакторной и многофакторной защитой данных. В чём преимущества одной над другой.
24. Чем отличается уязвимость системы от неисправностей в ней.
25. В чём суть метода гаммирования данных.
26. В чём преимущества метода шифрования данных: «одноразовый блокнот».

27. Что называется объектом защиты.
28. Как осуществляется шифрование данных в алгоритме AES.
29. В чем суть метода шифрования данных с помощью хэш-таблиц.
30. В чём состоит метод шифрования данных с помощью блоков.
31. Как проверить, достоверна ли переданная информация.
32. Что называется контрольным битом в сообщении.
33. Какова взаимосвязь между субъектом, предметом и объектом защиты.
34. Что называется бандитским криптоанализом.
35. Что представляет собой уязвимая среда в модели Долева-Яо.
36. В чём суть алгоритма Луна.
37. DDOS –атака, как вид угрозы информационной безопасности.
38. Программные закладки и их влияние на безопасность информации.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная литература:

1.Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7 (ЭБС ЗНАНИУМ)

2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз.(ЭБС ЗНАНИУМ).

3. Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М. : Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204811.html

б) дополнительная литература:

1.Агапов, А. В. Обработка и обеспечение безопасности электронных данных [Электронный ресурс] : учеб. пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. - М.: МФПУ Синергия, 2012. - 592 с. - (Сдаем госэкзамен). - ISBN 978-5-4257-0074-2. (ЭБС ЗНАНИУМ).

2. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4 (ЭБС ЗНАНИУМ).

3.Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.(ЭБС ЗНАНИУМ).

в) периодические издания

1. Информационная безопасность. Архив номеров. // Режим доступа: http://www.infosecurityrussia.ru/2015/itsec

2. Технологии защиты. Архив номеров. //Режим доступа: http://www.tzmagazine.ru/

3. SecurityNews. Архив номеров.//Режим доступа: http://www.secnews.ru/

в) интернет-ресурсы

1. Информационная безопасность // Режим доступа: http://protect.htmlweb.ru/p01.htm

2. Система информационной безопасности //Режим доступа: http://tvoi.biz/biznes/informatsionnaya-bezopasnost/sistema-informatsionnoj-bezopasnosti.html

3. Владимир Липаев. Основные факторы, определяющие технологическую безопасность информационных систем // Режим доступа: http://www.computer-museum.ru/histsoft/ji97061.htm.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

В качестве материально-технического обеспечения дисциплины используются следующие средства: проектор, наборы слайдов по учебной тематике, компьютерные классы с установленным ПО: VS 2012, 2013,2015, мультимедийные аудитории.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 02.03.02 Фундаментальная информатика и информационные технологии

Рабочую программу составил старший преподаватель Бухаров Д.Н. _____
(ФИО, подпись)

Рецензент
(представитель работодателя) Ген.директор ООО «ФС Сервис» Квасов Д.С. _____
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ФиПМ
Протокол № 1 от 03.09.2018 года
Заведующий кафедрой _____ Аракелян С.М.
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 02.03.02 Фундаментальная информатика и информационные технологии
Протокол № 1 от 03.09.2018 года
Председатель комиссии _____ Аракелян С.М.
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

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 _____