

2013
2014

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

УТВЕРЖДАЮ

Проректор
по учебно-методической работе



А.А.Панфилов

« 29 » 10 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

(наименование дисциплины)

Направление подготовки 02.03.01 Математика и компьютерные науки

Профиль/программа подготовки Математические методы в экономике и финансах

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)
8	3/108	26		26	56	Зачёт с оценкой
Итого	3/108	26		26	56	Зачёт с оценкой

Владимир 20 15

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины Защита информации являются: 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 находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем (ОПК-4).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

- 1) Знать: основные способы кодирования и шифрования информации; методы и способы защиты информации; современные криптографические алгоритмы (ОПК-4).
- 2) Уметь: реализовывать программно и использовать на практике математические алгоритмы для определения уязвимостей и защиты информации (ОПК-4).
- 3) Владеть: методами нахождения, анализа и программной реализации математических алгоритмов кодирования и шифрования информации. (ОПК -4).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 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	8	1-4	6		-	-	24	-	3 / 50%	Рейтинг-контроль №1
2	Основные методы и способы защиты информации	8	5-9	12		14	-	16	-	12 / 46%	Рейтинг-контроль №2
3	Современные криптографические алгоритмы и области их применения	8	10-13	8		12	-	16	-	10 / 50%	Рейтинг-контроль №3
Всего		8	13	26		26	-	56		25 / 48%	Зачет с оценкой

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. 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. (2ч.)
2. Одноразовый блокнот (4ч.)
3. Шифр Виженера.(2ч.)
4. Алгоритм RC4 (3ч)
5. Сеть Фейстеля(3ч.).
6. Шифр AES(4ч.).

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.

Рейтинговая система обучения

Рейтинг-контроль проводится три раза за семестр. Он предполагает оценку суммарных баллов по следующим составляющим: баллы на контрольных занятиях; качество выполнения домашних типовых заданий, рассматриваемых на практических занятиях. Распределение баллов по контрольным мероприятиям определяется лектором, ведущим дисциплину.

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:
«Kphrtocvkqreqlfgkuxgtaukosngogwjqlfqhkuwcnkucvkqr»
10. Раскодировать следующую строку сообщения, используя код Цезаря:
«Oljkw#vlljqdo#lv#d#rgh#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: характеристика.
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 Керкгоффа 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, характеристика.
21. Классификация алгоритмов ЭЦП.

Б. Вопросы к зачёту с оценкой

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. Хэш-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 кодировании 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 чём отличие прав доступа от правил доступа к данным.
5. Как рассчитать 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 чём 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 аффинной 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 чём 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. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лелешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз. (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. Методы и средства защиты информации [Электронный ресурс]: методические указания к лабораторным работам / С. В. Маскеев, М. А. Трофимов; Владимирский

государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), Кафедра вычислительной техники .— Электронные текстовые данные (1 файл: 317 Кб) .— Владимир : Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), 2013 .— 19 с. : ил. — Заглавие с титула экрана.— Электронная версия печатной публикации .— Библиогр.: с. 18 .— Свободный доступ в электронных читальных залах библиотеки.(Внутривузовские издания ВлГУ <http://e.lib.vlsu.ru/bitstream/123456789/3325/1/01254.pdf>>)

б) дополнительная литература:

1. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-369-01304-5, 200 экз.(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. Security News. 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 (ауд.511б,г,100, 122б, 106), мультимедийные аудитории.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС
ВО по направлению 02.03.01 Математика и компьютерные науки

Рабочую программу составил Касьянов А.А., доцент кафедры ФиПМ
(ФИО, подпись)

Рецензент
(представитель работодателя)

ООО "ПС Сервис"

Квасов Д.С. Ген. директор
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ФиПМ

Протокол № 81а от 29.01.15 года

Заведующий кафедрой

Аракелян С.М.

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии
направления 02.03.01 Математика и компьютерные науки

Протокол № 5/1 от 29.01.15 года

Председатель комиссии

Давыдов А.А.

(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 _____