2015

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» 01 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

(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)
7	5/180	36		18	90	Экз.(36)
Итого	5/180	36		18	90	Экзамен(36)

Владимир 2015

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины Безопасность информационных систем являются: изучение и практическое применение различных средств обеспечения безопасности и криптографических протоколов в современных информационных системах, а также знание методов устранения уязвимостей и программных ошибок в хранящихся в информационной системе данных.

Задачами дисциплины являются:

- изучение методов шифрования данных в информационных системах
- изучение криптографических протоколов и методов их функционирования
- изучение основных видов уязвимостей, влияющих на нормальное функционирование информационной системы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Данная дисциплина относится к вариативной части ОПОП раздел Б1 дисциплины по выбору. Логически и содержательно методологически данная дисциплина связана с дисциплиной «Защита информации». Для освоения данной дисциплины требуется знание методов кодирования и шифрования информации, умение распознавать уязвимости в информационных системах, готовность к решению профессиональных задач, связанных с обеспечением безопасности информационной системы.

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

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

- способностью использовать методы математического и алгоритмического моделирования при анализе управленческих задач в научно-технической сфере, в экономике, бизнесе и гуманитарных областях знаний (ПК-7).

1) Знать: основные способы кодирования и шифрования данных в информационных системах; криптографические протоколы, применяемые в работе информационных систем, алгоритмического моделирования при анализе управленческих задач в научно-технической сфере, в экономике, бизнесе и гуманитарных областях знаний (ПК-7).
2) Уметь: использовать методы математического и алгоритмического моделирования при анализе управленческих задач в научно-технической сфере (ПК-7).
3) Владеть: методами математического и алгоритмического моделирования для обеспечения безопасности информационной системы (ПК-7).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 5 зачетных единицы, 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	Информационные системы: виды и классификация.	7	1-2	6		-	-	20	-	3 / 50%	Рейтинг-контроль №1
2	Кодирование и шифрование данных в ИС	7	1-6	12		6	-	30	-	9 / 50%	
3	Криптографические протоколы безопасности в ИС	7	7-14	12		8	-	20	-	10 / 50%	Рейтинг-контроль №2
4	Методы обеспечения безопасности ИС	7	13-18	6		4	-	20	-	5 / 50%	Рейтинг-контроль №3
Всего		**7**	**18**	**36**		**18**	**-**	**90**		**27 / 50%**	**Экзамен (36)**

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Лекции

Раздел 1. Информационные системы: виды и классификация.

1. Понятие информационной системы. Структурный состав элементов информационной системы.
2. Виды информационных систем и их классификация.

Раздел 2. Кодирование и шифрование данных в ИС.

1. Понятие кодирования и шифрования данных. Алгоритмы шифрования.
2. Симметричные и асимметричные алгоритмы. Блочные шифры.
3. Понятие криптоанализа данных: виды криптоанализа.
4. Основные виды атак на данные в ИС.

Раздел 3. Криптографичнские протоколы безопасности в ИС.

1. Понятие криптобезопасности ИС. Протолы шифрования данных.
2. Уровни обеспечения безопасности данных в ИС.
3. Технические средства и программные продукты для обеспечения безопасности данных.

Раздел 4. Методы обеспечения безопасности данных в ИС.

1. Модель уязвимой среды Долева-Яо. Классификация и характеристики угроз безопасности данных.
2. Методы обеспечения безопасности данных в ИС.

Тематика лабораторных занятий.

1. Изучение методов кодирования данных. (2ч.)
2. Алгоритм шифрования данных SHA-5 (3ч.)
3. Блочные шифры.(2ч.)
4. Стеганография данных (2ч)
5. Одноразовый блокнот(3ч.).
6. Криптографические протоколы(4ч.).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В данной дисциплине используются следующие методы обучения:

- использование мультимедийных средств;
- разбор ситуаций при обнаружении уязвимости информационной системы;
- компьютерные симуляции.

- 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 и виды ИС.
2. Характеристика ИС.
3. Уровни безопасности ИС.
4. Участники информационного процесса: их роли и функции.
5. Права и правила доступа к информации.
6. Стандарты безопасности для ИС.
7. Структура данных в ИС.
8. Стандарты информационной безопасности в России.
9. Понятие доверенной системы.
10. Понятие безопасной системы.
11. Монитор обращений и его качества.
12. Ядро безопасности монитора обращений.
13. Политика безопасности.
14. Периметр безопасности.
15. Канал утечек.
16. Угрозы: виды и классификация.

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 B1 и его характеристика.
11. Класс B2: характеристика.
12. Класс B3: характеристика.
13. Класс A: 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. Информационная безопасность: 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. Уровни безопасности данных в ИС.

8. Участники информационного процесса: роли и функции.
9. Угрозы безопасности данных: 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. Нормативно-правовые основы обеспечения безопасности данных в ИС.
20. Несанкционированный доступ: понятие, виды, оценка степени угрозы безопасности данных в ИС.
21. Права и правила доступа к данным в ИС.
22. Стеганография: понятие, виды, применение при шифровании данных.
23. Квантовая криптография: понятие, методика кодирования, применение в ИС.
24. Квантовый криптоанализ: виды атаки на данные в ИС.
25. Хзш-таблицы: применение при кодировании данных.
26. Сеть Фейстеля: методика кодирования данных, применение в ИС.
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. Технические средства для обеспечения безопасности данных в ИС.
31. Вирусы:виды, классификация.
32. Вредоносные воздействия: понятие, виды, методы воздействия на информацию.
33. Криптографические протоколы: виды и классификация.
34. Методы защиты данных в ИС.
35. Простые подстановочные щифры: 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.

в) Самостоятельная работа

Самостоятельная работа по дисциплине представлена в нескольких видах:

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

2) 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. Кодирование и шифрование данных в ИС, 3. Криптографические протоколы безопасности в ИС.** Данные разделы дисциплины формируют у обучающихся практические навыки определения уязвимостей в ИС 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 данных в ИС.
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.

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. 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).

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. Монахов, Ю. М. Функциональная устойчивость информационных систем : учебное пособие : в 3 ч. / Ю. М. Монахов ; Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ) .— Владимир : Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), 2011- .— (Комплексная защита объектов информатизации ; кн. 22) .Ч. 1: Надежность программного обеспечения [Электронный ресурс] .— Электронные текстовые данные (1 файл: 560 Кб) .— 2011 .— 60 с. : ил. — Заглавие с титула экрана .— Электронная версия печатной публикации .— Библиогр.: с. 53-57 .— Свободный доступ в электронных читальных залах библиотеки
(Внутривузовские издания ВлГУ http://e.lib.vlsu.ru:80/handle/123456789/2972.)

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. 511г, 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 доцент кафедры ФиПМ Касьянов А.А. _____
(ФИО, подпись)

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

Программа рассмотрена и одобрена на заседании кафедры ФиПМ
Протокол № 8а 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 № _____ от _____ 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 _____