

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой программного обеспечения
и администрирования информационных систем



Артемов М. А.

08.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.31 Информационная безопасность

1. Шифр и наименование направления подготовки:

02.03.03 Математическое обеспечение и администрирование
информационных систем

2. Профиль подготовки: Прикладная информатика в юриспруденции

3. Квалификация (степень) выпускника: бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

программного обеспечения и администрирования информационных систем

6. Составители программы:

Барановский Евгений Сергеевич, к.ф.-м.н.

7. Рекомендована: НМС факультета ПММ протокол № 10 от 18.06.2018 г.

8. Учебный год: 2018/2019

Семестр: 7

9. Цели и задачи учебной дисциплины:

Цель курса – формирование у студентов знаний об объектах и задачах защиты компьютерных систем, способах и средствах нарушения информационной

безопасности, о принципах и подходах к решению задач защиты информации; а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных информационных систем в соответствии с действующим законодательством.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Информационная безопасность» относится к обязательным дисциплинам блока Б1 и изучается в 7-м семестре. Данная дисциплина непосредственно связана с дисциплинами «Информатика и программирование» и «Информационные системы и технологии».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p>Знать: <i>основные понятия информационной безопасности;</i> <i>основные направления защиты информации;</i> <i>законодательство Российской Федерации в области защиты информации;</i> <i>современные методы и средства защиты информации в информационно-телекоммуникационных системах;</i> <i>архитектуру защищённых экономических систем.</i></p> <p>Уметь: <i>разрабатывать политику информационной безопасности;</i> <i>проводить оценку угроз безопасности объекта информатизации;</i> <i>реализовывать простые информационные технологии реализующие методы защиты информации;</i> <i>применять методики оценки уязвимости в информационно-телекоммуникационных сетях;</i> <i>проектировать системы защиты информации.</i></p> <p>Владеть: <i>методами защиты информации;</i> <i>средствами защиты информации в сетях ЭВМ;</i> <i>навыками программирования алгоритмов криптографической защиты информации.</i></p>

12. Структура и содержание учебной дисциплины

12.1. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 3/108.

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	Сем. 7
Аудиторные занятия	50	50
в том числе:		
лекции	16	16
лабораторные	34	34
практические		

Самостоятельная работа	58	58
Итого	108	108
Форма промежуточной аттестации	Зачет с оценкой	

13.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение. Комплексный подход к обеспечению информационной безопасности	Понятие информационной безопасности. Виды угроз в компьютерных системах. Уровни информационной безопасности.
2	Методы и средства обеспечения безопасности информации	Защита информации от утечки по техническим каналам. Защита информации от несанкционированного доступа. Криптографические методы защиты информации.
3	Компьютерные вирусы и средства антивирусной защиты	Вирусы как вид угрозы информационной безопасности. Средства антивирусной защиты.
4	Стандарты защищенности информации в компьютерных системах	Стандарты и спецификации в области информационной безопасности

13.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				Всего
		Лекции	Лабораторные	Практические	Самостоятельная работа	
1	Введение. Комплексный подход к обеспечению информационной безопасности	4	8		14	26
2	Методы и средства обеспечения безопасности информации	4	8		14	26
3	Компьютерные вирусы и средства антивирусной защиты	4	8		16	28
4	Стандарты защищенности информации в компьютерных системах	4	10		14	28
	Итого:	16	34		58	108

14. Методические указания для обучающихся по освоению дисциплины

Работа с конспектами лекций, чтение литературы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
-------	----------

1	Основы управления информационной безопасностью: [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва: Горячая линия-Телеком, 2014 .— 243 с.
2	Информатика: базовый курс: [учебное пособие для студ. вузов]; под ред. С.В. Симоновича.— 3-е изд. — СПб. [и др.] : Питер, 2012 .— 637 с.
3	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретикочисловые методы криптографии. —СПб.: Лань, 2011. — 400 с. http://e.lanbook.com/books/element.php?pl1_id=1540

б) дополнительная литература:

№ п/п	Источник
4	Рябко Б. Я. Фионов А. Н. Основы современной криптографии и стеганографии. — М.: Горячая линия - Телеком, 2013. — 232 с.
5	Белов Е.Б. Основы информационной безопасности. [Электронный ресурс]: учебное пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков [и др.]. – Электрон. дан. – М.: Горячая линия-Телеком, 2006. – 558 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5121
6	Коробейников А. Г., Гатчин Ю. А. Математические основы криптологии [Электронный ресурс] : — Электрон. дан. — СПб.: Издательство НИУ ИТМО, 2004. — 106 с. — http://e.lanbook.com/books/element.php?pl1_id=43393

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – http://www.lib.vsu.ru/
8	ЭБС «Издательство Лань» http://e.lanbook.com/

16. Материально-техническое обеспечение дисциплины:

Требования к аудиториям для проведения лекционных и практических занятий: наличие доски и средств письма на ней, оснащение проекционной техникой и компьютером.

Требования к аудиторному оборудованию для проведения лабораторных занятий: наличие компьютерных классов с современной компьютерной техникой и соответствующим программным обеспечением.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

При проведении занятий используются среды и языки программирования Pascal, Visual Studio, C/C++.

18. Материально-техническое обеспечение дисциплины:

Для осуществления образовательного процесса по дисциплине необходимо: лабораторный класс, оборудованный персональными компьютерами или терминальными рабочими станциями.:

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-1 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. задач	Все разделы	Контрольная работа №1
	Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации.	Все разделы	
	Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ; навыками программирования алгоритмов криптографической защиты информации.	Все разделы	Контрольная работа №1
Промежуточная аттестация			КИМ1

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для зачета:

зачтено	достаточно полное знание учебного материала и успешное выполнение всех практических заданий.
не зачтено	существенные пробелы в знании учебного материала и наличие принципиальных ошибок в выполнении практических заданий

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Форма контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой ПОиАИС

_____ М. А. Артемов
подпись, расшифровка подписи

___.__.20__

Направление подготовки: 02.03.03 Математическое обеспечение и администрирование информационных систем

Дисциплина: Б1.Б.31 Информационная безопасность

Форма обучения: очная

Вид контроля: зачет

Вид аттестации: промежуточная

Контрольно-измерительный материал № 1

1. Виды угроз в компьютерных системах.
2. Асимметричное шифрование и его применение.
3. Определите время перебора всех паролей, если известно, что алфавит состоит из n символов, длина пароля k – символов, скорость перебора – s паролей в секунду и после каждого из m неправильно введенных паролей идет пауза в v секунд.

Преподаватель _____ Барановский Е. С.
подпись расшифровка подписи

Критерии оценки:

зачтено	достаточно полное знание учебного материала и успешное выполнение всех практических заданий.
не зачтено	существенные пробелы в знании учебного материала и наличие принципиальных ошибок в выполнении практических заданий

Пример заданий для контрольной работы

Б1.Б.21 Информационная безопасность

Вариант 1

1. Создайте текстовый файл, содержащий фамилию, имя, отчество студента в объеме 50 записей. Проведите архивирование файла. Любым редактором внесите изменения согласно заданию. В ответе отразите: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.
2. Разработайте приложение, реализующее алгоритм обмена ключами по алгоритму Диффи-Хеллмана. Ключи должны автоматически формироваться в файлы. Должна быть обеспечена наглядность выполнения алгоритма.

Критерии оценки: – оценка «отлично» выставляется студенту, если все задания выполнены правильно.

- оценка «хорошо» выставляется студенту, если большая часть заданий выполнена правильно, но имеются некоторые недочеты и погрешности, приводящие к незначительному искажению результатов в одном из заданий;
- оценка «удовлетворительно» выставляется студенту, если большая часть заданий выполнена правильно, но имеются ошибки и недочеты, приводящие к неверным результатам в одном задании;
- оценка «неудовлетворительно» выставляется студенту, если значительная часть работы не выполнена или допущены существенные ошибки, показывающие, что студент не владеет обязательными знаниями по данной теме.

Составитель _____ Е.С. Барановский