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.

31.08.2019 г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.26 Информационная безопасность

1. **Шифр и наименование направления подготовки:**

02.03.03 Математическое обеспечение и администрирование информационных систем

1. **Профиль подготовки:** Прикладная информатика в юриспруденции
2. **Квалификация (степень) выпускника:** бакалавр
3. **Форма обучения:** очная
4. **Кафедра, отвечающая за реализацию дисциплины:**

программного обеспечения и администрирования информационных систем

1. **Составители программы:**

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

1. **Рекомендована:** НМС факультета ПММ протокол № 10 от 15.06.2019 г.

1. **Учебный год:** 2019/2020 **Семестр:** 7

1. **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.

1. **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».

1. **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 | *Знать:*  *основные понятия информационной безопасности;*  *основные направления защиты информации;*  *законодательство Российской Федерации в области защиты информации;*  *современные методы и средства защиты информации в информационнотелекоммуникационных системах;*  *архитектуру защищённых экономических систем.*  *Уметь:*  *разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации;*  *реализовывать простые информационные технологии реализующие методы защиты информации;*  *применять методики оценки уязвимости в информационнотелекоммуникационных сетях;*  *проектировать системы защиты информации.*  *Владеть:*  *методами защиты информации;*  *средствами защиты информации в сетях ЭВМ;*  *навыками программирования алгоритмов криптографической защиты информации.* |

1. **Структура и содержание учебной дисциплины** 
   1. **Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —** 3/108.
2. **Виды учебной работы**

|  |  |  |
| --- | --- | --- |
| Вид учебной работы | Трудоемкость (часы) | |
| Всего | Сем. 7 |
| Аудиторные занятия | 48 | 48 |
| в том числе: лекции | 16 | 16 |
| лабораторные | 32 | 32 |
| практические |  |  |
| Самостоятельная работа | 24 | 24 |
| Контроль | 36 | 36 |
| **Итого** | **108** | **108** |
| Форма промежуточной аттестации | | Экзамен |

* 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 |

* 1. **Разделы дисциплины и виды занятий**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/ п | Наименование раздела дисциплины |  | Виды занятий (часов) | | |  |
| Лекции | Лабораторные | Практические | Самостоятельная работа | Всего |
| 1 | Введение. Комплексный подход к обеспечению информационной безопасности | 4 | 8 |  | 6 | 18 |
| 2 | Методы и средства обеспечения безопасности информации | 4 | 8 |  | 6 | 18 |
| 3 | Компьютерные вирусы и средства антивирусной защиты | 4 | 8 |  | 6 | 18 |
| 4 | Стандарты защищенности информации в компьютерных системах | 4 | 8 |  | 6 | 18 |
|  | Итого: | 16 | 32 |  | 24 | 72 |

1. **Методические указания для обучающихся по освоению дисциплины**

Работа с конспектами лекций, чтение литературы.

1. **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. втузов]; 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.](https://lib.vsu.ru/zgate?ACTION=follow&SESSION_ID=3431&TERM=%D0%A0%D1%8F%D0%B1%D0%BA%D0%BE,%20%D0%91%D0%BE%D1%80%D0%B8%D1%81%20%D0%AF%D0%BA%D0%BE%D0%B2%D0%BB%D0%B5%D0%B2%D0%B8%D1%87%5B1,1004,4,101%5D&LANG=rus) 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/> |

1. **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.

1. **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++.

1. **Материально-техническое обеспечение дисциплины:**

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

1. **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 информационнотелекоммуникационных 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 информационнотелекоммуникационных 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 |

* 1. **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 |

* 1. **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: экзамен

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:** − 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 несущественному 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.

# 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-Хелламана. 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 несущественному 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