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.32 Организация защиты информации

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

09.03.03 Прикладная информатика

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, кандидат физико-математических наук.
2. **Рекомендована:** НМС факультета ПММ протокол № 10 от 15.06.2019 г.

1. **Учебный год:** 2019/2020 **Семестр(ы): 7, 8**

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».

В результате изучения дисциплины студент должен:

**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.

**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.

**Владеть:**

* методами защиты информации;
* средствами защиты информации в сетях ЭВМ;

навыками программирования алгоритмов криптографической защиты информации.

1. **Компетенции обучающегося, формируемые в результате освоения дисциплины:**

|  |  |  |
| --- | --- | --- |
| Компетенция | | Планируемые результаты обучения |
| Код | Название |
| ОПК-3 | способность использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности | *Знать:*  *архитектуру защищённых экономических систем.*  *Уметь:*  *реализовывать простые информационные технологии реализующие методы защиты информации;* |
| ОПК-4 | способность 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;*  *Уметь:*  *проектировать системы защиты информации.* |
| ПК-11 | способность эксплуатировать и сопровождать информационные системы и сервисы | *Знать:*  *законодательство Российской Федерации в области защиты информации*  *Уметь*:  *применять методики оценки уязвимости в информационно-телекоммуникационных сетях;* |
| ПК-13 | способность осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем | *Уметь проектировать системы защиты информации.* |

1. **Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —** 4/144.

**Форма промежуточной аттестации:** зачет, зачет с оценкой

1. **Виды учебной работы**

|  |  |  |  |
| --- | --- | --- | --- |
| Вид учебной работы | Трудоемкость (часы) | | |
| Всего | Сем. 7 | Сем. 8 |
| Аудиторные занятия | 64 | 48 | 16 |
| в том числе: лекции | 48 | 32 | 16 |
| практические |  |  |  |
| лабораторные | 16 | 16 |  |
| Самостоятельная работа | 80 | 42 | 38 |
| Итого | 144 | 90 | 54 |
| Форма промежуточной аттестации | | Зачет | Зачет с оценкой |

* 1. **Содержание 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. **Темы (разделы) дисциплины и виды занятий**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование раздела дисциплины | Виды занятий (часов) | | | |  |
| Лекции | Практичес кие | Лаборат орные | Самостоятел ьная работа | Всего |
| 1 | Введение. Комплексный подход к обеспечению информационной безопасности | 12 |  | 4 | 19 | 35 |
| 2 | Методы и средства обеспечения безопасности информации | 12 |  | 4 | 19 | 35 |
| 3 | Компьютерные вирусы и средства антивирусной защиты | 13 |  | 4 | 20 | 37 |
| 4 | Стандарты защищенности информации в компьютерных системах | 11 |  | 4 | 22 | 37 |
|  | Итого: | 48 |  | 16 | 80 | 144 |

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 | Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. —СПб.: Лань, 2011. — 400 с. <http://e.lanbook.com/books/element.php?pl1_id=1540> |

**б) дополнительная литература:**

|  |  |
| --- | --- |
| № п/п | Источник |
| 3 | [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. |
| 4 | 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 |
| 5 | 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 |
| 6 | Электронный каталог Научной библиотеки Воронежского государственного университета.– http://www.lib.vsu.ru/ |
| 7 | ЭБС «Издательство Лань» http://e.lanbook.com/ |

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

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

Аудитория с проектором, доска.

1. **Фонд оценочных средств:**
   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) |
| ПК-11 способность эксплуатировать и сопровождать информационные системы и сервисы | Знать:  законодательство Российской Федерации в области защиты информации | Все разделы дисциплины | Комплект КИМ |
| Уметь:  применять методики оценки уязвимости в информационно-телекоммуникационных сетях; |
| ПК-13 способность осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем | Уметь проектировать системы защиты информации. | Все разделы дисциплины | Комплект КИМ |
| ОПК-4 способность 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; | Все разделы дисциплины | Комплект КИМ |
| Уметь:  проектировать системы защиты информации. |
| ОПК-3 способность использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности | Знать:  архитектуру защищённых экономических систем. | Все разделы дисциплины | Комплект КИМ |
| Уметь:  использовать смешанные стратегии | Все разделы дисциплины | Комплект КИМ |
| **Промежуточная аттестация** | |  | Комплект КИМ |

* 1. **Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации**

Для оценивания результатов обучения на зачете используется 2-балльная шкала: «зачтено» и «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

|  |  |  |
| --- | --- | --- |
| Критерии оценивания компетенций | Уровень сформирован ности компетенций | Шкала оценок |
| Достаточно полное знание учебного материала и успешное выполнение всех практических заданий. | *Повышенный или базовый уровень* | *Зачтено* |
| существенные пробелы в знании учебного материала и наличие принципиальных ошибок в выполнении практических заданий |  | *Не зачтено* |

Для оценивания результатов обучения на экзамене (зачете с оценкой) используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

|  |  |  |
| --- | --- | --- |
| Критерии оценивания компетенций | Уровень сформирован ности компетенций | Шкала оценок |
| Отличное знание теоретического материала, правильное и эффективное решение задачи, правильные ответы на тестовые вопросы.  Должны быть выполнены ВСЕ лабораторные работы | *Повышенный уровень* | *Отлично* |
| Хорошее знание теоретического материала, в целом правильное решение задачи.  НО: допускает незначительные ошибки в решении задачи. Неправильный ответ на тест.  ИЛИ: выполнены все показатели повышенного уровня, но не зачтена одна задача | *Базовый уровень* | *Хорошо* |
| Решение задачи не доведено до конца или недостаточное знание теоретического материала, ошибки в тестахНеоптимальное решение задачи и недостаточное владение теоретическим материалом.  ИЛИ: выполнены все показатели базового уровня, но по дисциплине не зачтены более одной задачи. | *Пороговый уровень* | *Удовлетворител ьно* |
| Задача не решена или серьезные пробелы в знании теоретического материала (с незнанием могут быть связаны и грубые ошибки в ответе на тестовые вопросы) | *–* | *Не удовлетворитель*  *но* |

* 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**

**19.3.1 Перечень вопросов к зачету с оценкой:**

1. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
2. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
3. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
4. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
5. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
6. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
7. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
8. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
9. Биометрические средства идентификации и аутентификации пользователей.
10. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
11. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
12. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
13. Законодательный уровень применения цифровой подписи.
14. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
15. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
16. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
17. Средства обеспечения информационной безопасности в ОС Windows’2000. Разграничение доступа к данным. Групповая политика.
18. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
19. Применение средств Windows 2000/XP для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
20. Разграничение доступа к данным в ОС семейства UNIX.
21. Пользователи и группы в ОС UNIX.
22. Пользователи и группы в ОС Windows’2000.
23. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
24. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
25. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
26. Распределенные информационные системы. Удаленные атаки на информационную систему.
27. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
28. Физические средства обеспечения информационной безопасности.
29. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
30. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
31. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
32. Виртуальные частные сети, их функции и назначение.

**19.3.2 Перечень вопросов к зачету**

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.

**19.3.4 Пример заданий для контрольной работы**

**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:**

|  |  |
| --- | --- |
| Отлично | Даны правильные развернутые ответы на все теоретические вопросы и верно выполнены все практические задания. |
| Хорошо | Даны правильные ответы на большую часть теоретических вопросов, но имеются некоторые недочеты, которые студент сам исправляет по замечанию преподавателя. Большая часть практических заданий выполнена правильно, но имеются недочеты и погрешности, приводящие к несущественному искажению результатов в одном из заданий. |
| Удовлетворительно | Даны правильные ответы на большую часть теоретических вопросов, но имеются неполные ответы и ошибочные утверждения. Большая часть практических заданий выполнена правильно, но имеются ошибки и погрешности, приводящие к неверному результату в одном из заданий. |
| Неудовлетворительно | Ответы на большую часть теоретических вопросов неверные. Значительная часть практических заданий не выполнена или допущены существенные ошибки, показывающие, что студент не владеет обязательными знаниями по данной теме. |

Составитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Барановский Е.С.

* 1. **Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме контрольных работ.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя практические задания, позволяющие оценить степень сформированности умений и навыков. При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.