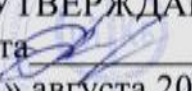


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета  С.М. Пасмурнов  
«31» августа 2017 г.

**РАБОЧАЯ ПРОГРАММА  
дисциплины**

**«Защита программ и данных»**

**Специальность** 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

**Специализация** Безопасность распределенных компьютерных систем

**Квалификация выпускника** специалист по защите информации

**Нормативный период обучения** 5 лет и 6 м.

**Форма обучения** очная

**Год начала подготовки** 2017

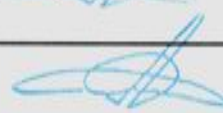
Автор программы

 /В.Н. Деревянко/

Заведующий кафедрой  
Систем информационной  
безопасности

 / А.Г. Остапенко /

Руководитель ОПОП

 / А.Г. Остапенко /

Воронеж 2017

## **1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ**

### **1.1.Целидисциплины**

Формирование навыков ценностно-информационного подхода к защите программ и данных в компьютерных системах

### **1.2.Задачiosoвoениядисциплины**

- подготовить специалиста с глубокими знаниями в области основ защиты программ и данных;
- научить основным принципам обеспечения безопасности программ и данных;
- изучение методологии анализа безопасности программ и данных, тестирования программ, оценке вероятности наличия в программном обеспечении разрушающих программных средств, а также обеспечению целостности и достоверности используемого программного кода

## **2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП**

Дисциплина«Защитапрограммиданных»относитсякдисциплинамбазово  
йчастиблокаБ1.

## **3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИ ПЛИНЕ**

Процессизучениядисциплины«Защитапрограммиданных»направленна  
формированиеследующихкомпетенций:

ОПК-9-способностьюразрабатыватьформальныемоделиполитикбезопа  
сности,политикууправлениядоступомиинформационнымипотокаимвкомпьюте  
рныхсистемахсучетомугрозбезопасностиинформации

ПК-5-способностьюучаствоватьвразработкеиконфигурированииипрогра  
мно-аппаратныхсредствзащитыинформации,включаязащищенныеоперацио  
нныесистемы,системыуправлениябазамиданных,компьютерныесети,системы  
антивируснойзащиты,средствакриптографическойзащитыинформации

ПК-12-способностьюпроводитьинструментальныймониторингзащищен  
ностикомпьютерныхсистем

ПК-14-способностьюорганизовыватьработыповыполнениюрежимазащ  
итыинформации,втомчислеограниченногодоступа

ПК-19-способностьюпроизводитьпроверкитехническогосостоянияипро  
филактическиеосмотрытехническихсредствзащитыинформации

| <b>Компетенция</b> | <b>Результатыобучения,характеризующие<br/>сформированностькомпетенции</b>                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------|
| ОПК-9              | Знатьязыки и системы программирования                                                                                       |
|                    | Уметьиспользовать языки и системы<br>программирования для решения профессиональных,<br>исследовательских и прикладных задач |
|                    | Владетьинструментальными средствами для<br>решения профессиональных, исследовательских и<br>прикладных задач                |
| ПК-5               | Знать функционал средств защиты информации                                                                                  |

|       |                                                                                                                                |
|-------|--------------------------------------------------------------------------------------------------------------------------------|
|       | Уметь участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации                              |
|       | Владеть доступными интерфейсами средств защиты информации                                                                      |
| ПК-12 | Знать требования к защищенности информационных систем                                                                          |
|       | Уметь проводить инструментальный мониторинг защищенности компьютерных систем                                                   |
|       | Владеть инструментами мониторинг защищенности компьютерных систем                                                              |
| ПК-14 | Знать требования режима защиты информации, в том числе ограниченного доступа                                                   |
|       | Уметь организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа                          |
|       | Владеть методами обеспечения режима защиты информации, в том числе ограниченного доступа                                       |
| ПК-19 | Знать показатели и критерии технического состояния технических средств защиты информации                                       |
|       | Уметь производить проверки технического состояния и профилактические осмотры технических средств защиты информации             |
|       | Владеть методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации |

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Защита программ данных» составляет 53 е.

Распределение трудоемкости дисциплины по видам занятий  
**очная форма обучения**

| Виды учебной работы                       | Всего часов | Семестры |
|-------------------------------------------|-------------|----------|
|                                           |             | 8        |
| <b>Аудиторные занятия (всего)</b>         | 72          | 72       |
| В том числе:                              |             |          |
| Лекции                                    | 36          | 36       |
| Лабораторные работы (ЛР)                  | 36          | 36       |
| <b>Самостоятельная работа</b>             | 72          | 72       |
| Часы на контроль                          | 36          | 36       |
| Виды промежуточной аттестации - экзамен   | +           | +        |
| Общая трудоемкость:<br>академические часы | 180         | 180      |

|         |   |   |
|---------|---|---|
| зач.ед. | 5 | 5 |
|---------|---|---|

## 5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

### 5.1Содержаниеразделовдисциплиныираспределениетрудовоемкостипо видам занятий

#### очнаяформаобучения

| № п/п        | Наименованиетемы                                                                                                                    | Содержаниераздела                                                                                                                                                                                                                                                                                                                                                                                                      | Лекц      | Лаб. зан. | СРС       | Всего, час |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------|-----------|------------|
| 1            | Введение в теорию обеспечения безопасности программного обеспечения и данных                                                        | Основные положения теории безопасности программ и данных. Угрозы безопасности программному обеспечению и данным. Теоретические основы дисциплины и терминология. Основные принципы обеспечения безопасности программного обеспечения и данных. Технологическая и эксплуатационная безопасность программ                                                                                                                | 6         | 6         | 12        | 24         |
| 2            | Методы и средства анализа безопасности программного обеспечения и данных                                                            | Контрольно-испытательные методы анализа безопасности программ и данных. Логико-аналитические методы контроля безопасности программ и данных. Сравнительный анализ логико-аналитических и контрольно-испытательных методов анализа безопасности программ и данных. Выявление уязвимостей программ и данных. Выбор программного обеспечения безопасности компьютерных систем. Модели поведения программного обеспечения. | 6         | 6         | 12        | 24         |
| 3            | Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность                                    | Обобщенные способы анализа программных средств на предмет наличия (отсутствия) разрушающих программных средств. Построение программно-аппаратных комплексов для контроля технологической безопасности программного обеспечения и данных.                                                                                                                                                                               | 6         | 6         | 12        | 24         |
| 4            | Расчет вероятности наличия разрушающих программных средств на этапе испытаний программного обеспечения и подходы к его исследованию | Постановка задачи. Обоснование множества информационных характеристик. Алгоритмы приближенных вычислений вероятностных характеристик наличия в программном обеспечении разрушающих программных средств. Обоснование критериев принятия решений о наличии в программном обеспечении разрушающих программных средств. Подходы к исследованию безопасности сложных программных комплексов.                                | 6         | 6         | 12        | 24         |
| 5            | Методы обеспечения надежности программ для контроля их технологической безопасности                                                 | Исходные данные, определения и условия. Анализ существующих моделей надежности программного обеспечения. Модель Нельсона. Оценка технологической безопасности программного обеспечения на базе модели Нельсона.                                                                                                                                                                                                        | 6         | 6         | 12        | 24         |
| 6            | Методы и средства обеспечения целостности и достоверности используемого программного кода                                           | Методы защиты программ и данных от несанкционированных изменений. Проверка целостности программ и данных. Схема подписи с верификацией по запросу. Примеры применения схемы подписи с верификацией по запросу. Основные подходы к защите программного обеспечения от несанкционированного копирования.                                                                                                                 | 6         | 6         | 12        | 24         |
| <b>Итого</b> |                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>36</b> | <b>36</b> | <b>72</b> | <b>144</b> |

### 5.2Переченьлабораторныхработ

1) Оценка уязвимости программного обеспечения компьютерных

систем.

- 2) Выбор рационального варианта средства защиты программного обеспечения компьютерных систем.
- 3) Формирование альтернативных вариантов комплексов средств защиты программного обеспечения компьютерных систем методом морфологического анализа.
- 4) Выбор рационального варианта комплекса средств защиты программного обеспечения компьютерных систем.

## **6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ**

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

## **7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНО ЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ**

**7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания**

### **7.1.1Этаптекущегоконтроля**

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

| <b>Компетенция</b> | <b>Результатыобучения,характеризующие сформированностькомпетенции</b>                                                  | <b>Критерии оценивания</b>                                                                                          | <b>Аттестован</b>                                             | <b>Неаттестован</b>                                             |
|--------------------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------|
| ОПК-9              | Знать языки и системы программирования                                                                                 | Знает операторы и конструкции языка                                                                                 | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|                    | Уметь использовать языки и системы программирования для решения профессиональных, исследовательских и прикладных задач | Умеет применять языки и системы программирования для решения профессиональных, исследовательских и прикладных задач | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|                    | Владеть инструментальными средствами для решения профессиональных, исследовательских и прикладных задач                | Владеет инструментальными средствами для решения профессиональных, исследовательских и прикладных задач             | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-5               | Знать функционал средств защиты информации                                                                             | Знает функционал основных типов и классов средств защиты информации                                                 | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

|       |                                                                                                         |                                                                                                                    |                                                               |                                                                 |
|-------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------|
|       | Уметь участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации       | Умеет разрабатывать и конфигурировать программно-аппаратные средства защиты информации                             | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | Владеть доступными интерфейсами средств защиты информации                                               | Владеет доступными интерфейсами средств защиты информации                                                          | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-12 | Знать требования к защищенности информационных систем                                                   | Знает требования к защищенности информационных систем                                                              | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | Уметь проводить инструментальный мониторинг защищенности компьютерных систем                            | Умеет проводить инструментальный мониторинг защищенности компьютерных систем                                       | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | Владеть инструментами мониторинг защищенности компьютерных систем                                       | Владеет инструментами мониторинг защищенности компьютерных систем                                                  | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-14 | Знать требования режима защиты информации, в том числе ограниченного доступа                            | Знает требования режима защиты информации, в том числе ограниченного доступа                                       | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | Уметь организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа   | Умеет организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа              | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | Владеть методами обеспечения режима защиты информации, в том числе ограниченного доступа                | Владеет методами обеспечения режима защиты информации, в том числе ограниченного доступа                           | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-19 | Знать показатели и критерии технического состояния технических средств защиты информации                | Знает показатели и критерии технического состояния технических средств защиты информации                           | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | Уметь производить проверки технического состояния и профилактические осмотры технических средств защиты | Умеет производить проверки технического состояния и профилактические осмотры технических средств защиты информации | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

|  |                                                                                                                                |                                                                                                                                |                                                               |                                                                 |
|--|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------|
|  | информации                                                                                                                     |                                                                                                                                |                                                               |                                                                 |
|  | Владеть методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации | Владеет методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

### 7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по четырех балльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции                                                      | Критерии оценивания                                      | Отлично                                                | Хорошо                                                                                | Удовл.                                                   | Неудовл.                             |
|-------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------------|
| ОПК-9       | Знать языки и системы программирования                                                                                 | Тест                                                     | Выполнение теста 90- 100%                              | Выполнение теста 80- 90%                                                              | Выполнение теста 70- 80%                                 | В тесте менее 70% правильных ответов |
|             | Уметь использовать языки и системы программирования для решения профессиональных, исследовательских и прикладных задач | Решение стандартных практических задач                   | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
|             | Владеть инструментальными средствами для решения профессиональных, исследовательских и прикладных задач                | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
| ПК-5        | Знать функционал средств защиты информации                                                                             | Тест                                                     | Выполнение теста 90- 100%                              | Выполнение теста 80- 90%                                                              | Выполнение теста 70- 80%                                 | В тесте менее 70% правильных ответов |
|             | Уметь участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации                      | Решение стандартных практических задач                   | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
|             | Владеть доступными интерфейсами средств                                                                                | Решение прикладных задач в                               | Задачи решены в полном                                 | Продемонстрирован верный ход                                                          | Продемонстрирован верный ход решения в                   | Задачи не решены                     |

|       |                                                                                                       |                                                          |                                                        |                                                                                       |                                                          |                                      |
|-------|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------------|
|       | защиты информации                                                                                     | конкретной предметной области                            | объеме и получены верные ответы                        | решения всех, но не получен верный ответ во всех задачах                              | большинстве задач                                        |                                      |
| ПК-12 | Знать требования к защищенности информационных систем                                                 | Тест                                                     | Выполнение тестов 90- 100%                             | Выполнение тестов 80- 90%                                                             | Выполнение тестов 70- 80%                                | В тесте менее 70% правильных ответов |
|       | Уметь проводить инструментальный мониторинг защищенности компьютерных систем                          | Решение стандартных практических задач                   | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи решены                        |
|       | Владеть инструментами мониторинг защищенности компьютерных систем                                     | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи решены                        |
| ПК-14 | Знать требования режима защиты информации, в том числе ограниченного доступа                          | Тест                                                     | Выполнение тестов 90- 100%                             | Выполнение тестов 80- 90%                                                             | Выполнение тестов 70- 80%                                | В тесте менее 70% правильных ответов |
|       | Уметь организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа | Решение стандартных практических задач                   | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи решены                        |
|       | Владеть методами обеспечения режима защиты информации, в том числе ограниченного доступа              | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи решены                        |
| ПК-19 | Знать показатели и критерии технического состояния технических средств защиты информации              | Тест                                                     | Выполнение тестов 90- 100%                             | Выполнение тестов 80- 90%                                                             | Выполнение тестов 70- 80%                                | В тесте менее 70% правильных ответов |
|       | Уметь производить                                                                                     | Решение стандартных практических задач                   | Задачи решены в                                        | Продемонстрирован                                                                     | Продемонстрирован верный                                 | Задачи решены                        |

|  |                                                                                                                                |                                                          |                                                        |                                                                                       |                                                          |               |
|--|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------|---------------|
|  | проверки технического состояния и профилактические осмотры технических средств защиты информации                               | технических задач                                        | полном объеме и получены верные ответы                 | верный ход решения всех, но не получен верный ответ во всех задачах                   | ход решения в большинстве задач                          |               |
|  | Владеть методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи решены |

## **7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков (или) опыта деятельности)**

### **7.2.1 Примерный перечень заданий для подготовки к тестированию**

#### **Задание № 1**

Вопрос:

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

Выберите один из 4 вариантов ответа:

- 1) пароли
- 2) анкеты
- 3) коды
- 4) ярлыки

#### **Задание № 2**

Вопрос:

От несанкционированного доступа может быть защищён:

Выберите несколько из 4 вариантов ответа:

- 1) каждый диск
- 2) папка
- 3) файл
- 4) ярлык

#### **Задание № 3**

Вопрос:

К биометрическим системам защиты информации относятся системы идентификации по:

Выберите несколько из 9 вариантов ответа:

- 1) отпечаткам пальцев
- 2) характеристикам речи
- 3) радужной оболочке глаза

- 4) изображению лица
- 5) геометрии ладони руки
- 6) росту
- 7) весу
- 8) цвету глаз
- 9) цвету волос

#### Задание № 4

Вопрос:

Какие существуют массивы дисков RAID?

Выберите несколько из 4 вариантов ответа:

- 1) RAID 0
- 2) RAID 1
- 3) RAID 10
- 4) RAID 20

#### Задание № 5

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) Для создания массива этого уровня понадобится как минимум два диска одинакового размера. Запись осуществляется по принципу чередования: данные делятся на порции одинакового размера (A1, A2, A3 и т.д.), и поочередно распределяются по всем дискам, входящим в массив.

2) Массивы этого уровня построены по принципу зеркалирования, при котором все порции данных (A1, A2, A3 и т.д.), записанные на одном диске, дублируются на другом.

- \_\_\_ RAID 0
- \_\_\_ RAID 1

#### Задание № 6

Вопрос:

Выберите типы вредоносных программ:

Выберите несколько из 6 вариантов ответа:

- 1) Вирусы, черви, троянские и хакерские программы
- 2) Шпионское, рекламное программное обеспечение
- 3) Потенциально опасное программное обеспечение
- 4) Операционная система Linux
- 5) Операционная система Windows

#### Задание № 7

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

- 1) сигнатуры. Сигнатура - это некоторая постоянная

последовательность программного кода, специфичная для конкретной вредоносной программы.

2) алгоритмы эвристического сканирования, т.е. анализа последовательности команд в проверяемом объекте.

\_\_\_ Для поиска известных вредоносных программ используются

\_\_\_ Для поиска новых вирусов используются

#### Задание № 8

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия. Основная задача состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

2) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

\_\_\_ Антивирусный монитор запускается

\_\_\_ Антивирусный сканер запускается

#### Задание № 9

Вопрос:

Компьютерные вирусы -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной

активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

#### Задание № 10

Вопрос:

По "среде обитания" вирусы можно разделить на:

Выберите несколько из 6 вариантов ответа:

- 1) загрузочные
- 2) файловые
- 3) макровирусы
- 4) очень опасные
- 5) не опасные
- 6) опасные

#### **7.2.2 Примерный перечень заданий для решения стандартных задач**

#### Задание № 11

Вопрос:

Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:

- 1) заражают загрузочный сектор гибкого или жёсткого диска.
  - 2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске.
  - 3) существуют для интегрированного офисного приложения MicrosoftOffice.
- \_\_\_ загрузочные вирусы  
\_\_\_ файловые вирусы  
\_\_\_ макровирусы

#### Задание № 12

Вопрос:

Сетевые черви -

Выберите один из 5 вариантов ответа:

- 1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
- 2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
- 3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
- 4) это программное или аппаратное обеспечение, которое проверяет

информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

#### Задание № 13

Вопрос:

Сетевые черви бывают:

Выберите несколько из 4 вариантов ответа:

- 1) Web-черви
- 2) почтовые черви
- 3) черви операционной системы
- 4) черви MS Office

#### Задание № 14

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) Профилактическая защита от таких червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

2) Профилактическая защита от таких червей состоит в том, что не рекомендуется открывать вложенные в сообщения файлы, полученные от сомнительных источников. А также рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

\_\_\_ Web-черви

\_\_\_ почтовые черви

#### Задание № 15

Вопрос:

Наиболее эффективны от Web-червей, Web-антивирусные программы, которые включают:

Выберите несколько из 3 вариантов ответа:

- 1) межсетевой экран
- 2) модуль проверки скриптов
- 3) антивирусный сканер

#### Задание № 16

Вопрос:

Межсетевой экран (брандмауэр) -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание № 17

Вопрос:

Троянская программа, троянец -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной

активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

#### Задание № 18

Вопрос:

Троянские программы бывают:

Выберите несколько из 4 вариантов ответа:

- 1) утилиты удалённого администрирования
- 2) программы - шпионы
- 3) рекламные программы
- 4) программы удаления данных на локальном компьютере

#### Задание № 19

Вопрос:

Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:

1) троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, в том числе они могут быть использованы для обнаружения и передачи конфиденциальной информации.

2) троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайн-платежей и банковских систем.

3) эти программы встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Эти программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять её злоумышленнику.

\_\_\_ Троянские утилиты удалённого администрирования

\_\_\_ Троянские программы - шпионы

\_\_\_ Рекламные программы

#### Задание № 20

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.

2) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров.

\_\_\_ DoS - программы

\_\_\_ DDos - программы

#### **7.2.3 Примерный перечень заданий для решения прикладных задач**

Вопрос № 1 Предоставление определённому лицу или группе лиц прав на выполнение определённых действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий называется:

- А Авторизацией
- Б Аутентификацией
- В Идентификацией
- Г Управлением доступом

Вопрос № 2 Сеть из взломанных компьютеров, на которых выполняются вредоносные программы, которая удаленно контролируется киберпреступниками и используются для DDoS-атак, рассылки спама, называется:

- А Брутфорс
- Б Воронка
- В Упаковщик
- Г Ботнет

Вопрос № 3 Обнаружение действий, направленных на НСД к информации, специальные воздействия на информацию в целях добывания, уничтожения, искажения и блокирования доступа к ней, а также реагирование на эти действия обеспечиваются:

- А Антивирусной защитой
- Б Обнаружением (предотвращением) вторжений
- В Ограничениями программной среды.
- Г Идентификацией и аутентификацией субъектов доступа и объектов доступа

Вопрос № 4 Какая была пропускная способность у самой мощной DDoS-атаки?

- А Около 500 Мбит/с
- Б Около 1 Гбит/с
- В Около 500 Гбит/с
- Г Более 1 Тбит/с

Вопрос № 5 Механизм обмана пользователя, при котором жертва думает, что щелкает по определенному объекту на странице, а на самом деле кликает по объекту, встроенному в страницу злоумышленником, называется:

- А Киберсквоттинг
- Б Словарная атака
- В Кликджекинг
- Г Поведенческий анализ

Вопрос № 6 Допустим, вы столкнулись с инцидентом в вашей сети. Что вы сделаете в первую очередь, прежде чем его исследовать?

- А Изолирую систему от корпоративной сети
- Б Перезапущу компьютер
- В Сделаю образ диска
- Г Сохраню дампы памяти

Вопрос № 7 Какие сервисы компании могут стать мишенью для

DDoS-атак?

- А Общеизвестные сайты и порталы для клиентов
- Б Серверы почты и сервисы сообщений
- В Файл-серверы и сервисы, обеспечивающие транзакции
- Г Все вышеперечисленное

Вопрос № 8 Что означает аббревиатура EDR?

А EpicDelayReduction (эпическое сокращение задержки) – технология, ускоряющая наиболее длительные операции

Б Это тикеркриптовалюты E-DinarCoin

В EndpointDetectionandRemediation – обнаружение атак на рабочих станциях и принятие корректирующих мер

Г EndpointDetectionandResponse – обнаружение атак на рабочих станциях и реагирование на них

Вопрос № 9 Дискреционная политика доступа:

А Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)

Б Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности

В Является алгоритмом формирования матрицы доступа

Г Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

Вопрос № 10 Программа, перехватывающая нажатия клавиш на клавиатуре и отправляющая их злоумышленникам, называется:

А Кликджекинг

Б Кейлоггер

В Кэшбэк

Г Криптор

Вопрос № 11 Какова конечная цель идентификации и аутентификации субъекта в системе?

А Его допуск к информации ограниченного пользования при положительном результате или отказ в допуске при отрицательном результате

Б Определение его принадлежности к числу пользователей или аппаратных устройств компьютера

В Определение времени, отведенного объекту (субъекту) на работу

Г Выделение объекту (субъекту) определенного объема памяти

#### **7.2.4Примерныйпереченьвопросовдляподготовкикзачету**

Непредусмотреноучебнымпланом

#### **7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач**

1. Понятие информационной безопасности. Основные составляющие информационной

безопасности.

2. Важность и сложность проблемы информационной безопасности

3. Программно-технические меры безопасности. Понятие сервиса информационной

безопасности. Архитектурная безопасность.

4. Понятие сервиса информационной безопасности. Идентификация и аутентификация.

5. Понятие сервиса информационной безопасности. Управление доступом.

6. Понятие сервиса информационной безопасности. протоколирование и аудит.

7. Понятие сервиса информационной безопасности. управление и анализ защищенности.

8. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.

9. Понятие сервиса информационной безопасности. экранирование и туннелирование.

10. Понятие сервиса информационной безопасности. криптография: шифрование.

11. Понятие сервиса информационной безопасности. криптография: контроль целостности.

12. Криптология : базовые понятия и терминология.

13. Криптографические примитивы и их свойства.

14. Модели основных криптоаналитических атак.

15. Антивирусная защита. История развития вирусов и их классификация. Методы защиты от вредоносных программ

#### **7.2.6. Методика выставления оценки при проведении промежуточной аттестации**

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов по задаче. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, за задачу оценивается в 10 баллов (5 баллов за верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

#### **7.2.7 Паспорт оценочных материалов**

| №п/п | Контролируемые разделы (темы) дисциплины | Код контролируемой компетенции   | Наименование оценочного средства                                                                         |
|------|------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------|
| 1    | Знать языки и системы программирования   | ОПК-9, ПК-5, ПК-12, ПК-14, ПК-19 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 2    | Уметь использовать языки и               | ОПК-9, ПК-5,                     | Тест, контрольная работа,                                                                                |

|   |                                                                                                         |                                   |                                                                                                          |
|---|---------------------------------------------------------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------|
|   | системы программирования для решения профессиональных, исследовательских и прикладных задач             | ПК- 12, ПК-14, ПК-19              | защита лабораторных работ, защита реферата, требования к курсовому проекту....                           |
| 3 | Владеть инструментальными средствами для решения профессиональных, исследовательских и прикладных задач | ОПК-9, ПК-5, ПК- 12, ПК-14, ПК-19 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 4 | Знать функционал средств защиты информации                                                              | ОПК-9, ПК-5, ПК- 12, ПК-14, ПК-19 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 5 | Уметь участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации       | ОПК-9, ПК-5, ПК- 12, ПК-14, ПК-19 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 6 | Владеть доступными интерфейсами средств защиты информации                                               | ОПК-9, ПК-5, ПК- 12, ПК-14, ПК-19 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |

### **7.3.Методическиматериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности**

Тестированиеосуществляется,либоприпомощикомпьютернойсистемыт естирования,либоиспользованиемвыданныхтест-заданийнабумажномносите ле.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатор омивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютер нойсистемытестирования,либоиспользованиемвыданныхзадачнабумажномн осителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязад ачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценки припроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютерн ойсистемытестирования,либоиспользованиемвыданныхзадачнабумажномно сителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязада чэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкип рипроведениипромежуточнойаттестации.

## **8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)**

### **8.1Переченьучебнойлитературы,необходимойдляосвоениядисципл**

## ины

### Основная литература:

1. Кащенко Г.А. Защита программного обеспечения от несанкционированного использования [Электронный ресурс]: Учеб.пособие / Г. А. Кащенко. - Электрон.текстовые, граф. дан. (559 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.
2. Кащенко, Г.А. Защита программ и данных [Электронный ресурс] / Г. А. Кащенко; Учеб.пособие. - Электрон.текстовые, граф. дан. (3,28 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.
3. Савинков, А.Ю. Разграничение доступа UNIX и LINUX: [Учеб.пособие] / А. Ю. Савинков. - Воронеж: ВПО, 2016. - ISBN 978-59907345-5-5: 100-00.

### Дополнительная литература:

1. Методические указания к самостоятельным работам по дисциплинам «Защита программ и данных», «Защита в операционных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост. Г. А. Кащенко. - Электрон.текстовые, граф. дан. (442 Кб). - Воронеж: ФГБОУ ВПО "Воронежскийгосударственныйтехническийуниверситет", 2015. - 1 файл. - 00-00.
2. Методические указания к лабораторным работам № 5–8 по дисциплинам «Защита в операционных системах», «Безопасность операционных систем» для студентов специальностей 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: А. Ю. Савинков, Н. А. Ленков, В. Н. Деревянко. - Электрон.текстовые, граф. дан. (424 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.
3. Методические указания к практическим занятиям по дисциплине «Защита в операционных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: А. Ю. Савиков, Н. А. Ленков, В. Н. Деревянко. - Электрон.текстовые, граф. дан. (332 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

**8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:**

- 1) Банк данных угроз безопасности информации – URL:

<http://bdu.fstec.ru>.

2) Информационно-правовая система «Законодательство России» // Официальный интернет-портал правовой информации – URL: <http://pravo.gov.ru/proxy/ips>.

3) Каталог стандартов // Официальный сайт Росстандарта – URL: <http://www.gost.ru/wps/portal/pages.CatalogOfStandarts>.

4) Официальный сайт ФСТЭК России – URL: <http://fstec.ru>.

## **9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**

Компьютерных класс с количеством персональных компьютеров из расчета 1 персональный компьютер на 2 обучающихся.

## **10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

По дисциплине «Защита программ данных» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

| Вид учебных занятий    | Деятельность студента                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Лекция                 | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии. |
| Лабораторная работа    | Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомиться с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.                                                                                                                             |
| Самостоятельная работа | Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:<br>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;                                                                                                                                                                                                                                                                         |

|                                       |                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | <ul style="list-style-type: none"> <li>- выполнение домашних заданий и расчетов;</li> <li>- работа над темами для самостоятельного изучения;</li> <li>- участие в работе студенческих научных конференций, олимпиад;</li> <li>- подготовка к промежуточной аттестации.</li> </ul>                            |
| Подготовка к промежуточной аттестации | <p>Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.</p> |