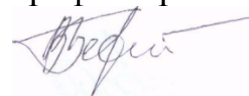


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**Федеральное государственное бюджетное образовательное учреждение высшего**  
**образования «Московский государственный университет технологий и управления**  
**имени К.Г. Разумовского (Первый казачий университет)»**

**Донской казачий государственный институт пищевых технологий и бизнеса**  
**(филиал) Федеральное государственное бюджетное образовательное учреждение**  
**высшего образования «Московский государственный университет технологий и**  
**управления имени К.Г. Разумовского (Первый казачий университет)»**

**«УТВЕРЖДАЮ»**

Заведующий кафедрой «МФиИТ»  
доктор физико-математических  
наук,  
профессор



**В.Н. Беркович**

## **РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**«Защита информации»**

*(наименование учебной дисциплины (модуля))*

По направлению подготовки:

**15.03.04 «Автоматизация технологических процессов и производств»**

Профиль подготовки:

**«Автоматизация технологических процессов и производств»**


Квалификация:

**Бакалавр**

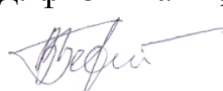
**Ростов-на-Дону 2017 г.**

Рабочая программа учебной дисциплины «Защита информации» разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 15.03.05 «Автоматизация технологических процессов и производств», профиль подготовки «Автоматизация технологических процессов и производств» (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 12 марта 2015 г. № 200 учебного плана по образовательной программе высшего образования «Автоматизация технологических процессов и производств».

Рабочая программа учебной дисциплины разработана рабочей группой в составе: д.ф-м.н., профессор Беркович В.Н.

Руководитель образовательной программы высшего образования  
к.т.н., доцент  Павлова И.В.

Рабочая программа учебной дисциплины обсуждена и утверждена на заседании кафедры «Математика, физика и информационные технологии»  
Протокол № 1 от «29» августа 2017 года

Заведующий кафедрой д. физ – мат н,  
ученая степень, ученое звание  Беркович В.Н.  
(подпись)

Рабочая программа учебной дисциплины рекомендована к утверждению представителями организаций-работодателей:

ООО «ДонСетьСтройПроект»,  
Начальник отдела АИИС КУЭ, МОП  
и ТСБ



(подпись)

С.Б. Бурцев

ООО «Джинт»,  
Генеральный директор, к.т.н.



(подпись)

И.В. Дерябкин

## Содержание

|  |    |
|--|----|
| 1. Цели и задачи дисциплины .....  | 4  |
| 1.1. Цели дисциплины.....  | 4  |
| 1.2. Задачи дисциплины.....  | 4  |
| 2. Требования к уровню освоения дисциплины .....   | 4  |
| 2.1. Уровень освоения дисциплины .....   | 4  |
| 2.2. Место дисциплины в структуре ООП ВПО. Связь с предшествующими и последующими дисциплинами. .... | 5  |
| 3. Компетенции:.....   | 6  |
| 4. Тематический план дисциплины .....  | 7  |
| 5. Содержание и структура дисциплины .....   | 11 |
| 5.1. Содержание дисциплины по видам занятий.....   | 13 |
| 5.1.1. Лекции .....  | 13 |
| 5.1.2. Практические занятия (семинары) .....   | 14 |
| 5.1.3. Лабораторный практикум.....   | 14 |
| 5.2. Самостоятельная работа студентов .....  | 14 |
| 6. Текущий контроль успеваемости и промежуточная аттестация .....                                    | 16 |
| 6.1. Текущий контроль успеваемости .....   | 16 |
| 6.1.1. Контроль самостоятельной работы студентов .....   | 16 |
| 6.1.2. Текущий контроль знаний студентов.....  | 16 |
| 6.3. Фонд оценочных средств.....   | 16 |
| 7. Учебно-методическое обеспечение дисциплины.....   | 20 |
| 7.1. Основная литература .....   | 20 |
| 7.2. Дополнительная литература.....  | 21 |
| 7.3. Периодические издания.....  | 21 |
| 7.4. Ресурсы Интернет .....  | 21 |
| 7.5. Программное обеспечение .....   | 21 |
| 7.6. Материально-техническая база.....   | 22 |
| 8. Организация образовательного процесса для лиц с ограниченными возможностями .....                 | 22 |
| 9. Список экзаменационных вопросов по дисциплине .....   | 23 |

## **1. Цели и задачи дисциплины**

### **1.1. Цели дисциплины**

Ознакомление с понятием информационной безопасности, ее составляющими и признаками; формирование представления о различных угрозах информации, сопутствующих рисках, источниках угроз и формах, которые они принимают.

Формирование базовых знаний о методах и средствах защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

### **1.2. Задачи дисциплины**

Изучить теоретические основы защиты информации в компьютерных системах, включая основные понятия и определения, криптографические модели и алгоритмы шифрования, алгоритмы аутентификации пользователей и средства разграничения прав доступа к информации и ее обработке.

Рассмотреть источники, риски и формы атак на информацию, классификации угроз информационной безопасности.

Получить представление о методологии составления требований к системам защиты информации, построения политик безопасности, познакомиться с международными и государственными стандартами безопасности, классификацией программно-технических способов и средств обеспечения информационной безопасности.

Приобрести практические навыки использования доступных технологий и средств защиты компьютерной информации, в том числе навыки администрирования и мониторинга корпоративных сетей и операционных систем.

Провести самостоятельную аналитическую работу с целью изучения и поиска решения актуальных задач компьютерной и сетевой безопасности.

## **2. Требования к уровню освоения дисциплины**

### **2.1. Уровень освоения дисциплины**

**В результате изучения дисциплины студенты должны знать:**

- основные понятия и направления в защите компьютерной информации;
- принципы системного анализа и классификации угроз информационной безопасности;
- различные типы уязвимостей программного обеспечения, методы их выявления;
- методы хранения, обработки, передачи и защиты информации;

- основные инструменты обеспечения многоуровневой безопасности в информационных системах;
- аппаратно-технические средства обеспечения безопасности хранения и обработки данных, защиты информации от сбоев и отказов оборудования;
- методы и средства обеспечения информационной безопасности компьютерных систем.

**В результате изучения дисциплины студенты должны уметь:**

- конфигурировать встроенные средства защиты операционной системы;
- проводить анализ защищенности компьютера и сетевой среды;
- устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения;
- конфигурировать и использовать инструменты резервного копирования и восстановления информации;
- организовывать виртуальные частные сети, обеспечивать их безопасность;
- конфигурировать и использовать один из межсетевых экранов;
- использовать технологии и средства шифрования информации и организации обмена данными с использованием электронной цифровой подписи;
- использовать типовые программные продукты, ориентированные на решение научных и технологических задач.

**В результате изучения дисциплины студенты должны владеть:**

- навыками самостоятельного приобретения с помощью информационных технологий новых знаний и умений, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности;
- основными методами, способами и средствами получения, хранения, переработки информации;
- навыками работы с компьютером как средством управления информацией;
- навыками работы с информацией в глобальных компьютерных сетях;
- методиками использования программных средств для решения практических задач;
- навыками разработки алгоритмов решения задач управления и проектирования объектов автоматизации.

## **2.2. Место дисциплины в структуре ООП ВПО. Связь с предшествующими и последующими дисциплинами.**

Дисциплина "Защита информации" принадлежит базовой части профессионального цикла. Для изучения данной дисциплины необходимы знания и умения, полученные обучающимися в ходе изучения дисциплин

"Информатика", "Информатика с элементами программирования", "Информационные технологии", "Программирование", "ЭВМ и периферийные устройства". В свою очередь, знание дисциплины необходимо для понимания материала дисциплин "Сети ЭВМ и телекоммуникации", "Операционные системы", "Базы данных", выполнения заданий преддипломной или преддипломной практики, написания выпускной квалификационной работы и дальнейшей профессиональной деятельности.

### **3. Компетенции:**

**ПК-1** - способность собирать и анализировать исходные информационные данные для проектирования технологических процессов изготовления продукции, средств и систем автоматизации, контроля, технологического оснащения, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством; участвовать в работах по расчету и проектированию процессов изготовления продукции и указанных средств и систем с использованием современных информационных технологий, методов и средств проектирования;

**ПК-2** - способность выбирать основные и вспомогательные материалы для изготовления изделий, способы реализации основных технологических процессов, аналитические и численные методы при разработке их математических моделей, методы стандартных испытаний по определению физико-механических свойств и технологических показателей материалов и готовых изделий, стандартные методы их проектирования, прогрессивные методы эксплуатации изделий;

**ПК-23** - способность выполнять работы по наладке, настройке, регулировке, опытной проверке, регламентному техническому, эксплуатационному обслуживанию оборудования, средств и систем автоматизации, контроля, диагностики, испытаний и управления, средств программного обеспечения, сертификационным испытаниям изделий;

**ПК-24** - способность выбирать методы и средства измерения эксплуатационных характеристик оборудования, средств и систем автоматизации, контроля, диагностики, испытаний и управления, настройки и обслуживания: системного, инструментального и прикладного программного обеспечения данных средств и систем;

**ОПК-2** - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

#### 4. Тематический план дисциплины

##### Очная форма обучения, учебный план 2015 г.

| Раздел дисциплины   |  | Количество часов |                    |                      |                        |          |
|---|--|------------------|--------------------|----------------------|------------------------|----------|
|   |  | СР               | Аудиторные занятия |                      |                        |          |
|   |  |                  | Лекции             | Практические занятия | Лабораторный практикум | Контроль |
| <b>Тема 1.</b> Общие вопросы информационной безопасности  |  | 2                | 2                  |                      |                        |          |
| <b>Тема 2.</b> Общая характеристика средств и методов защиты информации   |  | 2                | 2                  |                      |                        |          |
| <b>Тема 3.</b> Системный анализ угроз безопасности в компьютерных системах  |  | 2                | 2                  |                      | 3                      |          |
| <b>Тема 4.</b> Основные классы программных ошибок в различных средах исполнения и языках программирования и вытекающие из этого типы уязвимости |  | 3                | 2                  |                      | 4                      |          |
| <b>Тема 5.</b> Ошибки класса "Bufferoverflow" и их эксплуатация   |  | 4                | 3                  |                      | 4                      |          |
| <b>Тема 6.</b> Уязвимости в интерпретируемых языках типа "инъекция"   |  | 4                | 3                  |                      | 4                      |          |
| <b>Тема 7.</b> Классы атак DoS и DDoS. Методы борьбы с DoS- и DDoS-атаками  |  | 4                | 3                  |                      | 4                      |          |
| <b>Тема 8.</b> Ошибки в программном обеспечении типа RaceCondition и эксплуатация этого класса ошибок   |  | 4                | 3                  |                      | 4                      |          |
| <b>Тема 9.</b> Криптографические  |  | 3                | 3                  |                      | 4                      |          |

|  |     |    |    |  |    |  |
|--|-----|----|----|--|----|--|
| методы защиты информации   |     |    |    |  |    |  |
| <b>Тема 10.</b> RAID-системы различных уровней (0,1,5,10,50)   |     | 3  | 3  |  | 4  |  |
| <b>Тема 11.</b> Защита на уровне оборудования и операционной системы                                 |     | 3  | 3  |  |    |  |
| <b>Тема 12.</b> Принципы работы и назначение гипервизора. Защита при помощи виртуальных машин        |     | 3  | 3  |  | 3  |  |
| <b>Тема 13.</b> Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов. |     | 3  | 2  |  |    |  |
| <b>Итого</b>   | 108 | 40 | 34 |  | 34 |  |

#### Очно-заочная форма обучения, учебный план 2015 г.

| Раздел дисциплины   |  | Количество часов |                    |                      |                        |          |
|---|--|------------------|--------------------|----------------------|------------------------|----------|
|   |  | СР               | Аудиторные занятия |                      |                        |          |
|   |  |                  | Лекции             | Практические занятия | Лабораторный практикум | Контроль |
| <b>Тема 1.</b> Общие вопросы информационной безопасности  |  | 4                | 1,5                |                      |                        |          |
| <b>Тема 2.</b> Общая характеристика средств и методов защиты информации   |  | 5                | 1,5                |                      |                        |          |
| <b>Тема 3.</b> Системный анализ угроз безопасности в компьютерных системах  |  | 5                | 2                  |                      | 2                      |          |
| <b>Тема 4.</b> Основные классы программных ошибок в различных средах исполнения и языках программирования и вытекающие из этого типы уязвимости |  | 5                | 2                  |                      | 2                      |          |
| <b>Тема 5.</b> Ошибки класса "Bufferoverflow" и их  |  | 5                | 2                  |                      | 3                      |          |



|   |     |    |     |  |    |  |
|---|-----|----|-----|--|----|--|
| эксплуатация  |     |    |     |  |    |  |
| <b>Тема 6.</b> Уязвимости в интерпретируемых языках типа "инъекция"                                   |     | 5  | 2   |  | 3  |  |
| <b>Тема 7.</b> Классы атак DoS и DDoS. Методы борьбы с DoS- и DDoS-атаками                            |     | 5  | 2   |  | 3  |  |
| <b>Тема 8.</b> Ошибки в программном обеспечении типа RaceCondition и эксплуатация этого класса ошибок |     | 5  | 1,5 |  | 3  |  |
| <b>Тема 9.</b> Криптографические методы защиты информации   |     | 5  | 1,5 |  | 2  |  |
| <b>Тема 10.</b> RAID-системы различных уровней (0,1,5,10,50)  |     | 5  | 1,5 |  | 2  |  |
| <b>Тема 11.</b> Защита на уровне оборудования и операционной системы                                  |     | 5  | 1,5 |  |    |  |
| <b>Тема 12.</b> Принципы работы и назначение гипервизора. Защита при помощи виртуальных машин         |     | 5  | 1,5 |  | 2  |  |
| <b>Тема 13.</b> Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов.  |     | 5  | 1,5 |  |    |  |
| Итого   | 108 | 64 | 22  |  | 22 |  |

### Заочная форма обучения, учебный план 2015 г.

| Раздел дисциплины            |  | Количество часов |                    |                      |                        |          |
|------------------------------|--|------------------|--------------------|----------------------|------------------------|----------|
|                              |  | СР               | Аудиторные занятия |                      |                        |          |
|                              |  |                  | Лекции             | Практические занятия | Лабораторный практикум | Контроль |
| <b>Тема 1.</b> Общие вопросы |  | 4                | 0,25               |                      |                        |          |

|   |  |   |      |  |      |     |
|---|--|---|------|--|------|-----|
| информационной безопасности   |  |   |      |  |      |     |
| <b>Тема 2.</b> Общая характеристика средств и методов защиты информации   |  | 5 | 0,25 |  |      |     |
| <b>Тема 3.</b> Системный анализ угроз безопасности в компьютерных системах  |  | 5 | 0,25 |  | 0,25 | 0,5 |
| <b>Тема 4.</b> Основные классы программных ошибок в различных средах исполнения и языках программирования и вытекающие из этого типы уязвимости |  | 5 | 0,25 |  | 0,25 | 0,5 |
| <b>Тема 5.</b> Ошибки класса "Bufferoverflow" и их эксплуатация   |  | 5 | 0,25 |  | 0,5  | 1   |
| <b>Тема 6.</b> Уязвимости в интерпретируемых языках типа "инъекция"   |  | 5 | 0,25 |  | 0,5  | 0,5 |
| <b>Тема 7.</b> Классы атак DoS и DDoS. Методы борьбы с DoS- и DDoS-атаками  |  | 5 | 0,25 |  | 0,5  | 0,5 |
| <b>Тема 8.</b> Ошибки в программном обеспечении типа RaceCondition и эксплуатация этого класса ошибок   |  | 5 | 0,25 |  | 0,5  | 1   |
| <b>Тема 9.</b> Криптографические методы защиты информации   |  | 5 | 0,25 |  | 0,5  | 1   |
| <b>Тема 10.</b> RAID-системы различных уровней (0,1,5,10,50)  |  | 5 | 0,5  |  | 0,5  | 0,5 |
| <b>Тема 11.</b> Защита на уровне оборудования и операционной системы  |  | 5 | 0,5  |  |      |     |
| <b>Тема 12.</b> Принципы работы и назначение гипервизора.   |  | 5 | 0,5  |  | 0,5  | 0,5 |

|  |     |    |      |  |   |   |
|--|-----|----|------|--|---|---|
| Защита при помощи виртуальных машин  |     |    |      |  |   |   |
| <b>Тема 13.</b> Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов. |     | 5  | 0,25 |  |   |   |
| Итого  | 108 | 94 | 4    |  | 4 | 6 |

## 5. Содержание и структура дисциплины

### **Тема 1.** *Общие вопросы информационной безопасности*

Предмет, содержание и задачи курса. Его место среди других дисциплин учебного плана. Основные понятия и определения. Формы отчетности, основная и дополнительная литература. Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации. Глобализация информационных отношений. Объективная необходимость и общественная потребность в защите информации. Информация как объект правовой защиты. Сущность, общее содержание и цели защиты информации. Правовое регулирование вопросов защиты информации. Информационные войны, информационное оружие и информационный терроризм.

### **Тема 2.** *Общая характеристика средств и методов защиты информации*

Основные принципы реализации систем защиты информации. Классификация и общая характеристика основных методов и средств защиты информации в компьютерных системах. Организационные мероприятия по защите информации. Требования к системам защиты информации. Построение политик безопасности. Назначение и задачи служб безопасности. Международные и государственные стандарты безопасности. Повышение эксплуатационной надежности компьютерных систем. Контроль сбоев и отказов в работе оборудования. Резервирование технических средств. Помехоустойчивое кодирование. Коды, обнаруживающие и исправляющие ошибки. Защита информации от утечки по техническим каналам. Защита информации в компьютерных системах от несанкционированного вмешательства. Многоуровневая защита корпоративных сетей.

### **Тема 3.** *Системный анализ угроз безопасности в компьютерных системах*

Компьютерные системы как объект защиты. Содержательная сущность защиты КС: источники, риски и формы атак на информацию. Структурные и функциональные компоненты КС, нуждающиеся в защите. Классификация угроз информационной безопасности. Случайные угрозы: отказы, сбои,

ошибки, аварийные ситуации, побочные влияния внешней среды. Преднамеренные угрозы, злоумышленные действия людей. Саморепродуцирующиеся вредоносные программы.

**Тема 4.** *Основные классы программных ошибок в различных средах исполнения и языках программирования и вытекающие из этого типы уязвимости*

Ошибки как основной источник уязвимости информационных систем. Классификация наиболее типичных классов ошибок для наиболее распространенных технологий создания ПО.

**Тема 5.** *Ошибки класса "Bufferoverflow" и их эксплуатация*  
Указатель стека и переполнение автоматических массивов. Запуск удаленного Shell. Сетевое исполнение атак на переполнение буфера. Червь Морриса.

**Тема 6.** *Уязвимости в интерпретируемых языках типа "инъекция"*  
PHP-инъекции. SQL-инъекции.

**Тема 7.** *Классы атак DoS и DDoS. Методы борьбы с DoS- и DDoS-атаками*  
Цена отказа в обслуживании реальных информационных систем. Способы проведения атак на отказ в обслуживании. Блокирование типичных Dos-атак на уровне операционной системы. Методы борьбы с DoS- и DDoS-атаками.

**Тема 8.** *Ошибки в программном обеспечении типа RaceCondition и эксплуатация этого класса ошибок*

Особенности ошибок в параллельных программах. Проблемы использования временных файлов для синхронизации программ. Ошибки типа RaceCondition в ядре (на примере ОС Linux).

**Тема 9.** *Криптографические методы защиты информации*  
Введение в криптологию. Исторический обзор. Криптография и криптоанализ. Криптографические модели. Понятие криптостойкости системы защиты информации. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Bruteforce и радужные таблицы.

**Тема 10.** *RAID-системы различных уровней (0,1,5,10,50)*  
Защита информации от аппаратных сбоев и отказов оборудования физических носителей. RAID-системы различных уровней (0,1,5,10,50).

**Тема 11.** *Защита на уровне оборудования и операционной системы*  
Реализация механизма системных вызовов для архитектуры IA-32 (i386). Реализация поддержки защиты памяти в современных ОС. Модели безопасности основных ОС. Системы контроля доступа ОС. Межсетевой экран. Виртуальные частные сети и их безопасность. Программное обеспечение для защиты от вредоносного программного обеспечения. Непрерывное и периодическое резервирование данных.

**Тема 12.** *Принципы работы и назначение гипервизора. Защита при помощи виртуальных машин*

Принципы работы и назначение гипервизора. Защита при помощи виртуальных машин.

**Тема 13.** *Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов.*

Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов.

## **5.1. Содержание дисциплины по видам занятий**

### **5.1.1. Лекции**

| Раздел дисциплины (тема) | Название лекции  | Кол-во часов |
|--------------------------|--|--------------|
| <b>Тема 1.</b>           | Общие вопросы информационной безопасности  | 1            |
| <b>Тема 2.</b>           | Общая характеристика средств и методов защиты информации   | 1            |
| <b>Тема 3.</b>           | Системный анализ угроз безопасности в компьютерных системах  | 1            |
| <b>Тема 4.</b>           | Основные классы программных ошибок в различных средах исполнения и языках программирования и вытекающие из этого типы уязвимости | 1            |
| <b>Тема 5.</b>           | Ошибки класса "Bufferoverflow" и их эксплуатация   | 1            |
| <b>Тема 6.</b>           | Уязвимости в интерпретируемых языках типа "инъекция"   | 2            |
| <b>Тема 7.</b>           | Классы атак DoS и DDoS. Методы борьбы с DoS- и DDoS-атаками  | 2            |
| <b>Тема 8.</b>           | Ошибки в программном обеспечении типа RaceCondition и эксплуатация этого класса ошибок   | 2            |
| <b>Тема 9.</b>           | Криптографические методы защиты информации   | 2            |
| <b>Тема 10.</b>          | RAID-системы различных уровней (0,1,5,10,50)   | 1            |

|                 |  |    |
|-----------------|--|----|
| <b>Тема 11.</b> | Защита на уровне оборудования и операционной системы                                 | 2  |
| <b>Тема 12.</b> | Принципы работы и назначение гипервизора. Защита при помощи виртуальных машин        | 2  |
| <b>Тема 13.</b> | Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов. | 2  |
| Итого           |  | 20 |

### 5.1.2. Практические занятия (семинары)

Не предусмотрено программой

### 5.1.3. Лабораторный практикум

| Раздел дисциплины (тема) | Название лабораторной работы  | Кол-во часов |
|--------------------------|---|--------------|
| <b>Тема 3.</b>           | Знакомство с практическими методами анализа угроз безопасности ИС   | 4            |
| <b>Тема 4.</b>           | Демонстрация связи "ошибка в ПО - уязвимость системы"   | 4            |
| <b>Тема 5.</b>           | Детальное изучение механизма взлома ПО через переполнение буфера C-программы  | 4            |
| <b>Тема 6.</b>           | Детальное изучение механизма взлома ПО через PHP- и SQL-инъекции  | 4            |
| <b>Тема 7.</b>           | Проведение DoS-атаки на WEB-сервер  | 4            |
| <b>Тема 8.</b>           | Изучение эксплуатаций ошибки RaceCondition  | 4            |
| <b>Тема 9.</b>           | Создание защищенного соединения и обмен зашифрованными данными с помощью симметричных и асимметричных алгоритмов шифрования | 6            |
| <b>Тема 11.</b>          | Организация защищенных каналов связи с использованием VPN-технологий; защита периметра с использованием межсетевых экранов  | 6            |
| <b>Тема 12.</b>          | Освоение технологии виртуализации оборудования  | 4            |
| Итого                    |   | 40           |

### 5.2. Самостоятельная работа студентов

| Раздел дисциплины | Вид самостоятельной | Название (содержание) работы | Кол-во часов |
|-------------------|---------------------|------------------------------|--------------|
|-------------------|---------------------|------------------------------|--------------|

| (тема)  | работы                   |  |     |
|---------|--------------------------|--|-----|
| Тема 4  | Самостоятельное изучение | Изучение последствий программных ошибок для безопасности информационной системы                        | 17  |
| Тема 3  | Самостоятельное изучение | Изучение примеров успешных атак на различные информационные системы по материалам открытых источников  | 17  |
| Тема 8  | Самостоятельное изучение | Изучение примеров проведения и методов борьбы с атаками на ошибки синхронизации параллельных процессов | 18  |
| Тема 7  | Самостоятельное изучение | Изучение примеров проведения и методов борьбы с атаками на отказ в обслуживании                        | 17  |
| Тема 11 | Самостоятельное изучение | Изучение механизмов многопользовательской защиты на уровне ОС (на примере исходных текстов ОС Linux)   | 18  |
| Тема 6  | Домашнее задание         | Детальный разбор и эксперименты с ошибками типа "инъекция"   | 17  |
| Тема 5  | Домашнее задание         | Детальный разбор и эксперименты с ошибками типа "переполнение буфера"                                  | 17  |
| Тема 9  | Самостоятельное изучение | Изучение современных криптографических алгоритмов и систем   | 18  |
| Тема 12 | Самостоятельное изучение | Освоение технологии виртуализации и ее применение для защиты информационных систем                     | 17  |
| Итого   |                          |  | 156 |

## 6. Текущий контроль успеваемости и промежуточная аттестация

### 6.1. Текущий контроль успеваемости

#### 6.1.1. Контроль самостоятельной работы студентов

- Проверка домашних заданий.
- Проверка готовности студентов к выполнению лабораторных работ.

#### 6.1.2. Текущий контроль знаний студентов

Текущий контроль знаний (ТКЗ) студентов  
(в часы лабораторного практикума)

| Раздел дисциплины<br>(тема) | Содержание ТКЗ                                   | Кол-во<br>часов |
|-----------------------------|--|-----------------|
| <b>Темы 3,4,7,8,9,11,12</b> | Оценка уровня понимания<br>пройденного материала | 14              |
| <b>Темы 5,6</b>             | Оценка уровня понимания<br>механизма атаки       | 6               |

### 6.3. Фонд оценочных средств

#### Паспорт фонда оценочных средств

| Контролируемые разделы (темы)<br>дисциплины  | Наименование оценочного средства и<br>коды контролируемых компетенций   |
|--|---|
| Тема 1. Общие вопросы<br>информационной безопасности   | Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)  |
| Тема 2. Общая характеристика<br>средств и методов защиты<br>информации   | Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)  |
| Тема 3. Системный анализ угроз<br>безопасности в компьютерных<br>системах  | Собеседование (ОК-11, ОК-4, ОК-5, ОК-8)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)         |
| Тема 4. Основные классы<br>программных ошибок в различных<br>средах исполнения и языках<br>программирования и вытекающие<br>из этого типы уязвимости | Собеседование (ОК-11, ОК-12, ОК-13, ОК-5, ОК-8)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6) |
| Тема 5. Ошибки класса<br>"Bufferoverflow" и их эксплуатация  | Творческое задание (ОК-11, ОК-12, ОК-6, ОК-8, ПК-4, ПК-5, ПК-6)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6,                     |



|  |  |
|--|--|
|  | ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)  |
| Тема 6. Уязвимости в интерпретируемых языках типа "инъекция"                                   | Доклад, сообщение (ОК-3, ОК-6, ПК-2, ПК-4, ПК-5)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)                 |
| Тема 7. Классы атак DoS и DDoS. Методы борьбы с DoS- и DDoS-атаками                            | Собеседование (ОК-13, ОК-4, ПК-1, ПК-2, ПК-6)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)                    |
| Тема 8. Ошибки в программном обеспечении типа RaceCondition и эксплуатация этого класса ошибок | Собеседование (ОК-6, ПК-2, ПК-4, ПК-5)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)                           |
| Тема 9. Криптографические методы защиты информации   | Собеседование (ОК-11, ОК-13, ОК-4, ОК-8, ПК-2, ПК-4, ПК-5, ПК-6)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6) |
| Тема 10. RAID-системы различных уровней (0,1,5,10,50)  | Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)   |
| Тема 11. Защита на уровне оборудования и операционной системы                                  | Собеседование (ОК-11, ОК-12, ОК-13, ОК-4, ПК-1, ПК-2, ПК-6)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)      |
| Тема 12. Принципы работы и назначение гипервизора. Защита при помощи виртуальных машин         | Собеседование (ОК-12, ОК-4, ПК-2, ПК-6)<br>Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)                          |
| Тема 13. Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов.  | Промежуточная аттестация (ОК-11, ОК-12, ОК-13, ОК-3, ОК-4, ОК-5, ОК-6, ОК-8, ПК-1, ПК-2, ПК-4, ПК-5, ПК-6)   |

## Оценочные средства для текущей аттестации

### Доклад, сообщение

1. Доклад на тему "Детальный разбор и эксперименты с ошибками типа "инъекция""

*Критерий оценки.* На выступление одного студента отводится 5-10 минут. Проверяющий оценивает корректность изложенной информации, полноту изложения и глубину проработки рассмотренной темы. По результатам доклада студент получает оценку от 0 до 6 баллов. Освоение компетенций зависит от полученной оценки: 5-6 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

### Собеседование

1. Собеседование на тему "Изучение примеров атак на различные информационные системы"

*Критерий оценки.* На собеседование отводится 45 минут. Студенту предлагается 6 вопросов, на основе которых он излагает подготовленный материал по поставленной теме. Изложенный материал оценивается по шкале от 0 до 6 баллов. Освоение компетенций зависит от результата собеседования: 5-6 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

2. Собеседование на тему "Изучение последствий программных ошибок для безопасности информационной системы"

*Критерий оценки.* На собеседование отводится 45 минут. Студенту предлагается 6 вопросов, на основе которых он излагает подготовленный материал по поставленной теме. Изложенный материал оценивается по шкале от 0 до 6 баллов. Освоение компетенций зависит от результата собеседования: 5-6 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

3. Собеседование на тему "Изучение примеров проведения и методов борьбы с атаками на отказ в обслуживании"

*Критерий оценки.* На собеседование отводится 45 минут. Студенту предлагается 6 вопросов, на основе которых он излагает подготовленный материал по поставленной теме. Изложенный материал оценивается по шкале от 0 до 6 баллов. Освоение

компетенций зависит от результата собеседования: 5-6 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

4. Собеседование на тему "Изучение примеров проведения и методов борьбы с атаками на ошибки синхронизации параллельных процессов"

*Критерий оценки.* На собеседование отводится 45 минут. Студенту предлагается 6 вопросов, на основе которых он излагает подготовленный материал по поставленной теме. Изложенный материал оценивается по шкале от 0 до 5 баллов. Освоение компетенций зависит от результата собеседования: 5 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

5. Собеседование на тему "Изучение современных криптографических алгоритмов и систем"

*Критерий оценки.* На собеседование отводится 45 минут. Студенту предлагается 6 вопросов, на основе которых он излагает подготовленный материал по поставленной теме. Изложенный материал оценивается по шкале от 0 до 6 баллов. Освоение компетенций зависит от результата собеседования: 5-6 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

6. Собеседование на тему "Изучение механизмов многопользовательской защиты на уровне ОС"

*Критерий оценки.* На собеседование отводится 45 минут. Студенту предлагается 6 вопросов, на основе которых он излагает подготовленный материал по поставленной теме. Изложенный материал оценивается по шкале от 0 до 5 баллов. Освоение компетенций зависит от результата собеседования: 5 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

7. Собеседование на тему "Освоение технологии виртуализации и ее применение для защиты информационных систем"

*Критерий оценки.* На собеседование отводится 45 минут. Студенту предлагается 6 вопросов, на основе которых он излагает подготовленный материал по поставленной теме. Изложенный материал оценивается по шкале от 0 до 6 баллов. Освоение

компетенций зависит от результата собеседования: 5-6 баллов - компетенции считаются освоенными на продвинутом уровне; 3-4 - компетенции считаются освоенными на базовом уровне; 0-2 - компетенции считаются не освоенными.

### **Творческое задание**

1. Творческое задание "Детальный разбор и эксперименты с ошибками типа "переполнение буфера"

*Критерий оценки.* Студент должен реализовать программный проект, дополнить его пояснительной запиской и выступить с отчетом о проделанной работе. Оценке подлежит как корректность выполненной работы, так и степень творческого подхода студента. Если работа была выполнена некорректно, студент получает 0 баллов, а компетенции считаются не освоенными. В случае наличия незначительных ошибок в проделанной работе, студент получает 1 балл. Если ошибки отсутствуют, студент получает 2 балла. При корректно выполненной работе степень творческого подхода оценивается от 0 до 2 баллов. При сумме баллов от 1 до 2 компетенции считаются освоенными на базовом уровне. При сумме от 3 до 4 баллов компетенции считаются освоенными на продвинутом уровне.

### **Оценочные средства для промежуточной аттестации**

1. Вопросы к экзамену

*Критерий оценки.* Результат оценивается по шкале от 0 до 20 баллов: - 18-20 баллов - компетенции считаются освоенными на высоком уровне (оценка "отлично"); - 15-17 баллов - компетенции считаются освоенными на продвинутом уровне (оценка "отлично"); - 11-14 баллов - компетенции считаются освоенными на базовом уровне (оценка "хорошо"); - 8-10 баллов - компетенции считаются освоенными на удовлетворительном уровне (оценка "удовлетворительно"); - 0-7 баллов - компетенции считаются не освоенными (оценка "неудовлетворительно").

## **7. Учебно-методическое обеспечение дисциплины**

### **7.1. Основная литература**

1. Сычев, Ю. Н. Основы информационной безопасности. Учебн [Электронный ресурс] : практическое пособие / Ю. Н. Сычев. - М.: Евразийский открытый институт, 2010. - 328 с.
2. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс] : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, М. В. Рудановский. - М.: Флинта, 2011. - 100 с.

3. Информационная безопасность открытых систем Т.2: Средства защиты в сетях. / Запечников С.В., Милославская Н.Г., Толстой А.И. и др - М.: Горячая линия- Телеком, 2008
4. Ярочкин В.И. Информационная безопасность :учеб. для вузов. - М.: Академический проект, 2005

## **7.2. Дополнительная литература**

1. Н.Смарт Криптография. Техносфера, 2005 - 528с.
2. Д.Скляров Искусство защиты и взлома информации. БХВ-Петербург, 2004 - 288с.
3. С.Корт Теоретические основы защиты информации. Гелиос-АРВ, 2004 - 240с.
4. Низамутдинов М. Тактика защиты и нападения на web-приложения. БХВ-Петербург, 2005 - 432с.
5. ГрегХогланд, Гари Мак-Гроу Взлом программ: анализ и примеры кода. Вильямс, 2005 - 400с.
6. И. Д. Медведевский, Б. В. Семьянов, Д. Г. Леонов, А. В. Лукацкий Атака из Internet. СОЛОН - Р, 2002 - 368с.
7. Алексей Гультьев Виртуальные машины. Несколько компьютеров в одном. Питер, 2006 - 224с.
8. Олифер В. Г., Олифер Н. А. Сетевые операционные системы: Учебник для вузов. Питер, 2006 - 544с.

## **7.3. Периодические издания**

1. Безопасность информационных технологий. МИФИ,
2. Информационная безопасность. Гротек,
3. Защита информации. Инсайд. Издательский дома "Афина",

## **7.4. Ресурсы Интернет**

1. Тексты государственных концептуально-стратегических документов, Законов РФ, РД Гостехкомиссии и ФСТЭК. (<http://fstec.ru/>)
2. Информационный портал по безопасности SecurityLab.ru. (<http://www.securitylab.ru/>)

## **7.5. Программное обеспечение**

1. Компилятор языка C#
2. Интерпретатор языка PHP
3. Вычислители хэш-функций md5sum, sha1sum
4. Защищенные средства удаленного доступа ssh
5. WEB-сервер
6. VPN-сервер и клиент

## 7. Эмуляторы программного обеспечения различных платформ

### 7.6. Материально-техническая база

Лабораторные работы по дисциплине «Защита информации» проводятся в лабораториях web-технологий и прикладного программирования, оснащённых персональными ЭВМ, объединёнными в локальную вычислительную сеть вуза, необходимым системным и прикладным программным обеспечением.

Материально-техническое обеспечение лаборатории прикладного программирования, необходимое для выполнения лабораторных работ по дисциплине «Защита информации»:

- компьютерный класс № 1310 (лаборатория прикладного программирования): 15 ПЭВМ, объединённые в локальную вычислительную сеть на базе выделенного сервера приложений и web-сервера, аппаратное обеспечение ПЭВМ: процессор IntelOriginal LGA-1155 Pentium G840, ОП - 2048Mb DDR3, жёсткий диск – 500 Gb SATA-III Hitachi, программное обеспечение ПЭВМ: операционная система MSWindows 7, инструментальная среда NetBeans, пакет прикладных программ MSOffice, VisualStudio.net и другое программное обеспечение, указанное выше,

- компьютерный класс № 1312 (лаборатория web-технологий): 15 ПЭВМ, объединённые в локальную вычислительную сеть на базе выделенного сервера приложений и web-сервера, аппаратное обеспечение ПЭВМ: процессор - IntelPentiumSandyBridge G860, ОП - DIMM DDR 2Gb, жёсткий диск – 250 GbSeagate, программное обеспечение ПЭВМ: операционная система MSWindows 7, инструментальная среда NetBeans, пакет прикладных программ MSOffice, VisualStudio.net и другое программное обеспечение, указанное выше.

В компьютерных классах имеются мультимедийные средства: проекторы, экраны, ноутбуки.

## 8. Организация образовательного процесса для лиц с ограниченными возможностями

Организация образовательного процесса для лиц с ограниченными возможностями осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащённости образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн.

В образовательном процессе используются социально-активные и

рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.

Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

## **9. Список экзаменационных вопросов по дисциплине**

1. Анализ систем опознавания.
2. Безопасность в распределенных системах.
3. Управление доступом к системам.
4. Компьютерные вирусы и антивирусы.
5. Информационный терроризм.
6. Информационная безопасность как понятие.
7. Ошибки в программном и аппаратном обеспечении как основной источник уязвимостей информационных систем.
8. В каких современных областях информатики наиболее востребованы сведения, рассматриваемые в курсе "информационная безопасность"?
9. Приведите примеры технологий, которые берут сегодня на вооружение при реализации защищенных компьютерных систем.
10. Типичные уязвимости ПО, реализованного на языке "С".
11. Типичные уязвимости ПО, реализованного на языках PHP/Perl/SQL.
12. Типичные классы уязвимостей в коде ОС (на примере ОС Linux).
13. Анализ безопасности программного обеспечения путем исследования машинного кода. Утилита objdump.
14. Структура ассемблерного кода, полученного компиляцией типичной программы на языке "С". Указатель стека и указатель инструкций. Принципы использования уязвимостей типа BufferOverflow.
15. Уязвимости в интерпретируемых языках типа "инъекция".
16. PHP-инъекции.
17. SQL-инъекции.
18. Классы атак DoS и DDoS.
19. Методы борьбы с DoS- и DDoS-атаками
20. Что такое RaceCondition?

21. Почему в параллельных программах появляется новый тип уязвимости по сравнению с последовательными программами?
22. Назначение и основные классы алгоритмов шифрования данных. Криптография и криптоанализ.
23. Радужные таблицы.
24. Защита информации от аппаратных сбоев и отказов оборудования физических носителей.
25. RAID-системы различных уровней (0,1,5,10,50).
26. Реализация механизма системных вызовов для архитектуры IA-32 (i386).
27. Защита данных операционной системы от прикладных программ.
28. Принципы работы и назначение гипервизора. Что дает гипервизор в плане повышения защищенности компьютерных систем?
29. Аппаратная поддержка режима гипервизора в новейших процессорах фирмы Intel.
30. Методы современной криптографии. Стандарты AES и ГОСТ, структура базовых алгоритмов.
31. Классификация угроз информационной безопасности.
32. Встроенные средства защиты операционной системы семейства Linux.
33. Различия между многоуровневой и дискретной системой управления доступом и их совместное использование. Управление доступом на основе ролей.
34. Ограничение и изоляция компьютерных ресурсов на примере механизмов Cgroups и ulimits ядра Linux.
35. Инструменты резервного копирования данных. Типы резервирования. Применение планировщика задач для задачи резервирования данных.
36. Менеджер логических томов LVM операционных систем семейства Linux и резервирование данных в реальном времени с помощью механизма "снимков".
37. Уровни протокола SSH и их назначение.
38. Механизмы аутентификации и шифрования, реализованные в протоколе SSH.
39. Туннелирование сетевых соединений. Примеры механизмов туннелирования. Туннелирование посредством протокола SSH.
40. Организация виртуальных частных сетей и их безопасность. Методы построения ВЧС, их сходства, различия, недостатки.
41. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
42. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.



43. Достоинства и недостатки различных методов виртуализации с точки зрения обеспечения информационной безопасности компьютерных систем.
44. Назначение и методы построения "песочниц". Недостатки простых механизмов chroot и sandbox и их устранение.
45. Методы шифрования файловой системы. Безопасность данных в случае физического доступа к компьютерной системе.
46. Атаки на протоколы и службы Интернет. Методы и средства защиты.
47. Электронные сертификаты. Понятие инфраструктуры открытых ключей.
48. Преимущества технологии терминального доступа. Сетевые файловые системы. Обеспечение безопасности.
49. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.
50. Система единого входа в сеть на основе протокола Kerberos.
51. Каскадно-объединенное монтирование файловых систем. Файловая система UnionFS. Файловые системы с полным доступом поверх файловых систем с доступом на чтение.
52. Анализ системного журнала на предмет обнаружения несанкционированной активности.

#### **Лист регистрации изменений**

| №<br>п/п | Содержание изменения  | Реквизиты<br>документа<br>об утверждении<br>изменения    | Дата<br>введения<br>изменения |
|----------|---|--|-------------------------------|
| 1.       | Утверждена и введена в действие решением кафедры «Математика, физика и информационные технологии» на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 15.03.04 «Автоматизация технологических процессов и производств», профиль подготовки «Автоматизация технологических процессов и производств» (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 12.03.2015 г № 200 | Протокол заседания кафедры № 1 от «29» августа 2017 года |                               |