**Министерство науки и высшего образования РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Национальный исследовательский университет «МЭИ»**

---

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность компьютерных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

# Рабочая программа дисциплины
# ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

| | |
|---|---|
| **Блок:** | **Блок 1 «Дисциплины (модули)»** |
| **Часть образовательной программы:** | **Базовая** |
| **№ дисциплины по учебному плану:** | **Б1.Б.28** |
| **Трудоемкость в зачетных единицах:** | **6 семестр - 4;<br>7 семестр - 5;<br>всего - 9** |
| **Часов (всего) по учебному плану:** | **324 часа** |
| **Лекции** | **6 семестр - 28 часа;<br>7 семестр - 32 часа;<br>всего - 60 часов** |
| **Практические занятия** | **6 семестр - 28 часа;<br>7 семестр - 32 часа;<br>всего - 60 часов** |
| **Лабораторные работы** | **6 семестр - 14 часов;<br>7 семестр - 16 часов;<br>всего - 30 часов** |
| **Консультации** | **7 семестр - 18 часов;** |
| **Самостоятельная работа** | **6 семестр - 73,7 часа;<br>7 семестр - 77,2 часа;<br>всего - 150,9 часа** |
| **в том числе на КП/КР** | **7 семестр - 15,7 часов;** |
| **Иная контактная работа** | **7 семестр - 4 часа;** |
| **включая:<br>Контрольная работа<br>Реферат** | |
| **Промежуточная аттестация:** | |
| **Зачет с оценкой<br>Защита курсовой работы<br>Экзамен** | **6 семестр - 0,3 часа;<br>7 семестр - 0,3 часа;<br>7 семестр - 0,5 часа;<br>всего - 1,1 часа** |

**Москва 2020**

**ПРОГРАММУ СОСТАВИЛ:**

| | | |
|---|---|---|
| Преподаватель | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Поляк Р.И.<br>Идентификатор: Rbc0e923e-PoliakRI-10208dd2 | Р.И. Поляк |

**СОГЛАСОВАНО:**

| | | |
|---|---|---|
| Руководитель образовательной программы | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Баронов О.Р.<br>Идентификатор: R90d76356-BaronovOR-7bf8fd7e | О.Р. Баронов |
| Заведующий выпускающей кафедрой | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** освоение профессиональных компетенций по формированию готовности студентов разрабатывать системы защиты информации на основе применения методов и средств программно-аппаратной защиты информации

**Задачи дисциплины**

- сформировать у студентов системные теоретические знания и практические навыки по организации и технологии программно-аппаратной защиты информации.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

| **Код и наименование компетенции** | **Код и наименование индикатора достижения компетенции** | **Запланированные результаты обучения** |
|---|---|---|
| ОПК-3 способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач | | знать:<br>- основные руководящие правовые, методические, и нормативные документы по программно-аппаратной защите информации.<br><br>уметь:<br>- выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности. |
| ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | | знать:<br>- основные теоретические сведения: сущность, цели, задачи и принципы программно-аппаратной защиты информации.<br><br>уметь:<br>- производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе. |
| ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | | знать:<br>- основные руководящие правовые, методические, и нормативные требования по оценке защищенности средств программно-аппаратной защиты информации.<br><br>уметь:<br>- организовывать процесс аттестации объектов информатизации по требования безопасности информации и разрабатывать документальное |

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Запланированные результаты обучения |
|---|---|---|
| | | обеспечение. |
| ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | | знать:<br>- перечень, классификацию, принцип действия программно-аппаратных средств защиты информации.<br><br>уметь:<br>- выполнять действия по установке, конфигурированию и настройке программно-аппаратных средств защиты информации. |
| ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений | | знать:<br>- методы оценки эффективности мер программно-аппаратной защиты информации.<br><br>уметь:<br>- определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе. |
| ПСК-2 Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасносго функционирования объектов энергетики с элементами АСУ ТП | | знать:<br>- программно-аппаратные средства обеспечения защиты информации автоматизированных систем.<br><br>уметь:<br>- применять программные средства системного, прикладного и специального назначения для обеспечения безопасного функционирования объектов промышленности с элементами АСУ ТП. |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к обязательной части блока дисциплин основной профессиональной образовательной программе Безопасность компьютерных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 9 зачетных единиц, 324 часа.

| № п/п | Разделы/темы дисциплины/формы промежуточной аттестации | Всего часов на раздел | Семестр | Распределение трудоемкости раздела (в часах) по видам учебной работы | | | | | | | | | | Содержание самостоятельной работы/ методические указания |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Контактная работа | | | | | | | | СР | | |
| | | | | Лек | Лаб | Пр | Консультация | | ИКР | | ПА | Работа в семестре | Подготовка к аттестации /контроль | |
| | | | | | | | КПР | ГК | ИККП | ТК | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | Раздел 1. Введение | 22 | 6 | 4 | 2 | 4 | - | - | - | - | - | 12 | - | ***Подготовка курсовой работы:*** |
| 1.1 | Тема 1. Концептуальные основы информационной безопасности | 11 | | 2 | 1 | 2 | - | - | - | - | - | 6 | - | ***Подготовка к текущему контролю:*** Повторение материала по разделу "Раздел 1. Введение" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 1. Введение" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 1. Введение" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным |
| 1.2 | Тема 2. Основные понятия программно-аппаратной защиты информации | 11 | | 2 | 1 | 2 | - | - | - | - | - | 6 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты:<br>***Подготовка к контрольной работе:***<br>Изучение материалов по разделу Раздел 1. Введение и подготовка к контрольной работе<br>***Подготовка к практическим занятиям:***<br>Изучение материала по разделу "Раздел 1. Введение" подготовка к выполнению заданий на практических занятиях<br>***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Раздел 1. Введение"<br>***Подготовка реферата:*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты:<br>***Изучение материалов литературных источников:***<br>[1], 1-352<br>[4], 1-48 |
| 2 | Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений | 59 | | 14 | 7 | 14 | - | - | - | - | - | 24 | - | ***Подготовка курсовой работы:***<br>***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений" |
| 2.1 | Тема 3. Механизмы | 11 | | 2 | 1 | 2 | - | - | - | - | - | 6 | - | ***Подготовка к текущему контролю:*** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | обеспечения конфиденциальности доступа к информации на уровне операционных систем | | | | | | | | | | | | | Повторение материала по разделу "Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Раздел 2. Обеспечение конфиденциальности доступа к |
| 2.2 | Тема 4. Механизмы обеспечения конфиденциальности доступа к информации на уровне приложений | 16 | | 4 | 2 | 4 | - | - | - | - | - | 6 | - | |
| 2.3 | Тема 5. Программно-аппаратные средства криптографической защиты информации | 16 | | 4 | 2 | 4 | - | - | - | - | - | 6 | - | |
| 2.4 | Тема 6. Обеспечение конфиденциальности информации в IP-сетях | 16 | | 4 | 2 | 4 | - | - | - | - | - | 6 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | информации средствами операционных систем и пользовательских приложений" подготовка к выполнению заданий на практических занятиях<br>***<u>Подготовка реферата:</u>*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты:<br>***<u>Изучение материалов литературных источников:</u>***<br>[1], 1-352<br>[4], 76-154<br>[5], 38-91 |
| 3 | Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты | 45 | | 10 | 5 | 10 | - | - | - | - | - | 20 | - | ***<u>Подготовка курсовой работы:</u>***<br>***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты"<br>***<u>Подготовка реферата:</u>*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты:<br>***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты" подготовка к |
| 3.1 | Тема 7. Обеспечение доступности информации средствами операционной системы | 11 | | 2 | 1 | 2 | - | - | - | - | - | 6 | - | |
| 3.2 | Тема 8. Обработка информации на рабочих станциях и обеспечение ее доступности | 16 | | 4 | 2 | 4 | - | - | - | - | - | 6 | - | |
| 3.3 | Тема 9. Обеспечение доступности информации в локальных сетях | 18 | | 4 | 2 | 4 | - | - | - | - | - | 8 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | выполнению заданий на практических занятиях<br>***Подготовка к контрольной работе:*** Изучение материалов по разделу Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты и подготовка к контрольной работе<br>***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.<br>***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы<br>***Подготовка к текущему контролю:*** Повторение материала по разделу "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты"<br>***Подготовка расчетно-графического задания:*** В рамках расчетно-графического задания выполняется чертеж конструкции. Для выполнения чертежей выполняются предварительные расчеты основных показателей, которые указываются на чертеже. Задание выполняется индивидуально по вариантам. В качестве тем задания применяются следующие:<br>***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты" материалу. ***Изучение материалов литературных источников:*** [1], 1-352 |
| | Зачет с оценкой | 18.0 | | - | - | - | - | - | - | - | 0.3 | - | 17.7 | |
| | **Всего за семестр** | **144.0** | | **28** | **14** | **28** | - | - | - | - | **0.3** | **56** | **17.7** | |
| | **Итого за семестр** | **144.0** | | **28** | **14** | **28** | - | | - | | **0.3** | **73.7** | | |
| 4 | Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты | 78 | 7 | 24 | 10 | 24 | - | - | - | - | - | 20 | - | ***Подготовка курсовой работы:*** ***Подготовка к текущему контролю:*** Повторение материала по разделу "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты" материалу. |
| 4.1 | Тема 10. Механизмы контроля целостности данных | 18 | | 6 | 2 | 6 | - | - | - | - | - | 4 | - | |
| 4.2 | Тема 11. Обеспечение целостности информации средствами операционной системы | 18 | | 6 | 2 | 6 | - | - | - | - | - | 4 | - | |
| 4.3 | Тема 12. Обеспечение целостности информации с помощью программных и аппаратных средств | 20 | | 6 | 2 | 6 | - | - | - | - | - | 6 | - | |
| 4.4 | Тема 13. Обеспечение целостности при передаче информации по сетям | 22 | | 6 | 4 | 6 | - | - | - | - | - | 6 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты" ***Подготовка реферата:*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: ***Изучение материалов литературных источников:*** [3], 1-352 |
| 5 | Раздел 5. Комплексные системы защиты информации | 30 | | 8 | 6 | 8 | - | - | - | - | - | 8 | - | ***Подготовка курсовой работы:*** ***Подготовка к текущему контролю:*** Повторение материала по разделу "Раздел 5. |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5.1 | Тема 14. Обеспечение антивирусной защиты информационных систем | 30 | | 8 | 6 | 8 | - | - | - | - | - | 8 | - | Комплексные системы защиты информации" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 5. Комплексные системы защиты информации" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 5. Комплексные системы защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Раздел 5. Комплексные системы защиты информации и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Раздел 5. Комплексные системы защиты информации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Раздел 5. Комплексные системы защиты информации" ***Подготовка реферата:*** В рамках реферативной части студенту необходим |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: ***Изучение материалов литературных источников:*** [2], 1-352 |
| | Экзамен | 36.0 | | - | - | - | - | 2 | - | - | 0.5 | - | 33.5 | |
| | Курсовая работа (КР) | 36.0 | | - | - | - | 16 | - | 4 | - | 0.3 | 15.7 | - | |
| | **Всего за семестр** | **180.0** | | **32** | **16** | **32** | **16** | **2** | **4** | **-** | **0.8** | **43.7** | **33.5** | |
| | **Итого за семестр** | **180.0** | | **32** | **16** | **32** | **18** | | **4** | | **0.8** | **77.2** | | |
| | **ИТОГО** | **324.0** | **-** | **60** | **30** | **60** | **18** | | **4** | | **1.1** | **150.9** | | |

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

**3.2 Краткое содержание разделов**

*1. Раздел 1. Введение*

1.1. Тема 1. Концептуальные основы информационной безопасности

Основные понятия и определения в сфере информационной безопасности. Угрозы информации. Анализ методов и средств защиты информации..

1.2. Тема 2. Основные понятия программно-аппаратной защиты информации

Предмет и задачи программно-аппаратной защиты информации. Основные критерии оценки безопасности систем. Система организационных и руководящих документов РФ в области программно-аппаратной защиты информации..

*2. Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений*

2.1. Тема 3. Механизмы обеспечения конфиденциальности доступа к информации на уровне операционных систем

Понятия аутентификации и авторизации. Общие принципы. Задачи протокола аутентификации. Локальная и доменная регистрация. Протоколы аутентификации Windows. Автоматическая генерация и назначение сложных паролей в MS Windows. Исследование уязвимостей доступа к операционным системам MS Windows. Возможность и порядок загрузки операционной системы с внешних носителей. Работа с уда-ленным реестром. Организация хранения паролей в операционных системах ОС MS Windows. База данных учетных записей пользователей. Хранение паролей пользователей. Использование пароля. База данных SAM и возможные атаки на нее. Прозрачное шифрование. Шифрующая файловая система (EFS). Технология шифрования. Взаимодействие с пользователем. Восстановление данных. Агент восстановления данных..

2.2. Тема 4. Механизмы обеспечения конфиденциальности доступа к информации на уровне приложений

Обеспечение конфиденциальности электронных документов с использованием возможностей приложений MS Office. Защита документов MS Word и MS Excel. Защита VBA-макросов. Применение паролей MS Access и MS Outlook. Анализ уязвимостей системы за-щиты документов в приложениях MS Office. Программно-аппаратные средства контроля доступа: iButton, Proximity. Устройства ввода на базе смарт-карт. Устройства ввода на базе USB-ключей. Комбинированные устройства ввода. Основы биометрического доступа к ресурсам. Обзор биометрических технологий. Распознавание по: отпечаткам пальцев, форме руки, радужной оболочке глаза, форме лица, рукописному почерку, клавиатурному почерку, голосу. Идентификация по отпечаткам пальцев. Сканирование отпечатков пальцев. Методы распознавания. Подходы к защите от биометрических муляжей. Взаимодействие операционной системы и программного обеспечения для биометрической идентификации на при-мере продуктов компании Biolink Solutions. Программное обеспечение BioLink Authentication Center: назначение, принципы работы, компоненты..

2.3. Тема 5. Программно-аппаратные средства криптографической защиты информации

Полностью контролируемые компьютерные системы. Программная реализация функций криптографической защиты информации. Аппаратная реализация функций криптографической защиты информации. Устройства криптографической защиты данных: программно-аппаратный комплекс «Аккорд», персональное средство криптографической защиты информации (ПСКЗИ) ШИПКА..

2.4. Тема 6. Обеспечение конфиденциальности информации в IP-сетях

Основы построения IP-сетей и обеспечения безопасности информации в них. Особенности протокола TCP/IP. Виртуальные частные сети (VPN). Протоколы PPTP и L2TP. Анализ возможных уязвимостей протокола PPTP в реализации Micrsoft. Протоколы SSL и TLS. Протоколы IPSEC и распределение ключей. Протоколы IPSec и трансляция сетевых адресов. Обзор программно-аппаратного комплекса ViPNet CUSTOM..

## *3. Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты*

3.1. Тема 7. Обеспечение доступности информации средствами операционной системы

Управление правами доступа к ресурсам в операционных системах семейства MS Windows. Учетные записи пользователей и групп. Управление доступом и глобальными параметрами. Основные сведения об учетных записях групп. Оснастка "Локальные пользователи и группы". Настройка политик управления правами пользователей. Управление Windows при помощи консоли Computer Management Console. Практическое использование оснасток Консоли управление компьютером: «Локальные пользователи и группы», «Общие папки», «Редактор локальной групповой политики»..

3.2. Тема 8. Обработка информации на рабочих станциях и обеспечение ее доступности

Блокирование рабочей станции на аппаратном уровне. Аппаратные средства доверенной загрузки. Основные концепции и реализация аутентификации. Этапы доверенной загрузки. Использование аппаратных средств. Примеры существующих аппаратных средств. Аппаратный модуль доверенной загрузки "Аккорд-АМДЗ". Модуль доверенной загрузки «Криптон-замок/PCI». Программное обеспечение для ограничения доступа к внешним устройствам на примере DeviceLock. Управление электропитанием рабочих станций и серверов. Средства активной защиты информации от утечки по сети электропитания..

3.3. Тема 9. Обеспечение доступности информации в локальных сетях

Межсетевые экраны и их классификация. Определение типов межсетевых экранов. Межсетевые экраны прикладного уровня. Межсетевые экраны с пакетной фильтрацией. Гибридные межсетевые экраны. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана с использованием возможностей брандмауэра Windows..

## *4. Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты*

4.1. Тема 10. Механизмы контроля целостности данных

Метод контрольных сумм. Метод «циклического контрольного кода». Однонаправленные функции хэширования..

4.2. Тема 11. Обеспечение целостности информации средствами операционной системы

Обеспечение безопасности хранения данных в операционных системах семейства MS Windows. Технология теневого копирования данных. Ограничения теневого копирования томов. Установка и использование технологии теневого копирования томов. Служба фонового копирования тома Microsoft Volume Shadow Copy Service (VSS). Архивация данных. Работа с программой архивирования Backup. Стратегии архивации. Восстановление данных..

4.3. Тема 12. Обеспечение целостности информации с помощью программных и аппаратных средств

Терминология резервирования. Оперативное и автономное резервирование. Типы резервирования. Виды RAID-массивов. Исходные типы RAID-массивов. RAID-контроллеры. Основы резервирования данных. Варианты резервирования данных. Программные и программно-аппаратные средства резервного копирования информации. Резервное копирование папок/файлов и дисков/разделов. Программы для резервирования данных: Acronis True Image, Norton Ghost, Paragon Exact Image, Backup to DVD/CD, AP-BackUp..

4.4. Тема 13. Обеспечение целостности при передаче информации по сетям

Защищенные протоколы. Протокол HTTPS. Безопасность при использовании техно-логии передачи данных Wi-Fi. Возможности прослушивания трафика администратором Wi-Fi. WPA/WEP. Анализ уязвимостей Wi-Fi сетей и прослушивание трафика сети. WPA2..

*5. Раздел 5. Комплексные системы защиты информации*

5.1. Тема 14. Обеспечение антивирусной защиты информационных систем

Обеспечение антивирусной защиты сетевой инфраструктуры на основе приложений компании «Лаборатория Касперского». Kaspersky® Administration Kit .Развертывание антивирусной защиты в сети предприятия..

**3.3. Темы практических занятий**

1. 1. Технология защиты документов в приложениях MS Office.;
2. 3. Механизмы контроля целостности данных.;
3. 10. Проактивные технологии антивирусной защиты.;
4. 9. Работа с программным обеспечением для резервного копирования Acronis® Backup & Recovery™ 10 Workstation;
5. 8. Построение и анализ отказоустойчивости RAID-массивов различных типов.;
6. 7. Практическое использование программы архивирования данных Backup.;
7. 2. Возможности операционных систем MS Windows по ограничению прав пользователей.;
8. 5. Изучение возможностей и настройка аппаратного межсетевого экрана.;
9. 4. Реализация аппаратного блокирования рабочей станции с использованием аппаратного модуля доверенной загрузки "Аккорд-АМДЗ".;
10. 6. Изучение возможностей и настройка программного межсетевого экрана..

**3.4. Темы лабораторных работ**

1. 5.Механизмы контроля доступа специализированных средств защиты информации от НСД сетевых средств и ПЭВМ.;
2. 4.Использование программно-аппаратного комплекса «Аккорд».;
3. 3.Изучение программно-аппаратного комплекса биометрической аутентификации (BioLink Authentication Center/ Biolink U-Match).;
4. 2.Организация логического входа в операционные системы MS Windows с помощью аппаратных ключей.;
5. 1.Анализ уязвимостей доступа к операционным системам MS Windows..

**3.5 Консультации**

*Аудиторные консультации по курсовому проекту/работе (КПР)*

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты"
2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты"
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Раздел 5. Комплексные системы защиты информации"

*Групповые консультации по разделам дисциплины (ГК)*

1. Обсуждение материалов по кейсам раздела "Раздел 1. Введение"
2. Обсуждение материалов по кейсам раздела "Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений"
3. Обсуждение материалов по кейсам раздела "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты"
4. Обсуждение материалов по кейсам раздела "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты"
5. Обсуждение материалов по кейсам раздела "Раздел 5. Комплексные системы защиты информации"

*Индивидуальные консультации по курсовому проету /работе (ИККП)*

1. Консультации проводятся по разделу "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты"
2. Консультации проводятся по разделу "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты"
3. Консультации проводятся по разделу "Раздел 5. Комплексные системы защиты информации"

*Текущий контроль (ТК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 1. Введение"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты"
5. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 5. Комплексные системы защиты информации"

**3.6 Тематика курсовых проектов/курсовых работ**

**7 Семестр**

Курсовая работа (КР)
Темы:
- АМДЗ «Аккорд».
- Программный продукт SecretNet
- Программный продукт DeviceLock
- Средство биометрической аутентификации BioLink

**График выполнения курсового проекта**

| Неделя | 1 - 6 | 7 - 10 | 11 - 14 | Зачетная |
|---|---|---|---|---|
| Раздел курсового проекта | 1, 2, 3, 4 | 1, 2, 3, 4 | 1, 2, 3, 4 | Защита курсового проекта |
| Объем раздела, % | 40 | 40 | 20 | - |
| Выполненный объем нарастающим итогом, % | 40 | 80 | 100 | - |

| Номер раздела | Раздел курсового проекта |
|---|---|
| 1 | Раздел 1. Описание объекта анализа |
| 2 | Раздел 2. Описание достоинств и недостатков объекта анализа |
| 3 | Раздел 3. Разработка проекта программно-аппаратной защиты ЛВС |
| 4 | Раздел 4. Заключение |

**3.7. Соответствие разделов дисциплины и формируемых в них компетенций**

| Запланированные результаты обучения по дисциплине (в соответствии с разделом 1) | Коды индикаторов | Номер раздела дисциплины (в соответствии с п.3.1) | | | | | Оценочное средство (тип и наименование) |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| **Знать:** | | | | | | | |
| основные руководящие правовые, методические, и нормативные документы по программно-аппаратной защите информации | ОПК-3(Компетенция) | + | + | | | | Контрольная работа/Контрольная работа №1. «Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений» |
| основные теоретические сведения: сущность, цели, задачи и принципы программно-аппаратной защиты информации | ПК-1(Компетенция) | | | + | | | Реферат/Защита лабораторной работы №1; Защита лабораторной работы №2; Защита лабораторной работы №3; Защита реферата<br>Контрольная работа/Контрольная работа №2. «Обеспечение доступности информации применением средств программно-аппаратной защиты» |
| основные руководящие правовые, методические, и нормативные требования по оценке защищенности средств программно-аппаратной защиты информации | ПК-5(Компетенция) | | | + | | | Контрольная работа/Контрольная работа №3. «Обеспечение доступности информации применением средств программно-аппаратной защиты» |
| перечень, классификацию, принцип действия программно-аппаратных средств защиты информации | ПК-6(Компетенция) | | | | + | | Контрольная работа/Контрольная работа №4. «Обеспечение целостности доступа к информации средствами операционных систем и пользовательских приложений»<br>Контрольная работа/Контрольная работа №5. «Обеспечение целостности доступа к информации средствами операционных систем и пользовательских приложений» |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| методы оценки эффективности мер программно-аппаратной защиты информации | ПК-7(Компетенция) | | | | | + | Контрольная работа/Защита лабораторных работ №4; Защита лабораторных работ №5; Контрольная работа №7. «Комплексные решения программно-аппаратной защиты»<br>Контрольная работа/Контрольная работа №6. «Комплексные решения программно-аппаратной защиты» |
| программно-аппаратные средства обеспечения защиты информации автоматизированных систем | ПСК-2(Компетенция) | | + | | | | Контрольная работа/Контрольная работа №1. «Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений» |
| **Уметь:** | | | | | | | |
| выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности | ОПК-3(Компетенция) | | | + | | | Реферат/Защита лабораторной работы №1; Защита лабораторной работы №2; Защита лабораторной работы №3; Защита реферата<br>Контрольная работа/Контрольная работа №2. «Обеспечение доступности информации применением средств программно-аппаратной защиты» |
| производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе | ПК-1(Компетенция) | + | + | | | | Контрольная работа/Контрольная работа №1. «Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений» |
| организовывать процесс аттестации объектов информатизации по требования безопасности информации и разрабатывать документальное обеспечение | ПК-5(Компетенция) | | | | | + | Контрольная работа/Контрольная работа №5. «Обеспечение целостности доступа к информации средствами операционных систем и пользовательских приложений» |
| выполнять действия по установке, | ПК-6(Компетенция) | | | + | | | Контрольная работа/Контрольная работа |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| конфигурированию и настройке программно-аппаратных средств защиты информации | | | | | | | №3. «Обеспечение доступности информации применением средств программно-аппаратной защиты» |
| определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе | ПК-7(Компетенция) | | + | | | | Контрольная работа/Контрольная работа №1. «Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений» |
| применять программные средства системного, прикладного и специального назначения для обеспечения безопасного функционирования объектов промышленности с элементами АСУ ТП | ПСК-2(Компетенция) | | | | | + | Контрольная работа/Защита лабораторных работ №4; Защита лабораторных работ №5; Контрольная работа №7. «Комплексные решения программно-аппаратной защиты»<br>Контрольная работа/Контрольная работа №6. «Комплексные решения программно-аппаратной защиты» |

## 4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

### 4.1. Текущий контроль успеваемости

**6 семестр**

Форма реализации: Письменная работа

1. Контрольная работа №1. «Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений» (Контрольная работа)
2. Контрольная работа №2. «Обеспечение доступности информации применением средств программно-аппаратной защиты» (Контрольная работа)
3. Контрольная работа №3. «Обеспечение доступности информации применением средств программно-аппаратной защиты» (Контрольная работа)

Форма реализации: Проверка задания

1. Защита лабораторной работы №1; Защита лабораторной работы №2; Защита лабораторной работы №3; Защита реферата (Реферат)

**7 семестр**

Форма реализации: Письменная работа

1. Защита лабораторных работ №4; Защита лабораторных работ №5; Контрольная работа №7. «Комплексные решения программно-аппаратной защиты» (Контрольная работа)
2. Контрольная работа №4. «Обеспечение целостности доступа к информации средствами операционных систем и пользовательских приложений» (Контрольная работа)
3. Контрольная работа №5. «Обеспечение целостности доступа к информации средствами операционных систем и пользовательских приложений» (Контрольная работа)
4. Контрольная работа №6. «Комплексные решения программно-аппаратной защиты» (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

### 4.2 Промежуточная аттестация по дисциплине

*Зачет с оценкой (Семестр №6)*

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетной составляющих.

*Экзамен (Семестр №7)*

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.

*Курсовая работа (КР) (Семестр №7)*

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.

В диплом выставляется оценка за 7 семестр.

**Примечание:** Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1 Печатные и электронные издания:

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев . – М. : Форум, 2011 . – 352 с. – (Высшее образование) . - ISBN 978-5-91134-353-8 .;
2. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев . – М. : Форум, 2013 . – 352 с. – (Высшее образование) . - ISBN 978-5-91134-353-8 .;
3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев . – М. : Форум, 2012 . – 352 с. – (Высшее образование) . - ISBN 978-5-91134-353-8 .;
4. Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В.- "Программно-аппаратные средства обеспечения информационной безопасности", Издательство: "Горячая линия-Телеком", Москва, 2018 - (248 с.)
https://e.lanbook.com/book/111053;
5. Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков- "Программно-аппаратные средства защиты информационных систем", Издательство: "Тамбовский государственный технический университет (ТГТУ)", Тамбов, 2017 - (194 с.)
https://biblioclub.ru/index.php?page=book&id=499013.

### 5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции;
5. Windows Server / Серверная операционная система семейства Linux.

### 5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
9. **Портал открытых данных Российской Федерации** - https://data.gov.ru
10. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
11. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/

12. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
13. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
14. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
15. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
16. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
17. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
18. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

| Тип помещения | Номер аудитории, наименование | Оснащение |
|---|---|---|
| Учебные аудитории для проведения лекционных занятий и текущего контроля | Н-204, Учебная аудитория | парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран |
| | К-601, Учебная аудитория | парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран |
| Учебные аудитории для проведения практических занятий, КР и КП | М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации" | парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер |
| Учебные аудитории для проведения лабораторных занятий | М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации" | парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер |
| Учебные аудитории для проведения промежуточной аттестации | М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации" | парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер |
| | Ж-120, Машинный зал ИВЦ | сервер, кондиционер |
| Помещения для самостоятельной работы | НТБ-303, Компьютерный читальный зал | стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер |
| | К-307, Учебная лаборатория "Открытое программное обеспечение" | стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер |

| | | |
|---|---|---|
| | К-302, Учебная лаборатория "Информационно-аналитические технологии" | стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер |
| Помещения для консультирования | М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации" | парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер |
| Помещения для хранения оборудования и учебного инвентаря | К-202/2, Склад кафедры БИТ | стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования |

**Приложение А**

# БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

(название дисциплины)

**6 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-1 Контрольная работа №1. «Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений» (Контрольная работа)

КМ-2 Контрольная работа №2. «Обеспечение доступности информации применением средств программно-аппаратной защиты» (Контрольная работа)

КМ-3 Контрольная работа №3. «Обеспечение доступности информации применением средств программно-аппаратной защиты» (Контрольная работа)

КМ-4 Защита лабораторной работы №1; Защита лабораторной работы №2; Защита лабораторной работы №3; Защита реферата (Реферат)

**Вид промежуточной аттестации –** Зачет с оценкой.

| Номер раздела | Раздел дисциплины | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
|---|---|---|---|---|---|---|
| | | Неделя КМ: | 4 | 8 | 12 | 15 |
| 1 | Раздел 1. Введение | | | | | |
| 1.1 | Тема 1. Концептуальные основы информационной безопасности | | + | | | |
| 1.2 | Тема 2. Основные понятия программно-аппаратной защиты информации | | + | | | |
| 2 | Раздел 2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений | | | | | |
| 2.1 | Тема 3. Механизмы обеспечения конфиденциальности доступа к информации на уровне операционных систем | | + | | | |
| 2.2 | Тема 4. Механизмы обеспечения конфиденциальности доступа к информации на уровне приложений | | + | | | |
| 2.3 | Тема 5. Программно-аппаратные средства криптографической защиты информации | | + | | | |
| 2.4 | Тема 6. Обеспечение конфиденциальности информации в IP-сетях | | + | | | |
| 3 | Раздел 3. Обеспечение доступности информации применением средств программно-аппаратной защиты | | | | | |
| 3.1 | Тема 7. Обеспечение доступности информации средствами операционной системы | | | + | + | + |
| 3.2 | Тема 8. Обработка информации на рабочих станциях и обеспечение ее доступности | | | + | + | + |
| 3.3 | Тема 9. Обеспечение доступности информации в локальных сетях | | | + | + | + |
| | | Вес КМ, %: | 25 | 25 | 25 | 25 |

**7 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-5 Контрольная работа №4. «Обеспечение целостности доступа к информации средствами операционных систем и пользовательских приложений» (Контрольная работа)

КМ-6 Контрольная работа №5. «Обеспечение целостности доступа к информации средствами операционных систем и пользовательских приложений» (Контрольная работа)

КМ-7 Контрольная работа №6. «Комплексные решения программно-аппаратной защиты» (Контрольная работа)

КМ-8 Защита лабораторных работ №4; Защита лабораторных работ №5; Контрольная работа №7. «Комплексные решения программно-аппаратной защиты» (Контрольная работа)

**Вид промежуточной аттестации –** Экзамен.

| Номер раздела | Раздел дисциплины | Индекс КМ: | КМ-5 | КМ-6 | КМ-7 | КМ-8 |
|---|---|---|---|---|---|---|
| | | Неделя КМ: | 4 | 8 | 12 | 15 |
| 1 | Раздел 4. Обеспечение целостности информации применением средств программно-аппаратной защиты | | | | | |
| 1.1 | Тема 10. Механизмы контроля целостности данных | | + | + | | |
| 1.2 | Тема 11. Обеспечение целостности информации средствами операционной системы | | + | + | | |
| 1.3 | Тема 12. Обеспечение целостности информации с помощью программных и аппаратных средств | | + | + | | |
| 1.4 | Тема 13. Обеспечение целостности при передаче информации по сетям | | + | + | | |
| 2 | Раздел 5. Комплексные системы защиты информации | | | | | |
| 2.1 | Тема 14. Обеспечение антивирусной защиты информационных систем | | | + | + | + |
| Вес КМ, %: | | | 25 | 25 | 25 | 25 |

**Приложение Б**

# БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Программно-аппаратные средства защиты информации

(название дисциплины)

**7 семестр**

**Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по курсовой работе:**

КМ-1 Соблюдение графика выполнения КП
КМ-2 Оценка выполнения КП
КМ-3 Оценка оформления КП

**Вид промежуточной аттестации –** защита КР.

| Номер раздела | Раздел курсового проекта/курсовой работы | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 |
|---|---|---|---|---|---|
| | | Неделя КМ: | 6 | 10 | 14 |
| 1 | Раздел 1. Описание объекта анализа | | + | + | + |
| 2 | Раздел 2. Описание достоинств и недостатков объекта анализа | | + | + | + |
| 3 | Раздел 3. Разработка проекта программно-аппаратной защиты ЛВС | | + | + | + |
| 4 | Раздел 4. Заключение | | + | + | + |
| Вес КМ, %: | | | 40 | 40 | 20 |