АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Защита в операционных системах»

по специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

• приобретение общих представлений о реализации механизмов защиты информации в современных операционных системах;

• знакомство с основными концепциями организации безопасности на уровне операционных систем.

Задачи освоения дисциплины:

• изучение различных подходов реализации безопасности на уровне файловых систем и систем хранения данных;

• дать основы системного подхода к организации аутентификации и авторизации пользователей;

• дать основы системам проведения аудитов безопасности операционных систем.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита в операционных системах» относится к обязательной части Блока 1 «Дисциплины (модули)» Основной Профессиональной Образовательной Программы специалитета по специальности 10.05.01 – «Компьютерная безопасность», специализация «Математические методы защиты информации» (Б1.О.1.1.50).

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов информатики, основ информационной безопасности, аппаратных средства вычислительной техники, операционных систем, сетей и систем передачи данных.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин, как «Защита программ и данных», «Основы построения защищенных компьютерных сетей», «Основы построения защищенных баз данных», «Модели безопасности компьютерных систем».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития	Знать: Основные виды угроз информационной безопасности операционной системы.

методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	Основные системы защиты информации в операционных системах. Существующие средства защиты информации. Владеть: Терминологией по защите информации.
ОПК-12 – Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения.	Знать: Руководящие документы по описанию системы защиты объекта информатизации. Механизмы проведения аудита информационной безопасности. Методы сбора журналов событий. Руководящие документы по организации защиты операционных систем от НСД и НДВ. Особенности современных программно-аппаратных комплексов защиты информации. Методы реализации функций обеспечения целостности данных в современных операционных системах. Уметь: Формировать техническую документацию на защиту операционной системы. Настраивать и анализировать журналы информационной безопасности. Настраивать работу операционной системы с применением средств защиты информации. Восстанавливать целостность данных на основе современных программно-аппаратных комплексов.
ОПК-13 – Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.	Знать: Механизмы практической реализации защиты информации. Различные подходы к решению задач по защите операционных систем. Методы анализа уязвимостей современных операционных система. Уметь: Правильно настраивать системы защиты информации для операционных систем. Выявлять и ранжировать угрозы информационной безопасности. Комплексно применять механизмы защиты информации для операционной системы. Владеть: Навыками работы с современными реализациями механизмов защиты информации. Возможностями современного прикладного программного обеспечения для защиты ОС.

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение экзамена.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: лабораторные работы.

Итоговая аттестация проводится в форме: экзамен.