

Аннотация дисциплины С.1.1.27 Дисциплина. Безопасность операционных систем

Дисциплина "Безопасность операционных систем" изучается обучающимися по основной профессиональной образовательной программе "Безопасность автоматизированных систем критически важных объектов" направления подготовки "10.05.03 Информационная безопасность автоматизированных систем".

Дисциплина изучается в 5, 6 семестре. Общая трудоемкость дисциплины составляет 270/9 часов/з.ед. Самостоятельная работа заключается в выполнении работ, указанных в разделе 4.

В ходе изучения дисциплины осуществляется текущий контроль в форме технологии рейтингового контроля в соответствии с технологической карты дисциплины, размещенной на электронном курсе, а также промежуточный контроль в форме зачет, экзамен.

Целью изучения дисциплины является формирование следующих компетенций:

1. ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем
2. ОПК-7 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

В ходе изучения дисциплины последовательно рассматриваются темы:

1. Архитектурные особенности современных ОС.
Общая характеристика ОС; назначение и возможности систем семейства UNIX, систем семейства Windows. Интерфейс взаимодействия ОС с пользователями. Общие принципы управления ресурсами вычислительных систем. Понятия процесса (потока) в ОС. Средства межпроцессорного взаимодействия. Управление памятью в ОС. Виртуальная память.
2. Управление доступом.
Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Подходы к организации защиты в операционной системе. Этапы построения защиты. Административные меры защиты.
3. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.
Требования к правилам управления доступом. Дискреционное управление доступом. Матрица доступа. Изолированная программная среда. Мандатное управление доступом. Метки доступа. Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа. Средства динамического изменения полномочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом в Linux. Управление доступом в операционных системах семейства Windows. Субъекты, объекты, методы и права доступа, привилегии субъекта. Маркеры доступа субъектов, дескрипторы защиты объектов. Порядок проверки прав доступа, порядок назначения дескрипторов защиты создаваемым объектам. Средства динамического изменения полномочий субъектов: олицетворение субъектов доступа.
4. Идентификация, аутентификация и авторизация.
Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей. Аутентификация на основе паролей. Средства и методы защиты от компрометации и подбора паролей. Парольная аутентификация в Linux, библиотеки PAM. Парольная аутентификация в Windows,

средства управления параметрами аутентификации. Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы.

5. Аудит и регистрация событий.

Политика аудита. Аудит в ОС семейства UNIX/Linux. Управление подсистемой аудита в ОС Linux. Аудит в ОС семейства Windows Управление подсистемой аудита в ОС Windows. Инструментальные средства анализа журналов аудита.

6. Вспомогательные механизмы защиты информации.

Критические компоненты операционных систем, требующие дополнительных средств для повышения защищенности. Стеганографические и криптографические возможности современных ОС.

Основными стратегическими образовательными технологиями являются: лекционные занятия, практические и лабораторные занятия, процедуры самообучения.

В рамках указанных технологий применяются тактические образовательные технологии: задания, классическая лекция.