Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ

по дисциплине

«Б.1.1.29 Безопасность операционных систем»

направления подготовки
10.03.01 "Информационная безопасность"
Профиль "Безопасность автоматизированных систем"

форма обучения – очная
курс – 3
семестр – 5
зачетных единиц – 6
часов в неделю – 5
всего часов – 180,
в том числе:
лекции – 32
коллоквиумы – 16
практические занятия – 32
самостоятельная работа – 100
экзамен – 5 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: теоретическая и практическая подготовка специалистов в области эксплуатации современных операционных систем (ОС) для обеспечения их эффективного применения с учетом требований информационной безопасности и привитие навыков в использовании методов обеспечения защиты информации в ОС.

Задачи изучения дисциплины:

- изучение назначения и функций ОС;
- приобретение навыков управления ресурсами и задачами в ОС;
- освоение администрирования ОС;
- изучение требований к защите ОС;
- изучение методов и средств разграничения доступа в ОС;
- изучение аудита в ОС;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности ОС;
- приобретение навыков эффективной и безопасной эксплуатации ОС автоматизированных систем;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность проектировании средств защиты информации и средств контроля защищенности автоматизированных систем;
- приобретение навыков эффективного применения информационно-технологических ресурсов ОС с учетом требований информационной безопасности;
- приобретение навыков эффективного применения средств защиты информационно-технологических ресурсов ОС;
- формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы;
- формирование специальных теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность операционных систем» относится к числу базовой части дисциплин.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» - знать формы и способы представления данных в персональном компьютере, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; уметь

применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, дефрагментации и очистки диска и т.п.), пользоваться сетевыми средствами и внешними носителями информации для обмена данными; владеть навыками обеспечения безопасности информации с помощью типовых программных средств, навыками поиска и обмена информацией в глобальной сети Интернет;

«Технологии и методы программирования» - знать общие принципы построения и использования современных языков программирования высокого уровня, язык программирования высокого уровня (объектно-ориентированное программирование); уметь работать с интегрированной средой разработки программного обеспечения, использовать динамически подключаемые библиотеки; владеть навыками разработки, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» - знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности.

Дисциплина «Безопасность операционных систем» является предшествующей для изучения следующих базовых дисциплин: «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Организация ЭВМ и вычислительных систем».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3).

Студент должен знать:

- операционные системы персональных ЭВМ;
- принципы построения и функционирования, примеры реализаций современных операционных систем;
- функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;

- критерии оценки эффективности и надежности средств защиты ОС;
- принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- архитектуру системы безопасности ОС Windows XP/7/2008 R2;
- используемые в Windows XP/7/2008 R2 протоколы аутентификации, их достоинства и недостатки;
- управление учетными записями пользователей и групп в целях обеспечения безопасности;
- уязвимости ОС Windows XP/7/2008 R2 и методы их устранения;
- проблемы и особенности применения файловой системы с шифрованием (EFS), способы повышения уровня безопасности при использовании EFS;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
- принципы формирования политики информационной безопасности в автоматизированных системах.

Студент должен уметь:

- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;
- оценивать эффективность и надежность защиты операционных систем;
- планировать политику безопасности операционных систем;
- пользоваться нормативными документами по защите информации;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

- разрабатывать частные политики информационной безопасности автоматизированных систем;
- формулировать и настраивать политику безопасности распространенных операционных систем;
- разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации;

Студент должен владеть:

- навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;
- навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;
- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) операционных систем с учетом требований по обеспечению информационной безопасности;
- навыками эффективного применения средств разграничения доступа к ресурсам ОС (объектам Active Directory и файловой системы, сетевым ресурсам);
- навыками использования механизма групповых политик для централизованной настройки безопасных конфигурации рабочих станций и серверов;
- навыками применения дополнительных инструментов и утилит для управления системой безопасности ОС Windows XP/7/2008 R2;
- навыками организации централизованного сбора и анализа журналов регистрации для последующего разбора инцидентов;
- навыками построения системы управления обновлениями ОС Windows XP/7/2008 R2 и программного обеспечения на их основе;
- навыками использования рекомендаций ФСТЭК, ФСБ, Microsoft, NIST и других организаций по настройке средств безопасности Windows XP/7/2008 R2;
- профессиональной терминологией в области информационной безопасности;
- навыками работы с нормативными правовыми актами;
- навыками организации и обеспечения режима секретности;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- навыками безопасного использования технических средств в профессиональной деятельности.