Программа спецкурса для аспирантов по специальности 05.13.19
«Методы и средства защиты информации, информационная безопасность. Комплексный подход к проблеме обеспечения »

(полугодовой курс, 36 часов)

Подготовили: д.ф.-м.н., проф. В.А.Васенин, к.ф.-м.н., с.н.с. А.В.Галатенко, к.ф.-м.н., с.н.с. К.А.Шапченко, к.ф.-м.н., с.н.с. Ф.М.Пучков

Лекция 1. Комплексный подход к проблеме обеспечения ИБ (2 часа).
Выделение уровней комплексного подхода к обеспечению ИБ: законодательный, административно-организационный, операционный и программно-технический. Обзор мер и методов на уровнях комплексного подхода к обеспечению ИБ.

Лекция 2. Нормативно-правовой уровень обеспечения ИБ (2 часа).
Обзор нормативно-методической базы в области ИБ на примере руководящих документов ФСТЭК России, международного стандарта ИСО/МЭК 15408, серии международных стандартов ИСО 27000, нормативных документов в области защиты персональных данных.

Лекция 3. Принципы построения систем защиты в компьютерных системах (2 часа).
Основные принципы построения систем защиты информации в компьютерных системах. Модель угроз и модель нарушителя. Распространенные угрозы и атаки. Проектирование и выбор архитектуры системы защиты. Автоматизированные системы в защищенном исполнении.

Лекция 4. Программно-технический уровень обеспечения ИБ (2 часа).
Основные сервисы на программно-техническом уровне обеспечения ИБ. Классификация программно-технических методов и средств защиты информации.

Лекция 5. Методы идентификации и аутентификации в компьютерных системах (2 часа).
Идентификация и аутентификация в компьютерных системах. Общие положения создания систем и механизмов идентификации и аутентификации. Примеры реализации методов идентификации и аутентификации в операционных системах, в веб-приложениях.

Лекция 6. Методы логического разграничения доступа в компьютерных системах, часть 1 (2 часа).
Подход к определению безопасности в терминах доступов. Принцип монитора обращений. Дискреционные модели разграничения доступа на примере матриц доступов, списков прав доступа (ACL) и элементов дискреционного разграничения доступа в Unix-подобных операционных системах.

Лекция 7. Методы логического разграничения доступа в компьютерных системах, часть 2 (2 часа).
Анализ допустимых информационных потоков по модели разграничения доступа на примере модели «take-grant».

Лекция 8. Методы логического разграничения доступа в компьютерных системах, часть 3 (2 часа).
Мандатные многоуровневые модели разграничения доступа на примере модели Белла-Лападула

и модели Биба.

Лекция 9. Методы логического разграничения доступа в компьютерных системах, часть 4 (2 часа).
Ролевые модели разграничения доступа на примере семейства моделей RBAC96. Ролевые модели разграничения доступа с административными привилегиями на примере семейства моделей ARBAC97.

Лекция 10. Скрытые каналы в компьютерных системах (2 часа).
Скрытые каналы. Подходы к классификации скрытых каналов: каналы по времени, каналы по памяти, стеганографические каналы. Примеры реализации скрытых каналов. Подходы к ограничению пропускной способности скрытых каналов.

Лекция 11. Методы и средства защиты информации в компьютерных сетях и распределенных системах. Межсетевые экраны (2 часа).
Методы и средства защиты информации в компьютерных сетях и распределенных системах. Межсетевые экраны (МЭ): виды исполнения, основные компоненты, режимы функционирования. Основные схемы сетевой защиты на базе межсетевых экранов. Примеры реализации МЭ в операционных системах, маршрутизаторах, шлюзах сетевого уровня.

Лекция 12. Методы и средства защиты информации в компьютерных сетях и распределенных системах. Туннелирование и виртуальные частные сети (2 часа).
Методы и средства туннелирования и организации виртуальных частных сетей (VPN). Примеры распространенных реализаций в виде программных средств и аппаратно-программных комплексов.

Лекция 13. Протоколирование и активный аудит, часть 1 (2 часа).
Протоколирование и активный аудит. Методы мониторинга и обнаружения вторжений в распределенных информационно-вычислительных системах.

Лекция 14. Протоколирование и активный аудит, часть 2 (2 часа).
Основные методы анализа регистрационной информации на примере алгоритма статистического анализа регистрационной информации IDES.

Лекция 15. Методы обнаружения уязвимостей программного обеспечения, часть 1 (2 часа).
Распространенные уязвимости программного обеспечения. Подходы к классификации уязвимостей. Примеры основных классов уязвимостей программных средств: переполнения буфера и ошибки управления памятью, гонки потоков, арифметические переполнения, инъекции интерпретируемого кода. Методы обнаружения уязвимостей программного обеспечения.

Лекция 16. Методы обнаружения уязвимостей программного обеспечения, часть 2 (2 часа).
Информационная безопасность с точки зрения технологии программирования. Основные принципы безопасного программирования. Подходы к предотвращению возникновения уязвимостей.

Лекция 17. Методы обнаружения уязвимостей программного обеспечения, часть 3 (2 часа).
Обзор методов верификации программного обеспечения. Способы формального описания

программ, протоколов и предъявляемых к ним требований.

Лекция 18. Методы обнаружения уязвимостей программного обеспечения, часть 4 (2 часа). Методы обнаружения программных закладок и недекларированных возможностей. Методы защиты программ от изучения и разрушающих программных воздействий.