Приложение 3

Аннотация к рабочей программе дисциплины «Методы выявления нарушений информационной безопасности информационно-управляющих, информационно-логистических и автоматизированных систем, их аттестация»

по специальности 10.05.03 «Информационная безопасность АС» (специализация «Информационная безопасность автоматизированных систем на транспорте»).

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа).

Предполагаемые семестры: 9.

Форма контроля: экзамен.

Целью изучения дисциплины (модуля) является овладение студентами методами выявления нарушений информационной безопасности.

Задачами курса являются:

- ознакомление с общими принципами работы традиционных механизмов защиты и систем обнаружения атак;
- изучение различных классификаций атак и уязвимостей;
- изучение перечня источников информации об атаках;
- ознакомление с методами обработки и анализа собранной информации об атаках;
- ознакомление с инфраструктурой обнаружения атак;
- ознакомление с проблемами, присущими технологии обнаружения атак и их решениями.

Дисциплина относится к циклу Б1. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- сети и системы передачи информации;
- безопасность операционных систем;
- безопасность вычислительных сетей
- иностранный язык (английский).

Знания и практические навыки, полученные в результате освоения дисциплины, используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Раздел 1. Технология обнаружения атак

Тема 1.1. Традиционные средства защиты информации и их недостатки. Способы обхода межсетевых экранов. Уязвимости распространенных в России средств защиты.

Тема 1.2. События безопасности и уязвимости. Классификация уязвимостей. Атаки. Модель традиционной и распределенной атаки. Этапы и средства реализации атак.

Тема 1.3. Классификация атак. Базы данных атак и уязвимостей. Инциденты. Классификация нарушителей и их целей.

Тема 1.4. Необходимость применения технологии обнаружения атак и ее возможности. Совместное применение систем обнаружения атак и других средств защиты. Признаки атак.

Тема 1.5. Источники информации об атаках: журналы регистрации, сетевой трафик и т.д.

Тема 1.6. Методы обнаружения атак: экспертные системы, статистический анализ, нейросети и т.п. Обнаружение следов атак в "ручном" режиме. Контроль изменений файлов и каталогов. Анализ журналов регистрации и сетевого трафика. Анализ заголовков, процессов, сервисов и портов. Анализ уведомлений и внешних источников.

Тема 1.7. Классификация систем обнаружения атак.

Тема 1.8. Инфраструктура обнаружения атак. Подготовка и обучение персонала.

Определение политики безопасности.
Тема 1.9. Выбор и использование механизмов системной и сетевой регистрации. План управления журналами регистрации. Создание и применение карты сети.
Тема 1.10. Недостатки технологии обнаружения атак и способы их устранения.

Раздел 2. Выбор системы обнаружения атак

Тема 2.1. Системы анализа защищенности. Зарубежные и российские разработки. Системы анализа рисков. Классические системы обнаружения атак. Анализаторы протоколов и системы контроля журналов регистрации.
Тема 2.2. Обманные системы. Системы контроля целостности. Архитектура систем обнаружения атак и систем анализа защищенности. Системы обнаружения атак на уровне сети и межсетевые экраны.
Тема 2.3. Классы потребителей систем обнаружения атак и их требования. Небольшие и средние компании. Крупные компании с филиалами и транснациональные корпорации. Провайдеры Internet и провайдеры услуг. Критерии оценки систем обнаружения атак. Бесплатная или коммерческая система обнаружения атак. Приоритеты критериев в зависимости от класса потребителя.
Тема 2.4. Обоснование для руководства. Формула расчета потерь от атак. Экономическое обоснование выбора системы обнаружения атак. Обзор российского рынка систем обнаружения атак. Решения компаний Internet Security Systems, Cisco Systems, Symantec, Computer Associates, Network Associates, NFR Security, Enterasys Networks. Свободно распространяемые решения.
Тема 2.5. Варианты размещения систем обнаружения атак. Логическое и физическое размещение сенсоров. Коммутируемые сети. Глобальные сети.
Тема 2.6. Эксплуатация систем обнаружения атак. Выбор узла для установки системы обнаружения атак. Приобретение системы обнаружения атак. Выбор поставщика. Инсталляция и развертывание. Настройка правил. Настройка вариантов реагирования. Стратегия и тактика обнаружения атак. Проблемы, связанные с системами обнаружения атак. Атаки на системы обнаружения атак.

В результате изучения дисциплины выпускник должен обладать следующими компетенциями:

ОК-8: способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков;

ПК-5: способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

ПК-7: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем;

ПК-14: способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы;

ПК-17: способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;

ПК-18: способностью проводить инструментальный мониторинг защищенности автоматизированных систем;

ПК-30: способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;

ПК-31: способностью управлять информационной безопасностью автоматизированной системы;

ПК-32: способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций;

ПСК-10.6: способностью разрабатывать предложения по совершенствованию системы

аудита и управления информационной безопасностью автоматизированных и информационно-управляющих систем транспорта;

ПСК-10.10: способностью выявлять и прогнозировать угрозы информационной безопасности автоматизированных и информационно-управляющих систем транспорта, разрабатывать меры противодействия.

В результате изучения дисциплины специалист должен:

Знать:

– принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;

– основные протоколы компьютерных сетей;

Уметь:

– проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;

– проводить мониторинг угроз безопасности компьютерных сетей;

Владеть:

– профессиональной терминологией в области информационной безопасности;

– методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.