

Аннотация рабочей программы дисциплины (модуля) Б1.В.ДВ.05.02 Системы анализа уязвимостей ПО

Цели дисциплины

Целями освоения дисциплины Системы анализа уязвимостей ПО является формирование профессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов системного и аналитического мышления, овладение принципами организации процесса анализа защищенности автоматизированной системы.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;
- формирование навыков анализа программных реализаций на предмет наличия уязвимостей;
- использования систем обнаружения вторжений.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен проводить формализацию предметной области с целью создания информационной системы в сфере профессиональной деятельности	ПКС-1.1 - Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; ПКС-1.2 - Умеет определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; ПКС-1.3 – Владеет навыками определения параметров настройки программного обеспечения системы защиты информации автоматизированной системы;
ПКС-2	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКС-2.1 - Знает основные меры по защите информации в автоматизированных системах; ПКС-2.2 - Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах. Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах; ПКС-2.3 - Владеет навыками использования типовых программных средства резервирования и восстановления информации в автоматизированных системах.

Содержание разделов дисциплины

Тема 1. Понятие защищенности ИС

Понятие защищенности автоматизированной системы. Нормативная база. Методика анализа защищенности. Исходные данные обследуемой ИС. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.

Средства анализа параметров защиты. Классификация методов анализа параметров защиты (Security Benchmarks). Спецификации Security Benchmarks. Спецификации первого уровня для базового (минимального) уровня защиты. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.

Тема 2. Средства анализа защищенности сетевых сервисов

Уязвимости сетевых протоколов, служб, сервисов. Классификация средств анализа защищенности сетевых сервисов.

Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС. Функции, методика использования.

Тема 3. Средства анализа защищенности web-приложений

Анализ и классификация уязвимостей web-приложений. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC). Комплексная оценка защищенности web-приложения. Принцип «черного ящика» Принцип «серого ящика». Принцип «белого ящика». Инструментальные средства анализа защищенности web-приложения.