

Аннотация рабочей программы дисциплины (модуля)
Б1.В.ДВ.05.01 Анализ уязвимостей ПО

Цели дисциплины

Целями освоения дисциплины Анализ уязвимостей ПО является формирование профессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов системного и аналитического мышления, изучение основных видов уязвимостей программного обеспечения, освоение основных методов и средств анализа и устранения уязвимостей программных реализаций.

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;
- развитие навыков организации антивирусной защиты.

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. Предпосылки внедрения программных закладок

Утверждение о защищенности в рамках субъектно-ориентированной модели компьютерной системы. Условия для внедрения программной закладки. Факторы, мешающие добиться абсолютной защищенности компьютерной системы в реальности. Понятие эксплойта. Пример эксплойта: уязвимость сервиса RPC. Группы типичных уязвимостей программного обеспечения. Переполнение буферов. Переполнение буфера в стеке. Простейший пример переполнения буфера. Специальные встроенные средства защиты от переполнения буферов в современных средах программирования. Security cookie. Переполнение буфера в куче. Пример переполнения буфера в куче. Наиболее известные уязвимости, связанные с переполнением буферов. DEP. Недостатки DEP. ASLR. Отсутствие необходимых проверок, введенных данных. Эксплойт GetAdmin. Эксплойт %00. Эксплойты Internet Explorer и MSOffice XP. Некорректный контекст безопасности. Эксплойт AdminTrap. Системные окна на рабочем столе пользователя. Устаревшие функции. Эксплойт NetDDE. WMF Exploit (MS06-001). Другие уязвимости. Уязвимость program.exe.

Тема 2. Эволюция угроз

Вирусы. Черви. Khobe (обход антивирусной защиты). DoS-атаки. MAC-flooding. USB-флэш атака. Phishing. Подмена субдомена DNS. Сокращения названий субдоменов DNS. Троянский конь. SPAM. Scam. Instant Messaging.

Тема 3. Основные уязвимости

Badware. Атака через прокси-серверы. Potentially Unwanted Program (PUP - потенциально нежелательная программа). Атаки через WEB-серверы. Path Traversal (slash-атаки). Spyware. Атаки нулевого дня. Adware (Madware) и Grayware. Взломщик паролей. Dialer. Browser Hijackers. Bot-коды. Ransomware, Scareware и Rouge Security (rogueware). Rootkit. Crimeware. Cross-Site Scripting (CSS). Взлом WEB-приложений с помощью "отравленных" Cookie. Email bombing. Clickjacking и likejacking. Атаки Salami. XML-бомба. Pharming. ВНО.

Тема 4. Целевые атаки

Тенденции сетевой безопасности в последние годы. Vishing. Вредоносные программы, сопряженные с Web. Службы новостей RSS/ATOM. XSS Scripting. SQL Injection (SQLi). ARP-spoofing. Фальсификация межсайтовых запросов CSRF. Обход фильтра XSS. Экспоненциальные атаки XSS. Использование фальсификации заголовков запросов. Черные ходы в медиа-файлах. Атаки "Drive-by Download". Человек посередине (Man-In-The-Middle). SideJacking. Атака Man-In-The-Browser.

Тема 5. Атаки финансовых объектов

Starware. Grayware. Скрытые угрозы безопасности. Фальсификация имен файлов. Атаки APT. RFI-атака. Вставление удаленного файла. Несанкционированный доступ к машинам, отключенным от Интернет.