АННОТАЦИЯ ДИСЦИПЛИНЫ

«Защищенные информационные системы»

Дисциплина «Защищенные информационные системы» является частью программы магистратуры «Комплексные системы информационной безопасности» по направлению «10.04.01 Информационная безопасность».

Цели и задачи дисциплины

Цель дисциплины - освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности. Задачи дисциплины: - изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах; - изучение современных технологий построения безопасных информационных систем; - изучение этапов и технологий проектирования и создания безопасных информационных систем; - изучение современных программных и аппаратных средств защиты информации; - изучение основных угроз информации в современных информационных системах и сетях; - изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей; - формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации; - формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов..

Изучаемые объекты дисциплины

- методы и средства защиты информации в корпоративных вычислительных сетях и системах; - основные угрозы информации в современных сложных сетевых информационных системах; - программные, программно-аппаратные и аппаратные средства защиты информации, применяемые при обеспечении комплексной информационной безопасности; - программные средства анализа текущего уровня защищенности; - современные технологии построения безопасных информационных систем и сетей..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		2
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	83	83
- лекции (Л)	18	18
- лабораторные работы (ЛР)	24	24
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	36	36
- контроль самостоятельной работы (КСР)	5	5
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	61	61
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)	18	18
Общая трудоемкость дисциплины	180	180

Краткое содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
2-й семестр				
Безопасность web-ориентированного контента	2	0	2	4
Опубликование информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Список действий для обеспечения безопасности web-содержимого				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Развертывание систем обнаружения атак на предприятии	0	6	4	4
Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS. Цели и задачи использования IDS. Существующая политика безопасности. Организационные требования и ограничения. Ограничения на ресурсы, существующие в организации. Возможности IDS. Учет возможного роста организации. Предоставляемая поддержка программного продукта. Развертывание IDS. Стратегия развертывания IDS. Развертывание network-based IDS. Обработка выходной информации IDS. Типичные выходные данные IDS. Выполняемые IDS действия при обнаружении атаки. Компьютерные атаки и уязвимости, определяемые IDS. Типы компьютерных атак, обычно определяемые IDS. Определение расположения атакующего на основе анализа выходной информации IDS				
Различные типы окружений firewall’a	2	0	2	4
Принципы построения окружения firewall’a. DMZ-сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация. Конфигурация с двумя DMZ-сетями. Виртуальные частные сети. Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфра-структуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы. Политика безопасности firewall’a. Политика firewall’a. Реализация набора правил firewall’a. Тестирование политики firewall’a. Возможные подходы к эксплуатации firewall’a. Сопровождение firewall’a и управление firewall’ом. Физическая безопасность ок-ружения firewall’a. Администрирование firewall’a. Встраивание firewall’ов в ОС. Стратегии восстановления после сбоев firewall’a. Возможности создания логов firewall’a. Инциденты безопасности. Создание backup’ов firewall’ов				
Пример пакетных фильтров в ОС FreeBSD 6.0	2	0	2	4
Основные характеристики пакетных				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
фильтров в ОС FreeBSD. ПО пакетных фильтров. OpenBSD Packet Filter (PF) и ALTQ. Указание необходимости использования PF. Оп-ции ядра. Опции rc.conf. Указание необходимости использования ALTQ. Создание правил фильтрации. IPFILTER (IPF) firewall. Указание необходимости использования IPF. Опции ядра. Опции, доступные в rc.conf. Построение скрипта правил с использованием символьных подстановок. Набор правил IPF. Трансляция сетевых адресов(NAT).NAT для очень больших LAN. Использование пула публичных адресов. Port Redirection				
Безопасное использование службы доменных имен (DNS)	2	6	4	4
Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности для них. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Зонный файл. Name-серверы. Авторитетные name-серверы. Кэширующие name-серверы. Resolver'ы. Транзакции DNS. Запрос / ответ DNS. Зонная пересылка. Дина-мические обновления. DNS NOTIFY. Безопасность окружения DNS. Угрозы и обеспечение защиты платформы хоста. Угрозы ПО DNS. Угрозы для данных DNS.				
Системы обнаружения атак (Intrusion Detection Systems, IDS)	0	0	2	5
Понятие системы обнаружения атак. Почему следует использовать IDS. Типы IDS. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление. Скорость реакции. Информационные источники. Network-Based IDS. Host-Based IDS. Application-Based IDS. Анализ, выполняемый IDS. Определение злоупотреблений. Определение аномалий. Возможные ответные действия IDS. Активные действия. Сбор дополнительной информации. Изменение окружения. Выполнение действия против атакующего.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Пассивные действия. Тревоги и оповещения. Использование SNMP Traps. Возможности отчетов и архивирования. Возможность хранения информации о сбоях. Дополнительные инструментальные средства. Системы анализа и оценки уязвимостей. Процесс анализа уязвимостей. Классификация инструментальных средств анализа уязвимостей. Host-Based анализ уязвимостей. Network-Based анализ уязвимостей. Преимущества и недостатки систем анализа уязвимостей. Способы взаимодействия сканера уязвимостей и IDS. Проверка целостности файлов				
Реализация комплексной безопасной сетевой инфраструктуры для web-сервера	0	6	4	5
Топология сети. Демилитаризованная зона. Хостинг во внешней организации. Сетевые элементы. Роутер и firewall. Системы обнаружения проникновения (IDS). Сетевые коммутаторы и концентраторы. Список действий для обеспечения безопасности сетевой инфраструктуры. Администрирование web-сервера. Создание логов. Основные возможно-сти создания логов. Дополнительные требования для создания логов. Возможные параметры логов. Просмотр и хранение лог-файлов. Автоматизированные инструментальные сред-ства анализа лог-файлов. Процедуры создания backup web-сервера. Политики и стратегии выполнения backup’а web-сервера. Поддержка тестового web-сервера. Поддержка аутен-тичной копии web-содержимого. Восстановление при компрометации безопасности. Тестирование безопасности web-серверов. Сканирование уязвимостей. Тестирование проникновения. Удаленное администрирование web-сервера. Список действий для безопасного администрирования web-сервера				
Цель проекта информационной безопасности	2	0	2	4
Цель и задачи проекта. Требования регуляторов. Сохранение информации. Вы-явление источников и каналов утечки информации. Системный ландшафт. Права пользователей. Квалификация пользователей. Средства защиты.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Классификация firewall'ов и определение политики firewall'а	2	6	2	4
Классификация firewall'ов. Установление TCP-соединения. Пакетные фильтры. По-граничные роутеры. Пример набора правил пакетного фильтра. Stateful Inspection firewall'ы. Host-based firewall'ы. Персональные firewall'ы и персональные устройства firewall'а. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии firewall'а. Трансляция сетевых адресов (NAT). Статическая трансляция сетевых адресов. Скрытая трансляция сетевых адресов				
Локализация задачи. Способы хранения конфиденциальной информации	2	0	2	4
Локализация задачи. Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов. Хранение информации. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация. Локальные копии				
Обеспечение безопасности web-серверов	2	0	2	5
Причины уязвимости web-сервера. Планирование развертывания web-сервера. Безопасность лежащей в основе ОС. Безопасное инсталлирование и конфигурирование ОС. Применение Patch и Upgrade ОС. Удаление или запрещение ненужных сервисов и прило-жений. Конфигурирование аутентификации пользователя в ОС. Управление ресурсами на уровне ОС. Альтернативные платформы для web-сервера. Trusted ОС. Использование Appliances для web-сервера. Специально усиленные (pre-hardened) ОС и web-серверы. Тестирование безопасности операционной системы. Список действий для обеспечения безо-пасности ОС, на которой выполняется web-сервер. Безопасное инсталлирование и конфигурирование web-сервера. Безопасное инсталлирование web-сервера. Конфигурирование управления доступом. Разграничение доступа для ПО web-сервера.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Управление доступом к директории содержимого web-сервера. Управление влиянием web Bots. Использование программ проверки целостности файлов. Список действий для безопасного инсталлирования и конфигурирования web-сервера				
Нетехнические меры защиты. Уровни контроля информационных потоков	0	0	4	5
Нетехнические меры защиты от внутренних угроз. Психологические меры. Органи-зационные меры. Права локальных пользователей. Стандартизация ПО. Специфические решения. Работа с кадрами. Хранение физических носителей. Уровни контроля информационных потоков. Режим архива. Режим сигнализации. Режим активной защиты				
Технологии аутентификации и шифрования	0	0	2	5
Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS-сессии. Схемы шифрования SSL/TLS. Требования к реализации SSL/TLS. Список действий для технологий аутентификации и шифрования. Firewall прикладного уровня для web — ModSecurity. Взаимодействие ModSecurity с пакетным фильтром				
Основные направления защиты. Классификация внутренних нарушителей	2	0	2	4
Основные направления защиты. Защита документов. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные из-вне. Другие типы нарушителей				
ИТОГО по 2-му семестру	18	24	36	61
ИТОГО по дисциплине	18	24	36	61