План проспект курса

“Введение в информационную безопасность компьютерных систем”

Аннотация курса

Курс предназначен для магистров.

Лекции читаются _48_ академических часов.

Форма итогового контроля: устный экзамен с оценкой по итогам семестра.

Автор программы: Павел Пилюгин

Лектор: Александр Грушо, Иван Петров, Андрей Петухов, Павел Пилюгин.

Цели и задачи курса

Курс предназначен для ознакомления студентов с теорией и практикой обеспечений информационной безопасности в современных компьютерных сетях. Планируется рассмотреть основные классы проблем защиты информации в современных операционных системах и способов их решения, изучить необходимый набор программных средств, научиться решать практические задачи, связанные с информационной безопасностью.

В результате изучения дисциплины студент должен:

Знать:

- ✓ терминологию в области защиты информации от несанкционированного доступа (НСД), несанкционированного и неправомерного воздействия на информацию;
- ✓ угрозы безопасности информации в автоматизированных системах и вычислительных сетях;
- ✓ основные функции систем защиты от НСД:
- ✓ основные принципы, методы и технологии идентификации и аутентификации;
- ✓ основные политики систем управления доступом, их свойства и критерии безопасности;
- ✓ технологии и основные методы управления доступом к информации применяемые на практике;
- ✓ технологии регистрации и учета;

- ✓ технологии обеспечения целостности информации;
- ✓ технологии защиты информации и программного обеспечения от вредоносных программ;
- ✓ основы администрирования систем обеспечения информационной безопасности вычислительных систем;
- ✓ принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы;
- ✓ принципы технологии межсетевого экранирования и обнаружения вторжений;
- ✓ принципы организации информационных систем в соответствии с требованиями по защите информации;

Уметь:

- ✓ анализировать и оценивать угрозы информационной безопасности автоматизированных систем;
- ✓ осуществлять выбор функциональной структуры системы обеспечения безопасности информации, обрабатываемой в автоматизированных системах;
- ✓ обосновывать выбор технологий и средств обеспечения безопасности информации, обрабатываемой в автоматизированных системах.

Владеть навыками:

- ✓ определения угроз несанкционированного доступа к информации;
- ✓ выявления возможных методов реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
- ✓ оценки качества систем защиты информации.

ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость	Общая трудоёмкость	Контактная работа, часы	Самостоятельная работа, часы	Вид промежуточной аттестации

				ВСЕГО	Лекции	Лабораторные работы	Практические занятия		
5	10	3	180	48	48	-	-	32	Экз. (36 часов)

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа			Самостоятельная работа	Краткое содержание
	Лекции	Лабораторные работы	Практические занятия		
1. Задачи и методы обеспечения информационной безопасности	8			8	Основные понятия, цели и задачи и обеспечения информационной безопасности.
2. Теоретические основы информационной безопасности операционных систем и баз данных.	12			8	Модели и методы “теории безопасных систем”
3. Информационная безопасность вычислительных сетей.	12			8	Особенности сетевой безопасности, Вида атак и методы противодействия.
4. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем и вычислительных сетей	8				Новые виды угроз, угрозы требующие новых средств и методов противодействия.
5. Методическое и организационное обеспечение информационной безопасности	8				Оценка эффективности и управление безопасностью

Лекционные занятия

№ модуля	№ лекции	Объем занятий (часы)	Краткое содержание
1.	1.	2	**Основные понятия информационной безопасности и угрозы безопасности информации при ее обработке в автоматизированных системах (АС)**. Термины и определения. Классификация угроз несанкционированного доступа к информации в АС. Общая характеристика источников угроз несанкционированного доступа в АС. Общая характеристика уязвимостей АС и вычислительных сетей. Угрозы программно-математических воздействий. Компьютерные вирусы и “троянские кони”. Модели нарушителя. Основные функции систем защиты информации.
	2.	2	**Аутентификация и идентификация.** Процедура проверки подлинности субъектов и объектов, параметры парольной идентификации, особенности аутентификации в вычислительных сетях: задачи аутентификации, авторизации и акаунтинга (AAA).
	3.	2	**Модели управления доступом.** Модель системы защиты с полным перекрытием, субъектно-объектная модель системы защиты, понятие изолированной системы, особенности моделирования механизмов безопасности операционных систем и баз данных, основные виды моделей и политик управления доступом — ограниченность моделей и проблемы изменения прав доступа.
	4.	2	**Методы защиты в локальных ОС.** Методы аутентификации и разграничения доступа в операционных системах Windows и Linux.
2.	5.	4	**Дискреционные (матричные) модели управления доступом.** Матрица доступа, пятимерное пространства безопасности Хартсона, модели HRU и Take-Grant, основные результаты, их достоинства и недостатки, основные направления развития.

№ модуля	№ лекции	Объем занятий (часы)	Краткое содержание
	6.	4	**Мандатные модели управления доступом.** MLS модель «военной безопасности», модель Белла-ЛаПадулы, решетки безопасности. Модель Биба.
	7.	2	**Тематические модели управления доступом.** Тематические классификаторы и решетки мультирубрик.
	8.	2	**Ролевые модели управления доступом.** Использование функциональной структуры организации для управления доступом, индивидуально групповая модель управления доступом.
3.	9.	2	**Особенности и проблемы защиты информации в сетях.** Субъекты и объекты компьютерных атак в сетях, виды сетевых атак; методы защиты вычислительных сетей: задачи аутентификации, авторизации и акаунтинга (AAA), сервера безопасности (RADIUS, Kerberos). Задачи фильтрации сетевого трафика. Межсетевые экраны. Фильтрация пакетов. Анализ приложений. Анализ состояний. Прокси сервер. DLP системы. Понятие DMZ.
	10.	2	**Зональные модели и теоретико-игровые методы моделирования систем защиты.** Управление доступом в распределенных системах. Методы оптимизации и методы теории игр при моделировании систем защиты. Теоретико-игровые модели сетевых атак. Модели «доверия» в социальных сетях.
	11.	2	**Атаки на компьютерные сети и методы их обнаружения.** Реальность угроз. Типы атак. Структура типовой атаки. Сканирование. Атаки на разных уровнях протокола TCP\IP (ARP-спуффинг, атаки на маршрутизатор, атаки на DNS, атаки HTTP). Методы обнаружения вторжений.
	12.	2	**Атаки на компьютерные сети и методы их обнаружения.** Реальность угроз. Атаки на уровне приложений протокола TCP\IP (атаки HTTP). Методы защиты.

№ модуля	№ лекции	Объем занятий (часы)	Краткое содержание
	13.	2	**Защищенные сетевые протоколы.** Построение VPN, протоколы SSL,SSH,TLS,IPSec.
	14.	2.	**Безопасность WiFi сетей.** Сети с открытым доступом к каналам связи. Аутентификация, Авторизация – повышенные требования для WiFi сетей. Контроль доступа. Основные уязвимости и риски.
3.	15.	2.	**Проблемные вопросы обеспечения безопасности информации в распределенных вычислительных средах** Виртуальные вычисления в центрах обработки данных, «облачные вычисления».
	16.	2.	**Скрытые каналы утечки информации.** Понятие, виды (по памяти, по времени, статистические), обнаружение и методы противодействия; утечки информации в статистических БД; теоретико-вероятностная модель «невыводимости» и «невлияния».
	17.	2	**Анонимные сети.** Понятие анонимных сетей. Примеры анонимных сетей. TOR. I2P. Уязвимости. Обнаружение.
	18.	2.	**Безопасность SDN.** Разделение потока данных и управляющего потока. Возможные виды атак. Скрытые каналы**.**
4.	19.	2.	**Общие вопросы эффективности обеспечения безопасности.** Критериальные пространства безопасности. Задача оценки эффективности защиты информации. Понятие риска безопасности, вероятностная модель Клементса. Идентификация рисков, основания для управления рисками для обеспечения непрерывности. Измерение эффективности систем защиты в качественных и количественных шкалах. Экономические модели оценки эффективности. Классификации и упорядоченные классы требований безопасности. Стандарты безопасности.

№ модуля	№ лекции	Объем занятий (часы)	Краткое содержание
	20.	2.	**Специальные вопросы эффективности обеспечения безопасности.** Субъективность оценки эффективности, понятие доверия в безопасности, методы доверия, требования доверия, управление доверием, обеспечение уровня доверия к среде. Принципиальные ограничения моделей эффективности в условиях критических объектов безопасности и угроз инсайдера.
	21.	2.	**Общие вопросы управления безопасностью.** Эволюция подходов и моделей управления безопасностью. Процессный характер управления, этапы и факторы управления. Система управления, иерархия политик безопасности. Технологии и инструменты аудита безопасности. Мониторинг безопасности, идентификация событий безопасности, нормализация, корреляция и классификация событий безопасности.
	22.	2.	**Специальные вопросы управления безопасностью.** Управление фильтрацией прикладного уровня, мониторинг прикладного потока через контур сегмента вычислительной среды, угрозы ошибок фильтрации, задача оптимального фильтра. Технологии управление правами для различных моделей доступа, проблема администратора, расщепление полномочий. Технологии управление безопасностью в виртуальных средах: сертификация среды обработки, доверенный супервизор, функциональная и ресурсная инкапсуляция. Идеология «Общих критериев», сеть высокоуровневых сущностей, диалектика зависимости целей, предположений, угроз и политик для среды и объекта защиты, стойкость функций безопасности.

Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	8	Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Решение практических задач по реализации разграничения доступа в операционных системах Windows и Linux
2	8	Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы. Решение практических задач по по обнаружению сетевых атак.
3	8	Изучение материалов лекции №№ 9 - 14 и рекомендованной литературы. Решение задач с использованием различных моделей политик управления доступом.
1-4	8	Подготовка к экзамену