Информационная безопасность

152-ФЗ

Вводит понятие разных **уровней персональных данных**:

- общедоступные персональные данные (ПДн) - может быть получена из открытых источников
- специальные ПДн - расовые, религиозная информация и медицинские данные
- биометрические ПДн - физиологические и биологические особенности человека, на основании которых можно установить его личность

Трансграничная передача ПДн - передача ПДн оператором через государственную границу лицу иностранного государства

Защита программ от нелегального / несанкционированного копирования

Методы защиты

- самозащита
- лицензирование
- защита носителей
- аппаратура (HW)
- изменение фукнций
- ключевая информация
- защита от автоматизированного взлома

Лабораторная работа №1

Написать программу, которая работает в режиме инсталлятора. Она устанавливает другую программу, которая привязывается к конкретному компьютеру.
На защите перекинуть установленную программу на другой компьютер, она не должна запуститься. После установки на втором - всё норм.

Параметры:

- постоянные (аппаратные)
- переменные

Критерии:

- уникальность
- постоянность
- неизменность
- доступность

Для Windows:

- GetWindowsHWProfile
- WindowsManagmentInstrumentation (WMI) - WQL (н-р, select * Win32BIOS), есть утилита wmic (н-р, csproduct get name - вернет имя системы)

Для Linux:

- udevadm into
- /proc
- system_profiler
- SPHardwareDataType
- /var/lib/dbns/machine_id
- systcl

Для MacOS:

- Ioreg

Моделирование угроз

Заставить разработчика при проектировании систем мыслить конструктивно про защиту информации.

1. Определение активов (что?)

- ресурсы
- секретная информация
- контроли

2. Описание архитектуры (где?)

- границы системы
- функции

3. Декомпозиция системы

- области защиты (как?)

4. Определение угроз

Источники угроз:

- природные
- техногенные
- антропогенные:
    - умышленные
    - случайные

5. Документирование угроз

- цель атаки
- риск
- STRIDE - тип

> **S**poofing
>
> **T**ampering
>
> **R**epudiation
>
> **I**nformation disclosure
>
> **D**enial of service
>
> **E**levation of privilege

6. Оценка угроз

- DREAD

> **D**emage
>
> **R**eproducibility
>
> **E**xploitability
>
> **A**ffected users
>
> **D**iscoverability

Уровни возможностей

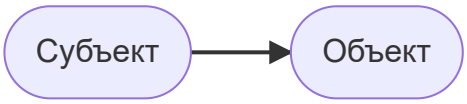
- низкий (пользуется только тем, что разрешили)
- средний (может привносить что-то свое)
- высокий (может добавлять в систему собственные компоненты)
- абсолютный (участвует в жизненном цикле самой системы)

Классы злоумышленников (хакеров)

- увлеченные (любители) - исследуют, развлекаются;
- профессиональные - зарабатывают деньги.

Модели доступа

1. Дискретная



2. Матричная

	Объект 1	Объект 2	Объект 3
Субъект 1	R		

	Объект 1	Объект 2	Объект 3
Субъект 2	W	R	
Субъект 3			R

3. Ролевая

	Роль 1	Роль 2	Роль 3
Субъект 1	X		X
Субъект 2		X	X

	Объект 1	Объект 2	Объект 3
Роль 1	R		
Роль 2	W	R	
Роль 3			R

4. Мандатная (у военных)

	ДСП	С	СС	ССОВ
ДСП	XXX	XXX	XXX	XXX
С		XXX	XXX	XXX
СС			XXX	XXX
ССОВ			XXX	XXX

> Уязвимость - это свойство системы, допускающее или реализующее создание угроз.

Лекция 1
Лекция 3