Информационная и компьютерная безопасность

Подготовлено: Рогожин Михаил по материалам Ассоциации Прогрессивных Коммуникаций и интернет-публикациям для общественного фонда

«Информ-Культура».

Введение

Информационная безопасность (IT Security, Infosec) это теория и практика использования компьютеров и информационных систем, позволяющая

- Предотвратить случайную потерю или повреждение информации и компьютерных систем людьми, использующими их.
- Разработать/настроить системы так, чтобы достичь максимального уровня их надежности и безопасности.
- Предотвратить случайную потерю или преднамеренную потерю или повреждение данных и оборудования другими людьми.

Базовые понятия компьютерной безопасности:

- Угрозы
- Уязвимости
- Атаки.

Виды угроз

- **угроза отказа в обслуживании** – любой файл или ресурс системы должен быть доступен в любое время при соблюдении прав доступа. Если что-то становится недоступным, то оно – бесполезно.
- **угроза целостности** (умышленное изменение, искажение, уничтожение). Обеспечение неизменности информации во время ее хранения и передачи.
- **угроза раскрытия** (кража, утечка)

Причины угроз

- Ошибки пользователей (по оценкам разных экспертов это от 75% до 90% всех сбоев, удалений и повреждений)
- Ошибки программного обеспечения
- Аппаратные поломки
- Преднамеренное повреждение (вирусы, мотивированное повреждение)
- Кражи
- Броски электропитания и форс-мажорные обстоятельства (наводнение, пожар)

Типичные угрозы в интернете

- **Сбой в работе**
- **Сканирование информации**
- **Использование информации** не по назначению
- **Неавторизованное удаление**, модификация или раскрытие информации
- **Проникновение** – атака неавторизованных людей или систем,
- **Маскарад**

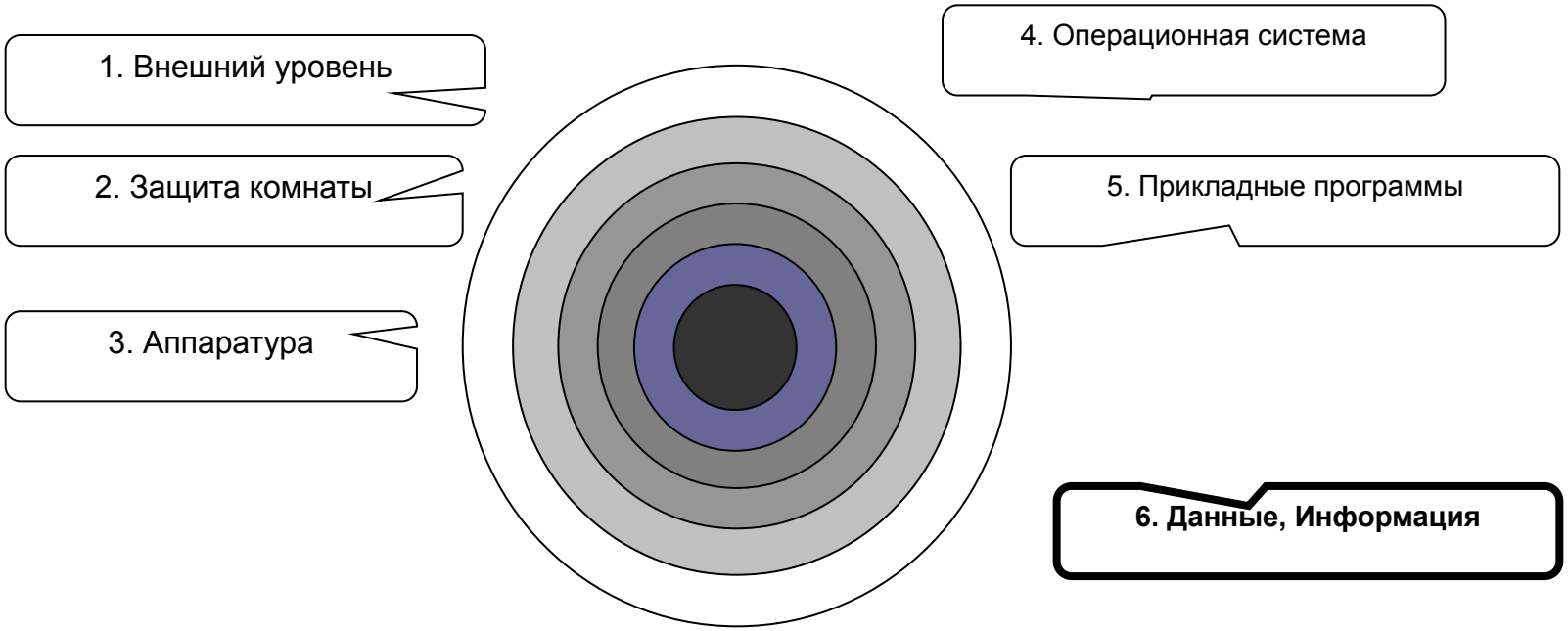
Классификация данных

- **Критическая информация:** Это - информация, которая требует более высоких гарантий чем обычно в отношении ее точности и полноты: информация о финансовых операциях или распоряжения руководства.
- **Коммерческая тайна:** Этот класс применяется к наиболее критической коммерческой информации. Ее неавторизованное разглашение может нанести серьезный вред организации, ее акционерам, деловым партнерам, и/ или клиентам.
- **Персональная информация:** этот класс применяется к информации о человеке, использование которой разрешено только внутри организации. Ее неавторизованное раскрытие может нанести серьезный вред организации и/или ее служащим.
- **Для внутреннего пользования:** Этот класс применяется ко всей остальной информации, которая не попадает ни в один из указанных выше классов. Хотя ее неавторизованное раскрытие нарушает политику, оно не может нанести какого-либо вреда организации, ее служащим и/или клиентам.

Барьеры доступа

- **Первый уровень** – Внешняя защита. Защита владений (зданий, сооружений).
- **Второй уровень** – Защита комнаты.
- **Третий уровень** – Аппаратное обеспечение компьютера.
- **Четвертый уровень** – Операционная система
- **Пятый** – Прикладные программы (защита и уничтожение конкретных данных)
- **Информация, данные**

Барьеры доступа



Виды доступа к информации

- Случайная кража.
- Целенаправленная (мотивированная) кража.
- Государственное (полицейское или иной силовой структуры) вторжение.

Пути получения информации:

- Акустический контроль помещения, автомобиля, непосредственно человека. - Контроль и прослушивание телефонных каналов связи, перехват факсовой и модемной связи, сотовой и радиосвязи.
- Перехват компьютерной информации, в том числе радиоизлучений компьютера, несанкционированное внедрение в базы данных.
- Скрытая фото- и видеосъемка, специальная оптика.
- Визуальное наблюдение за объектом.
- Несанкционированное получение информации о личности путем подкупа или шантажа должностных лиц соответствующих служб.
- Подкуп или шантаж сотрудников, знакомых, обслуживающего персонала или родственников, знающих о роде деятельности.