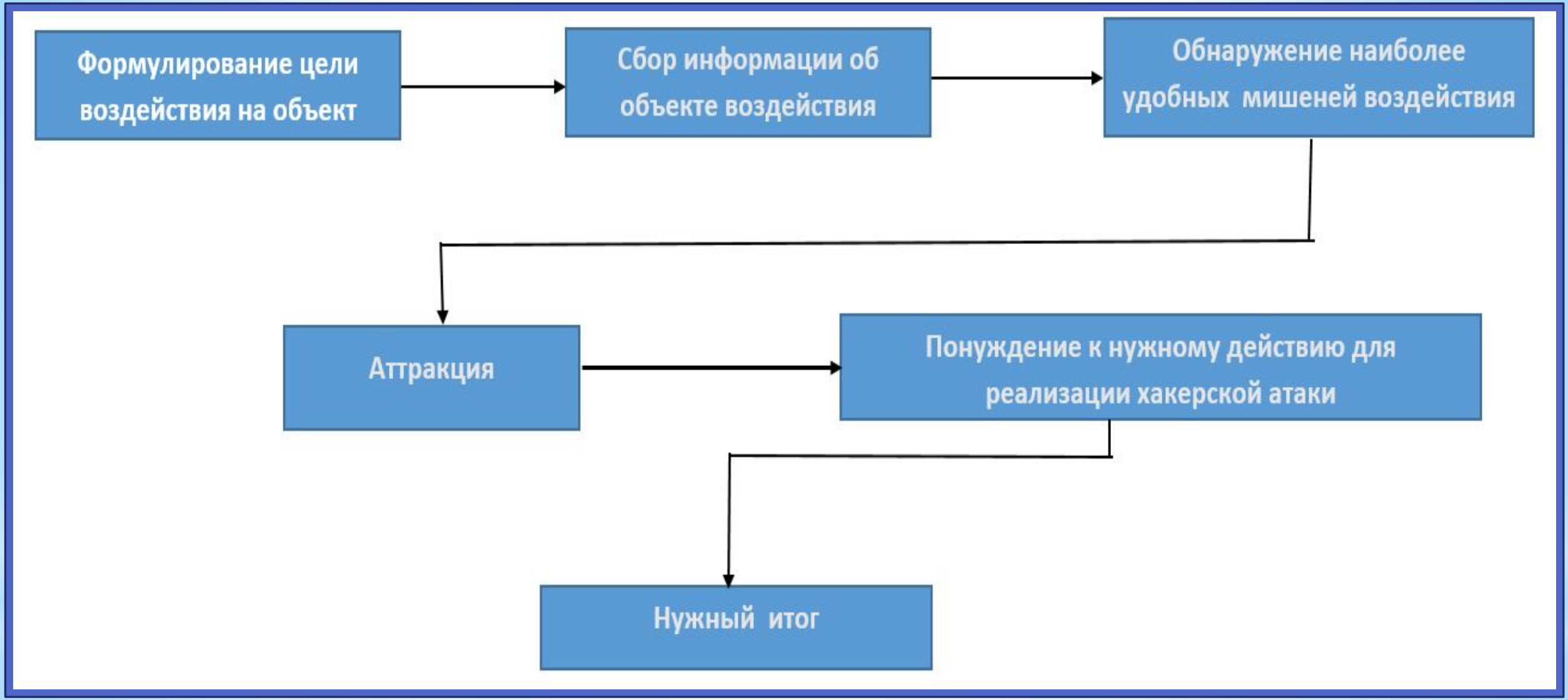
* **Лекция 3. Основная схема воздействия в социальной инженерии**
* План лекции:
* 1. Основная схема воздействия в социальной инженерии
* 2. Реальные примеры воздействия в социальной инженерии



* Основная схема воздействия в социальной инженерии

* возможность **взлома человека** и программирование его на совершение нужных действий
* применяется в большинстве случаев тогда, когда речь идёт об атаке на человека, который является частью компьютерной системы

* Социальное хакерство

* Один из основных каналов утечки клиентских баз данных – социальный
* Примеры
* Основные социоинженерные каналы утечки информации

*** Одна из основных областей применения социальной инженерии- кража клиентских баз данных**

ПОЛЬЗОВАТЕЛИ ЭВМ

основной источник угроз информационной безопасности

Виды сотрудников по уровню создания трудностей системному администратору

1. Квалифицированные, дисциплинированные пользователи;
2. Недостаточно квалифицированные, недисциплинированные пользователи
3. Пользователи-злоумышленники;
4. Иные.

Вредные качества пользователей 2 –й группы

- **Лень** - Хуже всего не те люди, которые бросают работу и уходят, а те, которые бросают работу и остаются.
- **Низкая квалификация**.
- **Халатность.**
- **Азарт.**

Иные

- сотрудники не имеющие прав доступа к компьютерной информации в организации.
- имеющие права доступа к компьютерной информации в организации, но не являющиеся ее сотрудниками
- не имеющие права доступ к компьютерной информации в организации, и не являющиеся ее сотрудниками.

Виды возможного ущерба

- Прямой материальный ущерб
- Косвенный материальный ущерб – упущенная выгода;
- Ущерб деловой репутации

Способы причинения умышленного ущерба

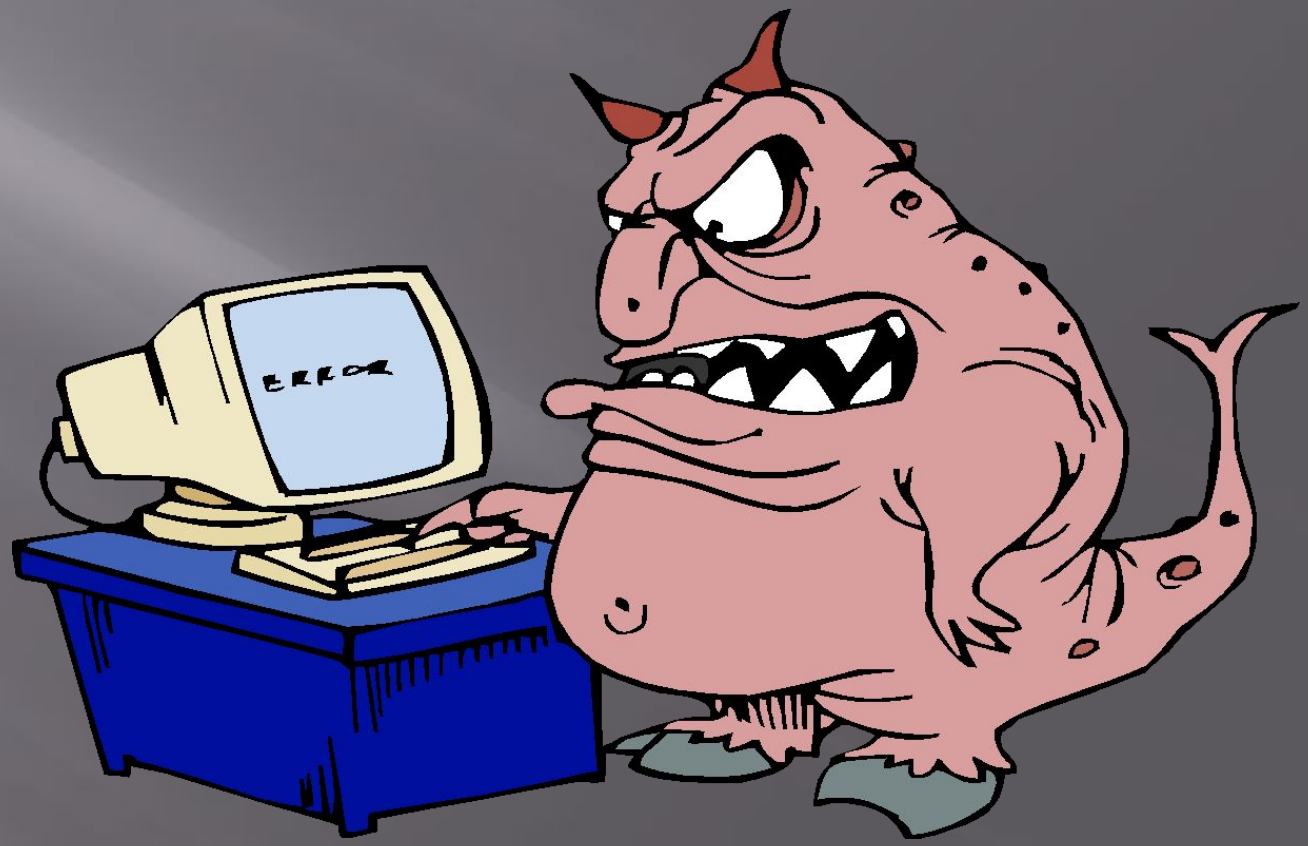
- разглашение информации;
- сбор и передача (копирование) информации;
- модификация (фальсификация) информации
- уничтожение информации;
- блокирование информации;
- нарушение работы ЭВМ, системы ЭВМ или их сети.

Почему человек применяет методы социальной инженерии?

- Обида, месть.
- Корыстные мотивы.
- Компромат.
- Чувство привязанности, влюбленности.

Признаки неправомерных действиях злоумышленников

- прямые
- косвенные



Источники данных о неправомерных действиях злоумышленников

- собственные наблюдения;
- показания очевидцев;
- показания технических средств наблюдения (дежурных и специальных).

Версии

- Нет нарушения информационной безопасности (Ошибка оценки поступившей информации)
- Есть нарушение, но оно совершено неумышленно.
- Есть умышленное нарушение.

- # Выявление нарушений защиты информации в организации и лиц к ним причастных
- Контакты с правоохранительными органами

Виды ответственности за нарушение информационной безопасности организации

- Дисциплинарно-материальная
- Гражданско-правовая
- Административная
- Уголовная

Признаки нарушений информационной безопасности организации:

- Прямые
- Косвенные
- Установленные с помощью аппаратно-программных средств
- Установленные на основании собственных наблюдений
- Установленные на основании информации, полученной из иных источников

Косвенные признаки, указывающие на нарушение информационной безопасности:

- хищение носителей информации;
- передача информации лицам, не имеющим к ней доступа;
- ненормальный интерес некоторых лиц к содержимому мусорных емкостей (корзин, баков и т. д.);
- нарушение заданного (нормального) режима функционирования компьютерных систем;

Косвенные признаки, указывающие на нарушение информационной безопасности:

- проявления вирусного характера;
- необоснованная потеря значительных массивов данных;
- показания средств защиты компьютерной техники;
- необоснованное нахождение в помещениях организации посторонних лиц, включая неплановый технический осмотр помещений, оборудования, различных средств и систем жизнеобеспечения представителями обслуживающих и контролирующих организаций;

Косвенные признаки, указывающие на нарушение ЗИ

- нарушение правил ведения журналов рабочего времени компьютерных систем (журналов ЭВМ) или их полное отсутствие;
- необоснованные манипуляции с данными: производится перезапись (тиражирование, копирование), замена, изменение, либо стирание без серьезных на то причин, либо данные не обновляются своевременно по мере их поступления (накопления);
- появление подложных либо фальсифицированных документов или бланков строгой отчетности;

Косвенные признаки, указывающие на нарушение ЗИ

- сверхурочная работа некоторых сотрудников организации без видимых на то причин, проявление повышенного интереса к сведениям, не относящимся к их функциональным обязанностям, либо посещение других подразделений и служб организации;
- выражение сотрудниками открытого недовольства по поводу осуществления контроля за их деятельностью;
- многочисленные жалобы клиентов.

Административные правонарушения в сфере защиты информации

- Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);
- Статья 13.12. Нарушение правил защиты информации;
- Статья 13.13. Незаконная деятельность в области защиты информации;
- Статья 13.14. Разглашение информации с ограниченным доступом.

Преступления связанные с нарушением защиты информации по УК РФ

- **Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.**
- **Статья 275 Государственная измена**
- **Статья 283. Разглашение государственной тайны**
- **Статья 272. Неправомерный доступ к компьютерной информации.**
- **Статья 273. Создание, использование и распространение вредоносных компьютерных программ**
- **Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.**

Формы контактов с правоохранительными органами

- Заявление о возбуждении дела
- Оказание содействия при проведении следственных действий в качестве специалистов
- Участие в расследовании в качестве эксперта в сфере компьютерных технологий
- Защита своих интересов и организации при расследовании дела