**6.  Социальный инжиниринг**

**Социальная инженерия** - совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним.

Социальная инженерия сегодня представляет собой комплекс практически ориентированных знаний в области управления социальными структурами и процессами, развивающийся по следующим направлениям:

- строительство социальных институтов, например, государственное строительство, реорганизация системы высшего образования и т.д. («социетальный» блок);

- региональное строительство (региональный блок);

- формирование местных сообществ (муниципальный блок);

- строительство организаций или «организационная инженерия» (организационный блок);

- формирование целевых групп и команд («групповая» инженерия). Избирательные технологии и другие способы продвижения лидеров или их команд являются составной частью всех блоков социоинженерной деятельности.

В образовательной практике идеи социальной инженерии реализуются путем применения современных образовательных технологий и активных методов обучения, а также посредством “насыщения” учебного процесса дисциплинами социоинженерного и организационного цикла, в том числе:

- теория и методы социальной инженерии;

- диагностика организаций;

- прогнозирование и моделирование развития организаций;

- организационное проектирование и программирование;

- социальное планирование;

- внедрение социальных новшеств в организации и т.д.;

- практикум по социальным технологиям;

- методы разрешения конфликтов.

Техники социальной инженерии:

1. Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) - вид [интернет-мошенничества](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE), целью которого является получение доступа к конфиденциальным данным пользователей — [логинам](https://ru.wikipedia.org/wiki/%D0%A3%D1%87%D1%91%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C) и [паролям](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C).

2. [Троянская программа](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) - вредоносная программа, используемая злоумышленником для сбора, разрушения или модификации информации, нарушения работоспособности компьютера или использования ресурсов пользователя в своих целях. Данная техника зачастую эксплуатирует любопытство, либо другие эмоции цели. Чаще всего злоумышленник отправляет жертве электронное сообщение, содержащее «интересный» контент, обновление антивируса, или другую информацию, способную ее заинтересовать. Открывая прикрепленный к письму файл, пользователь устанавливает себе на компьютер вредоносное программное обеспечение, позволяющее мошеннику получить доступ к конфиденциальной информации.

3. Сбор информации из открытых источников. Применение техник социальной инженерии требует не только знания [психологии](https://ru.wikipedia.org/wiki/%D0%9F%D1%81%D0%B8%D1%85%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F), но и умения собирать о человеке необходимую информацию. Относительно новым способом получения такой информации стал её сбор из открытых источников, главным образом из [социальных сетей](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C). К примеру, такие сайты как [livejournal](https://ru.wikipedia.org/wiki/%D0%96%D0%B8%D0%B2%D0%BE%D0%B9_%D0%96%D1%83%D1%80%D0%BD%D0%B0%D0%BB), «[Одноклассники](https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BD%D0%BE%D0%BA%D0%BB%D0%B0%D1%81%D1%81%D0%BD%D0%B8%D0%BA%D0%B8_%28%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C%29)», «[ВКонтакте](https://ru.wikipedia.org/wiki/%D0%92%D0%9A%D0%BE%D0%BD%D1%82%D0%B0%D0%BA%D1%82%D0%B5" \o "ВКонтакте)», содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником.

Для защиты крупных компаний и их сотрудников от мошенников, использующих техники социальной инженерии, часто применяются комплексные многоуровневые системы безопасности. Ниже перечислены некоторые особенности и обязанности таких систем.

**Физическая безопасность.** Барьеры, ограничивающие доступ в здания компании и к корпоративным ресурсам. Не стоит забывать, что ресурсы компании, например, мусорные контейнеры, расположенные вне территории компании, физически не защищены.

**Данные.** Деловая информация: учетные записи, почтовая корреспонденция и т. д. При анализе угроз и планировании мер по защите данных нужно определить принципы обращения с бумажными и электронными носителями данных.

**Приложения.** Программы, запускаемые пользователями. Для защиты среды необходимо учесть, как злоумышленники могут использовать в своих целях почтовые программы, службы мгновенной передачи сообщений и другие приложения.

**Компьютеры.** Серверы и клиентские системы, используемые в организации. Защита пользователей от прямых атак на их компьютеры, путем определения строгих принципов, указывающих, какие программы можно использовать на корпоративных компьютерах.

**Внутренняя сеть.** Сеть, посредством которой взаимодействуют корпоративные системы. Она может быть локальной, глобальной или беспроводной. В последние годы из-за роста популярности методов удаленной работы, границы внутренних сетей стали во многом условными. Сотрудникам компании нужно разъяснить, что они должны делать для организации безопасной работы в любой сетевой среде.

**Периметр сети.** Граница между внутренними сетями компании и внешними, такими как Интернет или сети партнерских организаций.