**«КИБЕРБЕЗОПАСНОСТЬ, МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЕ ИМ»**

**Работу выполнил:** Шакирянов Чингиз Маратович, студент 1 курса ФГБОУ ВО «КНИТУ-КАИ», Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ.

Как показывает мировая практика успешно проведённых взломов, большая часть проблем связана именно с проблемами с людьми. Если быть более точным - дело в их способности выдать любую информацию и совершать необдуманные действия. Социальная инженерия - совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату.

**Актуальность исследования:** Реализация мер эффективной кибербезопасности в настоящее время является достаточно сложной задачей, так как сегодня существует гораздо больше устройств, чем людей, а злоумышленники становятся все более изобретательными. Технологии безопасности малоэффективны в противостоянии хакерам, использующим методы социальной инженерии. В этой связи актуальной становится проблема работы с персоналом, обучение сотрудников применению политики безопасности и техникам противостояния социальным инженерам, что является залогом безопасности для баз корпоративной информации.

**Объект исследования:** социальная инженерия.

**Предмет исследования:** основные методы атак, применяемых в СИ и методы защиты от них.

**Цель исследования:** найти и разработать методы противостояния социальным инженерам.

**Задачи исследования:**

1. Изучить основные принципы работы СИ.
2. Выделить основные пути получения информации.
3. Разработать устройства СИ.
4. Проверить на практике уязвимость различных систем.
5. Разработать методы защиты от представленных устройств.

**Гипотеза:** в любой системе есть уязвимости, а самая главная уязвимость, человеческий фактор.

**Практическая значимость исследования:** данная работа может быть применена для наглядной демонстрации средств безопасности от СИ.

**Новизна исследования:** на сегодняшний день, уже существуют работы, посвящённые этой теме, но они рассматривают эту проблему поверхностно, а я попытался рассмотреть её изнутри, побывав в роли хакера и жертвы.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

<https://habr.com/company/croc/blog/189560>

<http://tailorjerry.com>

Кевин Д. Митник; Вильям Л. Саймон. Искусство обмана. - АйТи, 2004г.