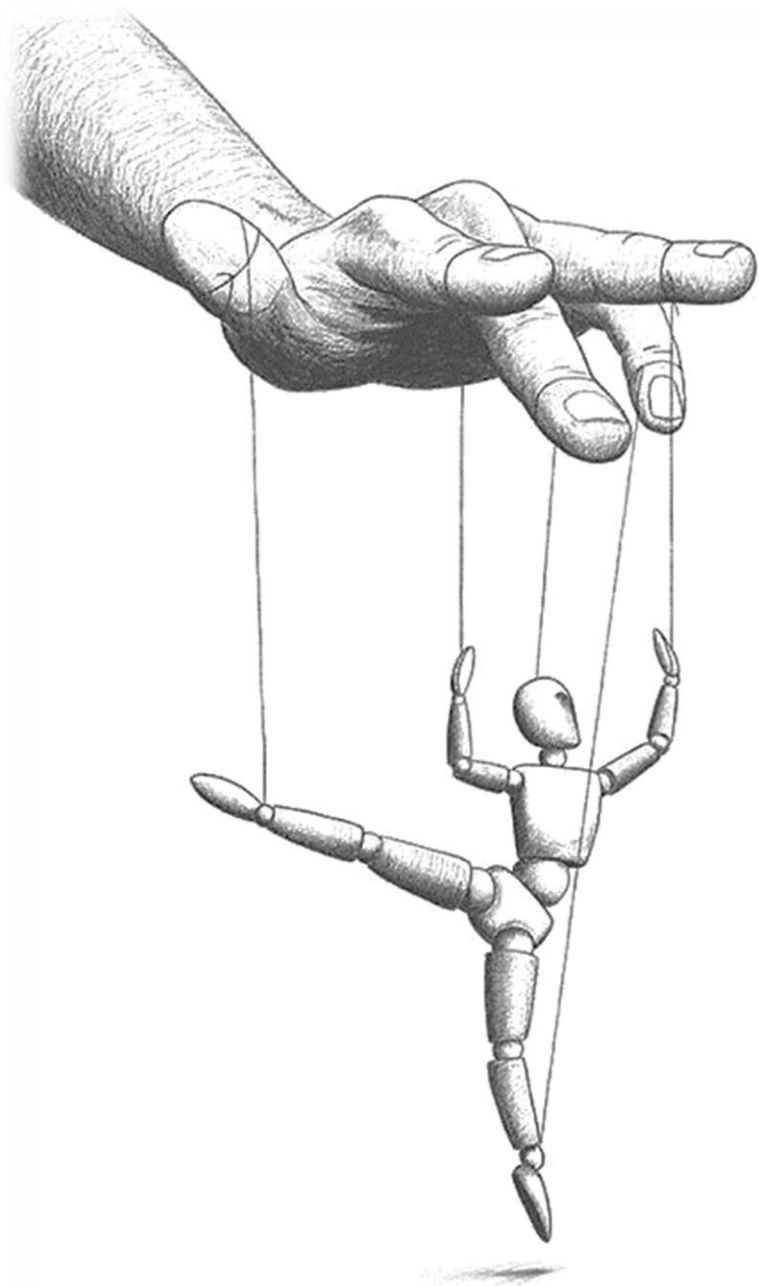


Социальная инженерия

в контексте информационной безопасности





Социальная инженерия (SI)

это методология управления поведением человека без применения специальных технических средств, ориентированная на эксплуатацию человеческих слабостей различными средствами манипуляции.



Основная задача

«подобрать ключ» к каждому конкретному человеку, сыграв на его чувствах и эмоциях таким образом, чтобы тот забыл про осторожность и совершил необходимые действия.

История

Первобытное общество

- Лидерство и влияние
- Соблазн и обман
- Дипломатические отношения



Древний мир

- Мифология и ритуалы
- Риторы и ораторы
- Символы власти
- Дипломатические уловки



Средневековье

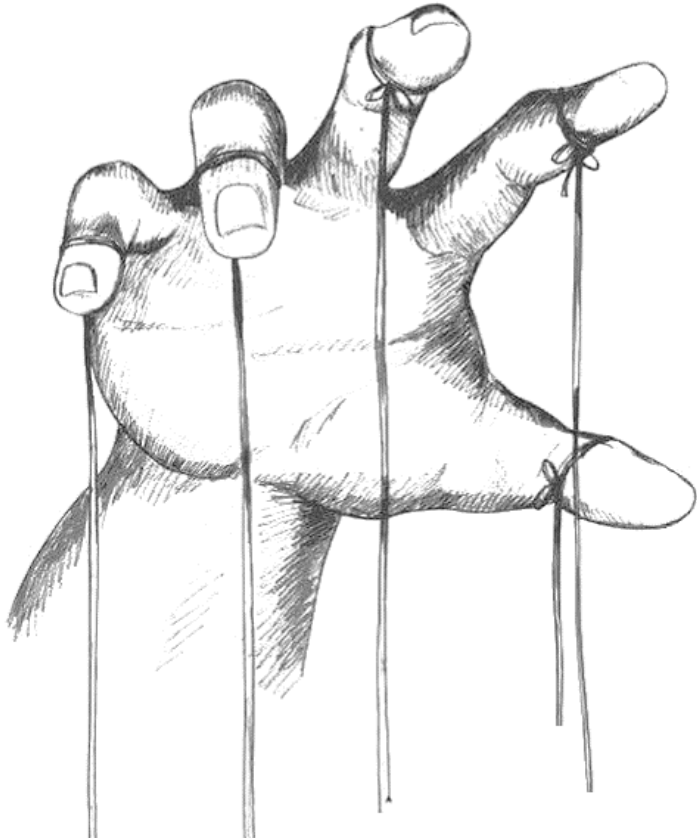
- Обман в торговле
- Религиозные манипуляции



Новейшее время

- Пропаганда
- Информационные войны





Кто и зачем использует:

- Бизнес и корпоративная среда
- Маркетинг
- Государство и политики
- Профессионалы коммуникаций
- Сотрудники спецслужб
- Журналисты, юристы
- Преступные сообщества

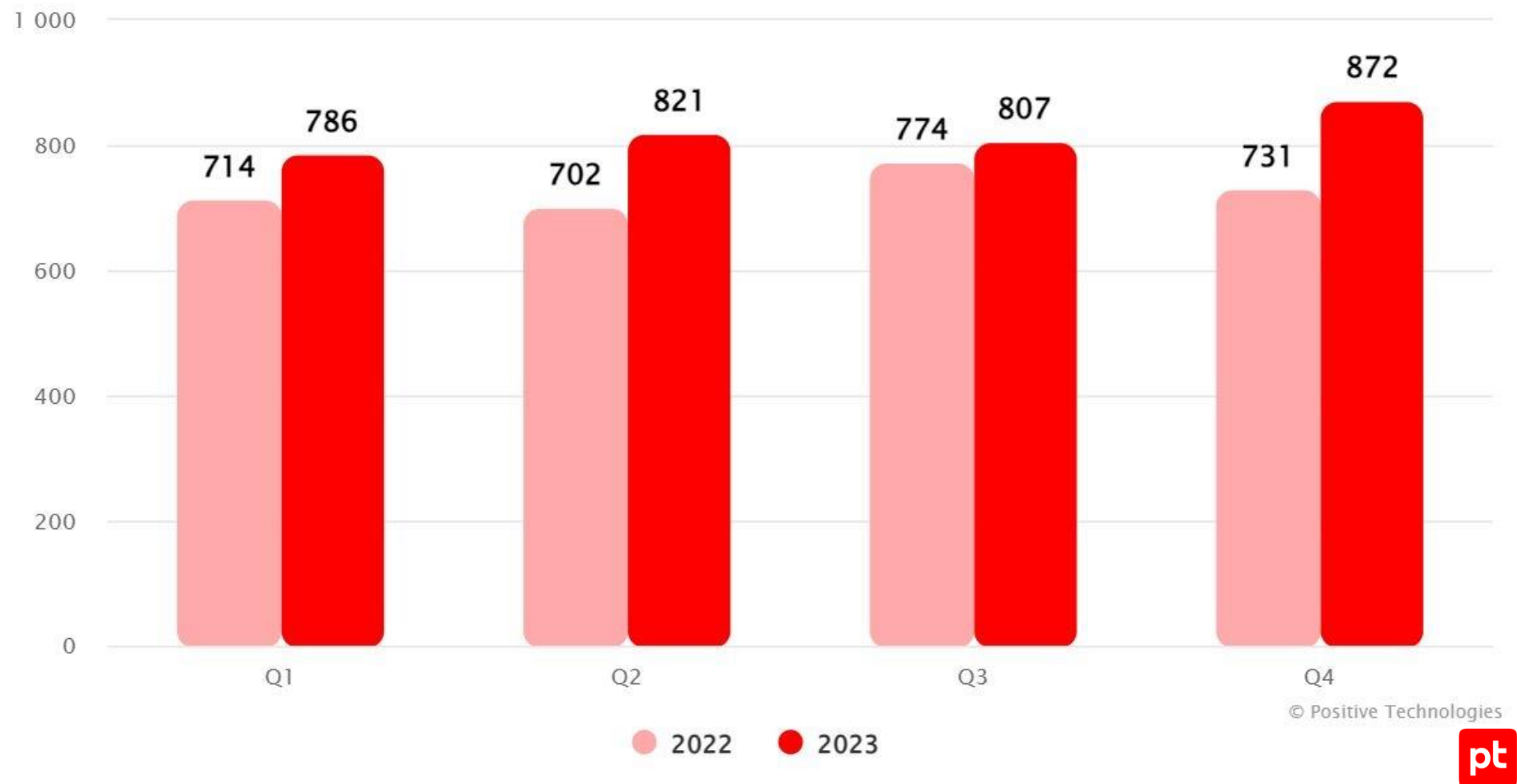
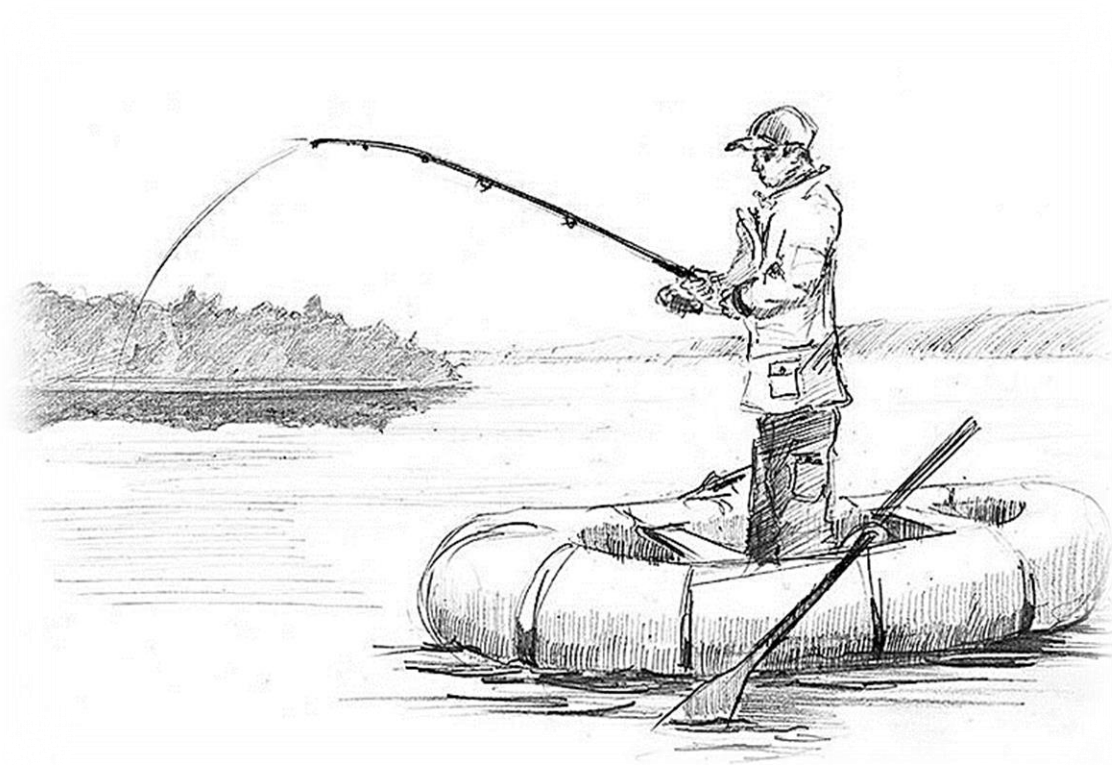


Рисунок 1. Количество атак в 2022 и 2023 годах (по кварталам)



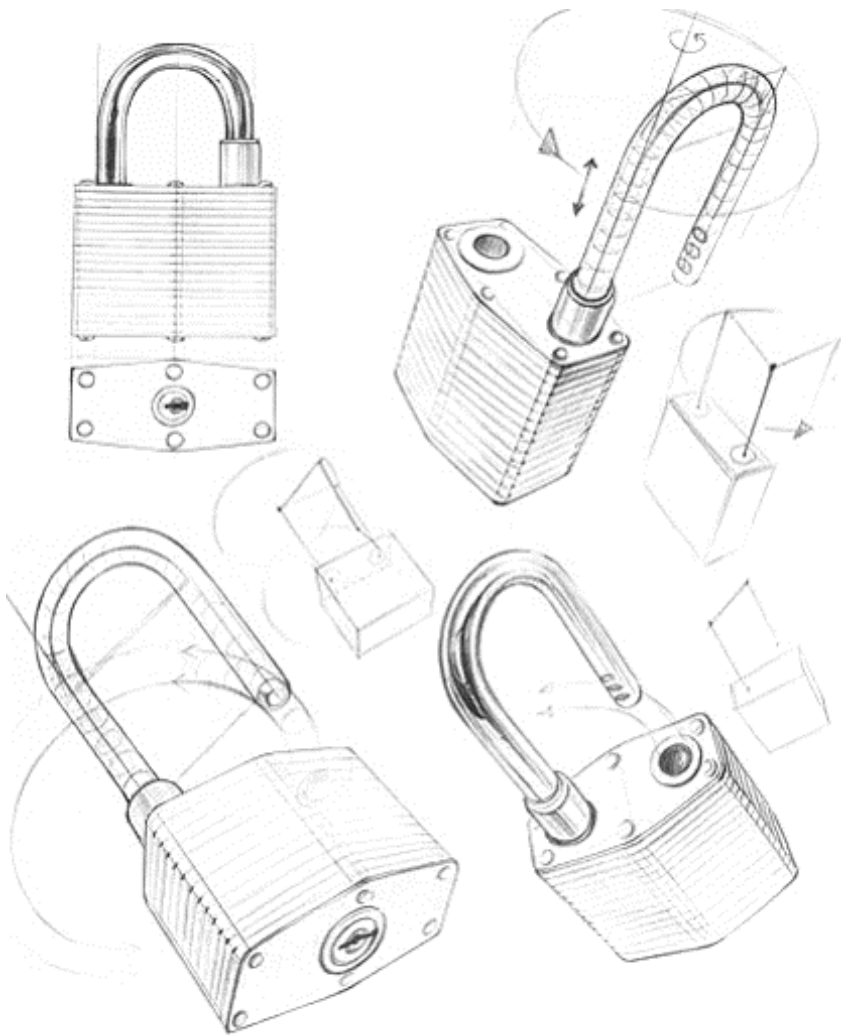
Рисунок 3. Методы атак (доля успешных атак)

Методы социальной инженерии:



- Фишинг
- Вишинг
- Смишинг
- Предтекстинг
- Фарминг
- Спуфинг
- Обратная СИ (Humint)

Обратная социальная инженерия



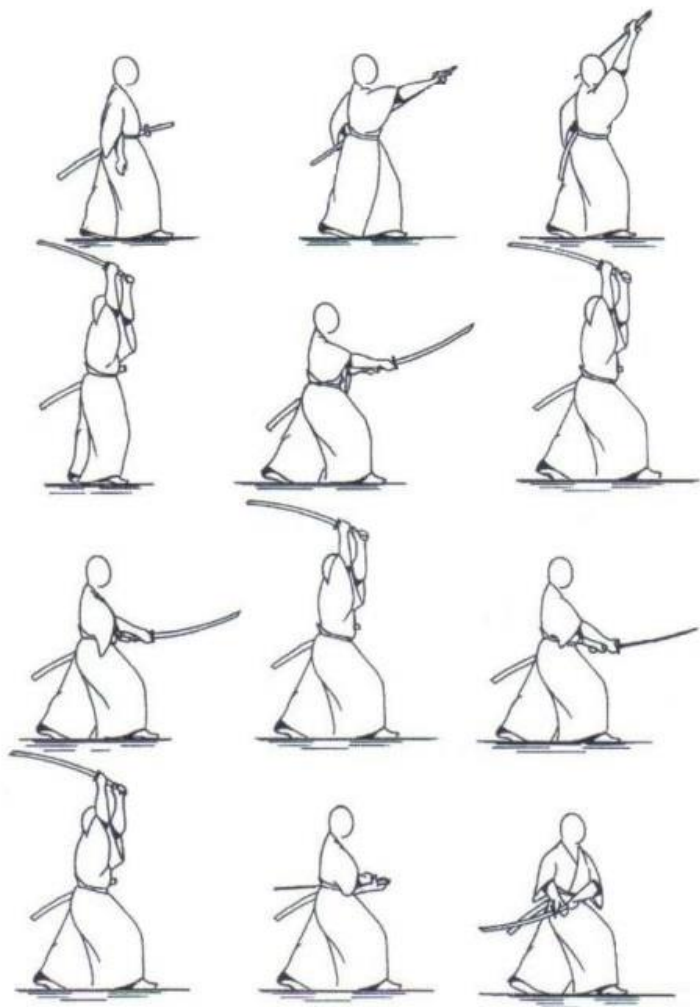
HUMAN INTELLIGENCE (HUMINT)

Метод заточенный на получение стратегически значимой информации через взаимодействие с человеком.



Задача

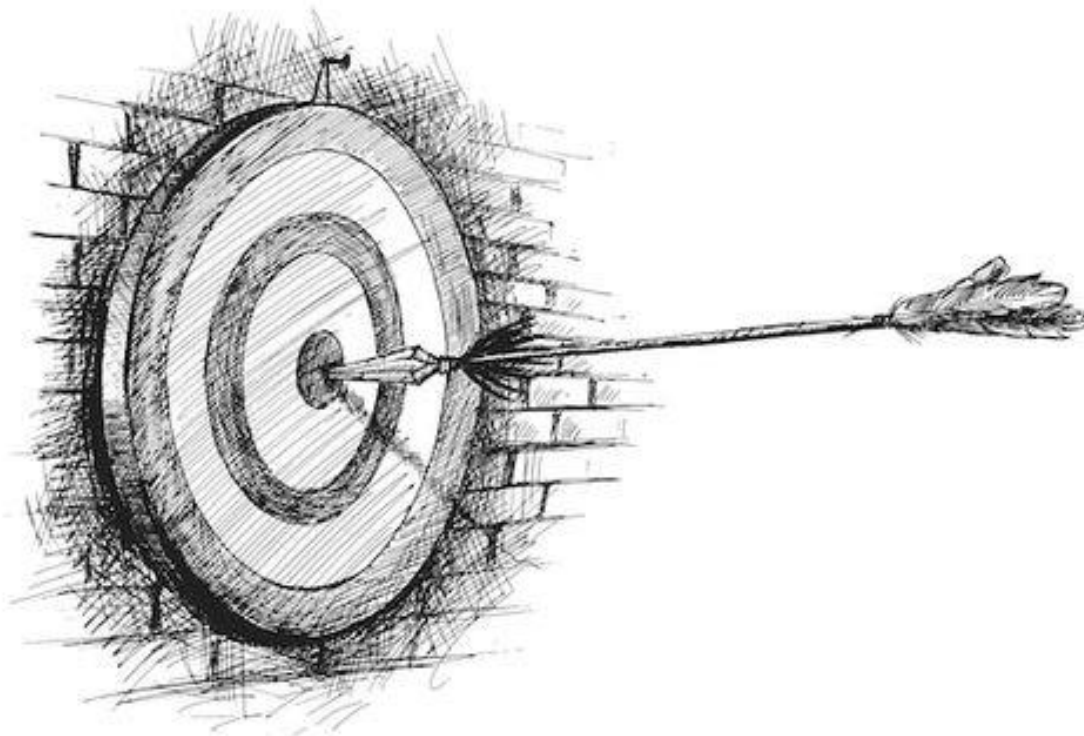
изучить человека, определить слабости,
подготовить легенду и получить
стратегически значимую информацию
через человека.



Техники HUMINT

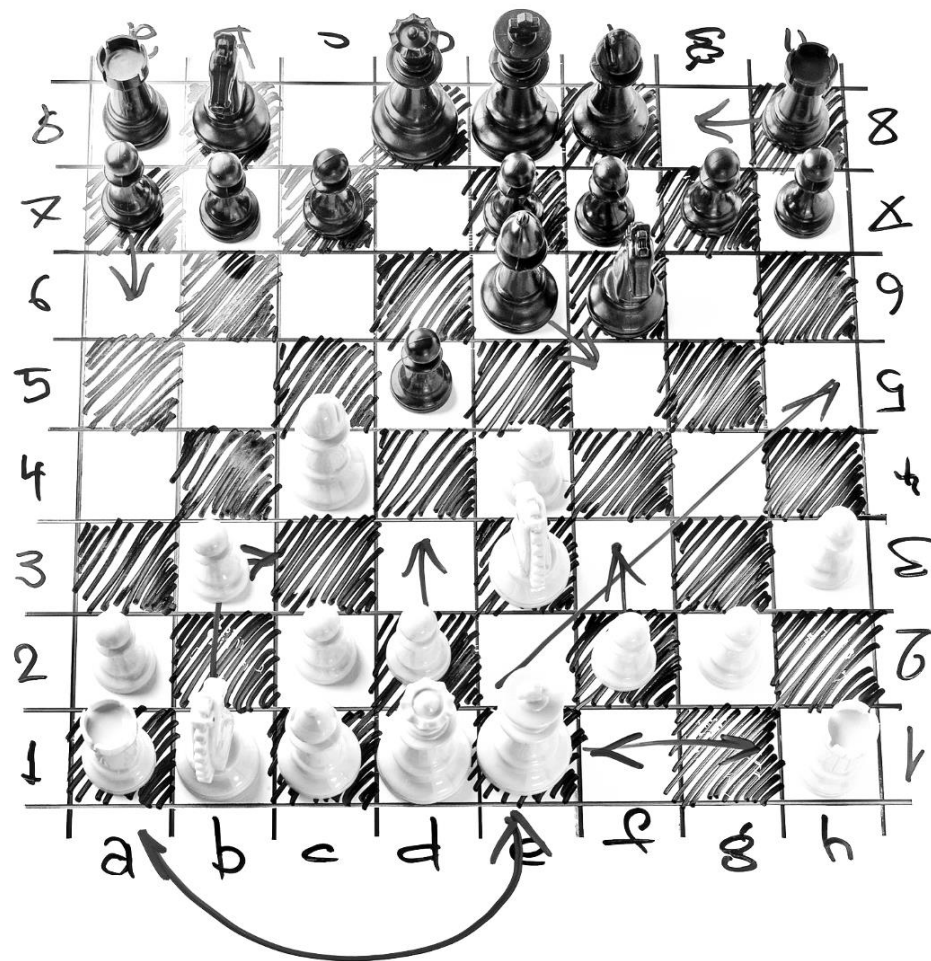
- Личное взаимодействие
- Вербовка информаторов
- Создание легенды
- Наблюдение и анализ поведения
- Использование социальных сетей
- Психологическая манипуляция

Цель SI

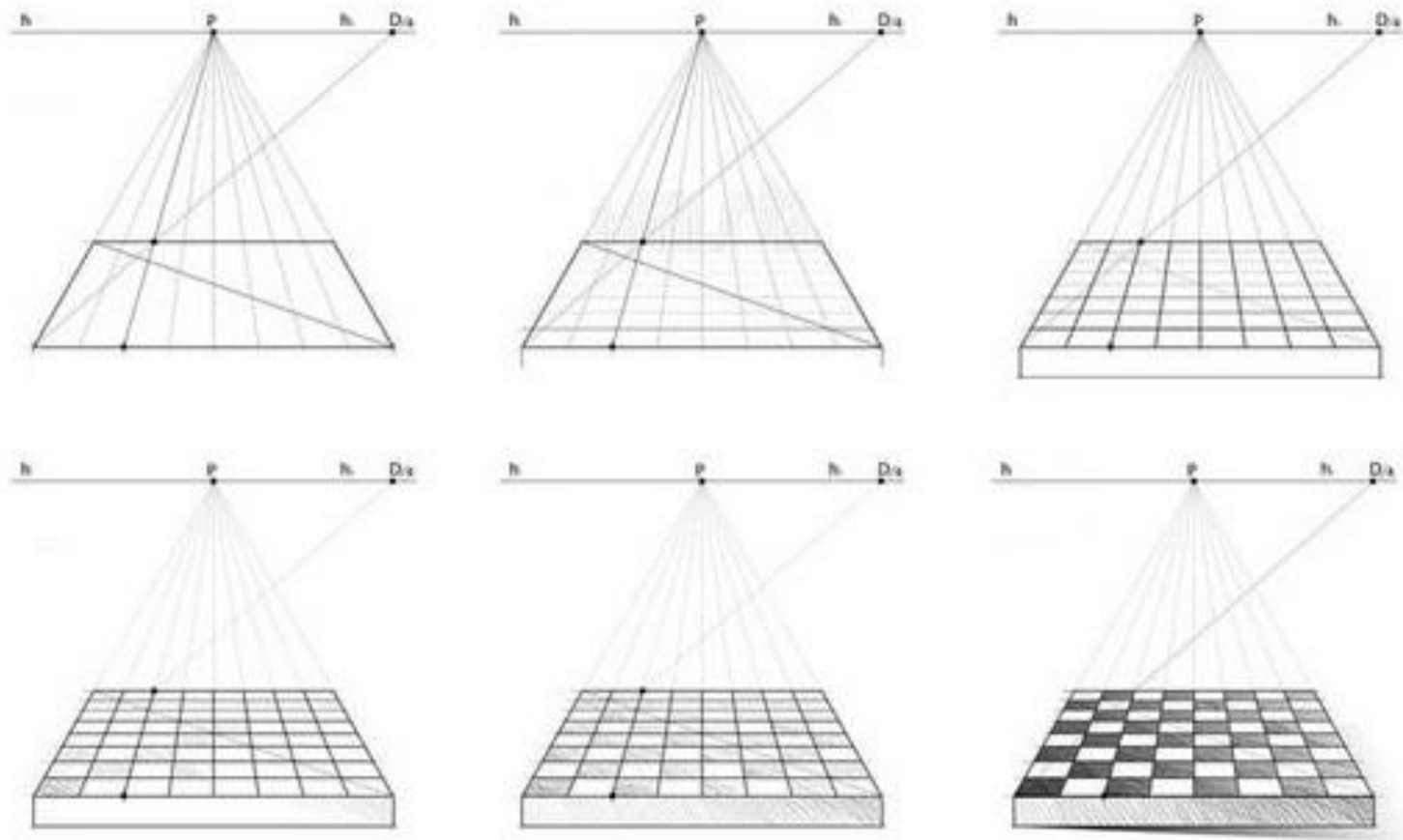


- Конфиденциальная информация
- Доступ к защищенным ресурсам
- Выполнения действий
- Финансовые активы
- Другие ценные объекты

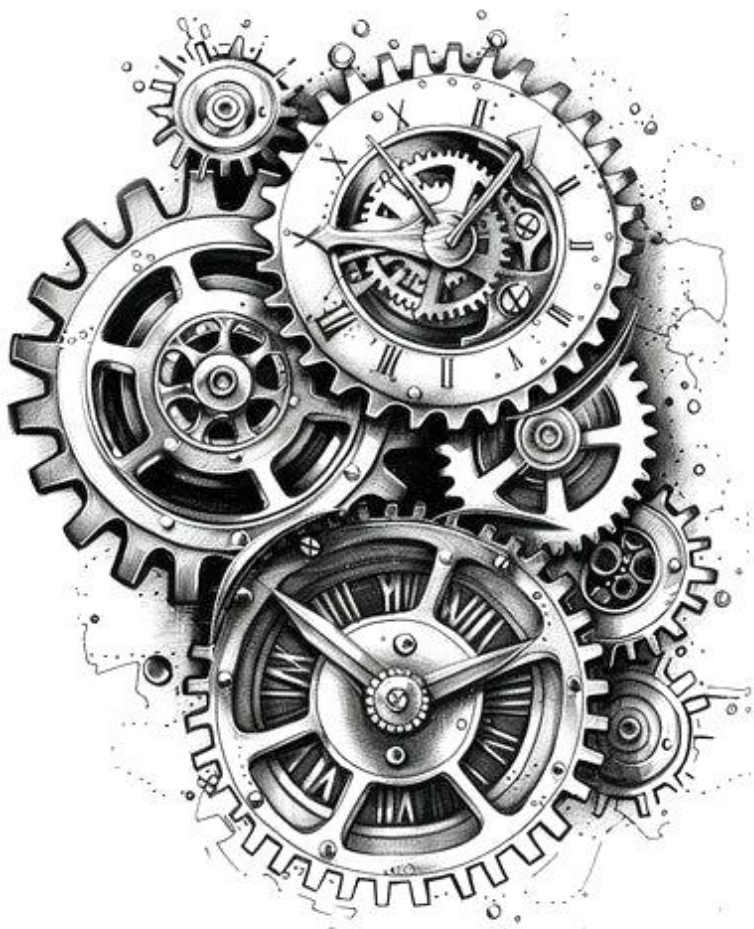
Алгоритм сложной атаки



Сбор информации о цели



Сбор информации по юридическому лицу:



- Специфика, структура, направления деятельности
- Внутренняя организационная структура, иерархия
- Физическое местонахождение офисов, часовой пояс
- Наличие регламента в бизнес-процессах и документообороте
- ФИО руководителей отделов и т. д.
- Количество сотрудников, формат занятости (офис или аутсорс)
- ОС, браузеры, ПО, антивирусы, почтовые клиенты и другой софт

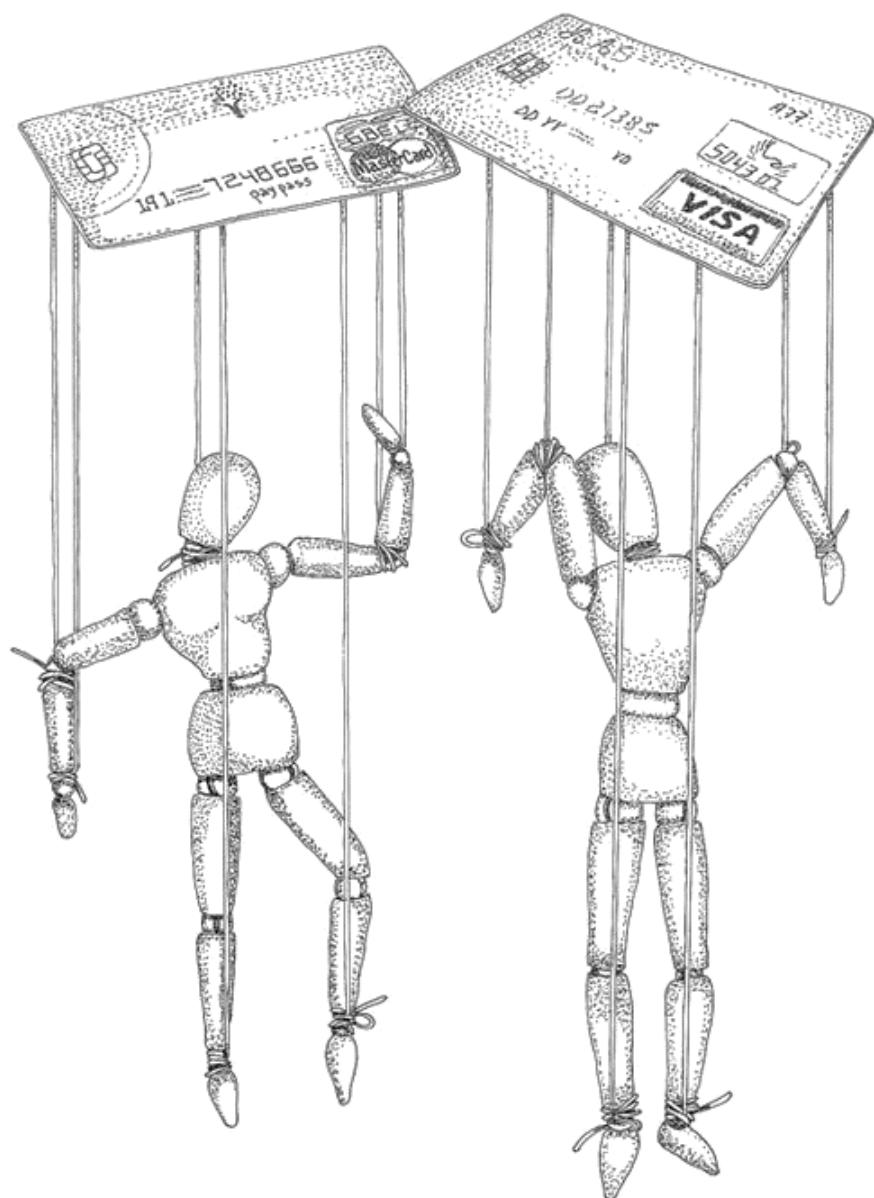
Сбор информации по физическому лицу:



- Персональные данные
- Места работы
- Адреса
- Хобби, интересы, увлечения
- Ближайшее окружение
- Семейное положение
- Аккаунты в социальных сетях
- Автобиография

Создание легенды





Основные слабости

- Доверчивость
- Желание помочь
- Страх и тревожность
- Жадность
- Эмоции и сочувствие
- Привычки и рутина
- Лень
- Авторитет

Психологические факторы атак

Страх	Невнимательность	Раздражение	Срочность
• Ваш компьютер заражен! • Против вас заведено уголовное дело.	• www.sberbank.ru • @gmail.com • @lsrgroup.ru	• Чтобы отписаться пройдите по ссылке:	Отчет прислать сегодня до 15:00
Любопытство	Жадность	Желание помочь	Авторитет
• Смотри где я тебя нашел: • А ты уже прошел опрос? • Вы выиграли приз!	• Скидка 50 % при оплате прямо сейчас.	Ваш коллега потерял карту, дайте его номер телефона для связи.	Письмо, звонок от руководителя или сотрудника спецслужб.

Потенциальные жертвы манипуляций

Люди с низкой самооценкой	Законопослушные люди
• Негативные убеждения о себе • Чувство неполноценности • Потребность в одобрении • Коммуникативные барьеры	• Приверженность традициям и обычаям • Ориентация на прошлое • Низкая социальная мобильность • Принятие решений на основе данных
Эмоционально зависимые	Рациональные
• Способность к сопереживанию • Чувствительность к окружающей среде • Искренность и честность • Творческое мышление • Необходимость в одиночестве	• Логическое мышление. • Объективность • Критическое мышление • Долгосрочное планирование • Способность к самоанализу

Методы влияния

Люди с низкой самооценкой	Законопослушные люди
1. Создание зависимости 2. Игра на чувствах вины и стыда 3. Поддержка и манипуляции 4. Создание образа "спасителя" 5. Завышенные ожидания 6. Разрушение самооценки	1. Ложные представления 2. Создание ситуации правового давления 3. Использование поддельных документов и лицензий 4. Апелляция к чувству долга и правильности 5. Угроза юридическими последствиями 6. Использование правдоподобных предложений
Эмоционально зависимые	Рациональные
1. Использование методов эмоционального шантажа 2. Вызывание жалости и сочувствия 3. Ложная романтика (романтические аферы) 4. Давление на чувства долга и ответственности 5. Создание ложного ощущения срочности 6. Дарение ложной надежды	1. Использование логики и аргументов 2. Создание чувства срочности 3. Презентация фейковых экспертов 4. Психология "социального доказательства" 5. Запутывание информации 6. Эмоциональное манипулирование

Установление контакта



Эскалация доверия



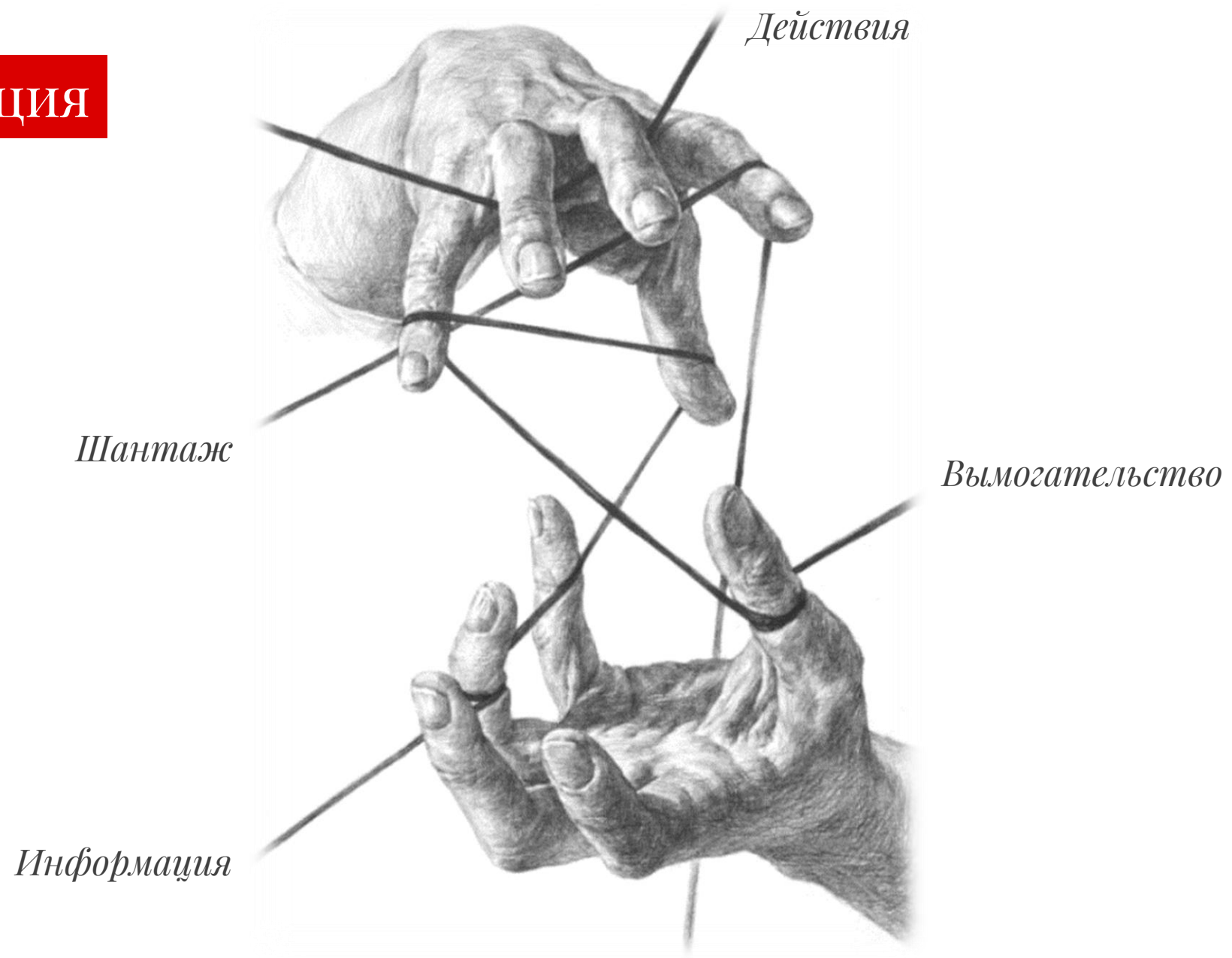
Получение информации



Получение доступа



Эксплуатация

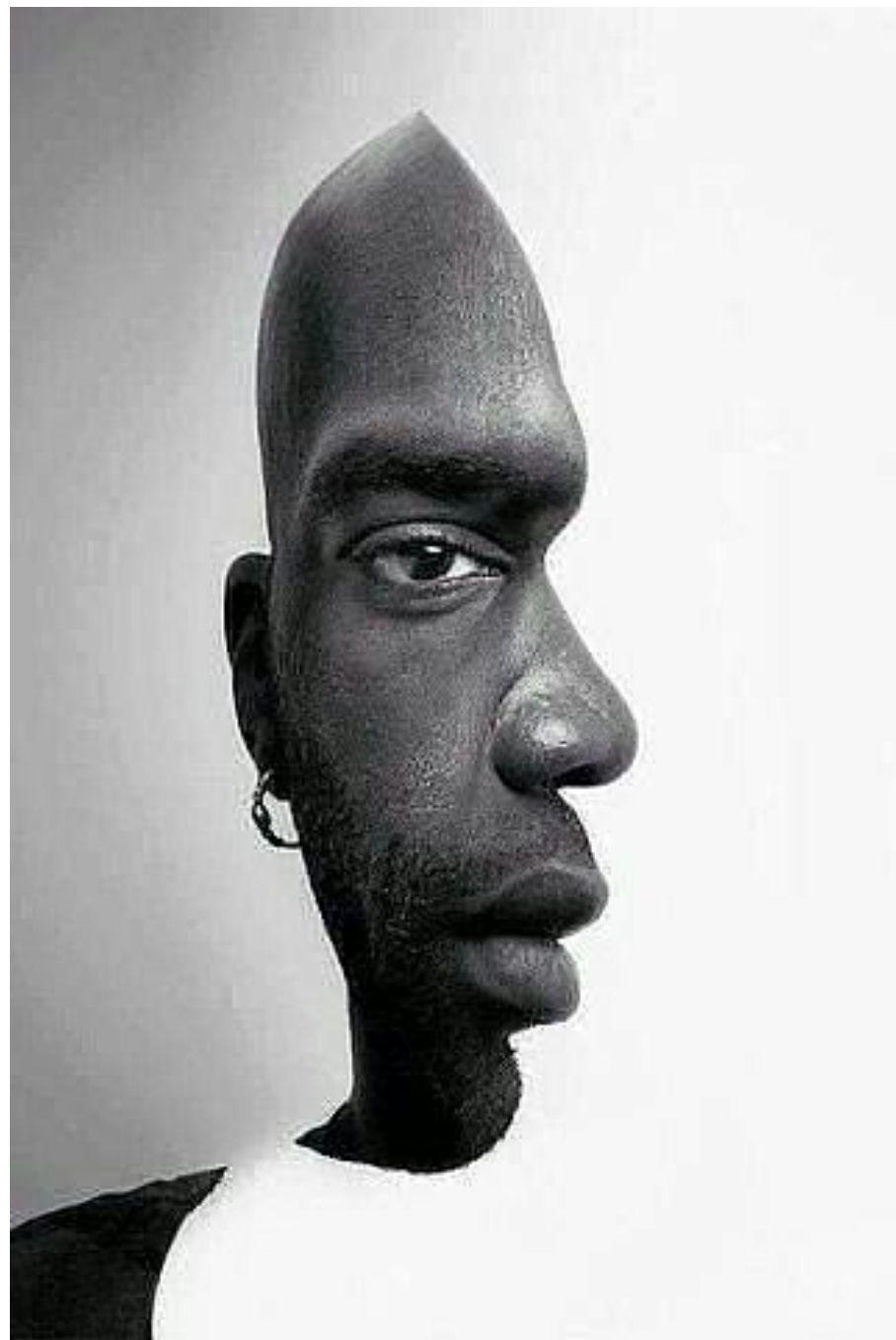


Соккрытие следов



Почему это работает?



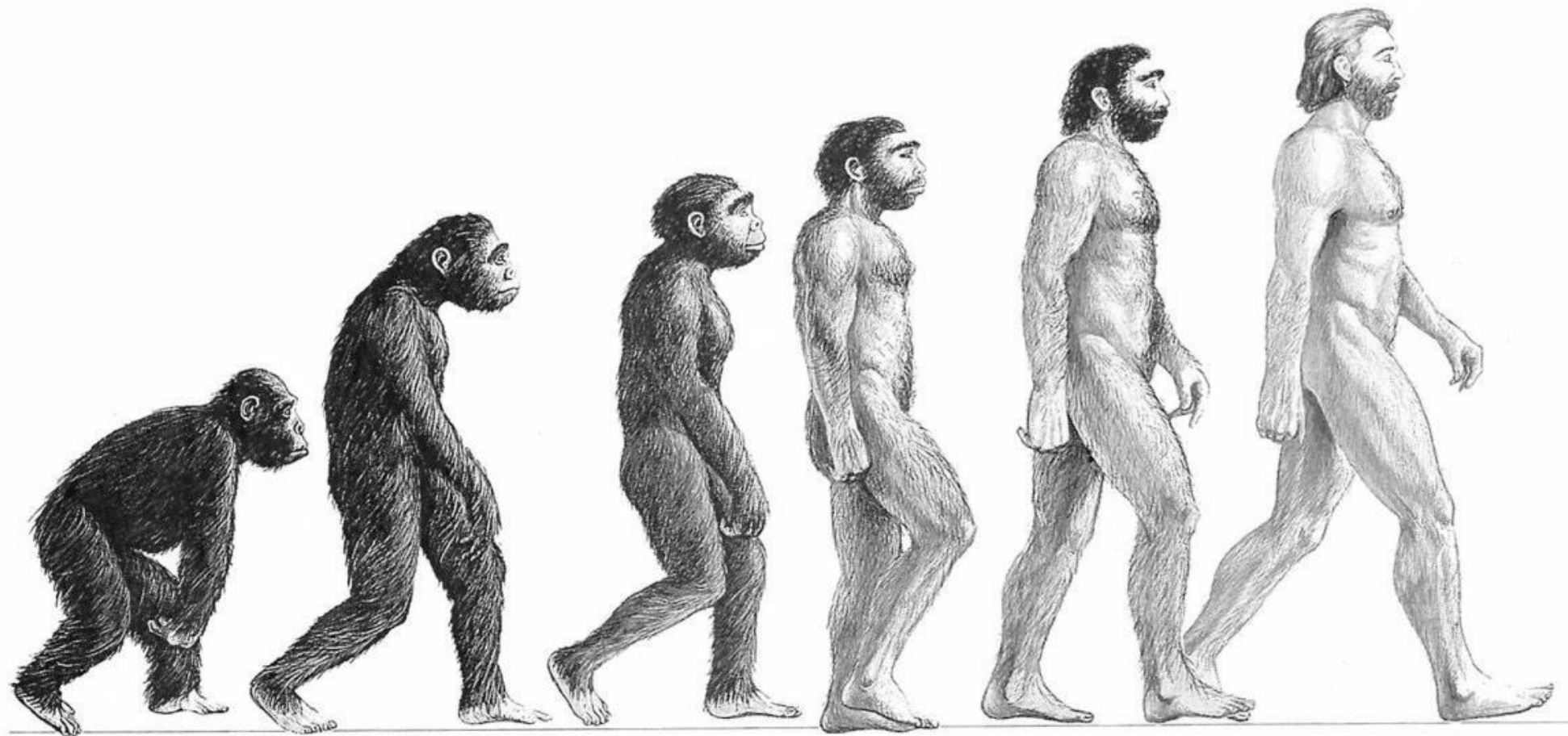




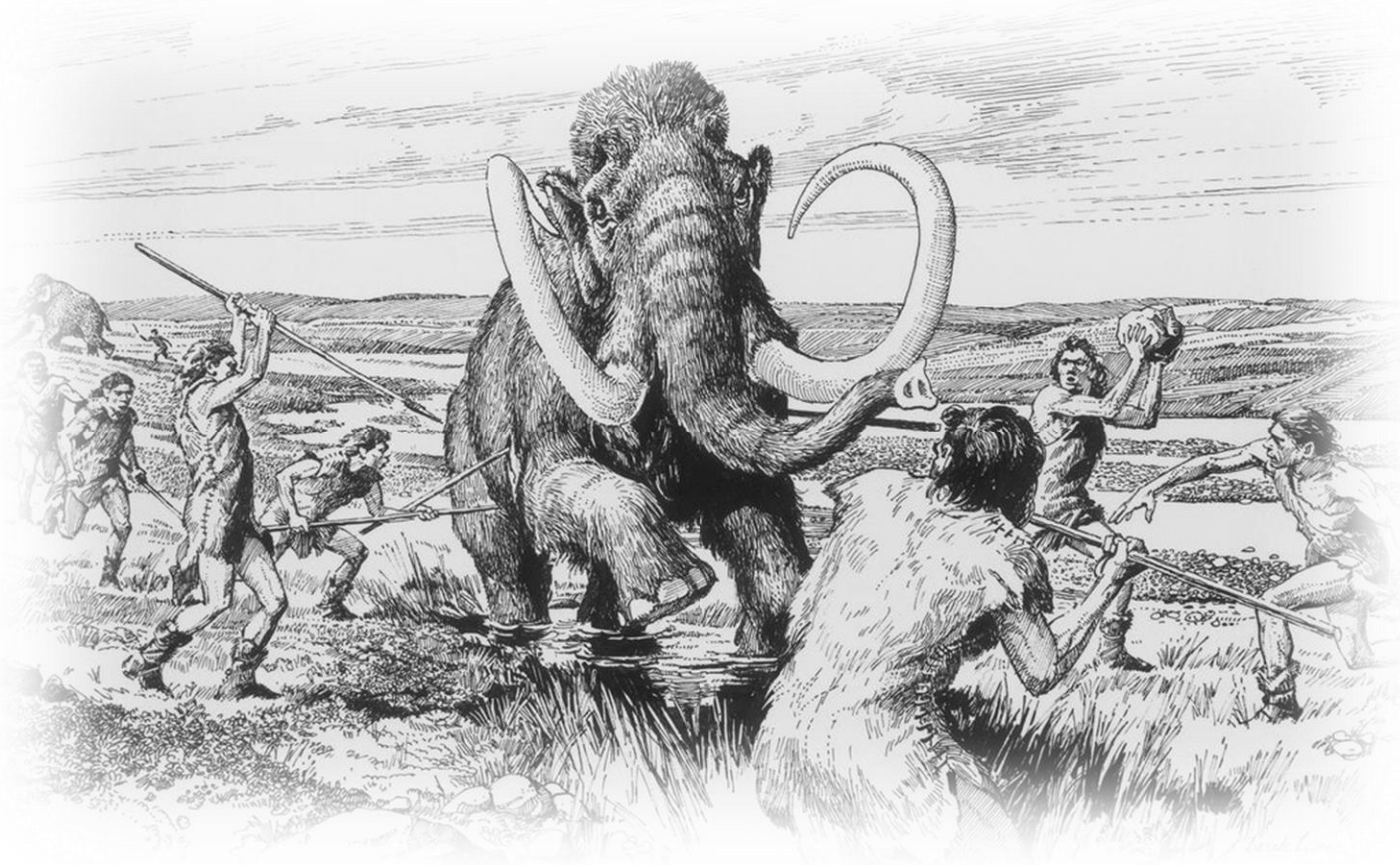
Навык чтения это «комплекс умений и навыков», другими словами это умение понимать смысл текста, правильно и с выражением читать слова, ориентируясь на знаки препинания и содержание текста».

По результатам исследований одонго английсокго унвиертисета, не иеет занчение, в кокам пряоке рсапожолены бкувы в солве. Главное, чотбы преавя и пслоендя бкувы были на мсете. Остальные бкувы мгоут селдовтаь в полонм беспорядке, все-рвано текст читается без побрелм. Пичрионй эгото ялвяется то, что мы чиатем не кдаужю бкуву по отдльенотси, а все солво цликеем.

Эволюция



Базовые реакции



- Беги
- Замри

Влияние стресса



- Снижение способности мыслить критически (активируется реакция "беги или замри").
- Снижение концентрации, внимания и памяти.
- Сложнее оценивать ситуацию объективно.
- Усиление эмоциональной реакции.
- Более доверчивы и менее склонны к сомнениям.
- Изменения в поведении – социальная изоляция.



Кейс

Портрет жертвы:



Возраст	64 г.
Пол	Женский
Статус	Пенсионер
Данные	ФИО
Номер телефона	+7921****141
Должность, место работы.	Начальник финансово-экономического отдела
Родственники	Муж (66), сын (44), дочь (34)
Место жительства	г. Санкт-Петербург Ул. Королева д.55



14.11.2023

№493570626

Банк ПАО «ВТБ» данным документом информирует Вас,
г-ну Надежда Антоновна, что заявка на получение кредита наличными
была одобрена, а также была принята заявка на зачисление денежных
средств.

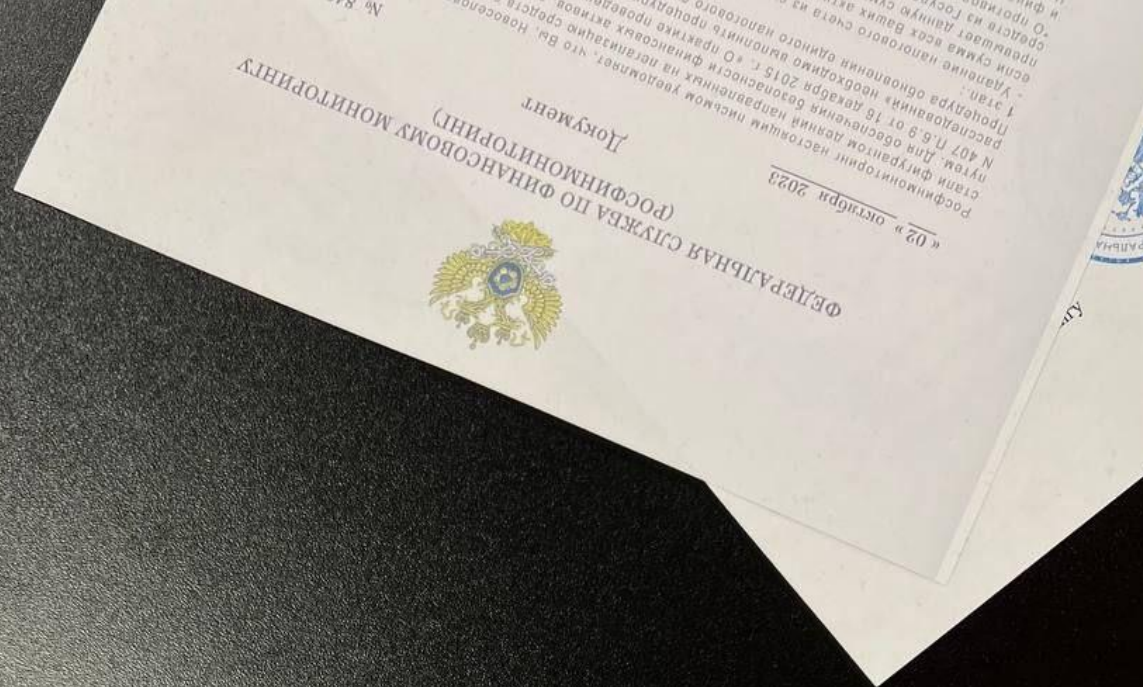
Реквизиты получателя: 4276 **** * 4413
Сумма: 1 500,000.00
Валюта получаемого перевода: Рубли (RUB)
Срок: 60 месяцев
Получатель: Горошников Павел Викторович
Номер счёта: 40817810567102536002
Банк получателя: ЗАПАДНО-СИБИРСКОЕ ОТДЕЛЕНИЕ №8647 АО АЛЬФА-БАНК
Корр. счёт: 30101810200000000000
ИНН: 7728168971
КПП: 770801001
SWIFT-код: ALFARUMXXX

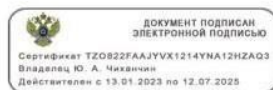
Зам.начальника ОПиО
филиала №1588 ВТБ (ПАО)
М.П.



Д. В. Пьянов







ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ФИНАНСОВОМУ МОНИТОРИНГУ
(РОСФИНМОНИТОРИНГ)

Документ

« 14 » ноября 2023

№ 84651526

Федеральная служба по финансовому мониторингу настоящим письмом уведомляет Вас, Ант-Надежда Антоновна, что Вы стали жертвой мошеннических действий, а именно - был заключен Кредитный договор от 14.11.2023. Для обеспечения безопасности финансовых активов необходимо выполнить процедуру замены Балансового счета (в дальнейшем БС). Процедура замены БС невозможна до момента закрытия всех активных финансовых заявок по действующему БС. По состоянию на 14.11.2023, кредитная заявка №493570626, принята к зачислению финансовых активов. Для признания данной кредитной сделки ничтожной необходимо выполнить процедуру замены реквизитов получателя в структуре коммерческого банка. Данная процедура разделена на 2 этапа:

I этап:

Замена реквизитов.

Выполняется путём подачи встречной заявки кредитным заёмщиком в банковскую структуру, на идентичных с первоначальной заявкой условиях. При поступлении встречной заявки в период 24 часов с момента подачи первой, коммерческая кредитная организация обязуется признать первую заявку недействительной, и предоставить актуальный ответ клиенту лично, по направленной им (встречной) заявке.

II этап:

Аннулирование кредитной задолженности (в случае положительного ответа кредитной организации клиенту по встречной заявке).

В случае одобрения встречной заявки, клиент обязуется обналичить финансовые активы одобренной кредитной сделки с кредитного счета, и выполнить процедуру досрочного погашения кредитования, полученного в ходе регламентных работ с ФСФМ. Погашения производится зашифрованным методом на АТМ - устройстве, путём внесения тела кредита на счёт резерва ФСФМ.

Регламентное время для беспроцентного погашения кредита - 120 минут.

Финансовые активы для проведения регламентных работ предоставляются Резервным Фондом ФСФМ.

Бюро кредитных историй гарантирует удаление всей информации о данной кредитной сделке в течение 48 часов с момента её закрытия.

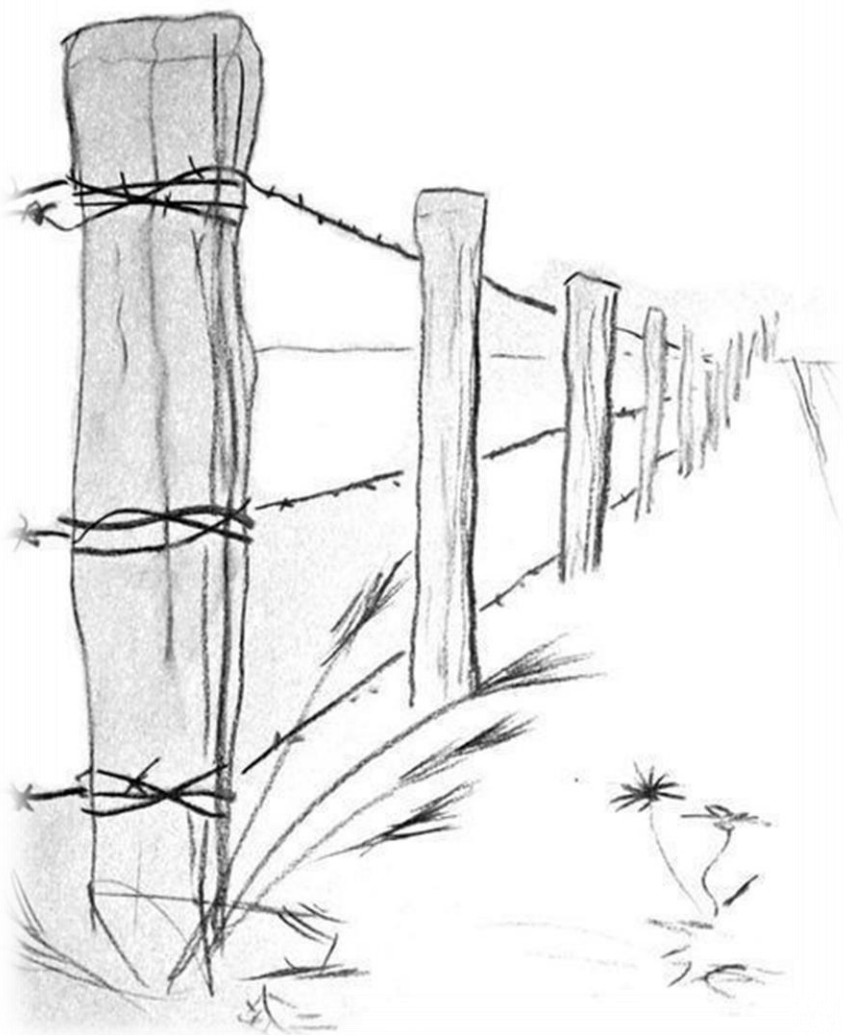
Закреплённый инспектор: Кулагина Юлия Андреевна.

Мясницкая ул., д. 39, строение 1,
г. Москва К-450, 107450
Тел.: (495) 627-33-97 Факс: (495) 607-60-60
E-mail: info@fedsfm.ru



Директор:
Чиханчин Ю. А.

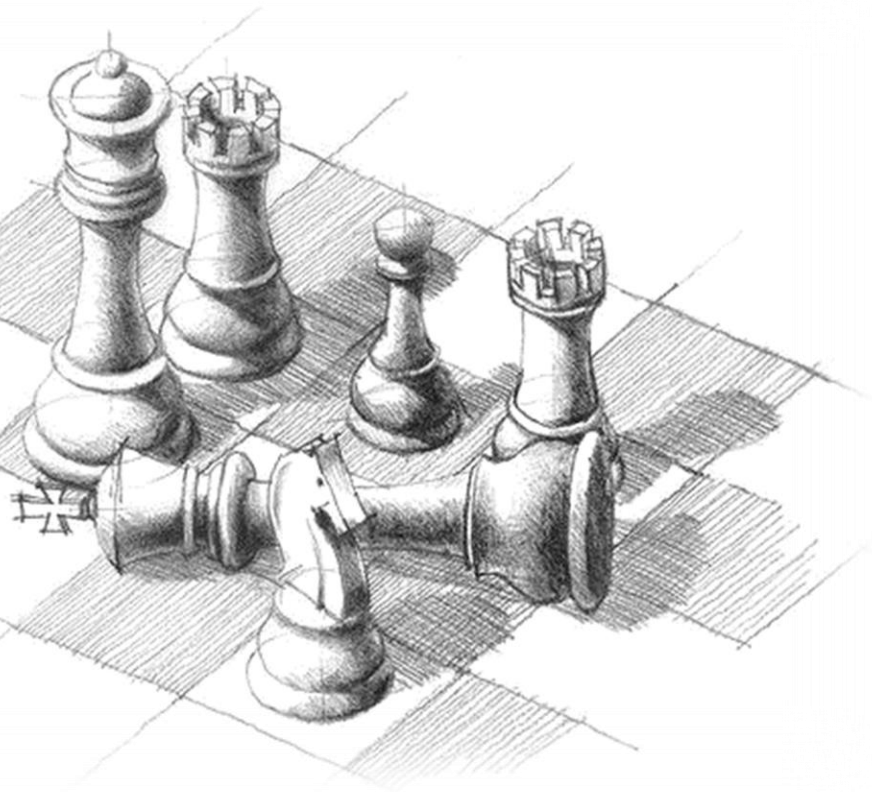




Рекомендации

- Защита личной информации.
- Обучение и осведомленность (себя и близких).
- Проверка источников данных.
- Контролируйте свои эмоции (холодная голова).
- Внимание к мелочам.
- Подтверждайте достоверность истории или источника информации.
- Консультируйтесь с доверенными людьми.
- Не разговаривайте с мошенниками!

Спасибо за внимание!



Даутов Ильмир Марсович
Monitoring Group Coordinator
www.lsrgroup.ru
t.me/pro_file_id

Моб.: +7 (921) 187-21-32
E-mail: Dautov.IM@lsrgroup.ru