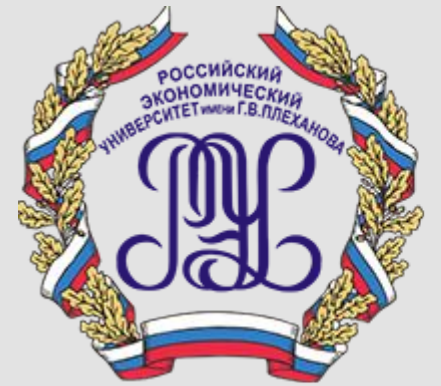


"Современные методы и техники «выведывания» информации"

Креопалов Владимир Владиславович, к.т.н.



План лекции

- Выведывание, как метод получения информации
- Методики используемые в процессе выведывания.
- Практический подход к получению информации от собеседника в процессе общения.
- Почему тактика выведывания столь действенна.
- Противостояние попыткам выведать информацию.



ВЫВЕДЫВАНИЕ

Контрразведывательный словарь. — Высшая краснознаменная школа Комитета Государственной Безопасности при Совете Министров СССР им. Ф. Э. Дзержинского. 1972.

Выведывание - метод получения фактической информации, заключающийся в целенаправленных беседах агента (доверенного лица, оперативного работника) с разрабатываемым (проверяемым) или его связями, в ходе которых, используя **закономерности психологии** (ассоциации по аналогии, по смежности и т. п.), а также **психические особенности личности собеседника**, выведывающий подводит его к непреднамеренному и непринужденному сообщению скрываемых сведений.

Методом выведывания пользуются также разведчики и агенты разведок капиталистических государств при добывании разведывательной информации.

Этот метод преследует несколько определенных целей:

1. Его применение должно привести к тому, что собеседник будет **самостоятельно**, инициативно делиться нужной нам информацией, давая ответы на наши вопросы (которых мы не задавали вслух) **прямо** или **косвенно**.
2. Наш собеседник не должен осознавать наш истинный интерес по отношению к нему, который необходимо надежно «**замаскировать**» в беседе.
3. Для того чтобы выполнялось первое и второе условие, сам факт коммуникации должен выполнять для нашего собеседника определенную функцию и иметь значение.

В идеальном виде такое общение должно нести нашему собеседнику некий удовлетворительный результат. Ибо если человек остался доволен беседой (скажем, победил в споре; получил признание своих незаурядных качеств; завел новое интересное знакомство, и т.д.), то он не будет искать дополнительных объяснений причинам состоявшейся беседы. А значит, наша истинная цель останется не раскрытой.

Техники выведывания

Процесс выведывания лежит на стыке:

- Методик психологии;
- Социальной инженерии;
- Нейро-лингвистического программирования (НЛП);
- Калибровки;
- Межличностного общения.

Н Л П

Упрощенно можно определить **НЛП** как систему для познания и изменения человеческого поведения и мышления.

Некоторые методики НЛП могут быть использованы (и используются) для скрытого управления человеком, включая, конечно, и манипулирование им.



Межличностное общение

Взаимодействие между людьми может быть охарактеризовано как **межличностное**, если оно удовлетворяет следующим критериям:

- в нем участвует *небольшое число людей* (чаще всего - группа из 2-3 человек); это *непосредственное взаимодействие*: его участники находятся в пространственной близости, имеют возможность видеть, слышать, касаться друг друга, легко осуществляют обратную связь; это так называемое *личностно-ориентированное общение*; предполагается, что каждый из его участников признает незаменимость, уникальность своего партнера, принимает во внимание особенности его эмоционального состояния, самооценки, личностных характеристик. Перечисленные критерии позволяют отличить межличностное общение как особый вид от межгруппового и массового общения, обозначить границу, отделяющую личностно-ориентированное общение от социально-ориентированного.

Чем менее стереотипным является восприятие людьми друг друга, чем глубже уровень взаимного самораскрытия партнеров, чем больше разнообразных и уникальных событий наполняют историю их отношений, тем корректнее будет назвать данное общение **межличностным**.

Межличностное общение - осуществляемое с помощью средств речевого и неречевого воздействия взаимодействие между несколькими людьми, в результате которого возникают психологический контакт и определенные отношения между участниками общения.

Калибровка

Коротко - это функция, сопоставления делений шкалы (на приборе) со значениями измеряемой величины.

Представьте, перед вами - незнакомый градусник. Он показывает 40 градусов. Много это или мало - хочется узнать. По Фаренгейту? По Цельсию?

*Вот Вы и произвели калибровку...
Человека тоже можно представить в виде прибора, чей язык вам пока неизвестен.*

С помощью
калибровки мы
можем узнать
как **данный**
человек
(интересующи
й нас):

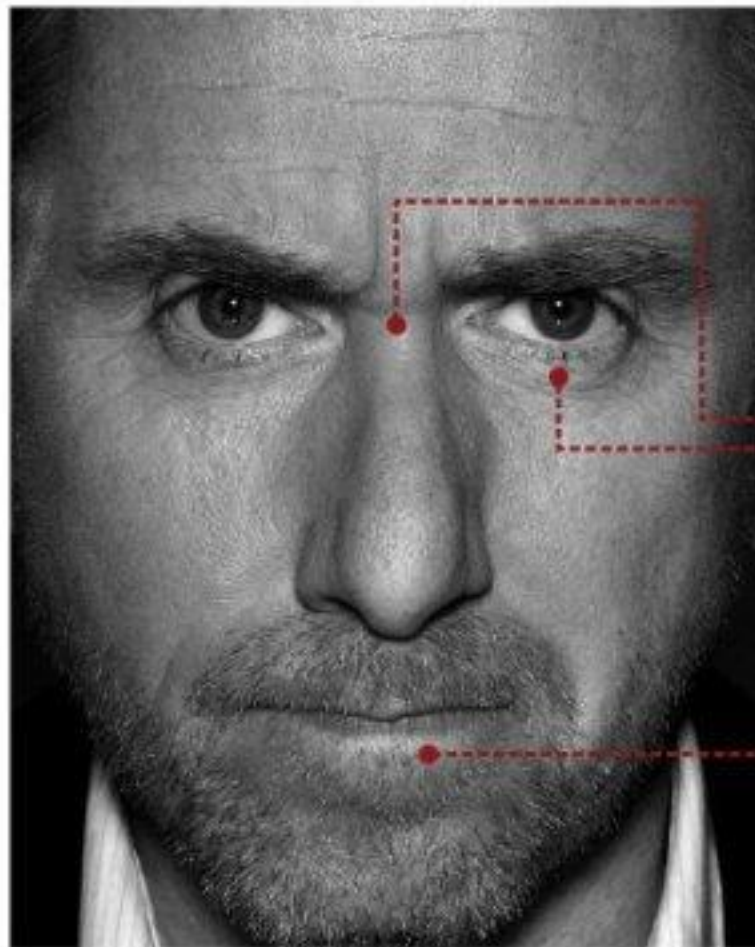
- перерабатывает информацию,
- как он входит в некое эмоциональное состояние,
- как он выходит из него.

КА Л И Б Р О В К А



Калибровка состояний другого человека - вещь долгая и серьёзная. Virtuozы умеют калибровать другого человека в ходе лишь получасовой беседы с ним и знать о нём практически всё - когда он врёт, когда вспоминает что-то приятное и т.д.

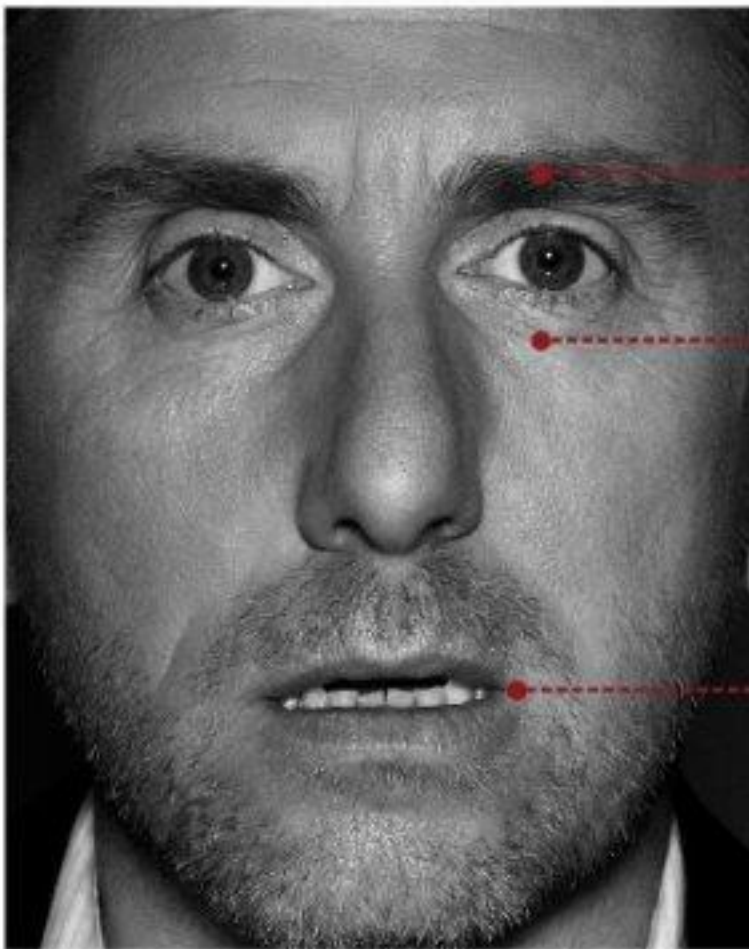
ЭМОЦИЯ ГНЕВ



Гнев

- ① Брови опущены и сведены вместе
- ② Блеск в глазах
- ③ Рот закрыт, губы сужены

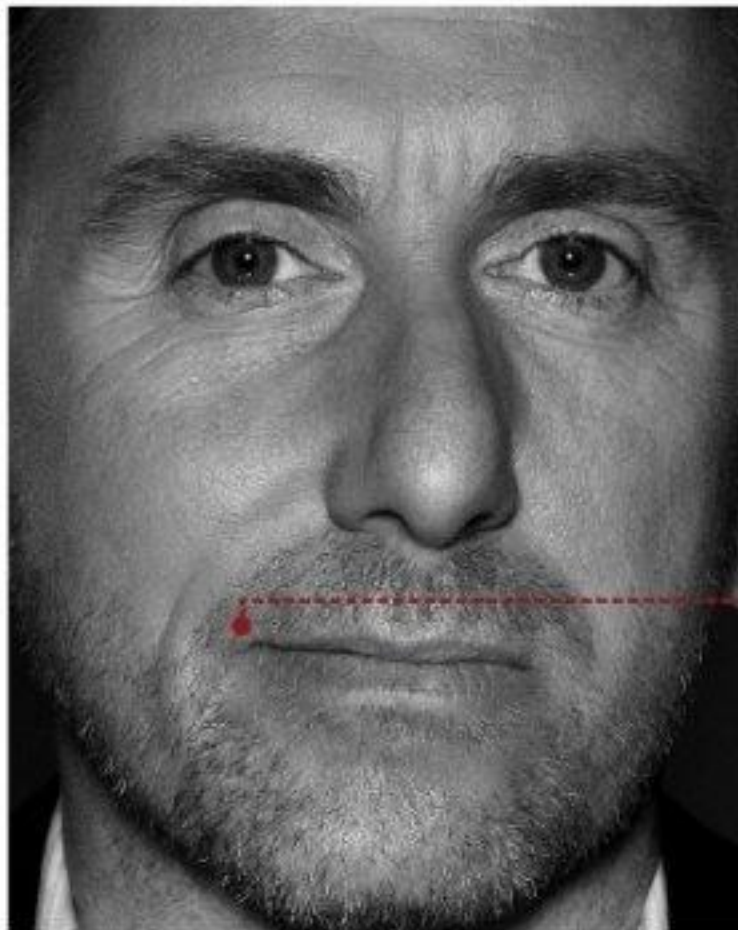
ЭМОЦИЯ УДИВЛЕНИЕ



Удивление

- ① Брови приподняты
- ② Глаза широко раскрыты
- ③ Рот приоткрыт

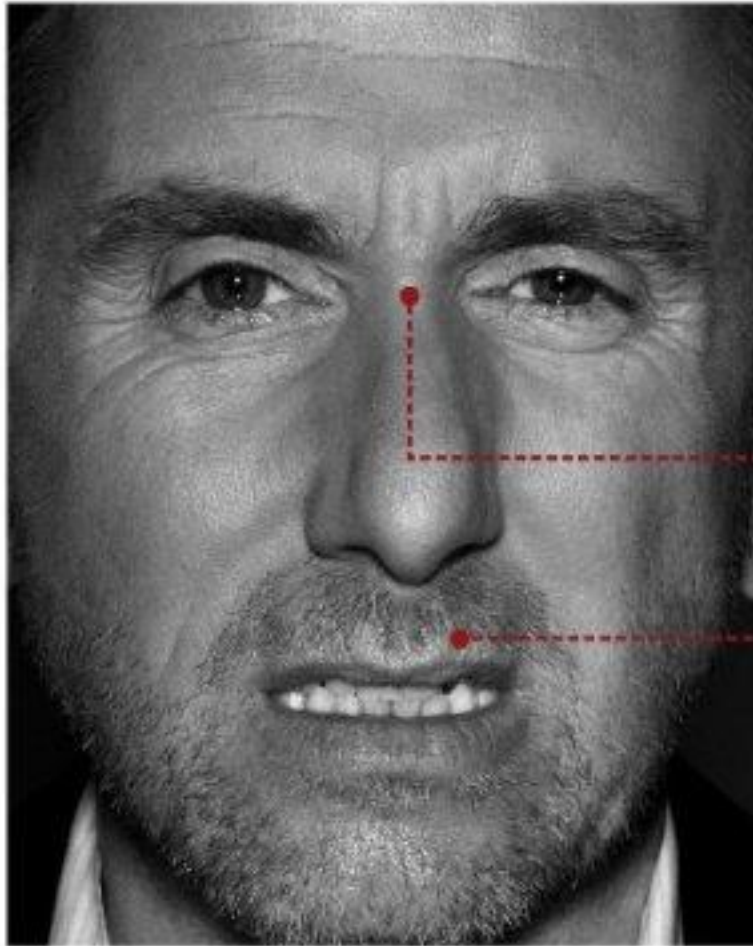
Эмоция ПРЕЗРЕНИЕ



Презрение

① Приподнятый уголок рта с одной стороны

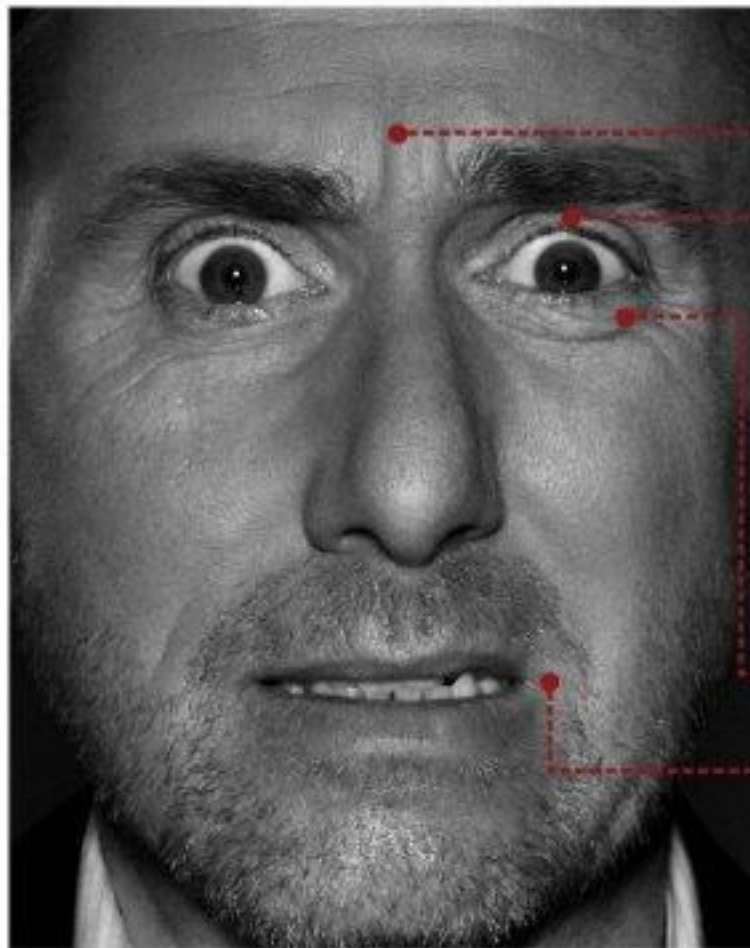
ЭМОЦИЯ ОТВРАЩЕНИЯ



Отвращение

- ① Сморщенное выражение лица
- ② Верхняя губа приподнята

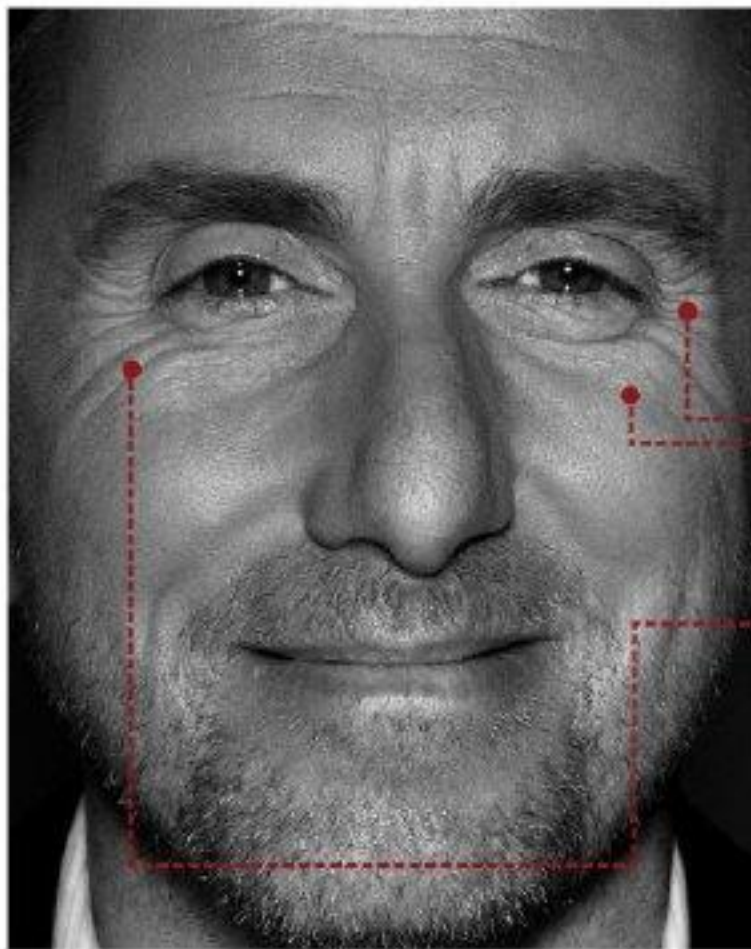
ЭМОЦИЯ СТРАХ



Страх

- 1 Брови приподняты и вытянуты
- 2 Верхние веки приподняты
- 3 Нижние веки напряжены
- 4 Губы немного вытянуты

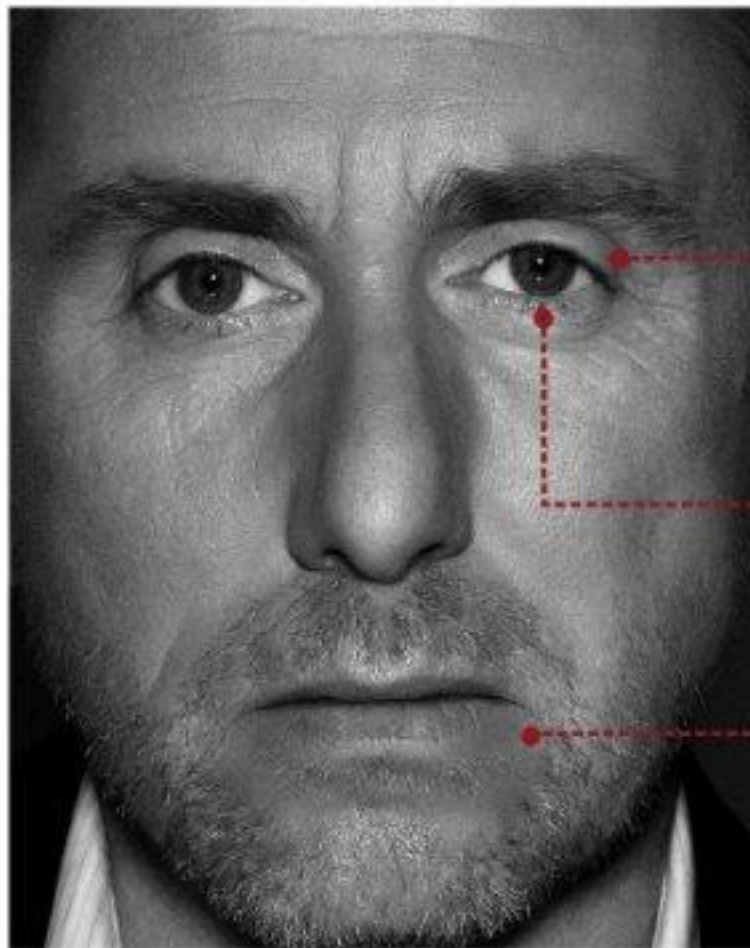
Эмоция СЧАСТЬЕ



Счастье

- ① Небольшие морщинки в уголках около глаз
- ② Щёки приподняты
- ③ Задействованы мышцы вокруг глаз

Эмоция ПЕЧАЛЬ



Печаль

- ① Верхние веки слегка опущены
- ② Рассеянный взгляд
- ③ Уголки рта слегка опущены

Социальная инженерия

Этот метод основан на использовании слабостей человеческого фактора и считается **очень разрушительным**.

Злоумышленник получает информацию, например, путем сбора информации о служащих объекта атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего. Злоумышленник может позвонить работнику компании (под видом технической службы) и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе. Очень часто этот трюк проходит.

Самое сильное оружие в этом случае — приятный голос и актёрские способности. Злоумышленник под видом служащего компании звонит в службу технической поддержки. Представившись от имени служащего, он просит напомнить свой пароль, либо меняет его на новый, сославшись на забывчивость. Имена служащих удается узнать после череды звонков и изучения имён руководителей на сайте компании и других источников открытой информации (отчётов, рекламы и т.п.). Дальше дело техники.

Используя реальные имена в разговоре со службой технической поддержки, злоумышленник рассказывает придуманную историю, что не может попасть на важное совещание на сайте со своей учетной записью удаленного доступа. Другим подспорьем в данном методе являются исследование мусора организаций, виртуальных мусорных корзин, кража портативного компьютера или носителей информации.

Техники и термины социальной инженерии

Претекстинг - это действие, отработанное по заранее составленному сценарию (претексту). В результате цель должна выдать определённую информацию, или совершить определённое действие. Этот вид атак применяется обычно по телефону.

Чаще эта техника включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований (например, персонализации: дата рождения, сумма последнего счёта и др.), с тем, чтобы обеспечить доверие цели.

ФИШИНГ

- техника, направленная на жульническое получение конфиденциальной информации.

Обычно злоумышленник посылает цели e-mail, подделанный под официальное письмо - от банка или платёжной системы - требующее "проверки" определённой информации, или совершения определённых действий. Это письмо обычно содержит линк на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и контентом, и содержащую форму, требующую ввести конфиденциальную информацию - от домашнего адреса до пин-кода банковской карты.

Выведывани е через социальные сети

Размещая информацию о себе, своих родных, своей компании и т.д., мы не задумываемся о то кто и как её может использовать.

Причём размещаем абсолютно добровольно, не задумываясь о вопросах безопасности.



Выведывани е через социальные сети

Агент, который ведёт беседу должен обладать рядом способностей. Он должен максимально раскрыть собеседника и в тоже время не выдать истинных намерений.

Сначала за объектом наблюдали со стороны, подмечая его привычки, манеру общения и т.д. Изучали особенности через общение с его окружением и только собрав достаточно сведений входили в прямой контакт.

С появлением социальных сетей вся работа в том числе и подготовительная гораздо упростилась. Можно очень подробно изучить привычки, особенности, пристрастия и др. изучая персональную страничку в соцсети. Социальные сети, это не только способ общения и обмена информацией, но и средство самовыражения. Кроме этого социальные сети для многих являются чем-то вроде онлайн дневников, в которых они делятся своими мыслями и наблюдениями, а также местом для хранения фотографий и других файлов.

В общем, всего лишь на одной страничке содержится столько информации о человеке, что иногда по ней можно увидеть практически весь его жизненный путь, ну и, конечно же, на основании социальной страницы можно сделать несколько предположений и о характере ее обладателя.

Практический подход к получению информации от собеседника в процессе общения

- Демонстрация осведомлённости;
- Выдвижение ложного тезиса, побуждение к спору;
- Использование легенды;
- Шок, замешательство (прием, который базируется на "перегрузе" восприятия человека, который вынуждает его снизить "бдительность" и случайно выдать скрываемую информацию);
- Прием забалтывания;
- Использование тщеславия и выражение сочувствия;
- Прием Коломбо;
- Прием игры на чувствах.

Почему тактика выведывани я столь действенна

Среди естественных аспектов, которые доступны опытному манипулятору, выделяют следующие:

- Желание казаться доброжелательным и любезным даже по отношению к малознакомым людям;
- Желание казаться хорошо информированным, особенно в профессиональных вопросах ;
- Желание человека ощущать свою востребованность и знать, что он вносит свой вклад в важное дело;
- Тенденция не ограничиваться рамками конкретной темы, поощряя чьи-то заслуги, либо пытаюсь представить что-либо в более выгодном свете;
- Склонность к распространению слухов ;
- Склонность недооценивать значимость информации, которой интересуются другие, особенно, если неизвестно, каким образом ее могут использовать;
- Склонность верить в честность и искренность других людей;
- Некоторые люди становятся более искренними, когда собеседник использует такие фразы, как «между нами», «не для протокола»;
- Желание показать преимущества своей позиции.

Противостояние попыткам вывести информацию

Необходимо знать, какого рода информацию не следует обсуждать с посторонними и быть бдительным во время бесед с людьми, которые ищут такие сведения. Не обсуждайте информацию с людьми, не имеющими к ней непосредственного отношения, включая личные сведения, касательно вашей семьи, либо ваших коллег по работе.

Вы можете
вежливо
отразить
попытку
выведать
тайные
сведения:

- Сказав, что они доступны в открытых источниках (сайты, пресс-релизы)
- Ответив на вопрос любым контрвопросом
- Спросив: «Чем вызван ваш интерес?»
- Ответив неопределенно
- Сказав, что не знаете ответа
- Сказав, что вы можете разъяснить конкретный вопрос в отделе службы безопасности
- Заявив, что не уполномочены обсуждать подобные вопросы
- Игнорируйте любой вопрос, или утверждение, которое, по вашему мнению, является неуместным и не относится к предмету разговора

По итогам лекции

Тестовые вопросы

- Что такое выводывание?
- На стыке каких технологий появилась эта методика?
- Почему тактика выводывания столь действенна?
- Как противостоять попыткам вывести информацию?



По итогам лекции



Основные определения

Тактика выведывания - это специфическая беседа, с помощью которой можно узнать о сведениях, недоступных на текущий момент в открытых источниках, действуя таким образом, тайный агент не вызовет подозрений в отношении своего интереса к определенным фактам. Как правило, данный способ манипулирования легко маскируем, на посторонний взгляд он не представляет собой большой угрозы, человеку, использующему этот метод, не составит большого труда опровергнуть обвинения в свой адрес и, что наиболее важно, такая тактика чрезвычайно эффективна. Манипулирование может проявляться как в устной и телефонной беседе, так и во время переписки по электронной почтой.

Если выведывание информации осуществляется хорошо подготовленным специалистом, этот процесс покажется всего лишь обычным разговором на отвлеченную тему, социальную или профессиональную. Человек может не отдавать себе отчета в том, что он стал мишенью, или что передал значимые сведения. Поэтому если вы предполагаете, что кто-то намеревался узнать у вас информацию, относящуюся к категории «секретно», в особенности о вашей работе, используйте систему противодействия вежливо отразите попытки выведать тайные сведения и сообщите представителям службы безопасности.

Спасибо за
внимание!

