«Социальная инженерия или человеческий фактор в информационной безопасности»

Спикер:

Гриценко Ольга Александровна

Психолог, семейный психолог, психотерапевт (метод КПТ), клинический психолог, практический психолог

Социальная инженерия - это совокупность методов и тактик воздействия, основанных на **психологическом манипулировании**, с целью контроля поведения человека и получения доступа к конфиденциальной информации.

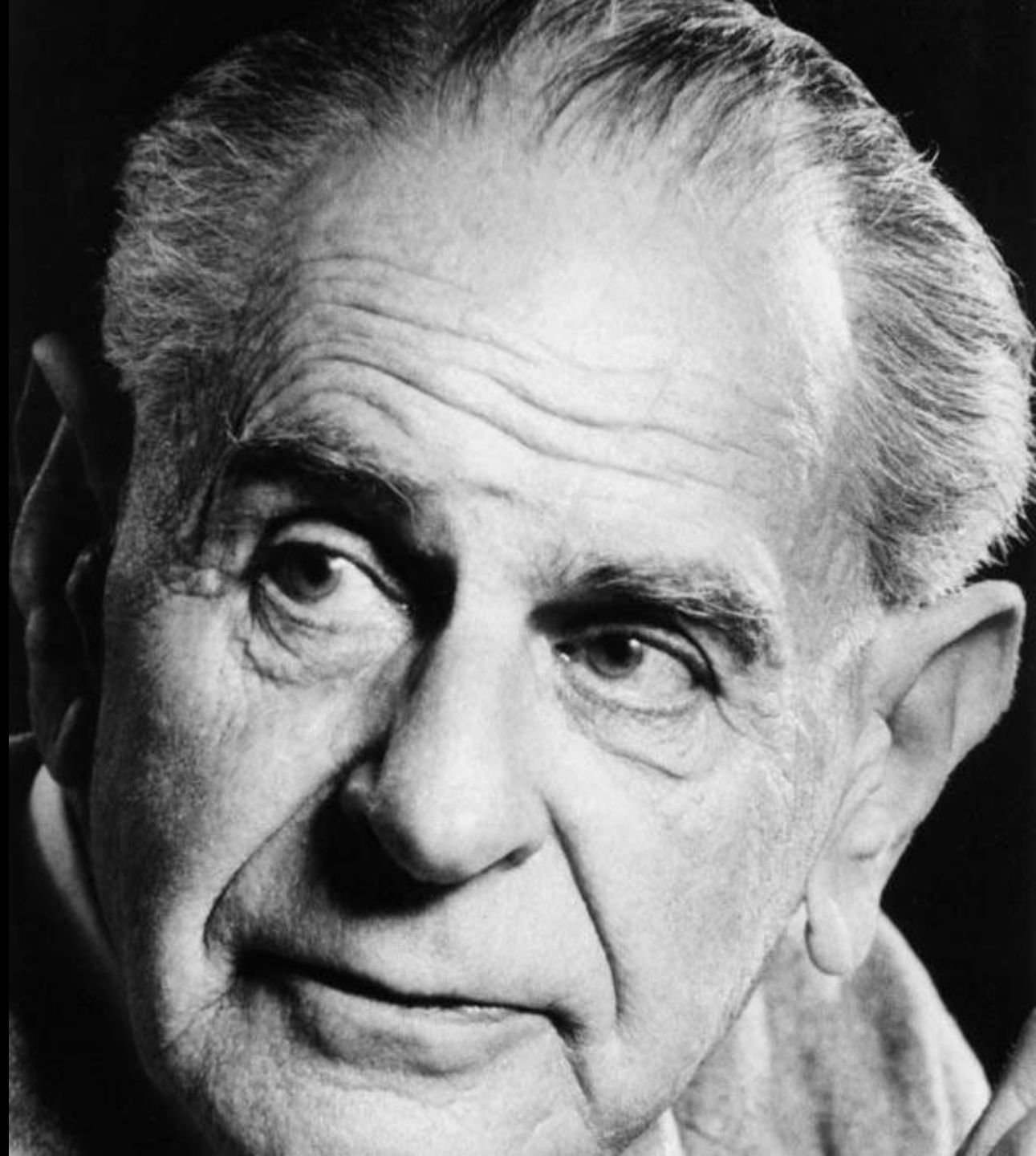
Метод основан на использовании слабостей человеческого фактора и считается крайне разрушительным, так как злоумышленник вторгается в личные границы человека.

.

Карл Поппер (1902-1994 гг)- австрийско-британский философ.

Впервые термин социальная инженерия был введён в книге Поппера **«Открытое общество и его враги»** («The Open Society and Its Enemies», 1945).

К. Поппер считает, что социальная инженерия ориентирована на управление социальными институтами которые могут изменяться без применения насилия, только при наличии демократии.



Алексей Капитонович Гастев (1882-1939гг) – русский революционер, руководитель Центрального института труда.

В 1921 г. ввел понятие социальной инженерии, предложив в своей статье по организации труда в социалистическом хозяйстве, новый тип работника, который меняется с логикой движения технологий (работа в системе человек-машина)

С развитием технологий термин социальная инженерия получает несколько иное значение

Кевин Митник — знаменитый социальный инженер, американский хакер.

Социальная инженерия — это манипулирование людьми, в том числе психологическое. Цель — заставить их совершить определённые действия или сообщить конфиденциальную информацию.

Митник был мастером социальной инженерии. Он мог обманом заставить людей выдавать ему важные данные или доступ к системам.

В 2001 году Митник написал книгу «Искусство обмана», посвящённую социальной инженерии. В ней он привёл множество примеров того, что проникнуть в информационную систему путём обмана человека значительно проще, чем путём взлома.

Принципы социальной инженерии строятся вокруг того, как люди думают и действуют. Главная задача — сыграть на чувствах и слабостях человека, вывести его из психологического равновесия, а после заставить сделать определенные действия.

ЭТАПЫ:

01 **Подготовка**. Мошенники предварительно изучают конкретного человека либо группу людей, например сотрудников определенной компании. Большинство информации, как правило, есть в открытом доступе: корпоративные сайты, фото и посты в социальных сетях.

02 **Установление контакта**. Инициировав взаимодействие, преступник строит доверительные отношения. Для этого мошенники апеллирует к каким-то фактам, событиям и информации, имеющим отношение к человеку или группе. Это имена и фамилии друзей, начальника или сведения о сделке, которую недавно провела компания.

03 **Начало атаки**. Как только доверие установлено, жертву атакуют. Например, просят перейти по ссылке, переслать письмо, открыть зараженный файл или перевести деньги.

04 **Отключение**. Сразу после того как пользователь выполняет требования, все контакты прекращаются. Через некоторое время пострадавший осознает, что его обманули. Но иногда атака может оставаться незамеченной длительно. Вплоть до момента, пока хакер сам не разоблачит себя.

Техники социальной инженерии:

Фишинг

- Кибератака с сообщениями, которые выглядят или звучат так, будто их отправила заслуживающая доверия организации или даже знакомый лично человек. Это может быть замаскированное письмо от банка, госструктуры, начальника или кого-то из коллег, родственников. В нем жертву просят перейти по ссылке, чтобы скачать приложение, открыть файл. Например, сообщение с подписью «Это ты на фото?». Наиболее распространен фишинг в e-mail-рассылках (массовые или целевые), соцсетях, смс или даже голосовых сообщениях. Последние мошенники генерируют при помощи ИИ на основе аудиосообщений владельцев взломанных в мессенджерах аккаунтов. В итоге человек получает голосовое, в котором его знакомый своим голосом, например, просит деньги в долг.

Страшилка

- Начинается с фишингового письма или всплывающего окна браузера, которое должно запугать пользователя и заставить немедленно выполнить что-то. Для этого в тексте чаще содержится угроза. Например, предупреждение, что обнаружены вирусы. Для правдоподобности мошенники используют логотипы реальных компаний

Техники социальной инженерии:

Претекстинг

Это социоинженерная схема по заранее отработанному сценарию (от англ. слова предлог). Мошенник звонит или пишет жертве, представляясь начальником, сотрудником банка, полиции или госструктуры. В беседе он обязательно упоминает какие-то личные факты или сведения, имеющие отношение к работе. Жертве сообщают, что возникла некая проблема (взломали данные сотрудников фирмы, совершена атака на счета в банке) и для ее решения нужна помощь. Чтобы усыпить бдительность хакеры, используют поддельные аккаунты, почтовые адреса и номера телефонов, а также сгенерированные ИИ видео. Целью атаки чаще бывают финансовые данные: номера карт

Техники социальной инженерии:

Услуга за услугу

Это форма социальной инженерии, когда злоумышленники предлагают услугу или выгоду в обмен на конфиденциальную информацию или доступ. Например, участие в опросе за вознаграждение. Однако в процессе общения мошенник постарается выяснить важную для себя информацию. Еще один сценарий — звонок из службы поддержки компании. Подставной сотрудник интересуется у жертвы о каких-либо проблемах с компьютером и доступом к системе, уверяя, что сбой затронул многих работников офиса. После он просит помочь разобраться в проблеме и, например, подробно описать процесс входа в систему.

Дорожное яблоко

Этот вид мошенничества строится на обычном любопытстве. Схема предельно проста: в офис компании подбрасывают флешку, на которой написано что-то завлекающее. Например, «Данные о зарплатах начальства» или «Списки сотрудников на увольнение». Далее преступникам остается только ждать, когда кто-то из сотрудников найдет ее и из любопытства вставит в свой компьютер.

Обратная социальная инженерия

Злоумышленник сначала создает проблему ("ломает" устройство), а затем предлагает помощь — в итоге пострадавшие сами дают ему доступ.

Возникает вопрос — в чем отличие от других методов социальной инженерии. Все очень просто: жертва сама обращается к атакующему, а не наоборот. Как будто это ее инициатива, а значит, мошенника вроде бы и не в чем обвинить.

На сайте МВД России есть специальный раздел «Внимание, мошенники!». В нем даются общие рекомендации, касающиеся безопасности пользования Интернетом при проведении финансовых операций, а также содержится информация о том, как действовать, чтобы не стать жертвой телефонных мошенников.

С одной стороны, рекомендации помогают посетителям сайта МВД избежать участи жертв, с другой, — отчасти и самим мошенникам совершенствовать свое «мастерство».

Ведь любая рекомендация одновременно приоткрывает те «уязвимые места», по поводу которых она дается, особенности групп риска, которым она адресована и т.д.

Иными словами, принцип «предупрежден — значит, вооружен» здесь может работать неоднозначно.

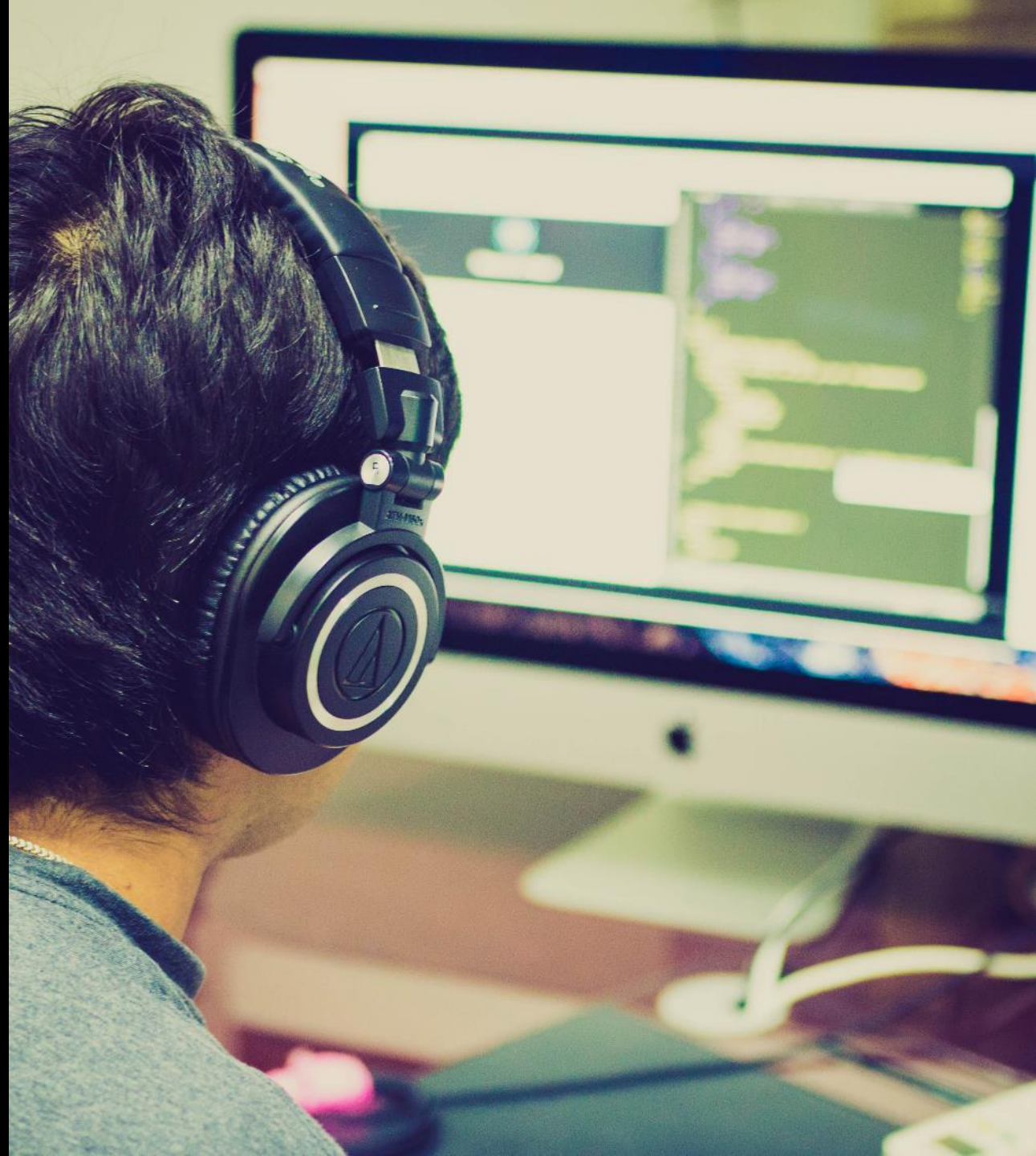
Психологический портрет лиц, совершающих преступления в сфере информационной безопасности

01 Возраст от 18 до 25 лет, мужчина, чаще воспитывался в «неполной» семье

02 Характерны сложные отношения с окружающими из-за этого имеют ярко выраженную потребность принадлежать к какой-нибудь группе ;

Занимаются индивидуальными формами деятельности; В общении для них характерны холодность, конфликтность, обидчивость и пониженная эмоциональность.

03 Характерна низкая самооценка, тревожность, склонность к депрессии, ощущающие свою незащищенность. Поэтому пребывание в "виртуальном" мире дает чувство уверенности. Их вдохновляют анонимность, отсутствие прямых контактов. Здесь эти личности могут изображать из себя того, кем они хотели бы быть в действительности. Сетевая среда является для них в определенной степени средством для бегства от действительности, в которой они чувствуют себя неуверенно.

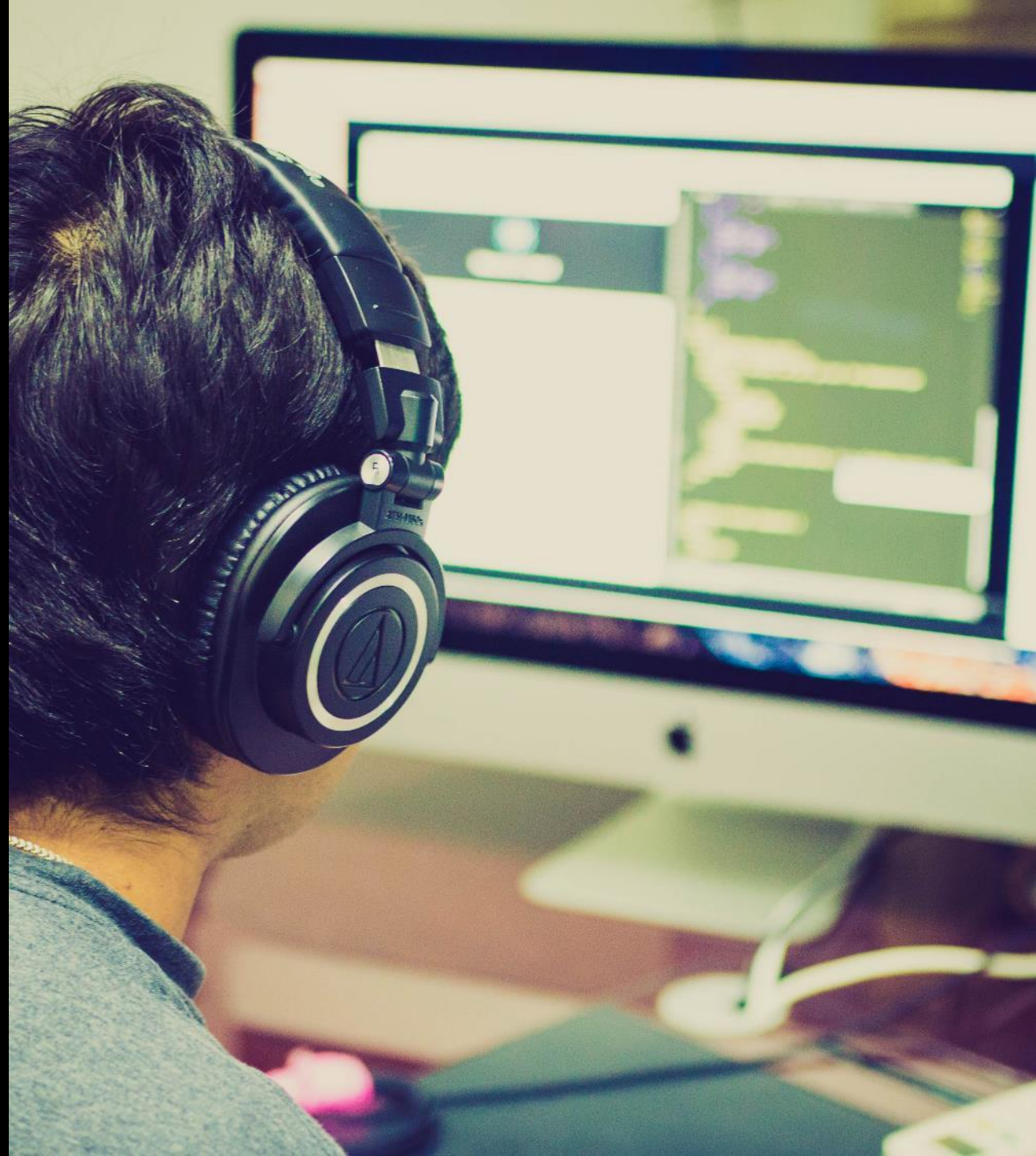


Психологический портрет лиц, совершающих преступления в сфере информационной безопасности

04 Наличие специфических положительных свойств: высокий уровень абстрактного мышления, познания в области информационных технологий, высокая работоспособность, упорство (настойчивость и методичность в достижении поставленных целей иногда даже граничат с параноидальностью)

05 Навязчивая потребность осуществлять «взлом». Данная потребность наблюдалась и у К. Митника. Выносивший приговор судья объявил, что видит определенную параллель между его пристрастием к взлому компьютерных сетей и влечением других людей к наркотикам!. В 46% изученных уголовных дел, возбужденных в России по фактам сетевых преступлений, обвиняемый в той или иной мере связывал свои действия с подобными мотивами.

Психопедагогика в правоохранительных органах №2 (2024)
А.Л. Осипенко Омская Академия МВД России



Самая большая дыра в информационной безопасности сидит напротив монитора

Психологический портрет жертв социальной инженерии

01 Люди до 50 лет: оптимизм, экстраверсия, открытость новому, развитый эмоциональный интеллект.

02 Люди старше 50 лет: интересы группы выше собственных, мотивированность, надежность

03 У всех групп:

Высокий уровень сотрудничества (доброта, доверчивость, теплота);
Высокий уровень самоконтроля;
Низкий уровень критичности;
Низкий уровень воображения;
Значимость ценностей безопасности (страх потерять имеющееся, а не потребность в обогащении)

Пирамида А. Маслоу

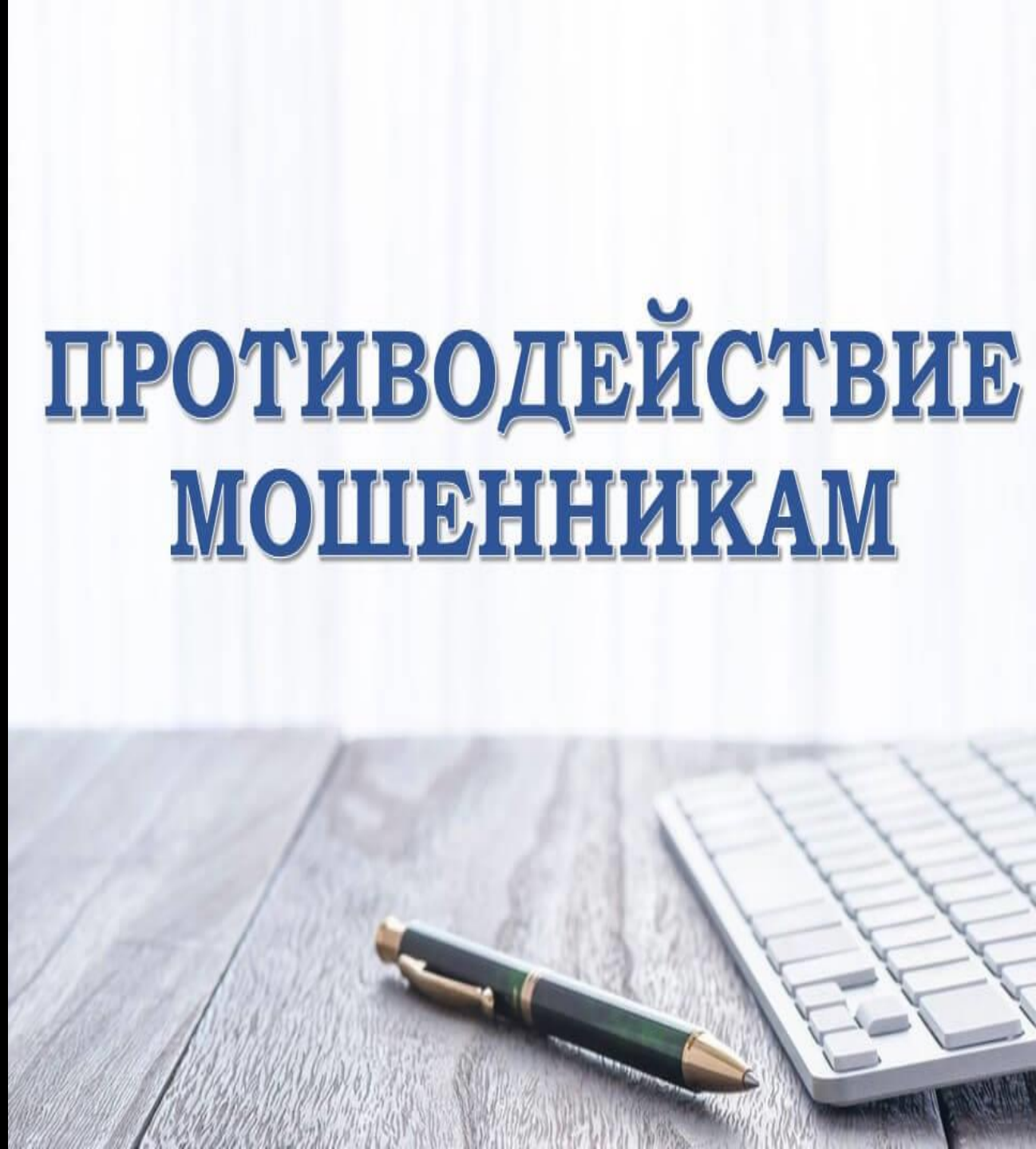
5. Самореализация (творчество, развитие)
4. Уважение (статус, признание, карьера, «быть лучшим»)
3. Социальные потребности (принятие, принадлежность к обществу)
2. Потребность в безопасности (уверенность в завтрашнем дне, стабильность, возможность отдыхать
1. Физиологические потребности (еда, тепло, жилье, секс)

Признаки манипуляции

1. Нарушение этикета (обращение к вам в неудобный момент, навязывание темпа разговора);
2. Появление внезапных чувств (вины, опасности, страха, паники, жалости);
3. Четкое осознание вами, что вы не в безопасности;
4. Наличие ограниченности во времени

Способы противостояния манипуляции:

- Тестирование (проверка) реальности;
- Замедление (отстранение);
- Заземление;
- Дыхание;
- Прогнозирование нескольких вариантов развития событий (не менее 2 сценариев);
- Сказать «нет» несколько раз;
- Бесконечное уточнение (верно я вас понимаю, вы хотите сказать, что…)



Тестирование(проверка) реальности

Вопросы самому себе:

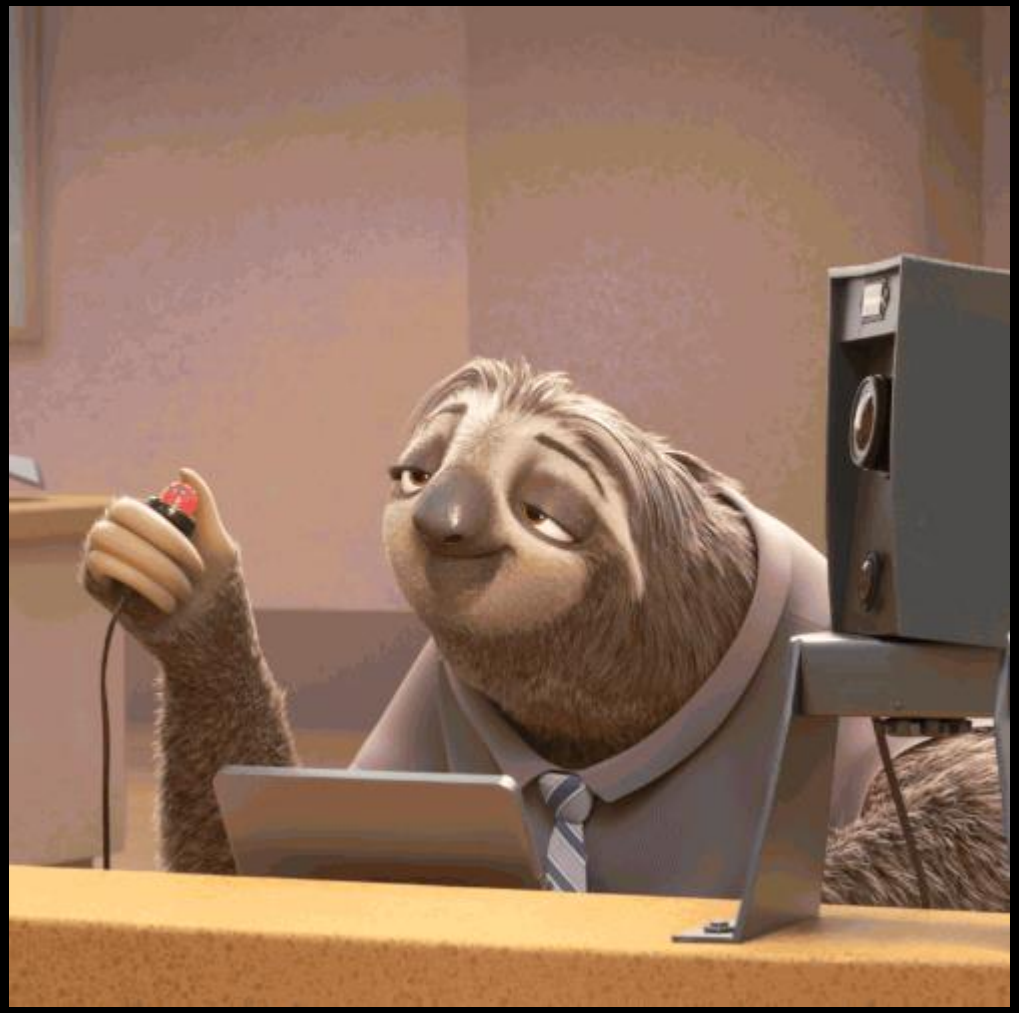
1. Где я сейчас нахожусь? Что меня окружает? Кто рядом со мной?
2. Что я знаю про моего оппонента? Есть ли доказательства тому, что я могу ему доверять?
3. Какие факты я знаю, вижу, слышу?
4. Что я сейчас чувствую? (страх, тревога, интерес);
5. Что я сейчас думаю?
6. Какие есть доказательства того, что эта мысль верна/не верна?
7. Что самое лучшее/худшее может произойти?
8. Что скорее всего случится?
9. Если бы мой друг, знакомый, родной человек попал в аналогичную ситуацию, чтобы я ему сказал?

Тестирование реальности - это когнитивный процесс, который предполагает оценку точности наших мыслей и убеждений по сравнению с реальным миром. Он опирается на критическое мышление, фактические данные и объективность, чтобы понять, являются ли наши мысли объективными (соответствует ли наше восприятие ситуации реальной действительности).

Вы не обязаны верить каждой мысли, которая приходит вам в голову. (Р. Лихи).

Замедление:

1. Делайте намеренные паузы;
2. Попытайтесь говорить медленно. Ведя диалог, не спешите отвечать.
3. Сконцентрируйтесь на одном деле. Например, попробуйте очень точно описать предмет, который находится рядом с вами.



5 – 4 – 3 – 2 – 1

ТЕХНИКА ЗАЗЕМЛЕНИЯ

Успокаивающая техника, которая соединяет вас с настоящим, исследуя пять чувств.

5 вещей, которые можешь увидеть

4 вещи, которые можешь потрогать

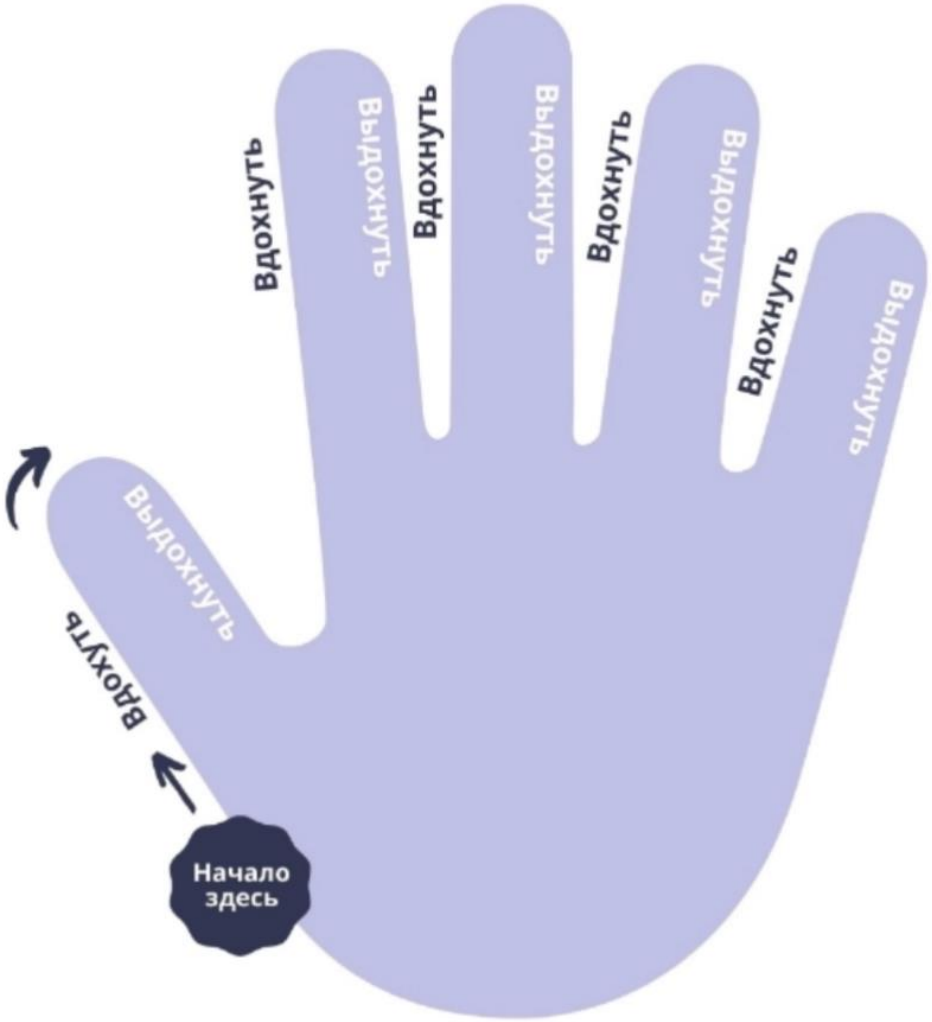
3 вещи, которые можешь услышать

2 вещи, которые можешь понюхать

1 вещь, которую можешь попробовать на вкус

УСПОКОЙСЯ

ДЫХАНИЕ НА 5 ПАЛЬЦЕВ



Медленно проведите указательным пальцем по внешней стороне руки, вдыхая, когда проводите пальцем вверх, и выдыхая, когда проводите вниз.
Вы также можете выполнять это дыхательное упражнение,

Дыхание:

Вы не обязаны:

- ✓ Отвечать, если вам не хочется;
- ✓ Стремиться всегда быть привлекательным;
- ✓ Быть рабом сказанных вами манипулятору слов;
- ✓ Разбираться во всем.

Вы имеете право:

- ✓ На ошибку;
- ✓ Быть не понятливым или чего-то не знать;
- ✓ Быть нелогичным;
- ✓ Сказать «Нет», «Я не хочу»;
- ✓ Не зависеть от того, как к вам относятся другие;
- ✓ Не оправдываться за свои поступки и намерения;
- ✓ Не объяснять и не извиняться за свое поведение перед манипулятором.

Спасибо за внимание!

Работаю с ситуативными затруднениями и глубинными травмами, с депрессиями, тревогами, с эмоциональным выгоранием, проблемами в отношениях, с паническими атаками, с апатией, переживанием горя, конфликтами и др.

8-922-958-88-02