Image not found or type unknown

# Что такое телефон? Как работает мобильная связь? [Углубленное упражнение]

deepening_activ_circular_400px-wit

Image not found or type unknown

Картинка. Надпись на картинке: Углубленные Упражнения
Рисунок на картинке: зеленый круг. Сверху картины дерево и по всему кругу распущены корни

Целью данного упражнения является углубление знаний о том, как работает мобильная связь, что поможет участникам_цам оценивать и планировать риски, связанные с мобильной связью. Фасилитаторы_ки должны включать это упражнение в любой семинар по мобильной связи, или убедиться, что все участники_цы уже знакомы с информацией, которую содержит данное упражнение. Оно является основой для оценки технических рисков мобильной связи.

Данное упражнение состоит из двух этапов:

- Практическая работа по исследованию телефона
- Вводная информация: данные о мобильной связи и соображения рисков

## Цели обучения, которым отвечает данное упражнение

- Понимание некоторых основных концепций работы мобильной связи для составления представления о потенциальных последствиях ее использования;

# Для кого предназначено данное упражнение?

Это упражнение для всех участников_ц  семинара по мобильной связи.

# Продолжительность

На выполнение этого упражнения потребуется приблизительно **45 минут.**

# Ресурсы, необходимые для данного упражнения

- Несколько мобильных телефонов для разбора и исследования
- Доска, слайд или учебный материал с указанием основных положений

# Техника проведения

В зависимости от наличия времени упомяните или обсудите, что в ходе данного упражнения мы будем говорить о мобильных технологиях – рассматривая устройства, которые легко помещаются в руке или в кармане и имеют коммуникационные функции от голосовых звонков и текстовых сообщений до веб-сервисов и услуг по передаче и обработке данных. Часть данного раздела будет относиться и к планшетам.

# Внутри наших телефонов – 5 минут

Разбор телефона по частям. Ваш телефон представляет собой маленький компьютер. Все участники_цы достают свой телефон и находят:

- Детали, которые слушают и воспроизводят звук: микрофоны, динамики
- Детали, которые просматривают и отображают визуальные эффекты: камеры, экраны
- Детали, которые отправляют и получают информацию из других источников: GPS, антенны, Wifi
- Детали компьютера, аппаратное обеспечение: аккумулятор, схема
- Память: SD карта, другая встроенная в телефон память
- Слот(ы) для SIM карты

# Идентификаторы устройства и SIM карты – 5 минут

У вашего телефона есть все эти детали, а также несколько идентифицирующих признаков, помимо марки, модели и ОС, у него есть два имени – идентификатор устройства и идентификатор SIMКарты. Важно знать об этом, поскольку вас могут идентифицировать по любому из них, и ваш телефон часто передает эту информацию, в особенности IMSI.

- **IMEI** это имя вашего устройства

Международный идентификатор мобильного оборудования (IMEI): https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- **IMSI** это имя вашей SIM карты

Международный идентификатор мобильного абонента (IMSI): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

# Наши телефоны в процессе коммуникации - 35 минут

Мы используем наши телефоны для общения с людьми: текстовые сообщения, сообщения в чатах, социальных сетях, приложениях, звонки. Наши мобильные устройства также передают информацию о наших телефонах и о нас самих – не только в виде сообщений, но и метаданные, наше местонахождение и т. д., и они могут быть связаны с другой

информацией о нас, такой как наши социальные сети, наши организационные сети, наши привычки и места работы.

Полезно быть в курсе этих вопросов, в основном для того, чтобы мы могли понять, каким образом наш мобильный телефон может действовать как устройство слежения в данный момент и как историческая запись о нашей деятельности в последующем.

# 1. Ваш телефон любит общаться

Ваш телефон обращается к различным типам сетей и через различные типы связи, чтобы сообщить о том, что он находится рядом, и чтобы установить связь или проверить, не хочет ли кто-нибудь подключиться.

## Операторы мобильной связи

Y операторов мобильной связи есть вышки и антенны, с которыми общается ваш телефон. Каждая антенна может охватывать определенную область. Ваш телефон связывается с той вышкой(вышками), к которой вы находитесь ближе всего. Он как **минимум передает ваш IMSI**, чтобы сообщить, услугами какого мобильного оператора вы пользуетесь, а также ваш номер, чтобы вы могли получать сообщения, звонки и коммуникации на свое устройство. Каждый раз, когда вы оказываетесь рядом с вышкой, вы как будто ставите отметку на картографической шкале времени, сообщая, где вы находитесь. Вы отмечаете, где вы находитесь, когда вы там находитесь, и чем вы занимаетесь на том месте с точки зрения использования вашего телефона.

## GPS

если у вас включена функция GPS, ваш телефон связывается со спутниками GPS, аналогично отмечая местонахождение, что является аналогичным установлению отметок на картографической шкале времени.

## Wifi

если эта функция включена, то при прохождении через беспроводные сети ваше устройство может как попытаться подключиться к ним, оставляя след в сети wifi, так и сделать запись имени сети в вашем телефоне.

## Bluetooth/NFC

если эти функции включены, другие устройства, которые используют Bluetooth и NFC, могут установить связь с вашим устройством, попытаться подключиться, поделиться файлами и т. д.

Фасилитация обсуждения с помощью вопросов: какие функции нужно оставлять включенными? Являются ли для вас записи о вашем местонахождении риском или нет?

# 2. Вы любите общаться

Мы используем наши телефоны для общения. Разные виды коммуникации по-разному отображаются во время общения и после отправки сообщения.

## SMS

текстовые сообщения и метаданные – в процессе коммуникации и после сохранения на вашем устройстве и у ваших операторов связи отправляются в открытом виде. Полезная аналогия – текстовое сообщение похоже на почтовую открытку. Если кто-то перехватит ее, то сможет прочитать все содержимое письма, а также метаданные (например, отправитель, получатель, время, дата).

## MMS

медиа-сообщения и метаданные – в процессе общения могут быть зашифрованы или нет, поэтому, если кто-то пытается перехватить ваше общение, возможность для перехватчика просмотреть сообщения зависит от шифрования сообщений. После отправки MMS сообщение хранится у вас, у получателя, а также у обоих мобильных операторов и на обоих устройствах, таким образом, при исследовании любого из них можно получить метаданные (например, отправитель, получатель, время, дата) а также содержание сообщения.

## Звонки

содержание звонков и метаданные - аналогично – звонки должны шифроваться в процессе разговора, но ваш провайдер, а также провайдер получателя сохраняет метаданные звонка (например, отправитель, получатель, время, дата), и, если ваш оппонент имеет доступ к вашим провайдерам, у них может быть доступ на прослушивание звонков или их записи.

Для получения дополнительной информации о приложениях и приложениях для сообщений смотрите:

- Обсуждение, вводная информация + практическая работа: выбор мобильных приложений

Примечание по государственной слежке: наблюдение со стороны государства зависит от страны. В некоторых странах у правительства есть доступ ко всем данным, которые хранятся у операторов связи – в таких случаях следует учитывать, что все метаданные и содержимое незашифрованных услуг доступны правительствам как в режиме реального времени, так и впоследствии, если по этим записям будет проводиться расследование.

Ваша лучшая защита от слежки – сквозное шифрование.

## 3. Телефон – это маленький компьютер

Программный «жучок»: телефон – это компьютер, и он может быть заражен вредоносным ПО, точно так же, как настольный компьютер или ноутбук. Как частные лица, так и правительства используют программное обеспечение для прослушивания устройств других людей.  Такое программное обеспечение часто использует части телефона как «жучок» или устройство слежения, прослушивая телефон с помощью микрофона или отправляя данные о местоположении.

## 4. Облако – это картотека (хранилище документов)

Некоторые данные, к которым мой телефон имеет доступ, вовсе не находятся в моем телефоне, они хранятся в облаке. «Облако» – это просто термин, и оно подразумевает «интернет», то есть данные, которые хранятся где-то физически на устройстве, которое подсоединено к интернету. Ваши приложения могут получать доступ к данным, которые находятся в облаке, а не на вашем устройстве.

Вопросы, которые необходимо учитывать: зашифрованы ли мои данные при передаче между мной и сервисом? Шифруются ли они при хранении в сервисе? Известны ли мне случаи, когда оппонентам удавалось получить доступ к этой информации – когда, как?

Примечание для фасилитатора_ки: в ходе вашего разговора участники_цы могут задавать вопросы о частях телефонов или рисках, связанных с упомянутыми вами методами коммуникации. Найдите время, чтобы ответить на вопросы. По возможности ведите список вопросов и тем, по которым участники_цы просят дополнительную информацию – для

ведения списка можно применить доску. Также рекомендуется вести список вопросов и тем, которые вы не успеете рассмотреть на этом семинаре, чтобы вернуться к ним позже во время семинара, или предложить в качестве дополнения после семинара.

# Дополнительные ресурсы

- 7 Способов найти номер IMEI или MEID вашего телефона: http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- Международный идентификатор мобильного оборудования (IMEI: https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
- Международный идентификатор мобильного абонента (IMSI): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

На сайте My Shadow компании Tactical Tech есть ряд отличных учебных пособий в помощь при изучении мобильных технологий.

- Материалы для скачивания на My Shadow: https://myshadow.org/materials
- Веб-сайт My Shadow: https://myshadow.org/

*Картинка с рисунком. На рисунке растения синего цвета

image-1605452256072.png
Image not found or type unknown

Revision #4
Created 24 April 2023 17:29:08 by Kira
Updated 29 June 2023 16:37:14 by Kira