**§1.Основные угрозы**

Для того, чтобы выявить основные угрозы, надо определить, что в наших смартфонах и планшетах необходимо защитить. Это, конечно,:

1. Данные об учетных записях. (В случае если у вас настроена синхронизация с Facebook, Twitter и т.п., то логины и пароли для этих систем хранятся в памяти телефона).

2. Телефонная книга и история СМС-переписки.

3. Данные Web-браузера. (В браузере могут храниться личные данные для авторизации на сторонних веб-серверах. В случае если у вас синхронизируется мобильный браузер (Google Chrome, Firefox, и т.д.) с настольной версией браузера, следует учесть, что со смартфона (планшета) можно получить доступ ко всем вашим паролям.)

4. Карта памяти, т.к. на карте хранятся фото и видеосъемка.

Все угрозы можно разделить на две большие группы: внешние и внутренние. К внешним угрозам относятся различные недоброжелательные сайты и вредоносные программы, которые могут передать третьей стороне ваши персональные данные, изменить или уничтожить их. Также к внешним угрозам можно отнести возможность перехвата данных по сети, особенно если подключаться через публичную Wi-Fi сеть (аэропорта, отеля, школы, библиотеки, кафе и т.д.). А к внутренним угрозам можно отнести, если телефон попал в руки к третьему лицу. Привычка пользоваться гаджетами в многолюдных местах усиливает вероятность кражи или утери этого устройства.

Итак, сформулируем основные виды угроз мобильных устройств:

1. нарушение конфиденциальности информации в результате доступа посторонних лиц к устройству, оставленному без присмотра;
2. нарушение конфиденциальности информации в результате кражи или утери устройства;
3. нарушение конфиденциальности информации в результате необдуманных действий пользователя;
4. доступ к конфиденциальной информации внешних нарушителей посредством установки и использования вредоносных программ;
5. хищение информации при получении или отправлении информации.