**§2. Способы защиты от угроз**

В этом параграфе разберем способы защиты от основных видов угроз мобильных устройств.

**2.1.Защита при нарушении конфиденциальности информации в результате доступа посторонних лиц к устройству, оставленному без присмотра.**

Если ваше мобильное устройство попало в руки к третьему лицу – первое, что становится на защиту ваших данных – это блокировка экрана. В каждой модели телефона или планшета предлагаются разные варианты, рассмотрим некоторые из них. Разблокирование экрана может производиться[[1]](#footnote-1):

1. Касанием к экрану (проведите пальцем по экрану) (фактически, защита отсутствует);

2. Распознавание лица (низкий уровень безопасности);

3. Лицо и голос (низкий уровень безопасности);

4. Подпись (низкий уровень безопасности);

В данном случае необходимо написать ключевое слово трижды. Именно с помощью данного слова и будет разблокировано устройство.

5. Рисунок (средний уровень безопасности);

Рисунок имеет среднюю степень безопасности. Для этого необходимо соединить в любом порядке не менее 4 точек на рисунке.

6. PIN (средний или высокий уровень безопасности);

PIN — последовательность цифр, не менее 4 символов. Естественно, чем длиннее строка цифр, тем выше уровень безопасности.

7. Пароль (высокий уровень безопасности).

Пароль — наиболее высокий уровень безопасности. Содержит сочетание букв и цифр.

Однако, чтобы извлечь карту памяти из телефона или планшета и прочитать ее никакой пароль не нужен. Для этого данные на карте памяти нужно зашифровать (создать «криптоконтейнер»[[2]](#footnote-2)), тогда прочитать их уже не получится. Шифрование – самый надежный способ защиты личных данных.[[3]](#footnote-3) Осуществляется средствами самой операционной системы, причем доступ к интернету для этого не нужен. Работает шифрование так: после включения шифрования все данные на устройстве и на карте памяти будут зашифрованы. Однако, если кто-то разблокирует устройство, он все равно получит доступ к данным, но это спасет данные, если кто-то попытается украсть карту памяти или прочитать данные без включения смартфона с его внутренней памяти, так как данные будут зашифрованы. При включении смартфона нужно будет вводить пароль, позволяющий расшифровать данные. Без ввода пароля смартфон дальше не загрузится. Это не просто ПИН-код, это ключ, которым зашифрованы данные. Недостаток шифрования – оно замедляет работу всего смартфона, после шифрования отменить его нельзя, только сброс до заводских настроек, шифрование не спасет, если кто-то попросит ваш телефон чтобы посмотреть, а сам в этот момент что-то установит.

Другой способ защиты – это запрет запуска определенных приложений и сокрытие папок из галереи. Такая защита не очень надежная, но в некоторых случаях, например, чтобы ребенок не смог запустить некоторые приложения или просмотреть некоторые фотографии, можно воспользоваться и такой функцией.

**2.2. Защита при нарушении конфиденциальности информации в результате кражи или утери устройства**

В этом случаи могут помочь все меры защиты, перечисленные в п.2.1. Но также следует рассказать о встроенных мерах защиты.

Сделать информацию на мобильном устройстве в случаи кражи или потери недоступной для других может помочь удаленная блокировка устройства, которая осуществляется через специальный сервис на сайте производителя. С помощью этого сервиса законный владелец может указать производителю заблокировать украденное или потерянное устройство. В этом случае разблокировать его можно будет только введя пароль от учетной записи владельца в сервисе производителя или предъявив производителю документы, подтверждающие покупку устройства.

Если же устройство утерено безвозвратно (сломалось, украли или потеряно), то утешением может служить сделанное недавно резервное копирование. Любое устройство может сломаться, утонуть и не подлежать восстановлению. Новый аппарат можно купить, а вот личную информацию восстановить не всегда возможно. С функцией резервного копирования можно сохранить все ваши данные: контакты, журналы вызовов, сообщения, медиа файлы (фото, музыка, видео) и приложения. Надо хотя бы раз в месяц делать резервное копирование.

Также стоит упомянуть о двухфакторной идентификации при подключении к особо важным сервисам (банковские программ, почта и т.п.). При таком способе идентификации используется не только логин и пароль к сервису (первый фактор), но и еще какой-нибудь способ для вашей идентификации, например отправка сообщения с одноразовым кодом, который необходимо ввести на сайте сервиса, отправляемого на ваш телефон после успешного ввода логина и пароля (второй фактор). Это поможет обеспечить безопасность даже в случае, если злоумышленник как-то узнал ваш логин и пароль.

**2.3.Нарушение конфиденциальности информации в результате необдуманных действий пользователя**

 Многие пользуются популярными в наше время социальными сетями Facebook, Вконтакте, Twitter, Instagram, YouTube, WhatsApp, Viber, Вконтакте и Одноклассники, выкладывают фотографии свои и с друзьями, видеоролики. Общение в сети – это хорошо, но не следует забывать, что не все используют социальные сети для общения, кто-то старается заработать на информации, так щедро выкладываемой самими пользователями. Никогда не стоит забывать о безопасности.

Надо понимать, что нарушение конфиденциальности персональных данных, вызванное собственными действия пользователя, может привести к проблемам уже не с информационной, а с физической безопасностью. Фотографии на фоне узнаваемых объектов, подписи с друзьями, данные о ваших родственниках, появившиеся в сообщениях в соц. сетях, могут быть использованы мошенниками для преступлений против них или вас. Метки геолокации, присутствующие в ваших сообщениях, помогут узнать места, где вы обычно бываете, а также время их посещения вами. Это не означает, что совсем не надо пользоваться соц. сетями, но надо подумать о последствиях, прежде чем что-то писать и выкладывать. Соблюдать баланс открытости и безопасности.

**2.4. Меры защиты при доступе к конфиденциальной информации внешних нарушителей посредством установки и использования вредоносных программ**

Для нахождения вредоносных программ на устройствах нужно использовать антивирусы, которые можно установить самостоятельно и главное вовремя их обновлять.

Также следует обновлять операционную систему, т.к. разработчики регулярно выпускают обновления для устранения брешей в безопасности приложений. Обновления предотвращают появление уязвимостей на вашем смартфоне и планшете. Тем ни менее, следует обращать внимание какого рода эти обновления.

Чтобы избежать вредоносных программ, надо устанавливать приложения только из проверенных источников и проверять требуемые приложением полномочия. Зачем, к примеру, калькулятору доступ к вашим контактам или фотографиям и видео? Некоторые приложения стараются получить доступ к адресной книге и вашему местоположению для того, чтобы потом присылать вам рекламу или отправлять СМС на платные номера. Перед установкой следует обратить внимание к чему запрашивает доступ приложение. Если вы используете Android-устройства и скачиваете приложения только из магазина Google Play, то снимите флажок напротив "Неизвестные источники" в настройках безопасности вашего телефона. Иногда, даже Google Play пропускает вредоносные программы. Всем хорошо известно, что большинство Android вирусов — поддельные приложения замаскированные под легитимные, поэтому не помешает проверить разработчика перед установкой приложения. Соблюдайте осторожность, иногда сайты для скачивая являются поддельными, замаскированными под официальные — всегда проверяйте адрес сайта (URL). Избегайте скачивания с пиратских сайтов.

**2.5. Способы защиты от хищения информации при получении или отправлении**

Для защиты данных от перехвата, которые передаются по сети, например, пароли к некоторым веб-страницам, сообщения в чатах социальных сетей, нужно использовать протокол HTTPS. Это вариант обычно используемого в Интернет для обмена информацией протокола HTTP, к которому добавлено шифрование всех передаваемых данных Далеко не все сайты используют протокол HTTPS, поэтому часть информации передается в открытом виде.

Когда браузер делает запрос к веб-сайту, этот запрос должен пройти через множество различных сетей, любая из которых может быть потенциально использована для прослушивания или для вмешательства в установленное соединение. С вашего компьютера на другие компьютеры вашей локальной сети, через роутеры и свитчи, через вашего провайдера и через множество других промежуточных провайдеров – огромное количество организаций ретранслирует ваши данные. Если злоумышленник окажется хотя бы в одной из них — у него есть возможность посмотреть, какие данные передаются. Итак, криптография позволяет защитить соединение от потенциальных злоумышленников, которые хотят воздействовать на соединение или просто прослушивать его. Для этого и нужно использовать протокол HTTPS (аббр. от англ. HyperText Transfer Protocol Secure) — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов SSL или TLS.[[4]](#footnote-4)

Пользуйтесь VPN при подключении к открытым, общественным WiFi сетям. VPN — Virtual Privat Network. Это первый, и часто единственный, способ, который позволяет организовать безопасное информационное пространство для обмена нескольких учреждений. Суть его — построение «туннеля» через незащищенную сеть (Интернет) от устройства пользователя, например, компьютера или смартфона, до сервера или даже целой сети (например, для удаленного подключения к сети своей работы). Все данные, передаваемые через такой туннель, шифруются. Это позволяет не только безопасно получать данные сайтов, но и обмениваться почтой и другой информацией, не опасаясь, что ее смогут перехватить.

1. Информация взята с сайта:

https://bezmaly.wordpress.com/2013/09/24/andr-3/ [↑](#footnote-ref-1)
2. Криптоконтейнер - это зашифрованный набор данных. [↑](#footnote-ref-2)
3. Камский В.А. «Защита личной информации в интернете, смартфоне и компьютере». – СПб.:Наука и техника, 2017. – Глава 15 Защита важных документов с помощью криптоконтейнера стр.223 [↑](#footnote-ref-3)
4. Материал из Википедии

https://ru.wikipedia.org/wiki/HTTPS [↑](#footnote-ref-4)