УДК 004.056

СОВРЕМЕННЫЙ СМАРТФОН: КАК ЗАЩИТИТЬСЯ ОТ ВЗЛОМА

Щеглова Елизавета Витальевна ИБс-211, Щеглова Полина Витальевна ИБс-211
Научный руководитель Прокопенко Е.В.. заведующий кафедрой (кафедра информационной безопасности)

ФГБОУ ВО «Кузбасский государственный технический университет

имени Т.Ф. Горбачева», Россия, Кемерово

Email: Elizaveta.shcheglova1@gmail.com

***Аннотация**: в данной статье рассматриваются возможные угрозы при использовании смартфона, а так же примеры защиты данных.*
Ключевые слова**: информационная безопасность, взлом, смартфоны, угрозы, защита информации**.

Введение

За двадцатилетний период смартфоны стремительно завоевали сердца миллионов людей, превратившись в неотъемлемый атрибут нашей повседневности. С момента выхода первого смартфона рынок пережил невероятный взлет. К 2025 году более 4 миллиардов человек по всему миру пользуются смартфонами, что эквивалентно более 40% населения нашей планеты. Основными средствами общения, получения информации, использования социальных сетей и управления личными деньгами стали смартфоны.

Несмотря на многочисленные достоинства, смартфоны не лишены и определенных рисков для безопасности. Взлом, кража личной информации и установка шпионского ПО — лишь малая часть возможных угроз.

Цель статьи

Предоставить практические советы по защите современных смартфонов от взлома и других угроз безопасности. Используя их, вы можете повысить уровень защиты своих данных и снизить риск утечки информации. Ответственность пользователей и их осведомленность о безопасности создают более безопасную среду для использования технологий в повседневной жизни.

1. Понимание угроз

Общение, хранение личной информации является неотъемлемой частью нашей жизни — эти функции выполняют современные смартфоны. Однако, чем больше их популярность, тем выше риски для безопасности. Понимание возможных угроз — первый шаг к защите устройства от взлома и утечки данных. Атаки на смартфоны могут быть физическими или удаленными. При физических атаках злоумышленник получает прямой доступ к устройству, такое может быть при краже. Если телефон не защищен, вся личная информация может оказаться в руках преступника. Удаленные атаки встречаются все чаще благодаря развитию технологий. Злоумышленники используют: вредоносные приложения, фишинг, незащищенные Wi-Fi сети.

Еще одна серьезная угроза — социальная инженерия, когда преступники манипулируют пользователями, чтобы получить доступ к их данным. Это может быть обман, давление или другие психологические приемы, заставляющие человека раскрыть личную информацию или установить вредоносное ПО.

Знание всех этих угроз помогает пользователям быть более внимательным и принимать меры для защиты своих устройств. Безопасность зависит не только от технологий, но и от осведомленности: чем больше вы знаете о рисках, тем лучше сможете обезопасить себя и свои данные.

2. Основные принципы безопасности

Для усиления защиты личных данных важным является использование надежных паролей и биометрической идентификации. Использование биометрических данных, таких как сканирование отпечатков пальцев или распознавание черт лица, обеспечивает надежный барьер безопасности. Кроме того, более сложную комбинацию символов, цифр и букв, злоумышленникам будет намного сложнее взломать. На платформах Android и iOS биометрическая аутентификация доступна в настройках безопасности, и обеспечивает быстрый и безопасный доступ к устройству.

Также важно своевременно обновлять операционную систему и установленные программы. Разработчики постоянно совершенствуют свои продукты, устраняя обнаруженные ошибки и расширяя их возможности. Включение автоматических обновлений на вашем смартфоне гарантирует, что вы используете обновленные версии программного обеспечения. Регулярная проверка обновлений помогает избежать воздействия известных киберугроз.

Кроме того, защита данных на смартфоне включает в себя шифрование информации. Шифрование преобразует ваши данные в недоступный для посторонних вид формат, это делает их бесполезными в случае кражи устройства. В большинстве смартфонов шифрование можно включить через настройки безопасности.

Не менее важным аспектом является резервное копирование данных. Оно позволяет восстановить информацию в случае потери или повреждения устройства. Существует множество способов резервного копирования

данных, такие как Google Drive и iCloud, локальные копии на компьютере. Гарантированную сохранность данных обеспечивает настройка автоматического резервного копирования.

Следуя данным принципам, вы сможете значительно повысить уровень защиты вашего смартфона и сохранить личные данные в безопасности.

3. Безопасное использование приложений

Для защиты данных и устройства от различных угроз очень важно безопасное использование приложений. Одно из ключевых правил - это установка приложений только из официальных источников. Приложения, загруженные из сторонних сайтов, могут содержать вредоносные программы, шпионское ПО, вирусы, которые способны украсть данные и повредить устройство. Такие приложения часто не получают обновлений безопасности, что делает их уязвимыми для атак. Поэтому всегда стоит обращать внимание на разработчика приложения: как правило, более надежны известные компании с хорошей репутацией.

Рекомендуется тщательно проверять безопасность приложений перед установкой на смартфон. Важно изучить отзывы и рейтинги других пользователей, так как это может дать представление о надежности приложения. Также стоит обратить внимание на запрашиваемые разрешения. Если приложение требует доступ к данным, которые не соответствуют его функционалу — например, фотоаппарат для приложения для заметок — это может быть поводом для настороженности.

Также важно регулярно проверять разрешения установленных приложений. Рекомендуется минимизировать разрешения, предоставляя доступ только к тем данным, которые необходимы для работы приложения. Например, если приложение для создания заметок запрашивает доступ к вашим контактам или местоположению, это может быть совершенно излишним.

Периодическая проверка разрешений также поможет вам оставаться в безопасности. Если вы заметили, что какое-то приложение запрашивает доступ к данным, которые не нужны для его работы, стоит рассмотреть возможность его удаления или ограничения доступа к этим данным.

Безопасное использование приложений — важный аспект защиты вашего смартфона от хакеров и утечек данных. Установка приложений только из официальных источников и тщательная проверка разрешений помогут снизить риски и защитить ваши личные данные. Будьте осторожны при установке новых приложений и всегда проверяйте настройки безопасности вашего устройства.

Заключение

В заключении хочется сказать, что защита современного смартфона от взлома является важной задачей, требующей очень внимательного подхода и

комплексных действий. С учетом растущих угроз в цифровом мире, каждый должен осознавать важность соблюдения простых, но эффективных мер безопасности. Значительно снизятся риски взлома если регулярно обновлять операционную систему, использовать надежные пароли и многофакторную аутентификацию, а так же быть осторожным при установке новых приложений. Так мы сможем защитить свои данные и наслаждаться всеми преимуществами, которые предоставляют современные смартфоны.

Список литературы:

1. Бланк, И. А. (2019). Основы информационной безопасности. М.: Наука.
2. Лебедев, В. И. (2021). Интернет-угрозы: Как защитить свои данные. М.: Альпина Паблишер.
3. Петров, А. Н. (2022). Безопасность мобильных технологий и информационных систем. М.: Фаир-Пресс.
4. Шевченко, С. В. (2021). Кибератаки на мобильные устройства: защита и предотвращение. М.: Аспект Пресс.