Умные часы предлагают множество полезных функций, от отслеживания активности до уведомлений о сообщениях. Однако, как и любые устройства с возможностью подключения сторонних девайсов, они подвержены риску взлома и требуют защиты. Василий Шутов, преподаватель кафедры КБ-1 «Защита информации» РТУ МИРЭА, подчёркивает, что первым шагом к защите является установка надёжного пароля или PIN-кода, который не так легко взломать, как простые комбинации. Некоторые модели умных часов также поддерживают биометрическую аутентификацию, такую как скан отпечатка пальца, что значительно повышает уровень безопасности.

Основное внимание следует уделить регулярному обновлению программного обеспечения умных часов. Это позволяет производителям исправлять обнаруженные уязвимости и улучшать защиту устройств. Важно также убедиться, что ваше устройство всегда использует последнюю версию программного обеспечения для минимизации рисков.

Шифрование данных на умных часах и связанном с ними смартфоне также играет ключевую роль в защите от вредоносных программ. Важно активировать функцию шифрования и проверить её настройки для обеспечения безопасности передачи данных. Однако нужно быть осторожным при установке сторонних приложений — предпочтение следует отдавать официальным магазинам приложений, чтобы избежать возможных угроз безопасности.

Отключение Bluetooth и Wi-Fi, когда они не используются, помогает усилить защиту умных часов от потенциальных атак злоумышленников. Эти соединения могут стать «точками входа» для вредоносного ПО. Наконец, активация функции удалённого стирания данных на случай утери или кражи умных часов позволит удалить личную информацию и предотвратить её незаконное использование.