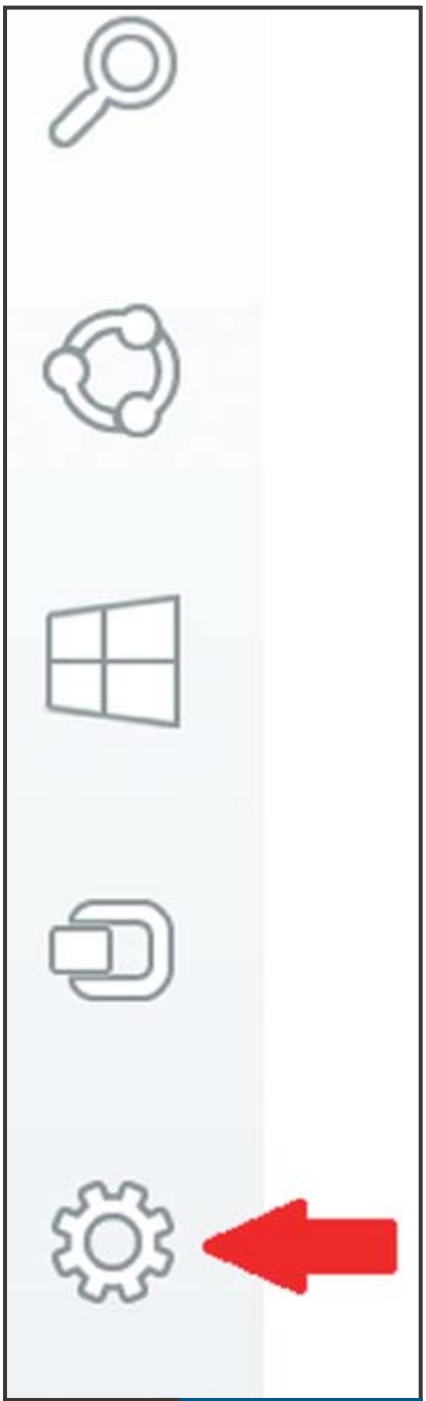
# Аутентификация на планшетах

Владимир Безмалый



Экран 1 Изменение параметров

С появлением планшетов перед нами сразу же возникла проблема аутентификации на этих переносных устройствах. С одной стороны, требуется устойчивая аутентификация, с другой — нужно, чтобы она была удобной, ведь набор сложного пароля и ранее представлял собой непростую для большинства пользователей процедуру, а на планшете набор сложного пароля еще более неудобен. В данной статье мы рассмотрим, как осуществляется аутентификация на планшетах под управлением операционных систем Windows 8.1 и Android.

## Аутентификация на планшетах под Windows 8.1

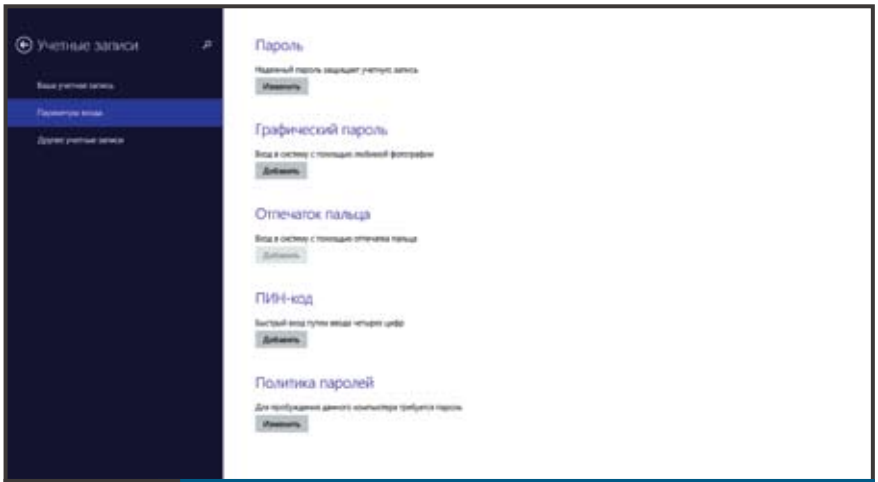
Аутентификация на планшетах под Windows 8.1 будет внешне неотличима от аутентификации под Windows 8. В этой версии операционной системы от Microsoft разработчикам удалось соединить, казалось бы, несоединимое: с одной стороны, пользователь создает устойчивый пароль, а с другой — получает удобные средства аутентификации:

- графический пароль;
- PIN-код из четырех цифр;
- возможность применения биометрической аутентификации (отпечаток пальца).

Вместе с тем необходимо учесть, что все эти удобства не будут работать, если у вас не задан обычный пароль. Таким образом, вначале нам следует задать его.

Если для вашей учетной записи обычный пароль не создан, нажмите комбинацию клавиш Win+I и выберите пункт «Изменение параметров компьютера» или поместите курсор мыши в правый верхний угол экрана для вывода панели Charms (экран 1). Выберите указанный стрелкой значок и далее пункт «Изменение параметров компьютера», затем «Учетные записи» и «Параметры входа» (экран 2).

Учтите, что перед тем, как создать графический пароль, PIN-код или обеспечить вход с использованием отпечатка пальца, вам потребуется создать пароль для соответствующей учетной




Экран 2 Учетные записи. Параметры входа

записи. Рекомендуемые требования к паролю выглядят довольно стандартно: не менее 9 знаков в трех наборах символов из четырех. Например, большие и маленькие буквы и цифры. Итого получаем 26+26+10=62 символа. Таким образом, сложность пароля 629 символов. Запомните эту цифру, она нам еще пригодится. На мой взгляд, все остальные варианты аутентификации — это не более чем просто удобство, причем снижающее устойчивость парольной защиты.

## Отпечаток пальца

Для того чтобы использовать отпечаток пальца, вам вначале потребуется задать пароль для своей учетной записи. А затем выбрать в окне «Параметры входа» вариант «Отпечаток пальца».

Чтобы использовать отпечаток пальца (экран 3), сначала необходимо 4 раза добавить отпечаток пальца в базу для его запоминания, а затем еще 4 раза. Таким образом, сканирование каждого пальца придется выполнить 8 раз. Не поленитесь сделать это для всех 10 пальцев. Ведь вполне возможна ситуация, когда по какой-то причине (загрязненный датчик, порез на пальце и т. д.) отпечаток просто не распознается.

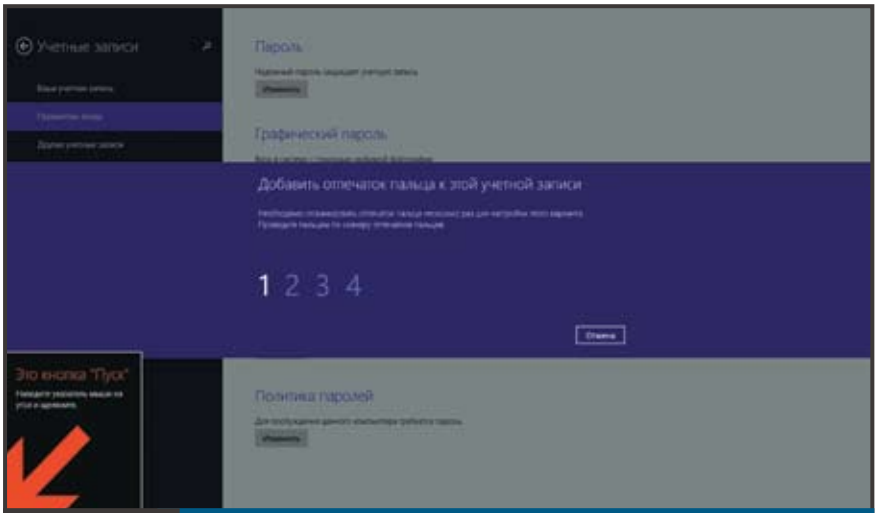
## Графический пароль

Выберите вариант «Графический пароль». В появившемся окне (экран 4) потребуется вначале выбрать базовый экран (фотографию), который будет служить основой для пароля. Далее необходимо с помощью жестов, то есть касаясь экрана пальцами или двигая мышью, «нарисовать» на экране комбинацию окружностей, прямых линий и других геометрических элементов.

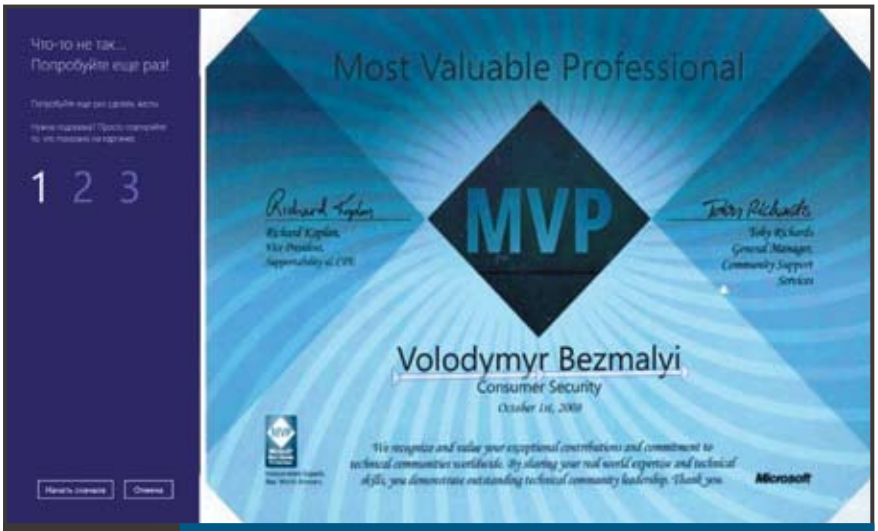
При этом вы можете выбрать замкнутую область на экране или соединить пару произвольных точек (см. экран 4). Проделайте это трижды. Теперь ваш пароль готов, и вы можете использовать его для аутентификации. Вместе с тем стоит учесть, что уже известны случаи успешных атак на графический пароль.

## Персонализированный вход в систему

Фактически графический пароль состоит из двух компонентов:




Экран 3 Использовать отпечаток пальца




Экран 4 Задать графический пароль

- изображения из вашей коллекции рисунков;
- набора линий (жестов), которые вы наносите поверх изображения.

Вы сами выбираете картинку, что поможет лучше запомнить пароль, и сами решаете, какие ее части наиболее интересны вам. В наборе жестов чаще всего выделяются линии и окружности. При этом дополнительным параметром безопасности является направление движения руки при рисовании. Ведь при рисовании круга или линии на выбранном изображении Windows запоминает, каким образом они были нарисованы. Поэтому тот, кто пытается воспроизвести графический пароль, должен знать не только выбранные части изображения и порядок их выделения, но и направление, а также начальные и конечные точки нарисованных линий и окружностей.

## Как работает графический пароль

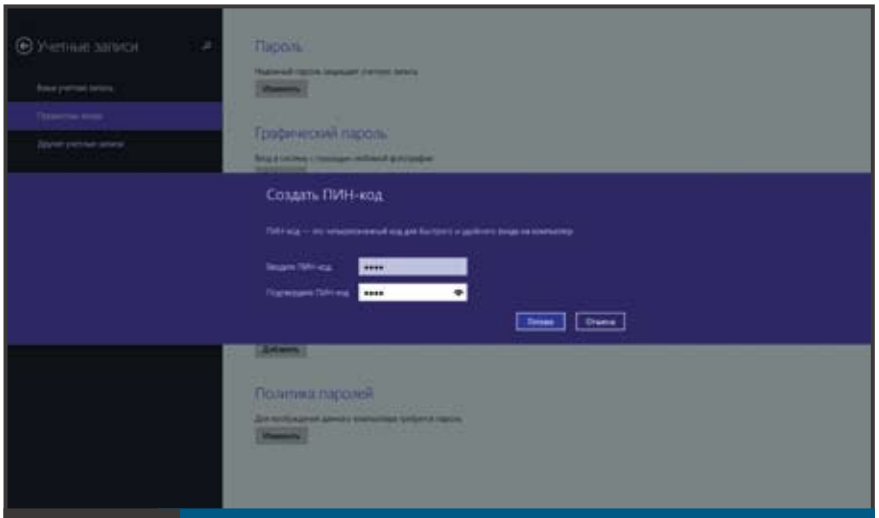
После того как вы выбрали изображение, на нем формируется сетка. Самая длинная сторона изображения разбивается на 100 сегментов, затем разбивается короткая сторона и создается сетка, по которой рисуются жесты. Отдельные точки ваших жестов определяются их координатами (x, y) на сетке. Для линии запоминаются начальные и конечные координаты и их порядок, используемый для определения направления рисования линии. Для окружности запоминаются координаты точки

Таблица 1 Количество уникальных паролей в зависимости от длины пароля (в пароле используются только строчные буквы латинского алфавита)

| Длина | Количество уникальных паролей |
|---|---|
| 1 | 26 |
| 2 | 676 |
| 3 | 17 576 |
| 4 | 456 976 |
| 5 | 11 881 376 |
| 6 | 308 915 776 |
| 7 | 8 031 810 176 |
| 8 | 208 827 064 576 |

Таблица 2 Количество уникальных комбинаций

| Длина | 10-разрядный PIN-код | Простой пароль из набора знаков a-z | Графический пароль из нескольких жестов |
|---|---|---|---|
| 1 | 10 | 26 | 2 554 |
| 2 | 100 | 676 | 1 581 773 |
| 3 | 1 000 | 17 576 | 1 155 509 083 |
| 4 | 10 000 | 456 976 | 612 157 353 732 |
| 5 | 100 000 | 11 881 376 | 398 046 621 309 172 |
| 6 | 1 000 000 | 308 915 776 | |
| 7 | 10 000 000 | 8 031 810 176 | |
| 8 | 100 000 000 | 208 827 064 576 | |




Экран 5 Задать PIN-код

центра, радиус и направление. Для касания запоминаются координаты точки касания.

При попытке выполнения регистрации с помощью графического пароля введенные жесты сравниваются с набором жестов, введенных при настройке графического пароля. Рассматривается разница между каждым жестом и принимается решение об успешности проверки подлинности на основе найденного количества ошибок. Если тип жеста неправильный (должен быть круг, а вместо него линия), проверка подлинности не будет пройдена. Если типы жестов, порядок ввода и направления совпадают, проверяется, насколько эти жесты отличаются от введенных ранее, и принимается решение о прохождении проверки подлинности.

## Безопасность и подсчет жестов

Чтобы определить необходимое количество жестов, соответствующее нашим целям в плане безопасности пароля, сравним графический пароль с другими способами проверки подлинности, а именно с PIN-кодом и простым текстовым паролем.

Анализ количества уникальных комбинаций PIN-кода довольно прост. В четырехразрядном PIN-коде (4 разряда с 10 независимыми возможными значениями в каждом из них) может быть $10^4$ или 10 тыс. уникальных комбинаций.

Анализ текстовых паролей может быть упрощен, если предположить, что пароли — это последовательность знаков, состоящая из строчных букв (их 26), прописных букв (тоже 26), цифр (10) и символов (10). В простейшем случае, когда пароль состоит только из n строчных букв, возможны 26n перестановок. Если пароль может иметь длину от 1 до n знаков, количество перестановок будет следующим:

$$\sum_{i=0}^{n} 26^n$$

Например, пароль, состоящий из 8 букв, имеет 208 млрд возможных комбинаций, что большинству пользователей покажется вполне достаточным количеством. В таблице 1 показано, как количество уникальных паролей меняется в зависимости от длины пароля.

Для определения количества комбинаций пароля из нескольких жестов воспользуемся таблицей 2, приведенной в статье Стивена Синофски «Выполнение входа с помощью графического пароля» по адресу http://blogs.msdn.com/b/b8_ru/archive/2011/12/22/signing-picture-password.aspx.

Как можно заметить, использование трех жестов обеспечивает значительное количество уникальных комбинаций жестов и такую же надежность, как пароль из 5–6 случайно выбранных знаков. Уточню еще раз: графический пароль добавлен в качестве способа регистрации в системе как дополнение к текстовому паролю, а не вместо него!

### PIN-код

В случае с PIN-кодом вам достаточно просто задать четырехзначный PIN-код (экран 5).

### Что нужно учесть

Аутентификация в Windows 8.1 возможна и с помощью учетной записи Live ID, биометрической аутентификации, а также кода PIN. В более старых версиях операционной системы пароль на домашних компьютере хранился в файле SAM. Соответственно, для компрометации этого пароля злоумышленнику нужен был физический доступ к системе и привилегии SYSTEM. Что же получается сегодня? С выходом Windows 8.1 потенциальному злоумышленнику будет куда легче взломать систему, потому что в системе аутентификации появились новые слабые звенья. Естественно, хакеру потребуется просто найти наиболее уязвимое из них.

Например, возьмем регистрацию в системе с помощью Live ID. Для конечного пользователя это несомненное удобство: забыл пароль — зашел на сайт Live ID с другого компьютера, воспользовался услугой смены пароля, и можно регистрироваться на своем компьютере с новым паролем. Но, несомненно, это и повышает шансы злоумышленников. Опять-таки, пользователь будет работать за другим компьютером, пароль к Live ID может храниться вместе с остальными паролями в браузере и т. д. И что самое интересное, и пароль Live ID, и PIN, и графический пароль, и биометрический — все они используются для дополнительного хранения и шифрования обычного пароля для регистрации в системе.

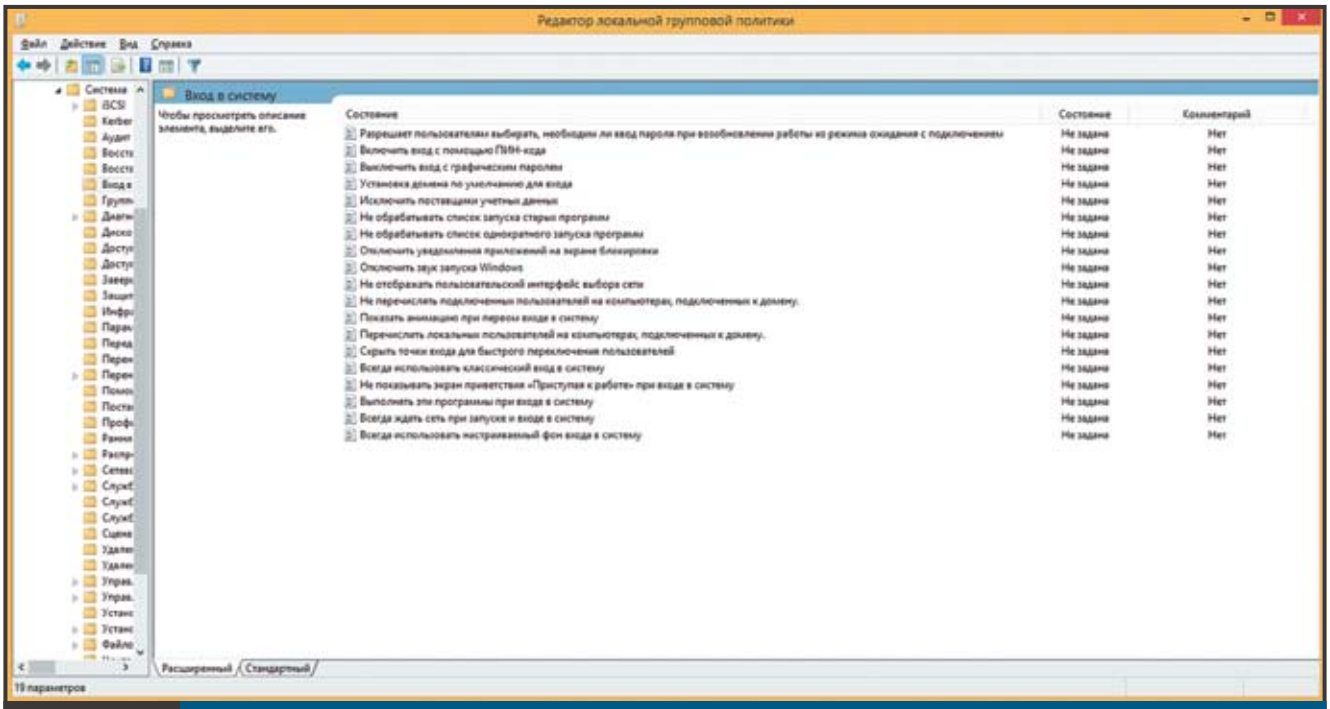
Поясню, почему эти звенья связаны с обычным паролем. Если пользователь выбрал аутентификацию по графическому паролю, то, в сущности, сам графический пароль применяется в качестве ключа для хранения и шифрования обычного пароля. Таким образом, получается, что, кроме SAM, обычный пароль будет храниться еще в одном месте. Если пользователь выбрал регистрацию с Live ID, то обычный пароль (текстовый, но зашифрованный с помощью Live ID) будет храниться в третьем месте и т. д.

В Windows 8 для расшифровки текстового пароля пользователя даже не нужны были PIN, графический или биометрический пароли, достаточно было привилегий администратора, чтобы расшифровать текстовые пароли всех учетных записей. Явный прокол в реализации!

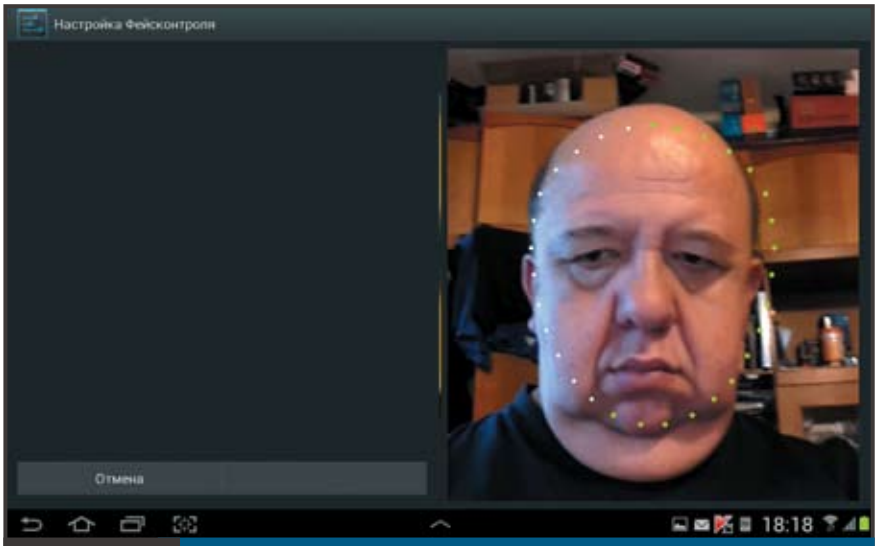
Учетная запись на базе Live ID более защищена. Пароль в текстовом виде уже не хранится. В SAM хотя и хранится хэш пароля Live ID, но он используется для расшифровки другого реального хэша. То есть, например, все пароли DPAPI, EFS, сертификаты шифруются на базе реального хэша, а не того, что в SAM. А реальный хэш уже шифруется более стойким алгоритмом pbkdf2 (SHA256) с несколькими тысячами итераций. Так что защита заметно усилилась. Думаю, в будущих версиях Windows потихоньку будут переходить на этот тип, так как их обычный хэш SAM перебирается уже со скоростью миллиардов паролей в секунду.

### Управление через политики

Несомненно, новые системы аутентификации сделаны для удобства конечных пользователей. Так что с этой точки зрения пользователь, разумеется, выиграет. Для тех же из вас, кто озабочен устойчивостью парольной аутентификации, разработчики Microsoft предусмотрели отключение графического пароля с помощью редактора локальной групповой поли-




Экран 6 Параметры входа в систему




Экран 7 Распознавание лица

тики. Для этого необходимо набрать в командной строке

```
gpedit.msc
```

и войти в редактор групповой политики в раздел «Конфигурация компьютера», затем «Административные шаблоны», «Система», далее «Вход в систему» и «Выключить вход с графическим паролем» (по умолчанию не задан), как показано на экране 6. Логично предположить, что для планшетов данный параметр необходимо выключить (графический пароль будет включен), а для всех остальных — включить (графический пароль будет выключен).

## Аутентификация на планшетах с Android

Встроенные средства аутентификации мы рассмотрим на примере планшета Samsung Note 10.1.

Разблокирование экрана этого планшета может производиться следующим образом:

1. Прикосновение к экрану (фактически защита отсутствует).
2. Распознавание лица (низкий уровень безопасности).
3. Лицо и голос (низкий уровень безопасности).
4. Подпись (низкий уровень безопасности).
5. Экран (средний уровень безопасности).
6. PIN (средний или высокий уровень безопасности).
7. Пароль (высокий уровень безопасности).

Рассмотрим перечисленные варианты подробнее.

***Распознавание лица.*** Выберите в меню «Распознавание лица». Внимательно прочтите текст и продолжите настройку (экран 7).

***Лицо и голос.*** Настройка данного пункта меню ничем не отличается от предыдущего пункта, поэтому не будем рассматривать его подробно.

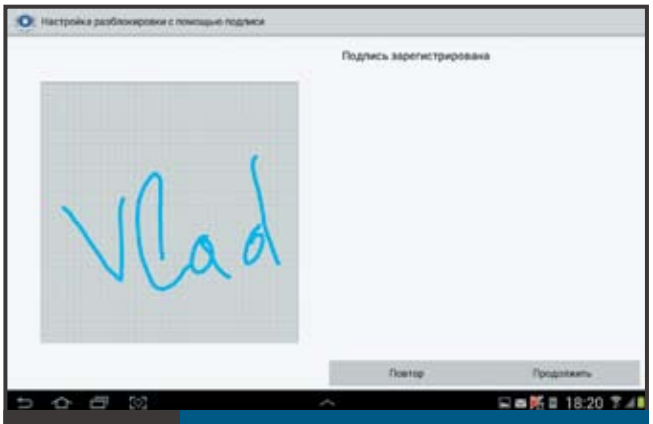
***Подпись.*** В данном случае вам необходимо написать ключевое слово (предлагается написать ваше имя) трижды. Именно с помощью данного слова и будет разблокировано ваше устройство (экран 8).

***Экран.*** Этот вариант имеет среднюю степень безопасности. Для его использования необходимо соединить в любом порядке не менее четырех точек на рисунке (экран 9). Отмечу, что, если вы забыли экран:

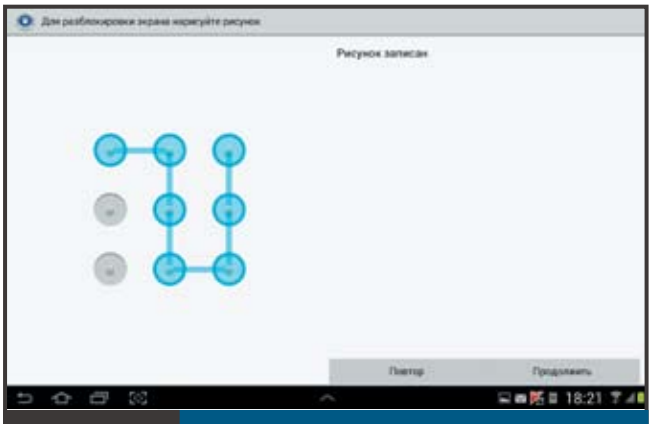
- количество неверных попыток рисования ограничено (5 раз), в различных моделях телефонов количество попыток может доходить до 10 раз;
- после того как вы использовали все попытки, но так и не нарисовали экран правильно, телефон блокируется на 30 секунд;
- телефон запрашивает логин и пароль вашей учетной записи Gmail;
- этот метод сработает только в том случае, если телефон или планшет подключен к Интернету. В противном случае производится перезагрузка и возврат к настройкам производителя.

***PIN-код.*** Последовательность цифр PIN-кода, не менее четырех символов. Естественно, чем длиннее строка цифр, тем выше уровень безопасности.

***Пароль.*** Пароль — наиболее высокий уровень безопасности. Содержит сочетание букв и цифр. Если вы используете пароль для досту-




Экран 8 Подпись




Экран 9 Графический пароль

па, можете использовать вариант «Шифрование телефона».

### Шифрование памяти телефона

Данная функция доступна для смартфонов и планшетов, использующих операционную систему Android версии 4.0 и выше (экран 10). Вместе с тем в бюджетных моделях смартфонов она может отсутствовать. Вы сможете задействовать шифрование только в том случае, если у вас установлена блокировка экрана с помощью пароля. С помощью шифрования вы можете сохранить данные пользователя из памяти смартфона (планшета). Необходимо учесть, что программа при этом не шифрует SD-карту. Шифрование может занять до 1 часа в зависимости от объема памяти устройства.

Если вы забыли пароль, то единственным выходом является сброс до заводских настроек. Естественно, все пользовательские данные будут утеряны.

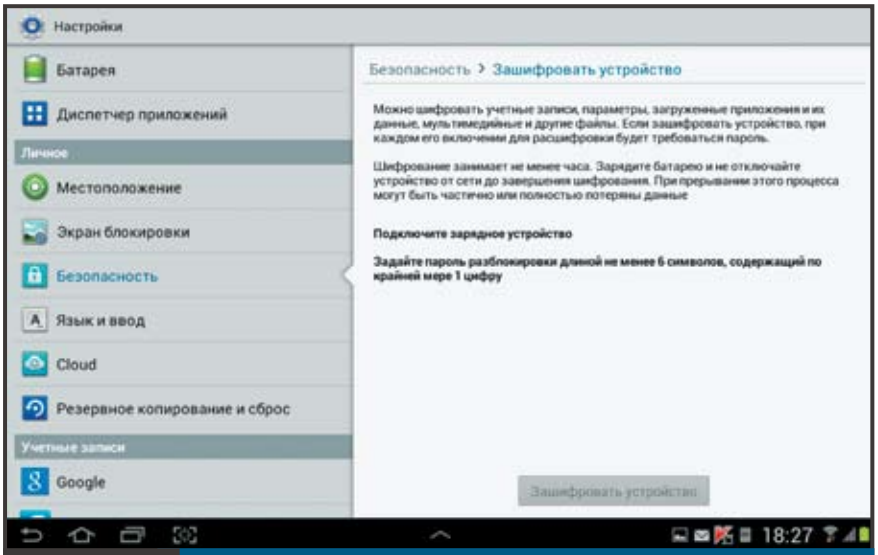
Недостатки реализации шифрования на планшетах с Android я бы выделил следующие:

1. Доступно только в Android 4.0 и выше.
2. Шифрование доступно не на всех моделях смартфонов (планшетов). Чаще всего встречается в телефонах от Samsung, HTC, Philips. Некоторые китайские модели тоже имеют функцию шифрования. У телефонов от HTC эта функция расположена в разделе «Память».
3. Пользователю необходимо постоянно вводить довольно сложный (6–10 символов) пароль, даже если надо просто позвонить.
4. Если вы хотите снять защиту, то сделать это можно только путем полной перезагрузки телефона, сбросив настройки до заводских.

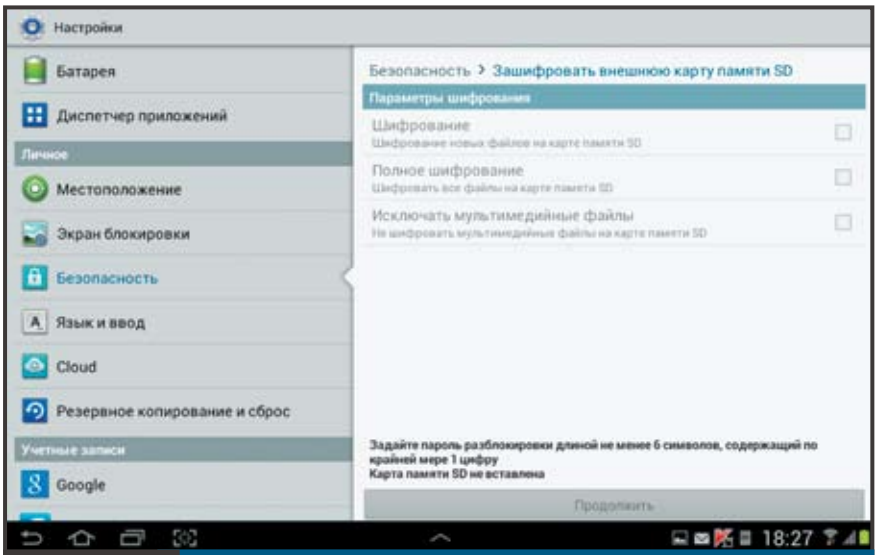
Очень важно отметить факт необратимости шифрования внутренней памяти телефона. Единственный способ отказаться от шифрования — полный сброс настроек.

### Шифрование внешней SD-карты

Данная функция входит в стандартный пакет Android 4.1.1 для планшетов. Во многих бюджетных устройствах она отсутствует. Функция обеспечивает надежную защиту данных на внешней SD-карте. Здесь могут храниться личные фотографии и текстовые файлы с информацией коммерческого и личного характера (экран 11).



Экран 10 Зашифровать устройство



Экран 11 Зашифровать внешнюю SD-карту

Шифрование внешней SD-карты позволяет зашифровать файлы на SD-карте, не изменяя их названий, файловой структуры, с сохранением предварительного просмотра графических файлов (иконки). Функция требует установки блокировочного пароля на дисплей длиной не менее 6 символов (из них не менее одной цифры). При смене пароля происходит автоматическое перешифрование.

### Баланс удобства и защиты

Встроенные средства защиты являются достаточно удобными инструментами защиты данных на мобильных телефонах и планшетах. Вместе с тем стоит учесть, что оптимальным для обеспечения безопасности на планшетах является полное шифрование всего устройства (включая SD-карту) и использование пароля длиной не менее 8 знаков, включающего символы трех наборов из четырех.

**Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor**