Визитка

ВЛАДИМИР БЕЗМАЛЫЙ, *MVP, KL CP,*
Microsoft Security Trusted Advisor, bezmaly@hotmail.com

Аутентификация в Windows 10

В отличие от Windows 8 в Windows 10 можно отсканировать любое число пальцев. Но я настоятельно рекомендую провести эту операцию для всех 10. Рассмотрим настройку разных способов аутентификации в Windows 10

Сегодня только ленивый не слышал о проблеме паролей. Но, увы, пользователи свои пароли регулярно забывают либо выбирают их чрезвычайно легкими для последующего взлома. В целях создания удобств аутентификации для пользователей в Windows 10 применяются те же методы, что и в Windows 8. То есть выбор графического пароля, создание ПИН-кода и биометрическая аутентификация. Причем следует учесть, что вначале создается пароль, затем ПИН-код, и только после этого становится доступной биометрическая аутентификация с помощью отпечатка пальца.

Давайте рассмотрим подробнее, как это делается.

Итак, вы установили пароль, когда устанавливали Windows, и решили его сменить. Для этого выберите «Пуск → Параметры → Учетные записи» (см. рис. 1) и перейдите в «Параметры входа» (см. рис. 2).

Для использования технологии Windows Hello потребуется создать ПИН-код. Для этого выбираем «Добавить ПИН-код» (см. рис. 3).

После того как ПИН-код установлен, можно настроить вход по отпечатку пальца. Для этого вначале придется войти с ПИН-кодом (см. рис. 4), а уж затем настраивать вход по отпечатку пальца (см. рис. 5).

В отличие от Windows 8 в Windows 10 можно отсканировать любое число пальцев. Но я настоятельно рекомендую провести эту операцию для всех 10. Ведь руки могут быть грязными, или вы можете травмироваться.

Рисунок 1. Учетные записи

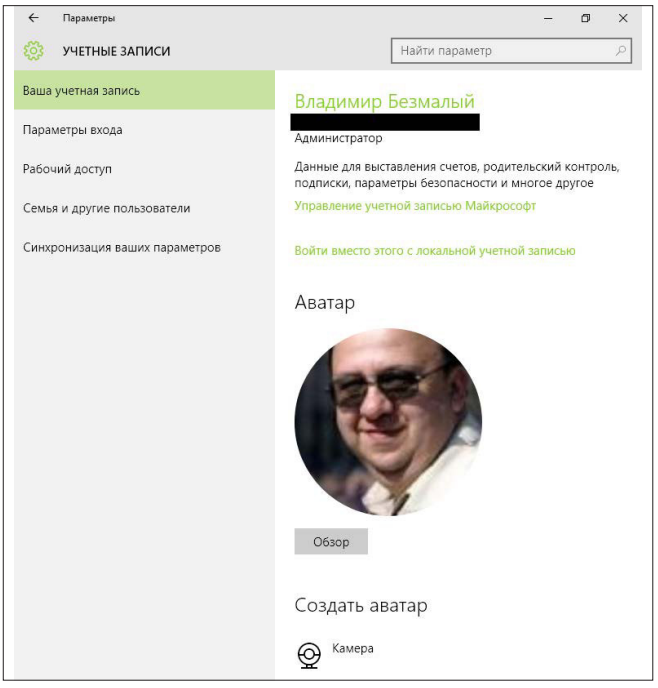
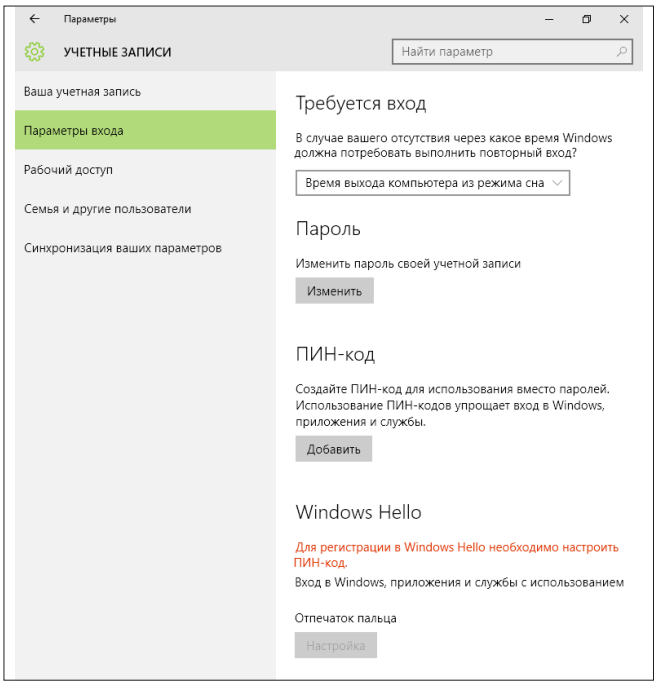


Рисунок 2. Параметры входа



Но, с другой стороны, это не так страшно, ведь при входе вам каждый раз будут задавать вопрос, какой способ аутентификации выберете:

- Пароль
- ПИН-код
- Отпечаток пальца
- Графический пароль

Графический пароль

Выберите вариант «Графический пароль». В появившемся окне вначале нужно выбрать базовый экран (фотографию), который будет служить основой для пароля (см. рис. 6). Далее необходимо с помощью жестов, то есть касаясь экрана пальцами или двигая мышью, «нарисовать» на экране комбинацию окружностей, прямых линий и других геометрических элементов (см. рис. 7).

При этом можете выбрать на экране замкнутую область или соединить пару произвольных точек. Проделайте это трижды. Пароль готов, можете использовать его для аутентификации. Вместе с тем стоит учесть, что уже известны случаи успешных атак на графический пароль.

До недавних пор атака на такие пароли считалась невозможной, т.е. осуществить атаку перебором (brute force) не представлялось возможным, поскольку пользователь, как правило, рисует пальцем или курсором мыши произвольную фигуру на произвольной фотографии.

Ученые из университетов Аризоны и Делавэра, а также исследователи из GFS Technology нашли способ взлома графических паролей. Для осуществления атаки brute force они применили систему распознавания образов и разработали специальное приложение, перебирающее варианты в порядке снижения их вероятности. Как правило, на изображениях людей пользователь чаще всего отмечает или обводит глаза и носы, далее в порядке убывания частоты использования следуют руки и пальцы, рты и челюсти, лица и головы.

Данный способ взлома пароля срабатывает на фотографиях весьма успешно. Стоит отметить, что системы справляются с определением графического пароля даже на портретах, где, кроме лица, запечатлены и нестандартные объекты.

Персонализированный вход в систему

Фактически графический пароль состоит из двух компонентов:

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

Вы сами выбираете картинку, что поможет лучше запомнить пароль, и сами решаете, какие ее части наиболее интересны.

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.

Рисунок 3. Настройка ПИН-кода

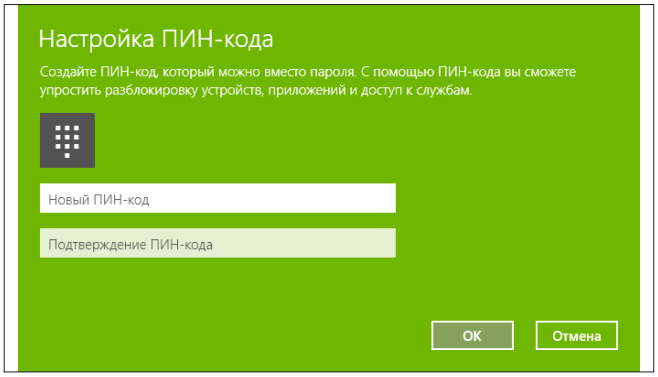


Рисунок 4. Вход по ПИН-коду

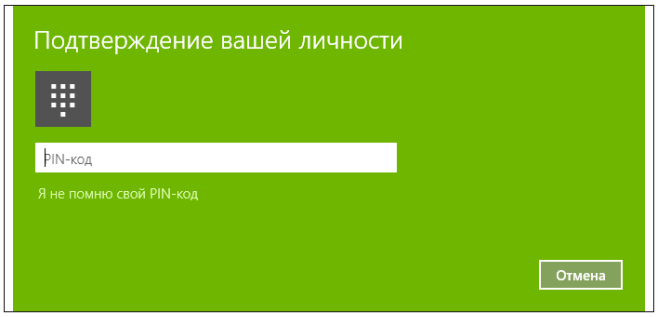


Рисунок 5. Сканирование отпечатка пальца

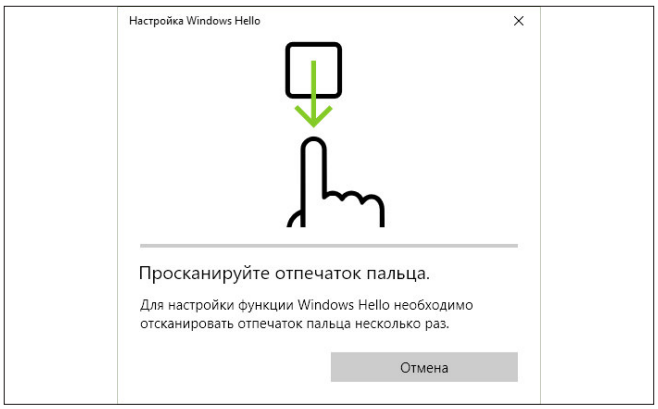
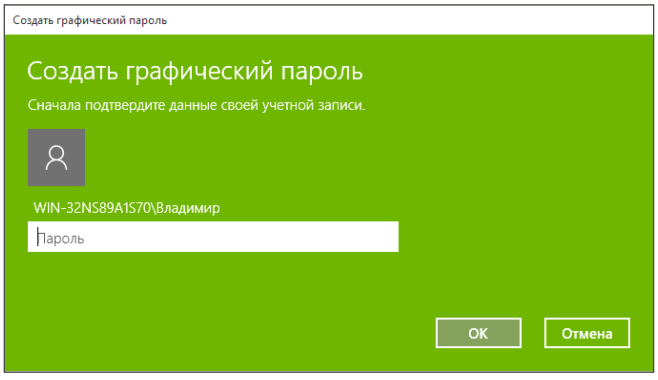


Рисунок 6. Графический пароль



Как работает графический пароль

После того как изображение выбрано, 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 центра, радиус и направление. Для касания запоминаются координаты точки касания.

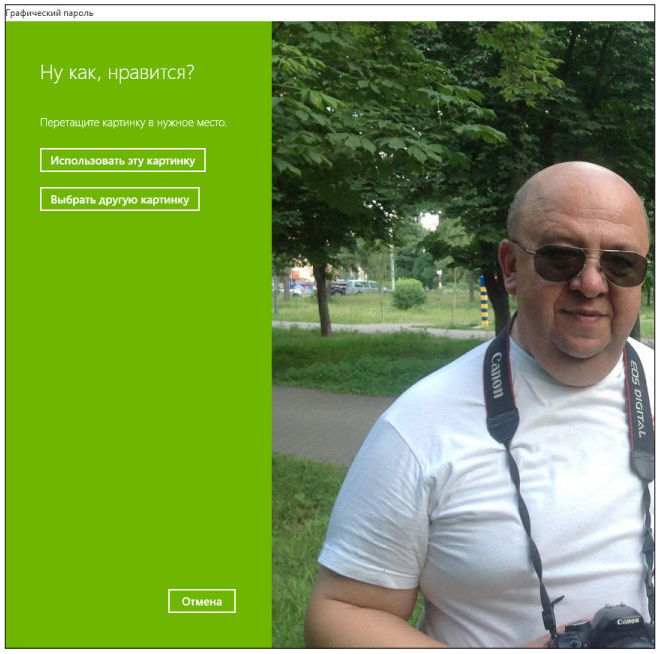
При попытке выполнения регистрации с помощью графического пароля введенные жесты сравниваются с набором жестов, введенных при настройке графического пароля. Рассматривается разница между каждым жестом и принимается решение об успешности проверки подлинности на основе найденного количества ошибок. Если тип жеста неправильный (должен быть круг, а вместо него линия), проверка подлинности не будет пройдена. Если типы жестов, порядок ввода и направления совпадают, то рассматривается, 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 ПИН-кодом и простым текстовым паролем.

Анализ количества уникальных комбинаций ПИН-кода довольно прост. В четырехразрядном ПИН-коде (4 разряда с 10 независимыми возможными значениями в каждом из них) может быть 10 в четвертой степени или 10 000 уникальных комбинаций.

Рисунок 7. Настройка графического пароля



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 26^n 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 восьми букв, имеет 208 миллиардов 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» [1].

Как можно заметить, использование трех жестов обеспечивает значительное количество уникальных комбинаций жестов и такую же надежность, как у пароля из пятишести случайно выбранных знаков.

Уточним: графический пароль добавлен в качестве способа регистрации в системе как дополнение к текстовому паролю, а не вместо него!

Вместе с тем необходимо отметить, что, несмотря на удобство биометрической аутентификации, она, на мой взгляд, остается все же скорее именно удобством, а не самостоятельным методом. Почему?

Да потому, что при создании новой учетной записи пользователя в системе мы, как обычно, должны вначале ввести его пароль и лишь затем приступить к биометрической аутентификации. Нельзя сделать вход в операционную систему без ввода пароля, используя только средства биометрии. Кроме того, стоит вспомнить и о недостатках биометрической аутентификации. Поговорим об этом немного подробнее.

Для аутентификации в Windows 10 применяется учетная запись от Microsoft. При этом данная учетная запись характеризуется двумя параметрами – именем пользователя (логин) и паролем. Если для входа на сайт и OneDrive вы используете двухэтапную аутентификацию, то при первом входе в систему от вас потребуют и получение кода в виде SMS-сообщения или другим удобным способом.

Некоторым пользователям не очень-то удобно каждый раз набирать пароль (или они его забывают по какой-то причине). Для них еще в Windows 8 были придуманы следующие способы аутентификации:

- графический пароль;
- ПИН-код;
- биометрическая аутентификация (по отпечатку пальца; сегодня сюда добавляется сканирование радужной оболочки глаза).

Однако стоит отметить, что все эти способы – лишь удобство. И применить их без обычного пароля невозможно!

К недостаткам биометрической аутентификации по отпечаткам пальцев, без сомнения, можно отнести тот факт,

что большинство используемых сегодня на ПК и планшетах сканеров довольно легко скомпрометировать муляжами. А изготовить муляж отпечатка совсем просто.

Кроме того, использование биометрических сканеров для аутентификации, на мой взгляд, опасно еще и тем, что сам цифровой «отпечаток» при этом хранится на ПК локально и теоретически есть возможность его хищения.

Если вы по какой-то причине не можете войти в свою учетную запись с помощью отпечатка пальца, вы всегда можете набрать свой пароль.

Что нужно учесть

Вместе с тем стоит учесть, что аутентификация в Windows 10 возможна и с помощью учетной записи Live ID, биометрической аутентификации, а также ПИН-кода. В более старых версиях операционной системы пароль на домашнем компьютере хранился в файле типа SAM. Соответственно, для компрометации этого пароля злоумышленнику нужен был физический доступ к системе и привилегии SYSTEM. Что же получается сегодня? С выходом Windows 10 потенциальному злоумышленнику будет куда легче скомпрометировать 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 ПИН, 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. Таким образом, узнав пароль Live ID, несложно восстановить и оригинальный текстовый пароль.

Управление через политики

Несомненно, новые системы аутентификации сделаны в угоду конечному пользователю. Так что в плане удобства пользователь, разумеется, выиграет. Для тех же из вас, кто озабочен устойчивостью парольной аутентификации, разработчики Microsoft предусмотрели отключение графического пароля с помощью редактора локальной групповой политики.

Несмотря на появление новых способов аутентификации, необходимо отметить, что базовым в любом случае остается парольный способ

Для этого необходимо набрать в командной строке:

```
gpedit.msc
```

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

• • •

Несмотря на появление новых способов аутентификации, необходимо отметить, что базовым в любом случае остается парольный способ. Все остальные – это скорее удобство, а не безопасность. EOF

[1] Статья Стивена Синофски «Выполнение входа с помощью графического пароля» – http://blogs.msdn.com/b/b8_ru/archive/2011/12/22/signing-picture-password.aspx.

Ключевые слова: безопасность, пароль, аутентификация, ПИН.

Таблица 1. Количество уникальных паролей в зависимости от длины пароля

Длина пароля	Уникальные пароли
1	26
2	676
3	17576
4	456976
5	1181376
6	308915776
7	80318110176
8	208827064576

Таблица 2. Количество уникальных комбинаций из нескольких жестов

Длина	10-разрядный ПИН-код	Простой пароль из знаков a-z	Графический пароль из нескольких жестов
1	10	26	2554
2	100	676	1581773
3	100	17576	1155509083
4	10000	456976	612157353732
5	100000	11881376	398046621309172
6	1000000	308915776	
7	10000000	803181176	
8	100000000	208827064576	