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 вам 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;

• PIN-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!

Биометрическая аутентификация в Windows 10

Для того чтобы использовать биометрическую аутентификацию, вы должны выбрать: Пуск — Параметры — Учетные записи — Параметры входа — Отпечаток пальца.

После этого вам предложат отсканировать отпечатки ваших пальцев. Чтобы использовать отпечаток пальца, сначала необходимо вначале четыре раза добавить его в базу для запоминания, а затем проделать ту же операцию в открывшемся новом окне еще четыре раза. Таким образом, сканирование каждого пальца придется выполнить восемь раз. Не поленитесь сделать это для всех десяти пальцев. Ведь вполне возможна ситуация, когда по какой-то причине (загрязненный датчик, порез на пальце и т. д.) отпечаток просто не распознается.

К недостаткам биометрической аутентификации по отпечаткам пальцев, без сомнения, можно отнести тот факт, что большинство используемых сегодня на ПК и планшетах сканеров довольно легко можно 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.

Графический пароль

Выберите вариант «Графический пароль». В появившемся окне вначале нужно 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 на экране замкнутую область или соединить пару произвольных точек. 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.

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.

Как работает графический пароль

После того как вы выбрали изображение, на нем формируется сетка. Самая длинная сторона изображения разбивается на сто сегментов, затем разбивается короткая сторона на столько же сегментов 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, с помощью которого определяется направление рисования линии. Для окружности запоминаются координаты точки центра, радиус и направление. Для касания запоминаются координаты точки касания.

При попытке 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 (скажем, 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.

Как настроить двухфакторную аутентификацию при входе в Windows 10

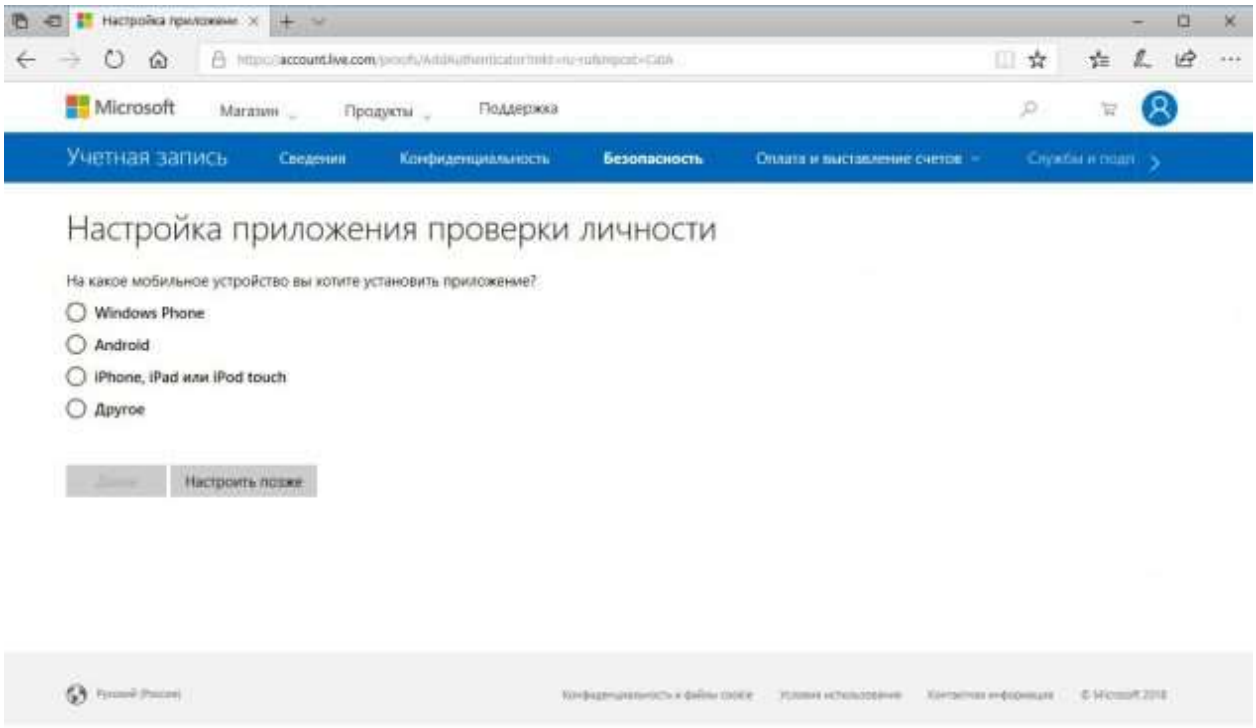
Двухфакторная аутентификация значительно повышает защиту вашего компьютера. Даже если злоумышленник каким-то образом узнает ваш пароль, он всё равно не сможет войти в систему без случайно генерируемого кода на вашем телефоне.

Чтобы настроить эту опцию, прежде всего нужно установить на смартфон приложение для аутентификации. Лучше выбрать Microsoft Authenticator, родное приложение для Windows 10, или популярное и универсальное Google Authenticator.

Теперь включим двухэтапную аутентификацию в Windows 10. Учтите, что для этого придётся связать свою учётную запись с аккаунтом Microsoft, если вы ещё этого не сделали.

1. Откройте «Параметры» и выберите «Учётные записи».
2. На вкладке «Ваши данные» щёлкните на «Войти вместо этого с учётной записью Microsoft».
3. Выберите «Управление учётной записью Microsoft». В браузере откроется страница с параметрами вашей учётной записи. Отыщите раздел «Безопасность».
4. Откройте «Дополнительные параметры безопасности». Система может попросить ввести код подтверждения, отправленный на ваш электронный адрес.
5. Найдите на странице пункт «Настройка двухшаговой проверки» и включите двухфакторную аутентификацию.

Теперь нажмите на «Установить приложение проверки личности». Вам будет предложено выбрать вашу мобильную ОС и установить приложение Microsoft Authenticator. Также вы можете выбрать пункт «Другое», если хотите использовать Google Authenticator.



На экране появится QR-код. Просканируйте его вашим мобильным аутентификатором, и аккаунт настроится автоматически.

Теперь при входе в Windows 10 система будет запрашивать случайный код, генерируемый приложением на вашем телефоне.