УДК 004.457 **Технические науки**

Митрошина Е.В., *студентка 5 курса электротехнического факультета,*
Пермский национальный исследовательский политехнический университет

ПРИМЕНЕНИЕ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ ФУНКЦИИ WINDOWS HELLO ОТ MICROSOFT

Аннотация. В статье рассматривается обеспечение безопасности операционной системы Windows с помощью функции биометрической проверки подлинности Windows Hello.

Ключевые слова: биометрические данные, идентификация, аутентификация, информационная безопасность.

Abstract. The article describes the security of the Windows operating system using function biometric authentication Windows Hello.

Keywords: biometric data, identification, authentication, information security.

В наше время одним из самых перспективных направлений в системах контроля доступа становится использование биометрических данных человека. Такой способ аутентификации очень удобен, так как кражи идентификационных данных вызывают обеспокоенность в современном обществе. В настоящее время такие методы аутентификации, как пароли и различные электронные ключи, которые можно украсть, потерять или забыть, уже не достаточны для обеспечения безопасности. Соответственно использование биометрических данных человека, становится одним из самых перспективных направлений в системах контроля доступа [1].

Windows Hello — это функция биометрической проверки подлинности, повышающая ее надежность и обеспечивающая защиту от возможной

подмены информации благодаря сопоставлению отпечатков пальцев и распознаванию лиц [2].

Windows Hello позволяет сотрудникам предприятия использовать в качестве альтернативного способа разблокировки устройства отпечатки пальцев или распознавание лиц. Проверка подлинности осуществляется за счет ввода уникального биометрического идентификатора в то время, как происходит получение доступа к учетным данным Microsoft Passport конкретного устройства. Эта функция исключает возможности перемещения между устройствами, не предполагает передачу данных на сервер и не может быть легко удалена с устройства. Таким образом, если одно устройство используют несколько сотрудников предприятия, то каждый из них будет получать доступ с помощью своих собственных биометрических данных.

Биометрические данные, используемые функцией Windows Hello, хранятся только на локальном устройстве, что позволяет обеспечивать защиту информации от различных атак. Так как уникальные биометрические данные не перемещаются и не передаются на внешние устройства или серверы, что обеспечивает отсутствие единственной точки сбора информации, которая может быть скомпрометирована и в результате чего злоумышленник получит доступ к биометрическим данным.

Служба Hello призвана решать типичные проблемы пользователей, возникающие при работе с паролями:

-пароли могут быть трудны для запоминания, и пользователи часто повторно используют пароли на нескольких сайтах;

-взломы сервера могут раскрывать симметричные сетевые учетные данные;

-пароли могут подлежать атакам с повторением пакетов;

-пользователи могут непреднамеренно предоставить свой пароль вследствие фишинга [3].

Основные преимущества функции Windows Hello:

1. Данная функция повышает уровень защиты учетных данных, так как осуществляет проверку подлинности по средствам подключения к Microsoft Passport. Теперь злоумышленнику гораздо сложнее получить доступ к нужной информации, так как появляется необходимость в одновременном получении устройства и биометрических данных.

2. Простая проверка подлинности. Становится не актуальной проблема «забытых паролей».

3. Функция Windows Hello встроена в операционную систему, поэтому добавлять дополнительные биометрические устройства и политики в рамках скоординированного развертывания или для отдельных сотрудников или групп можно с использованием групповой политики или поставщика служб конфигурации (CSP) управления мобильными устройствами (MDM) [2].

Биометрическое распознавание обеспечивает более надежную аутентификацию пользователей, чем пароли и удостоверяющие личность документы, и является единственным способом обнаружения злоумышленников. Хотя биометрические системы не являются абсолютно надежными, исследователи значительно продвинулись вперед по пути идентификации угроз. Также особое внимание уделяется разработке мер противодействия угрозам безопасности, что значительное повышает надежность систем, а новые алгоритмы для защиты биометрических шаблонов частично устраняют опасения по поводу защищенности систем [4].

Библиографический список

1. Биометрическая аутентификация: проблемы будущего. [Электронный ресурс] // Information Security. URL: http://www.itsec.ru/articles2/Oborandteh/biometricheskaya-autentifikaciya-problemy-buduschego (дата обращения: 15.01.2017).

2. Биометрия Windows Hello на предприятии. [Электронный ресурс]. URL: https://technet.microsoft.com/ru-ru/library/mt633827(v=vs.85).aspx (дата обращения: 15.01.2017).

3. Управление проверкой личности с помощью Windows Hello для бизнеса. [Электронный ресурс]. URL: https://habrahabr.ru/company/microsoft/blog/314822/ (дата обращения: 16.01.2017).

4. Биометрическая аутентификация: защита систем и конфиденциальность пользователей. [Электронный ресурс]. URL: https://www.osp.ru/os/2012/10/13033122/ (дата обращения: 16.01.2017).