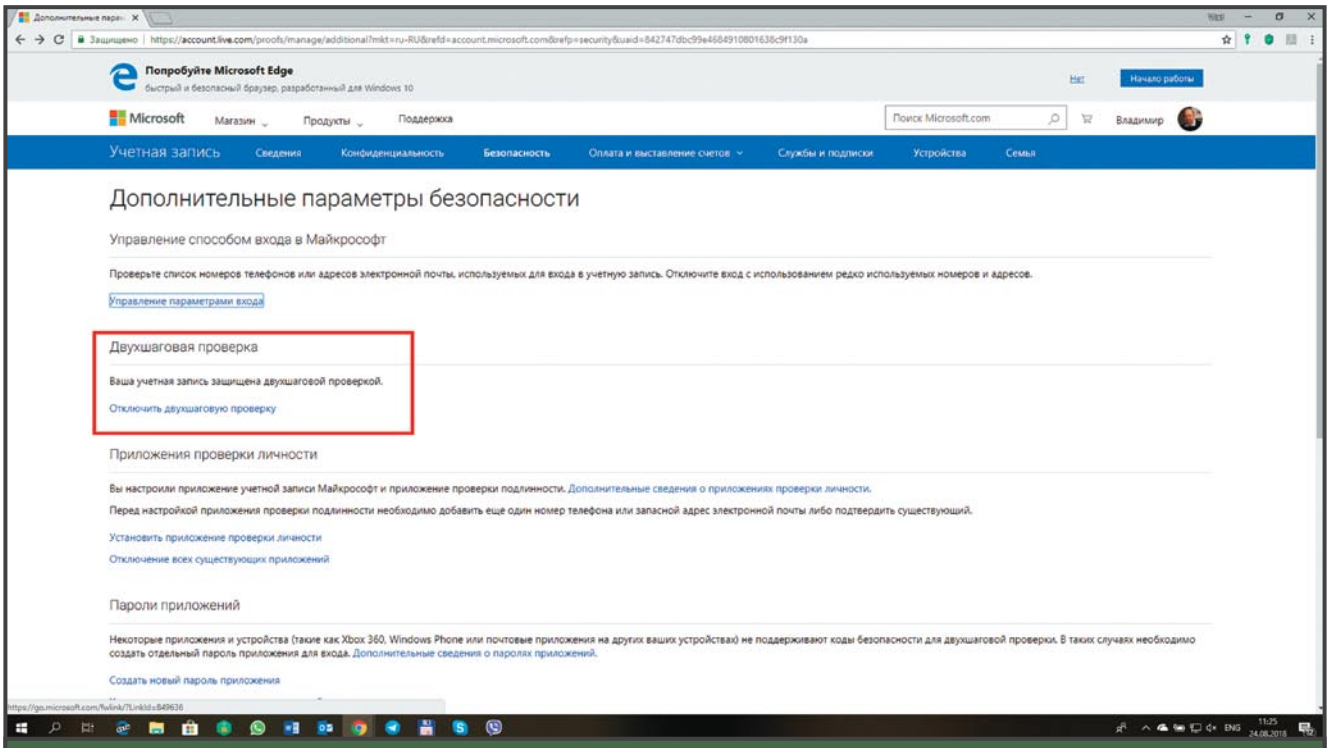
Аутентификация без SMS

Двухфакторная аутентификация в службах электронной почты и социальных сетях

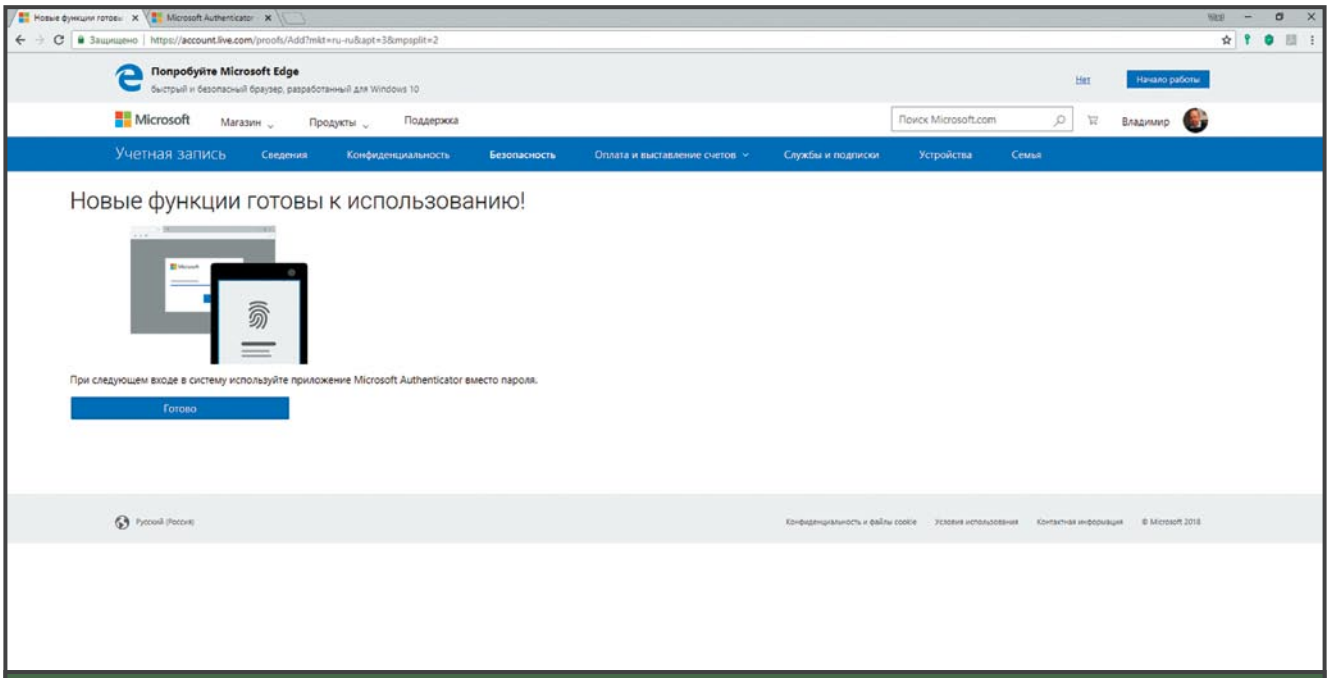
Владимир Безмалый

О двухфакторной (двухэтапной) аутентификации написано множество статей. И тем не менее до сих пор этот способ аутентификации не получил широкого распространения. Несмотря на то что уже много лет в службах Google применяется двухэтапная аутентификация, на сегодня с ней работает порядка 10% пользователей. Почему так происходит? Попробуем разобраться.

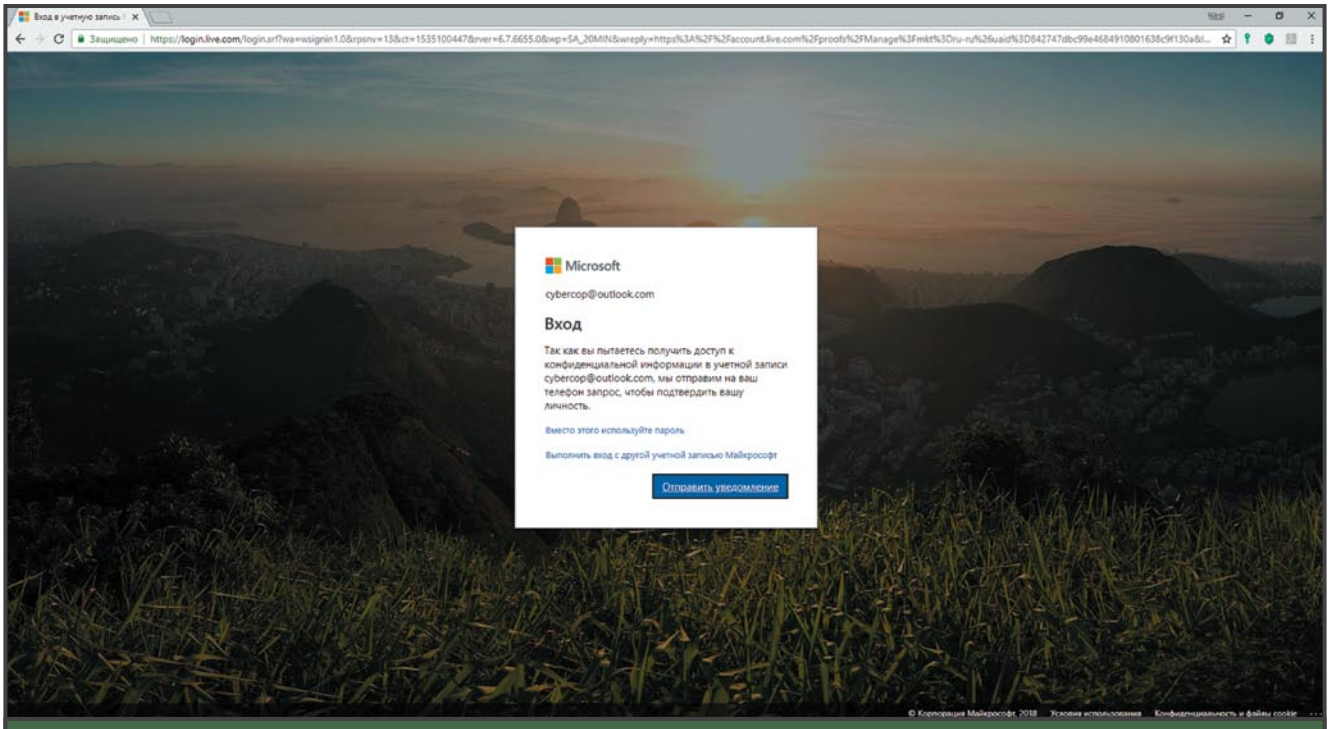
Двухфакторной называется такая аутентификация, при которой производится проверка двух разных факторов. Обычно факторы аутентификации подразделяются на знание чего-то, обладание чем-то и биометрию. Двухфакторная аутентификация должна состоять из факторов разных типов. Например, использование смарт-карты с обязательным вводом PIN-кода: первый фактор — владение смарт картой, а второй — знание PIN-кода. Часто встречаются термины «двухфакторная аутентификация» и «двухэтапная (двухшаговая) аутентификация».



Экран 1. Дополнительные параметры безопасности



Экран 2. Используйте Microsoft Authenticator



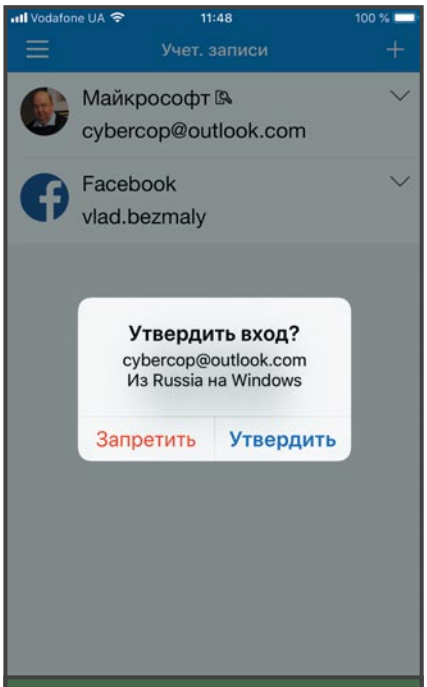
Экран 3. Вход

Двухэтапная аутентификация

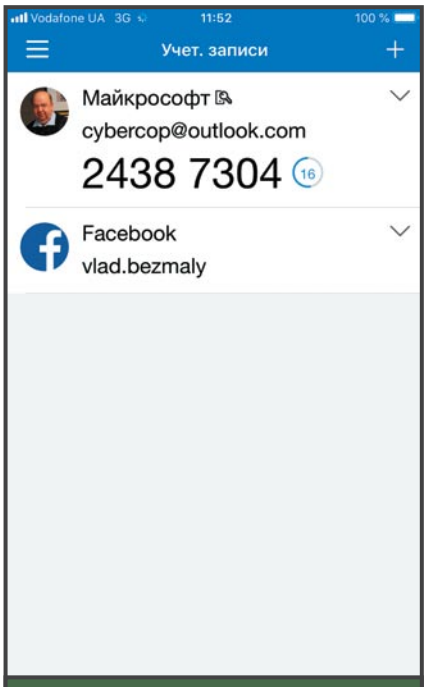
Двухэтапная аутентификация предусматривает два последовательных проверочных действия, они выполняются поэтапно. Примером такой двухэтапной аутентификации может служить достаточно распространенное совмещение проверки пароля с последующей проверкой одноразового кода из SMS. После ввода статического пароля приложение или сервер аутентификации проверяет его и, если пароль был верным, отправляет SMS на привязанный номер. Этот метод аутентификации требует предварительной проверки пароля, так как для того, чтобы отправить SMS-сообщение, нужно узнать, кому именно его отправлять. В качестве триггера на отправку сообщения используется событие успешной аутентификации по паролю.

Использование SMS для аутентификации

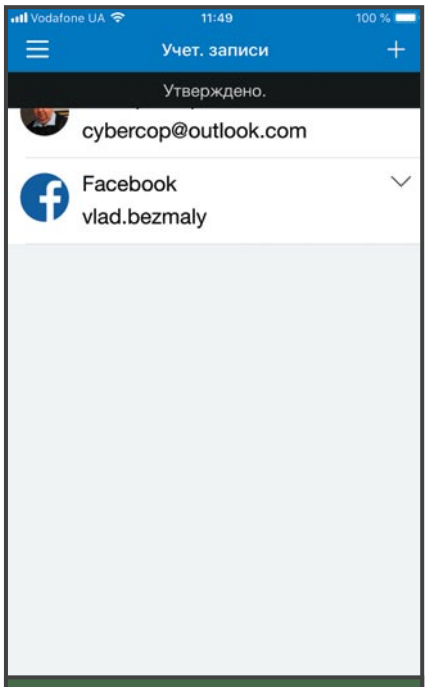
Напомню, что метод аутентификации, использующий SMS, организацией NIST сегодня применять для защиты не рекомендуется. Существует огромное количество примеров атак на этот метод



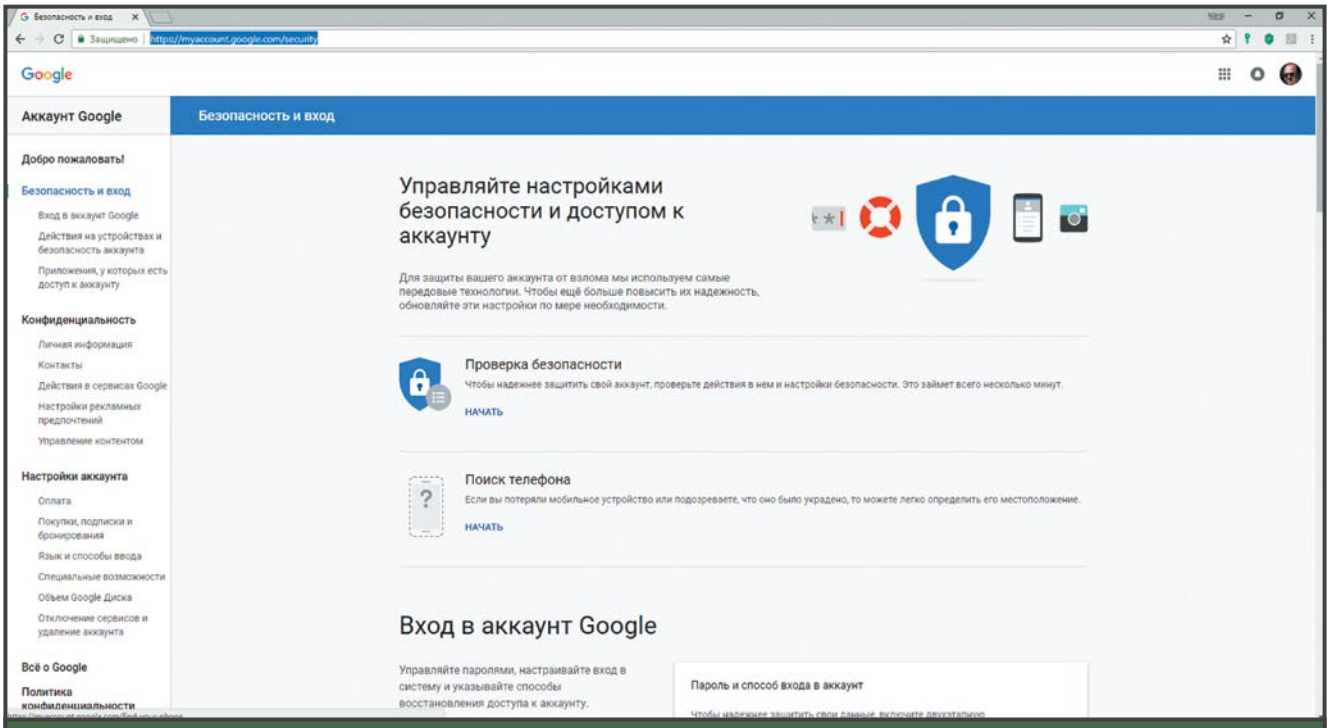
Экран 4. Утверждение входа на экране iPhone



Экран 5. Подтверждение входа с помощью кода



Экран 6. Вход утвержден



Экран 7. Настройка безопасности Google

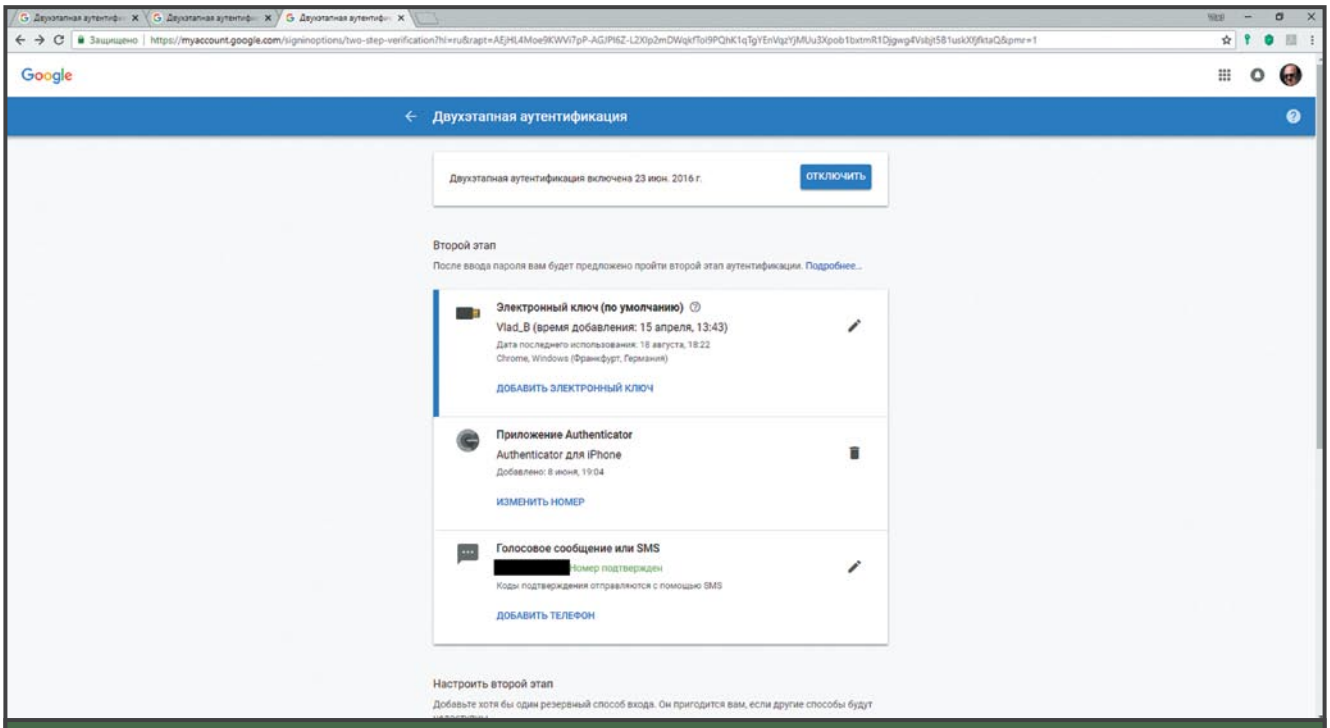
аутентификации. А значит, нет гарантии того, что правильно введенный код из SMS однозначно подтверждает владение телефоном (SIM-картой).

Естественно, ваша защита должна быть адекватна угрозам и потенциальному ущербу. В некоторых случаях SMS может быть удобным способом доставки второго фактора, например когда речь не идет о доступе к финансам или конфиденциальной информации.

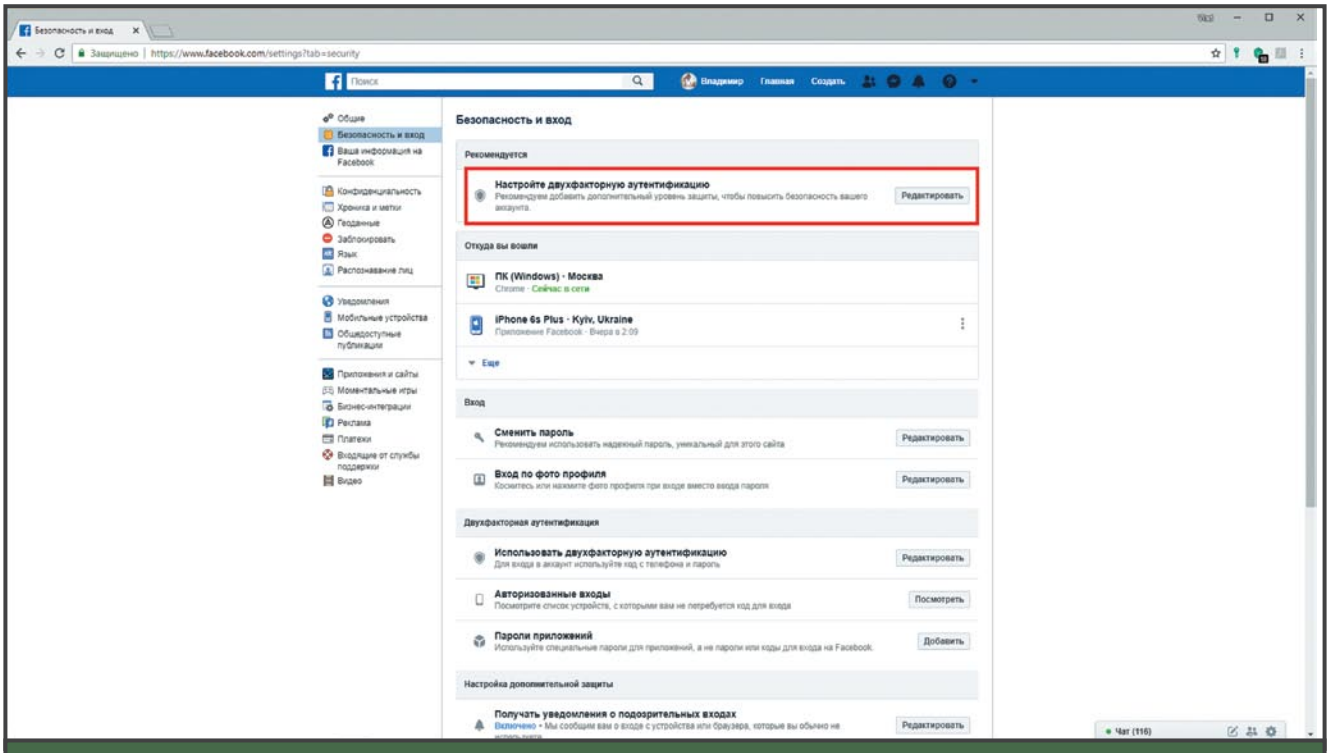
Почему же пользователи не применяют двухэтапную аутентификацию? Как мы убедились, в наше время не всегда можно доверять аутентификации с помощью SMS. На то есть несколько причин, и одна из них — атаки типа «человек посередине», Man-In-The-Middle (MITM). Сегодня многие говорят о том, что можно перехватить SMS и, соответственно, скомпрометировать двухэтапную аутентификацию. Но действительно ли все так плохо?

Двухэтапная аутентификация в службах Microsoft

Начиная с Windows 10 многие стали использовать для аутентификации учетные записи Microsoft. Для

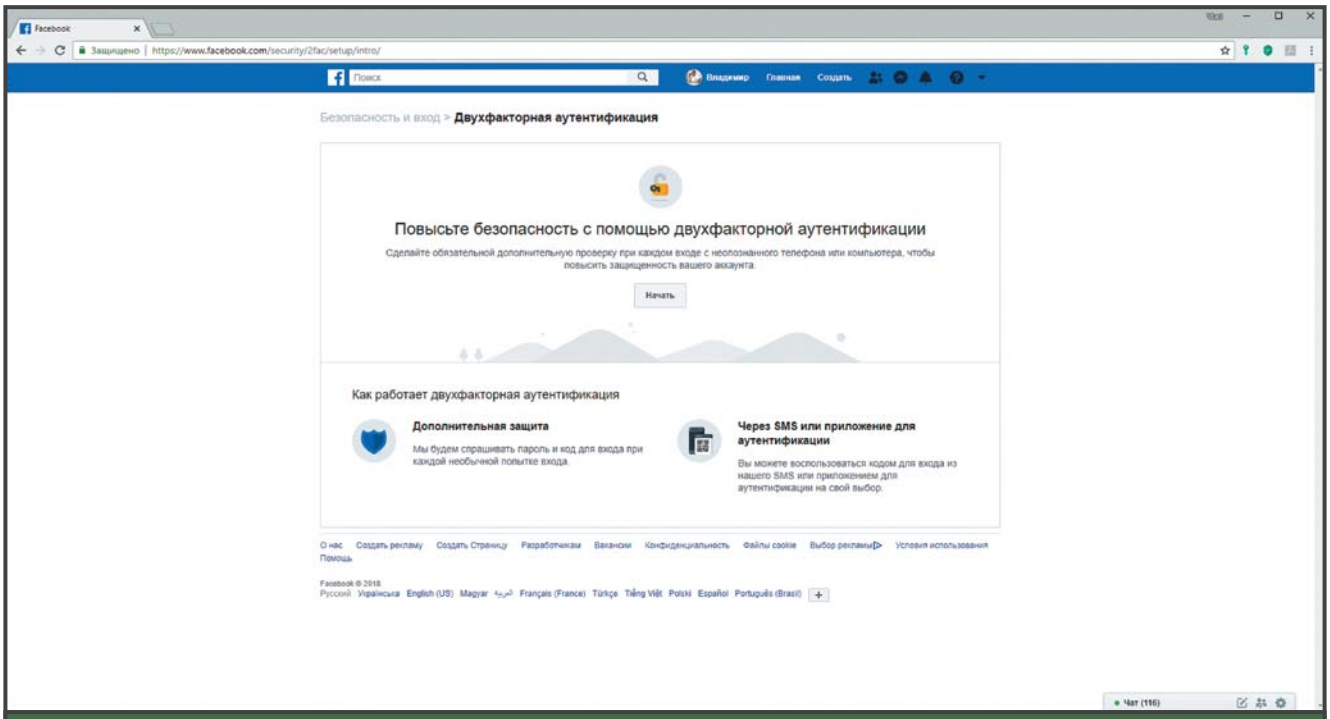


Экран 8. Выбор второго этапа аутентификации

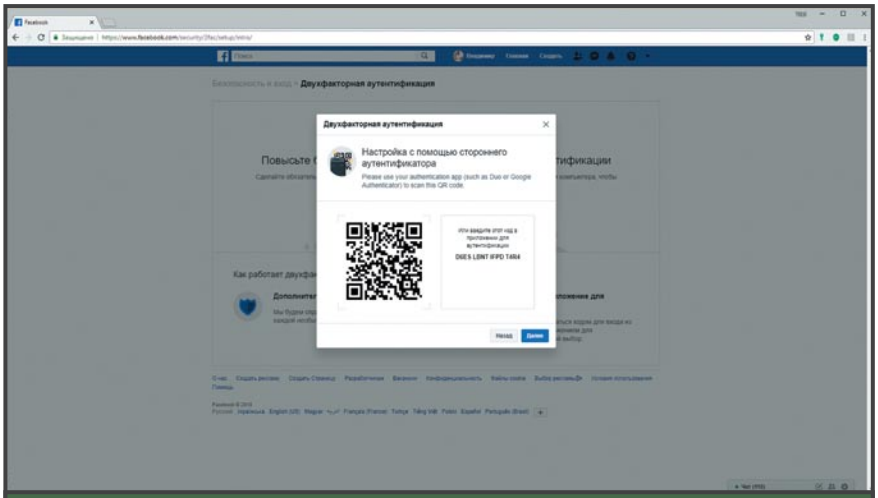


Экран 9. Настройки двухэтапной аутентификации Facebook

аутентификации обычно применяется просто пароль. Однако, если вы решите настроить двухэтапную аутентификацию, потребуется зайти на сайт www.outlook.com и выбрать пункты меню «Просмотр профиля», «Безопасность», «Дополнительные параметры безопасности» (экран 1). На данном этапе вы настроили получение SMS на указанный номер телефона. Но ведь нас с вами это не интересует, верно? Как же быть дальше? А дальше вы можете настроить генератор Microsoft Authenticator на своем мобильном устройстве, как показано на экране 2. Это приложение можно настроить на той же странице в «Приложении проверки личности» по адресу: https://www.microsoft.com/en-us/account/authenticator? cmp=ro5tgz_myvfdy. Здесь же вы сможете при желании выбрать другой язык страницы. Приложение Microsoft Authenticator доступно в магазинах Google Play или Apple Store.



Экран 10. Настройка двухфакторной аутентификации



Экран 11. Настройка с помощью стороннего приложения

Итак, второй этап выполнен, вы установили приложение. Теперь вы сможете получать второй фактор непосредственно на своем смартфоне, без помощи SMS (экран 3).

Вместе с тем, если вы используете iPhone, то вам на выбор будет предложено задействовать «пароль+код» или просто утверждать свой вход в систему непосредственно с телефона без ввода пароля либо нажатием на число, соответствующее появившемуся на экране, как показано на экране 4. При этом выбор осуществляется из трех возможных вариантов. Как видите, это очень удобно. Подтверждается ваш выбор (авторизация в службе) с помощью отпечатка пальца, как показано на экранах 5 и 6.

Двухэтапная аутентификация в Google

Для настройки двухэтапной аутентификации нужно использовать страницу https://myaccount.google.com/security (экран 7).

Выберите вариант «Двухэтапная аутентификация», как показано на экране 8. Таким образом, второй этап аутентификации может осуществляться как с помощью электронного ключа и генератора (приложение Authenticator), так и с помощью SMS. Я рекомендую использовать первые два способа как более безопасные.

Аутентификация в социальных сетях

Аутентификацию в социальных сетях мы рассмотрим на примере Facebook. Для включения двухэтапной аутентификации в Facebook пройдите по пунктам меню «Настройки», «Безопасность и вход», «Настройте двухфакторную аутентификацию» (экраны 9 и 10).

Схожим с ранее описанным образом вы сможете настроить двухфакторную аутентификацию с помощью специального приложения, как показано на экране 11.

Итак, мы убедились, что сегодня для двухэтапной аутентификации вовсе не обязательно использовать SMS. Можно применять либо аппаратную аутентификацию (ключ), либо приложение-генератор.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, Kaspersky Lab Certified Consultant, Kaspersky Lab Certified Trainer, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor