УДК 004

Обзор методов двухфакторной аутентификации

Голубь Илья Сергеевич
Приамурский государственный университет имени Шолом-Алейхема
Студент

Глаголев Владимир Александрович
Приамурский государственный университет имени Шолом-Алейхема
к.г.н., доцент кафедры информационных систем, математики и правовой информатики

Аннотация
Данная статья посвящена обзору методов двухфакторной аутентификации. Проводится анализ существующих методов от Google и Яндекса, проведено сравнение, выявлены плюсы и недочеты.
Ключевые слова: безопасность, двухфакторная аутенфикация, методы двухфакторной аутенфикации.

Overview of two-factor authentication methods

Golub Ilya Sergeevich
Sholom-Aleichem Priamursky State University
Student

Glagolev Vladimir Alexandrovich
Sholom-Aleichem Priamursky State University
Candidate of Geographical Sciences, Assistant Professor of the Department of Information Systems, Mathematics and Legal Informatics

Abstract
This article provides an overview of two-factor authentication methods. The analysis of existing methods from Google and Yandex is conducted, a comparison is made, the pros and cons are revealed.
Keywords: security, two-factor authentication, two-factor authentication methods.

Актуальность двухфакторной аутенфикации в наше время очень высока. В наше время существует огромное количество разных уловок и способов украсть логин и пароль от учетной записи: вход на сайт через незаметную для пользователя подмену официального сайта; ввод учетных данных в социальных сетях; слабая защита сайта; использование небезопасных сертификатов и т.д.

Генерация самоподписанного сертификата и использование его для защиты данных было рассмотрено в данной статье [4]. В статье Л.Шапиро

рассмотрены разные методы двухфакторной аутенфикации, варианты внедрения и т.д. [7]. Еще один метод двухфакторной аутентификации, а именно метод клавиатурного подчерка, был рассмотрен в статье А.В. Еременко [3]. В работе Джозефа Гуалдони «Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication» описываются методы защиты транзакций с помощью двухфакторной авторизации с случайными кодами [1].

Целью работы является обзор вариантов аутенфикации у двух наиболее известных сервисов и написание инструкции к ее включению. Были поставлены следующие задачи: рассмотреть варианты двухфакторной аутенфикации в Google и Яндекс; найти различия, плюсы и недочеты; составить алгоритм включения данных возможностей.

Главной проблемой информационной безопасности данных являются слабые пароли. Наиболее правильный способ защиты данных в данной ситуации – это двухфакторная аутентификация. Такой способ аутентификации пользователя проходит в два этапа: ввод логина и пароля и ввод одноразового пароля, сгенерированного при помощи аппаратного токена, мобильного приложения, или полученного в SMS-сообщения.

Суть двухфакторной аутентификации заключается в том, что даже если мошенник сможет заполучить логин и пароль, то будет скомпрометирован всего лишь один фактор, так как для получения одноразового пароля (OTP) необходимо специальное устройство – токен, который находится только у пользователя [2].

Одним из самых известных и популярных решений для двухфакторной аутентификации является GoogleAuthenticator. Своей популярностью этот генератор одноразовых паролей обязан доступности открытого программного приложения (open-source) и возможность доработки функционала под нужды своей компании.

Но так как данный токен разработан только для авторизации в сервисах Google, в следствие этого возникают следующие недостатки: доработка возможна, но все изменения будут сделаны вами самостоятельно за дополнительные средства на свой страх и риск; нет никаких гарантий, что после внесения изменений, в приложении не откроется слабых мест, в случае взлома системы вся ответственность будет лежать на ваших же плечах.

Рассмотрим алгоритм включения двухфакторной авторизации в Google:

1. Нужно авторизоваться в аккаунте Google.

Рис.1 Панель приложений Google

2. Зайти в настройки аккаунта.

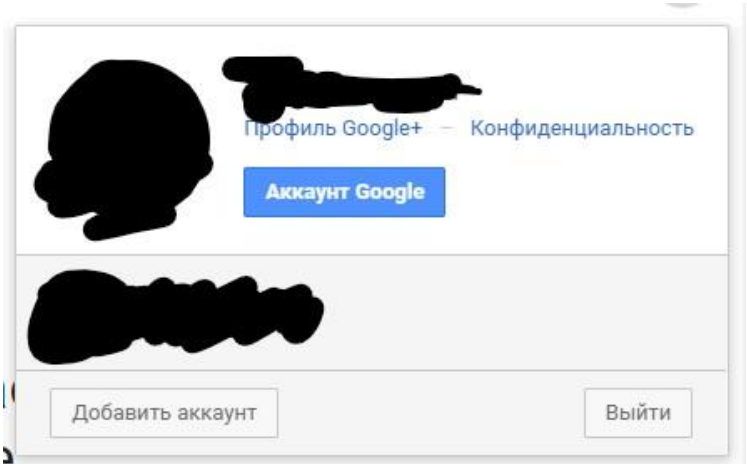

Рис. 2 Панель аккаунта Google

3. Зайти в раздел безопасность и выбрать пункт «Двухэтапная аутенфикация. Сервис запросит подтверждения того, что это ваш аккаунт и потребует ввести пароль, после этого откроется страница настроек двухфакторной аутенфикации.

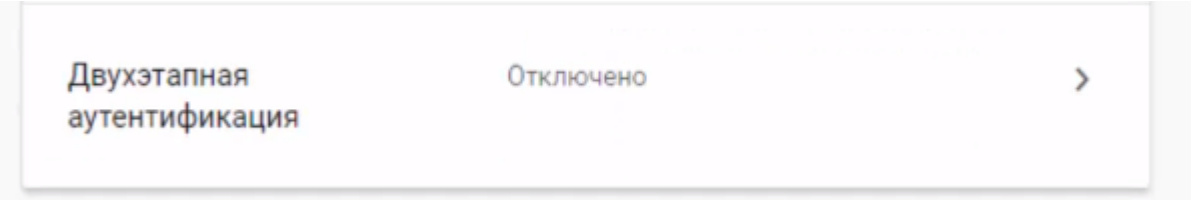

Рис. 3 Пункт меню безопасности Google

4. Потребуется выбрать нужный вам смартфон из авторизованных в Google и нажать кнопку «Отправить уведомление». Это действие нужно для подтверждения доступа к смартфону, возможно потребуется ввести номер телефона повторно.

5. Следующим этапом будет выбор способа получения кода для аутенфикации: смс или голосовое сообщение.

6. Через не большой промежуток времени на выбранный номер телефона придет сообщения с кодом для активации двухэтапной аутенфикации. Для завершения нужно будет ввести код в нужное поле и нажать кнопку «Включить».

7. При авторизации в аккаунте Google можно будет установить флажок на «Запомнить код на этом компьютере» и тогда система больше не будет запрашивать код для данного устройства.

Главный минус двухфакторной аутентификации Google – то, что это всего лишь токен, а для внедрения двухфакторной аутентификации нужен еще и сервер, соответственно, пользователю нужно будет разработать серверную часть самостоятельно [6].

У другого известного интернет-гиганта есть немного другой вид двухфакторной аутенфикации.

После включения двухфакторной аутентификации в Яндекс.паспорт вам надо будет установить приложение Яндекс.Ключ через App Store или Google Play. В форме авторизации на главной странице Яндекса, в Почте и Паспорте появились QR-коды. Для входа в учётную запись необходимо считать QR-код через приложение – и всё. Если считать QR-код не получается, например не работает камера смартфона или нет доступа к интернету, приложение создаст одноразовый пароль, который будет действовать всего 30 секунд.

Необходимо рассмотреть работу механизмов двухфакторной аутентификации. RFC 6238 или RFC 4226 двухэтапные. Первый этап – обычная аутентификация логином и паролем. Если он прошел успешно, сайт проверяет, «нравится» ему эта пользовательская сессия или нет. И, если «не нравится», просит пользователя «доаутентифицироваться». Распространенных методов «доаутентификации» два: отсылка SMS на привязанный к аккаунту номер телефона и генерация второго пароля на смартфоне. В основном для генерации второго пароля используется TOTP по RFC 6238. Если пользователь ввел второй пароль верно, сессия считается полностью аутентифицированной, а если нет, то сессия теряет и «предварительную» аутентификацию. Оба способа – отправка SMS и генерация пароля – доказательства обладания телефоном и потому являются фактором наличия. Пароль, вводимый на первом этапе, – фактор знания. Поэтому такая схема аутентификации – не только двухэтапная, но и двухфакторная.

Теперь перейдем к алгоритму активации двухфакторной авторизации в яндексе:

1. Необходимо подтвердить номер телефона, который привязан к аккаунту.

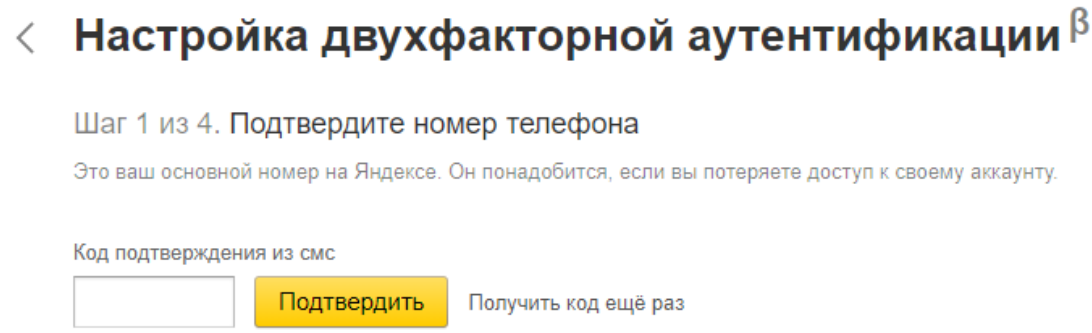

Рис. 4. Подтверждение номера телефона

2. Необходимо создать четырёхзначный пин-код для двухфакторной аутентификации, восстановить доступ при его утере можно будет только с помощью службы поддержки.

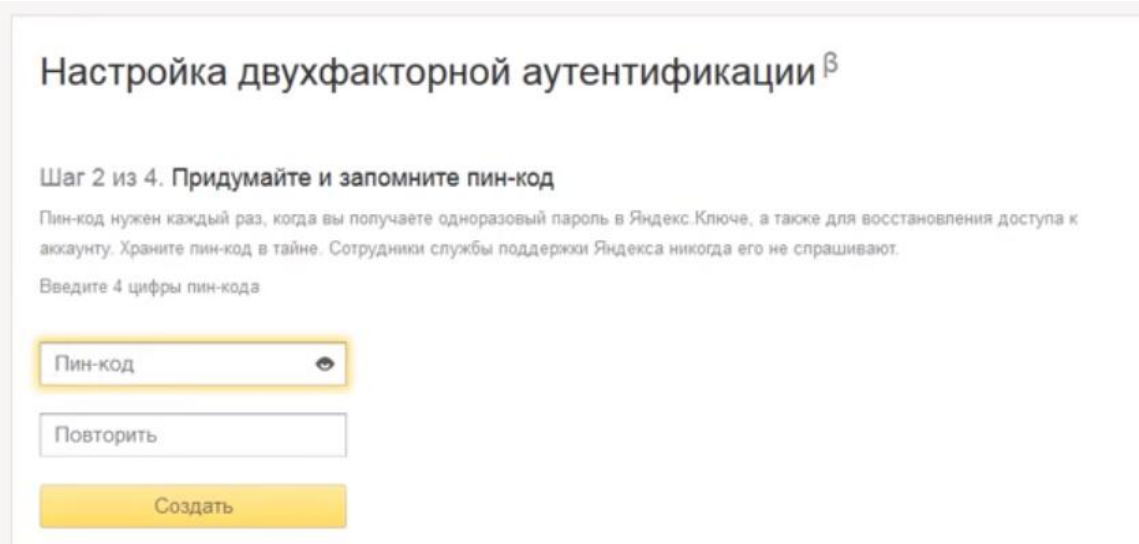

Рис. 5. Создание пин-кода

3. Необходимо скачать и установить приложение Яндекс.Ключ. Оно необходимо для того, что бы генерировать одноразовые пароли для аккаунта, его можно установить через AppStore и Google Play.

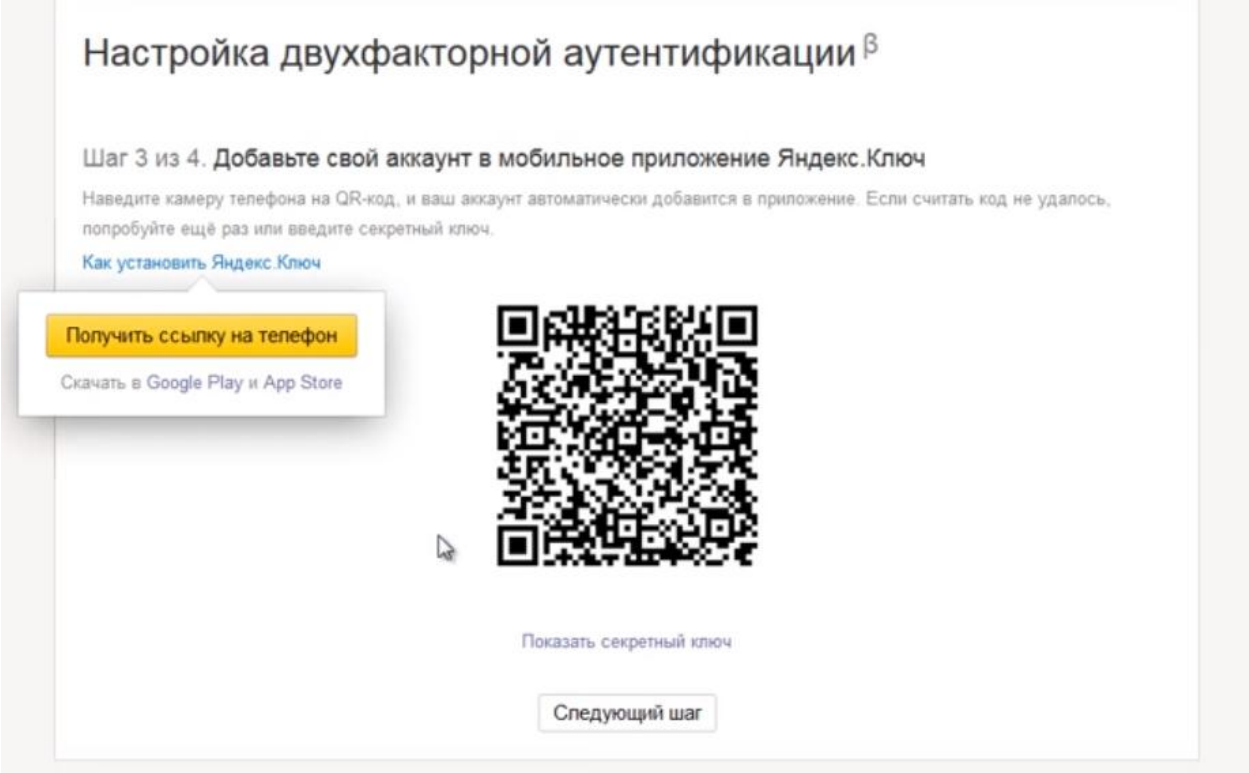

Рис. 6. Добавление аккаунта в мобильное приложение Яндекс.Ключ

4. Необходимо нажать в приложении кнопку добавить аккаунт в приложение и отсканировать с помощью камеры мобильного телефона QR-код, либо нужно нажать на кнопку показать секретный ключ и добавить его вручную.

5. Необходимо ввести одноразовый пароль для проверки правильности настроек, тогда включится двухфакторная авторизации.

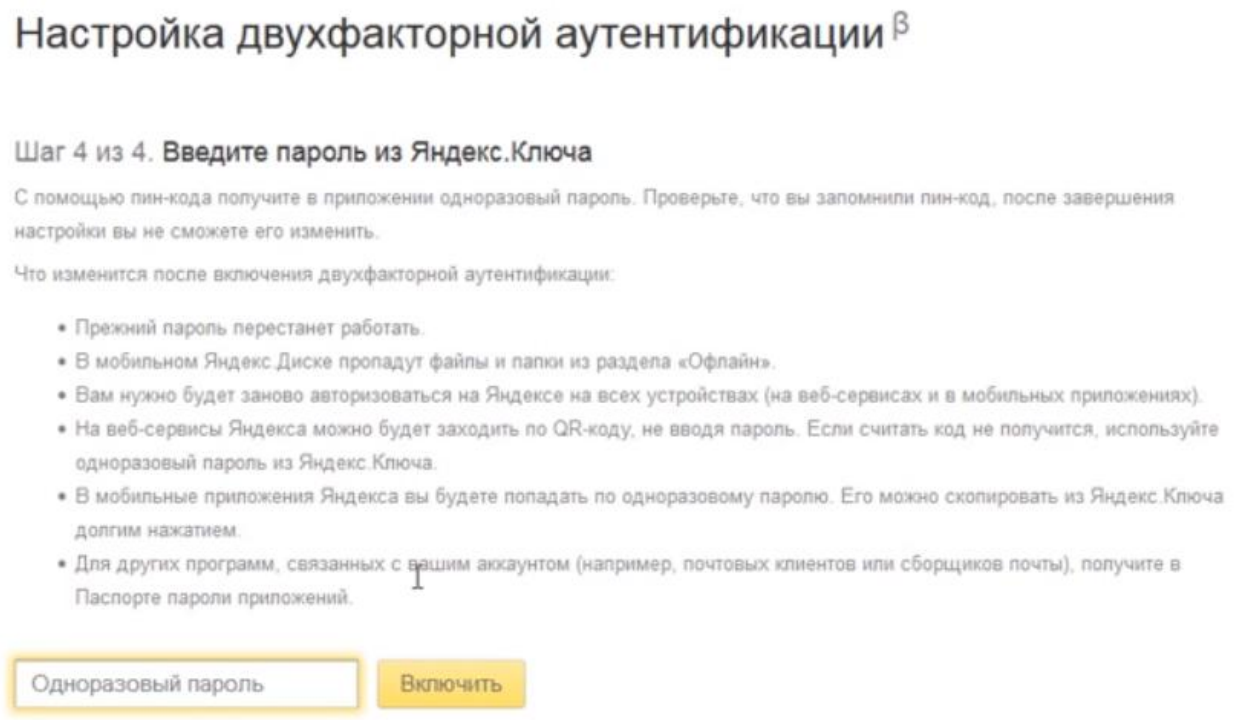

Рис. 7. Ввод пароля из Яндекс. Ключа

Таким образом, по итогам рассмотрения программного обеспечения, предназначенного двухфакторная авторизация нужна однозначно тем, кто использует ящики для работы или хранения важных данных. Для определения эффективной защиты в дальнейшем необходимо провести более тщательное исследование информационных технологий. Плюсы данной системы аутентификации являются повышенная защищенность; не обязательно запоминать пароль, теперь можно использовать устройство для входа; сложность в взломе данного варианта входа; контроль входа в учетную запись с любой точки WWW; войти в учетную запись можно только Вашем в присутствии. К недочетам относится следующие пользователь самостоятельно формирует список приложений, для доступа к которым используется двухфакторная авторизации; наличие постоянной SIM-карты для доступа получения SMS-оповещения в сервисе Google Authenticator; контроль выхода из внешних стационарных и мобильных устройств; наличие интернет соединения с сервисами авторизации.

В данной работе был проведен обзор и сравнение двух вариантов двухфакторной аутенфикации в одних из самых больших компаний.

Поставленные задачи выполнены полностью, проведено сравнение, выявлены плюсы и недочеты. Так же, приведены алгоритмы включения данного способа аутенфикации с подробными иллюстрациями и комментариями.

Исходя из обзора видно, что данный метод дает большую уверенность защищенности личных данных, упрощения способа авторизации в аккаунте. На данный способ нужно переводить всем пользователям, кто хочет быть уверен в безопасности своих данных.

Библиографический список

1. Gualdoni J., Kurtz A., Myzyri I., Wheeler M., Rizvi S. Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication // Procedia Computer Science. 2017. № 114.
2. Борисова Е. А. Использование двухфакторной аутентификации при защите персональных данных // Символ науки. 2016.
3. Еременко А.В., Сулавко А.Е. «Двухфакторная аутентификация пользователей компьютерных системна удаленном сервере по клавиатурному почерку» // Прикладная информатика. 2015.
4. Ленкин А.В., Голубь И.С., Глаголев В.А. SSL-сертификаты. Получение, генерация и подключение // Постулат. 2018. №9. С. 12.
5. Майский Р.А., Губина О.В. Информационно-аналитической обеспечение управления предприятием на основе компьютерной технологий // Актуальные проблемы науки и техники. Сборник научных трудов IV Международной научно-практической конференции молодых ученых. 2012. С. 199-203.
6. Хлыстова Д.А., Попов К.Г. К вопросу о моделировании угроз персональным данным пользователей в системах дистанционного обучения образовательных организаций // Международный студенческий научный вестник. 2016. № 3-1. С. 96-97.
7. Шапиро Л. Active directory domain services. Двухфакторная аутентификация. Теоретические основы // Системный администратор. 2014. №7-8. С. 92-93.