**Идентификация, аутентификация и авторизация**

На самом деле никакого обмена не происходило. Произошли поочередно три процесса: идентификация, аутентификация и авторизация. Данная статья поможет понять, как происходят эти процессы, когда они происходят, в какой последовательности и как с их помощью защитить свои персональные данные и денежные средства.

**Определения**

Идентификация, аутентификация и авторизация – три процесса защищающие Ваши данные или денежные средства от доступа посторонних лиц.

Понимание процессов придет быстрее, если дать им определения.

* Идентификация — процесс распознавания пользователя по его идентификатору.
* Аутентификация — процедура проверки подлинности, доказательство что пользователь именно тот, за кого себя выдает.
* Авторизация — предоставление определённых прав.

Для начала этих теоретических знаний будет достаточно. Вернемся к примеру с доступом в онлайн-банкинг. Каждое действие пользователя и системы рассмотрим подробно.

**Механизмы идентификации, аутентификации и авторизации**

Находясь на сайте банка, пользователь решает зайти в личный кабинет, чтобы сделать денежный перевод. На странице личного кабинета система вначале просит ввести идентификатор. Это может быть логин, имя и фамилия, адрес электронной почты или номер мобильного телефона.

*Какой конкретно вид данных необходимо ввести – зависит от ресурса. Данные, которые указывались при регистрации, необходимо ввести для получения доступа. Если при регистрации указывалось несколько типов данных – и логин, и адрес электронной почты, и номер мобильного, то система сама подскажет что ей конкретно нужно.*

Ввод этих данных необходим для идентификации человека за монитором как пользователя конкретно этого банка.

Если пользователь в качестве идентификатора ввел «Александр Петров», и система нашла в своей базе запись о пользователе с таким именем, то идентификация завершилась.

После идентификации следует процесс аутентификации, в котором пользователю нужно доказать, что он является человеком, который регистрировался под именем Александр Петров.

Для доказательства необходимо наличие одного из типов аутентификационных данных:

* Нечто, присущее только пользователю. Биометрические данные: сканеры лица, отпечатки пальцев или сетчатки глаза.
* Нечто, известное только пользователю. Сюда относятся pin-коды, пароли, графические ключи, секретные слова.
* Нечто, имеющееся у пользователя. В данном качестве может выступать токен, то есть компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации владельца. Самые простые токены не требуют физического подключения к компьютеру – у них имеется дисплей, где отображается число, которое пользователь вводит в систему для осуществления входа; более сложные подключаются к компьютерам посредством USB и Bluetooth-интерфейсов.

Самый распространенный тип аутентификационных данных – это пароль. Именно поэтому так важно создавать и правильно хранить свои пароли. Подробнее об этом можно прочитать в статьях [«Создание надежных паролей»](https://safe-surf.ru/users-of/article/580656/) и [«Как правильно выбирать и хранить пароли»](https://safe-surf.ru/users-of/article/577752/).

После ввода пользователем пароля система проверяет: соответствует ли условный пароль «Q45fp02@13» пользователю с именем Александр Петров. Таким образом происходит аутентификация.

Если все верно, и пара логин-пароль верны, то система предоставит пользователю доступ к его ресурсам и совершение банковских операций, то есть произойдет авторизация.

Описанные процессы всегда происходят только в таком порядке: идентификация, аутентификация, авторизация. Вся цепочка потеряет смысл, если, например, сайт сначала предоставит доступ к денежным средствам пользователя, а потом будет уточнять, он ли это на самом деле.

Процессы идентификации, аутентификации и авторизации характерны не только для онлайн-банкинга, но и для электронной почты, социальных сетей и других ресурсов.

В реальной жизни мы также сталкиваемся идентификацией, аутентификацией и авторизацией. Примером может служить проверка документов сотрудником полиции. Вы представились как Александр Петров, и сотрудник полиции идентифицировал Вас как Александра Петрова. Для аутентификации необходим паспорт, в котором видно, что Александр Петров выглядит так же, как и вы. Авторизацией в данном случае будет то, что сотрудник отпустит вас и пожелает счастливого пути, т.е. предоставит право свободного перемещения.

Процессы идентификации, аутентификации и авторизации есть во многих сферах. Даже в простейших детских сказках. Сказка «Волк и семеро козлят» является идеальным примером для демонстрации.

Здесь козлята выступают в роли системы безопасности, идентифицируя каждого, кто подходит к двери. В качестве данных для аутентификации выступает биометрия – тонкий голосок мамы-козы. И если в первый раз волк не смог пройти аутентификацию (его выдал грубый голос), то со второй попытки (после того как ему перековали горло, и он запел тонким голоском) он аутентифицировался как мама-коза и козлята «авторизовали» его в свою избу.

Несмотря на то, что сказка закончилась благополучно, доступ к козлятам был получен неправомерно. Волку удалось обмануть процессы идентификации и аутентификации и тем самым пройти авторизацию.

Если в старой детской сказке это оказалось возможным, то что говорить о современных злоумышленниках. Чтобы защитить свои денежные средства и персональные данные и козлят от волка от злоумышленника необходимо использовать более сложные способы аутентификации.

**Многофакторная аутентификация**

Многофакторная аутентификация представляет собой метод, при котором пользователю для доступа к учетной записи или подтверждения операции с денежными средствами необходимо двумя различными факторами доказать, что именно он владелец учетной записи или что именно он осуществляет вход.

Среди видов многофакторной аутентификации наиболее распространена двухфакторная аутентификация (2FA — 2-factor authentication) – метод, при котором пользователю для получения доступа необходимо предоставить два разных типа аутентификационных данных, например, что-то известное только пользователю (пароль) и что-то присущее только пользователю (отпечаток пальца).

Доступ к ресурсам через ввод логина и пароля, является однофакторной аутентификацией, поскольку для входа используется только один тип аутентификационных данных — известный пользователю пароль.

**Однофакторная двухэтапная аутентификация**

Благодаря тому, что смартфоны стали неотъемлемой частью нашей жизни, именно они стали одним из способов подтверждения личности пользователя. Они являются токенами для доступа к различным ресурсам. В этом случае одноразовый пароль генерируется или с помощью специального приложения, или приходит по SMS – это максимально простой для пользователя метод.



Аутентификация происходит следующим образом:

1. Пользователь вводит логин и пароль, указанные при регистрации. Если данная пара корректна (логин есть в базе и соответствует паролю) система высылает одноразовый пароль, имеющий ограниченное время действия.
2. Пользователь вводит одноразовый пароль и, если он совпадает с тем, что отправила система, то пользователь получает доступ к своей учетной записи, денежным средствам или подтверждает денежный перевод.

Даже если злоумышленник получит логин и пароль для учетной записи (с помощью вредоносной программы, кражи записной книжки с паролями или методами социальной инженерии и фишинга), то после ввода этих данных система отправит на привязанный мобильный телефон пользователя одноразовый код с ограниченным временем действия. Без одноразового кода мошенник не сможет похитить денежные средства.

Двухфакторная аутентификация

Двухфакторная аутентификация — то, чем мы так или иначе пользуемся при получении доступа к важной информации в сети Интернет. Ввиду возрастающего количества разных сервисов и все чаще случающихся атак на пользовательские [аккаунты](http://security.mosmetod.ru/paroli/121-login-parol-i-uchetnaya-zapis) (как, например, перехваты контроля над учетными записями) мы решили рассказать о том, что это такое, как она работает и почему ее стоит использовать везде, где это возможно.

Что такое двухфакторная аутентификация?

Двухфакторная аутентификация — это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения.

На практике это обычно выглядит так: первый рубеж — это логин и [пароль](http://security.mosmetod.ru/paroli/2-bezopasnost-parolej), второй — специальный код, приходящий по SMS или электронной почте. Всё чаще второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы — это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти.



Конечно, двухфакторная защита — не панацея от [взлома аккаунта](http://security.mosmetod.ru/moshennichestvo-v-seti/92-bezopasnost-v-sotssetyakh), но достаточно надежный барьер, серьезно усложняющий [злоумышленникам](http://security.mosmetod.ru/zashchita-ot-virusov/42-kto-sozdaet-vredonosnye-programmy) доступ к чужим [данным](http://security.mosmetod.ru/personalnye-dannye) и в какой-то степени нивелирующий недостатки классической [парольной защиты](http://security.mosmetod.ru/paroli/statistika-vybora-parolya). Ведь у паролей, на которых основано подавляющее большинство авторизационных механизмов в Интернете, есть неизбежные недостатки: короткие и простые пароли легко запомнить, но так же легко подобрать, а длинные и сложные трудно взломать, но и запомнить непросто. По этой причине многие люди используют довольно тривиальные пароли, причем сразу во многих местах. Второй фактор в подобных случаях оказывается крайне полезен, поскольку, даже если пароль был скомпрометирован, злоумышленнику придется или раздобыть мобильник жертвы, или украсть ее почтовый ящик.

Несмотря на многочисленные попытки современного человечества заменить [пароли](http://security.mosmetod.ru/paroli/62-zashchita-ot-moshennikov) чем-то поинтереснее, полностью избавиться от них оказалось не так просто, так что двухфакторную аутентификацию можно считать одним из самых надежных механизмов защиты на сегодняшний день. Кстати, этот метод удобен еще и тем, что способен предупреждать хозяина аккаунта о [попытке взлома](http://security.mosmetod.ru/onlajn-platezhi/55-vzlom-internet-bankinga): если на ваш телефон или почту вдруг приходит сообщение с одноразовым кодом при том, что вы никаких попыток логина не предпринимали, значит, вас пытаются взломать — самое время менять оказавшийся ненадежным пароль!

Где можно включить двухфакторную аутентификацию?

Ответом на этот вопрос может служить простое правило: если используемый вами сервис содержит важные для вас данные и позволяет включить двухфакторную аутентификацию, активируйте ее не раздумывая! [Интернет-банкинг](http://security.mosmetod.ru/onlajn-platezhi/61-sovety-po-internet-bezopasnosti-dlya-zashchity-deneg-i-kreditnykh-kart), аккаунты в соцсетях, учетка в iCloud, почтовые ящики и особенно ваши учетные записи — все это однозначно стоит защитить двухфакторной аутентификацией. Сервисы Google, Apple и все основные социальные сети позволяют это сделать в настройках без особого труда.

В общем, если аккаунт и его содержимое вам дороги, не игнорируйте возможность усилить защиту.

Какие еще существуют виды двухфакторной аутентификации?

Выше уже упоминалась рассылка специального кода в виде SMS и email-сообщений, USB-ключи и смарт-карты, используемые преимущественно для доступа к некоторым видам интернет-ресурсов и VPN-сетям. Кроме того, существуют еще генераторы кодов (в виде брелока с кнопкой и небольшим экранчиком), технология SecureID и некоторые другие специфические методы, характерные в основном для корпоративного сектора.

Есть и менее современные интерпретации: например, так называемые TAN-пароли (TAN, Transaction Authentication Number — аутентификационный номер транзакции). Возможно, вы даже сталкивались с ними, если были клиентом какого-нибудь не самого прогрессивного банка: при подключении интернет-банкинга клиенту выдавалась карточка с заранее сформированным списком одноразовых паролей, которые вводятся один за другим при каждом входе в систему и/или совершении транзакции.

Кстати, ваша банковская карта и PIN тоже формируют систему двухфакторной аутентификации: карточка — «ключ», которым вы владеете, а PIN-код к ней — «ключ», который вы запоминаете.

Кроме этого, существует и биометрический способ идентификации пользователя, который часто выступает в роли вторичного фактора защиты: одни системы подразумевают сканирование отпечатка пальца, другие определяют человека по глазам. Но пока это все менее распространенные методы, хотя и куда более популярные, чем те, которые ориентируются по «рисунку» сердцебиения или же электромагнитные татуировки, которые по примеру радиочипов могут служить вторичным фактором аутентификации пользователя.