

Запольская Татьяна Александровна
магистрант кафедры «Кибербезопасность информационных систем»
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия
Научный руководитель:

Сосновский Иван Александрович
к.т.н., доцент кафедры «Кибербезопасность информационных систем»
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

Повышение безопасности аккаунтов с помощью двухфакторной аутентификации

Аннотация. В данной статье рассматривается роль двухфакторной аутентификации как важного элемента кибербезопасности. Анализируются недостатки традиционной парольной защиты и обосновывается необходимость перехода к более надежным методам. Подробно описывается принцип работы двухфакторной аутентификации. Приводятся сравнительные характеристики различных методов двухфакторной аутентификации, выделяются их преимущества и потенциальные уязвимости. Рассмотренный метод защиты информации является эффективным и доступным средством для значительного повышения уровня защиты персональных данных и цифровых аккаунтов в сети Интернет.

Ключевые слова: двухфакторная аутентификация, кибербезопасность, информационная безопасность, защита данных, пароль, одноразовый код, приложение-аутентификатор, аппаратный ключ, биометрия, фишинг, взлом аккаунтов.

Zapolskaya Tatyana Alexandrovna
Master's student of the Department of Cybersecurity of information systems
Don State Technical University
Rostov-on-Don, Russia
Scientific Supervisor:

Sosnovskiy Ivan Alexandrovich
Candidate of Technical Sciences, Associate Professor of the Department of Cybersecurity of
Information Systems
Don State Technical University
Rostov-on-Don, Russia

Improve account security with two-factor authentication

Abstract. This article examines the role of two-factor authentication as an important element of cybersecurity. The disadvantages of traditional password protection are analyzed and the need for a transition to more reliable methods is justified. The principle of two-factor authentication is described in detail. Comparative characteristics of various two-factor authentication methods are given, their advantages and potential vulnerabilities are highlighted. The considered method of information protection is an effective and affordable means to significantly increase the level of protection of personal data and digital accounts on the Internet.

Keywords: two-factor authentication, cybersecurity, information security, data protection, password, one-time code, authenticator application, hardware key, biometrics, phishing, account hacking.

На сегодняшний день, когда наша жизнь неразрывно связана с цифровым пространством, защита личных данных является важнейшей составляющей. Пароли,

долгое время являющиеся основным барьером на пути злоумышленников, сегодня уже не обеспечивают достаточного уровня безопасности. Взломы, утечки баз данных и фишинг делают уязвимыми даже самые сложные комбинации символов. На смену этому устаревшему методу приходит более надежный механизм - двухфакторная аутентификация (далее ДА), обеспечивающая безопасность аккаунтов.

Проблемой в данной статье является обеспечение безопасности данных в сети. Целью данной статьи является рассмотрение метода защиты аккаунтов в сети с помощью технологии двухфакторной аутентификации.

Традиционный пароль, с помощью которого осуществляется вход в аккаунт, это уязвимая информация, которую можно украсть, подобрать или узнать обманным путем. Статистика киберпреступлений значительно выросла: большое количество учетных записей ежедневно становятся целью атак. Один и тот же пароль, используемый на нескольких ресурсах, увеличивает риски. То есть стоит взломать один менее защищенный сервис, и под угрозой окажутся все остальные. Именно в этом заключается недостаток однофакторной системы.[1]

К основным угрозам для паролей относятся:

1. Фишинг;
2. Брут-форс атаки;
3. Социальная инженерия;
4. Утечки данных.

Фишинг – вид мошенничества, осуществляющийся путем создания мошенниками поддельных сайтов, имитирующих страницы входа легитимных сервисов; вводя пароль пользователем на такой странице злоумышленники получают все учетные данные.

Брут-форс атаки – вид мошенничества, который заключается в автоматизированном подборе паролей с помощью специального программного обеспечения.

Социальная инженерия – вид мошенничества, заключающийся в манипулировании пользователем с целью добровольной выдачи пароля;

Утечки данных - крупномасштабные взломы баз данных компаний, после которых все пароли переходят в открытый доступ.

На смену однофакторной системе приходит двухфакторная аутентификация. Двухфакторная аутентификация - это метод контроля доступа, для которого требуется не один, а два независимых доказательства вашей личности. Эти доказательства берутся из следующих категорий:

1. Имеющийся пароль для входа в аккаунт - это стандартный пароль или PIN-код;
2. Генерация дополнительных кодов - осуществляется с помощью смартфона или устройств, генерирующих код (например, смартфон с приложением-аутентификатором (Google Authenticator, Microsoft Authenticator), SMS с одноразовым кодом, USB-ключ (YubiKey) или токен);
3. Биометрические данные – это уникальные биологические характеристики владельца страницы (отпечаток пальца, сканирование лица или сетчатки глаза).[2]

Таким образом, даже если злоумышленник каким-то образом завладеет паролем от аккаунта, он не сможет получить доступ к нему без ввода дополнительных кодов или биометрических данных, которые физически ему недоступны.

Рассмотрим методы двухфакторной аутентификации подробнее.

Первым методом ДА является использование SMS-сообщения с кодом. Это самый распространенный, однако не самый безопасный метод. Код, отправленный на ваш номер телефона, уязвим к перехвату через SIM-своппинг (несанкционированный перенос номера на другую SIM-карту). Данный метод необходимо использовать, если другие недоступны.

Вторым методом ДА являются голосовые звонки. Данный метод аналогичен предыдущему, однако в данном случае код произносится автоматическим роботом.

Данный метод имеет те же риски, что и SMS-сообщения.

Третьим методом является применение приложений-аутентификаторов. Это более надежный вариант. Приложение (например, Google Authenticator, Microsoft Authenticator, Aegis) генерирует одноразовые коды, которые обновляются каждые 30 секунд. Они не требуют подключения к интернету и не зависят от мобильной сети, что делает их безопаснее SMS-сообщений. Важное преимущество данного метода заключается в том, что многие приложения позволяют создавать резервные копии ключей в зашифрованном облаке.

Четвертым методом ДА является отправка Push-уведомления. Этот метод является одним из эффективных и безопасных методов. Это удобный способ, при котором на доверенное устройство пользователя приходит запрос на вход в самом приложении. Достаточно нажать «Подтвердить» в уведомлении. Это минимизирует риск фишинга, так как уведомление привязано к легитимному приложению.

Еще одним методом ДА является применение аппаратных ключей. Данный метод показывает максимальную степень защиты. Он осуществляется с помощью специальных USB-, NFC- или Bluetooth-устройств, которые необходимо физически подключить или активировать для подтверждения входа. Данный метод применяется для защиты самых важных аккаунтов, таких как корпоративные системы, электронные почты и финансовые сервисы. [3]

К наиболее важным серверам, требующим защиту, относятся:

1. Электронная почта, которая является ключом ко всем остальным аккаунтам, так как почта привязывается к другим сайтам; взлом почты означает возможность сброса паролей;
2. Финансовые сервисы, такие как онлайн-банки, платежные системы; криптовалютные кошельки;
3. Социальные сети и мессенджеры;
4. Облачные хранилища, содержащие личные данные пользователя;
5. Игровые и развлекательные платформы, на которых часто указываются способы платежей.

К преимуществам двухфакторной аутентификации относятся:

1. Значительное повышение безопасности;
2. Защита от фишинга;
3. Контроль и оповещения о попытках входа;
4. Соответствие требованиям безопасности и стандартам для корпоративных политик безопасности.[4]

Так, двухфакторная аутентификация - это важный этап в кибербезопасности, заключающийся в беспарольной аутентификацией, где основную роль будут играть биометрия и аппаратные ключи. Эта технология позволяет входить в аккаунты с помощью отпечатка пальца или лица, без ввода пароля, что полностью исключает риск фишинга и краж паролей.

Таким образом, в современной цифровой экосистеме двухфакторная аутентификация перестала быть обычной опцией, а стала базовым стандартом цифровой безопасности для каждого пользователя. Включив двухфакторную аутентификацию в социальных сетях, почтовых ящиках, банковских и облачных сервисах, пользователь «ставит барьер» на пути киберпреступников. Это простой, но эффективный шаг к тому, чтобы личная информация оставалась в безопасности.

Список источников

1. Гейст, Э. Современная криптография и безопасность коммуникаций. — М.: Издательский дом «Вильямс», 2021. — С. 215–230;
2. Сляров, Д. В. Защита информации в эпоху цифровых технологий. — СПб.:

БХВ-Петербург, 2019. — С. 154–167;

3. Кларк, Д. Безопасность в сети: практическое руководство для пользователя. — М.: Эксмо, 2022. — С. 88–105;

4. Материалы онлайн-портала «Хакер»: Статья «SIM-своппинг: как мошенники крадут ваши номера и как от этого защититься». — 2023. — [Электронный ресурс]. — URL: <https://www.xakep.ru/> (дата обращения: 10.11.2025г).