ORES
Научно-практический электронный журнал
**Оригинальные исследования (ОРИС)**, *ISSN 2222-0402*
www.ores.su
original-research.ru

**УДК 004.056.53**

# ОБХОД ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ: СОВРЕМЕННЫЕ МЕТОДЫ И ЗАЩИТА

**Тарасов Кирилл Олегович,**
Студент КФ МГТУ Им Баумана
Калуга, Россия
kirill.tarasov1371@gmail.com

**Фадеев Вячеслав Олегович,**
Студент КФ МГТУ Им Баумана
Калуга, Россия
fadeevvo@student.bmstu.ru

**Буракова Мария Сергеевна,**
Ассистент КФ МГТУ Им Баумана
Калуга, Россия
m.burakova@bmstu.ru

**Аннотация**

В данной статье рассматриваются современные техники обхода двухфакторной аутентификации (2FA) и методы защиты от них. Основное внимание уделяется различным методам атак, в частности таким как: фишинг, использование вредоносного ПО, социальная инженерия, атаки на уязвимости в протоколах и системах, а также атаки на резервные коды и методы восстановления. Каждая приведённая техника обхода аутентификации рассматривается на конкретном примере, объясняется механизм возможных атак. В статье автор подчеркивает важность комплексного подхода к обеспечению безопасности и повышения осведомленности пользователей для предотвращения обхода двухфакторной аутентификации. Целью данного исследования является выявление наиболее эффективных техник защиты, предотвращающих взлом.

**Ключевые слова:** 2FA, ПО, Фишинг, Социальная инженерия, Кейлоггер, YubiKey, IDS, UBA.

# BYPASSING TWO-FACTOR AUTHENTICATION: MODERN METHODS AND PROTECTION

**Tarasov Kirill Olegovich,**
Student BMSTU
Kaluga, Russia
kirill.tarasov1371@gmail.com

**Fadeev Vyacheslav Olegovich,**
Student BMSTU
Kaluga, Russia
fadeevvo@student.bmstu.ru

**Burakova Maria Sergeevna,**
Assistant BMSTU
Kaluga, Russia
m.burakova@bmstu.ru

ABSTRACT

This article discusses modern techniques for bypassing two-factor authentication (2FA) and methods of protection against them. The main focus is on various attack methods, in particular such as: phishing, malware use, social engineering, attacks on vulnerabilities in protocols and systems, as well as attacks on backup codes and recovery methods. Each of the above authentication bypass techniques is considered on a specific example, and the mechanism of possible attacks is explained. In the article, the author emphasizes the importance of an integrated approach to ensuring security and raising user awareness to prevent circumvention of two-factor authentication. The purpose of this study is to identify the most effective security techniques to prevent hacking.

**Keywords:** 2FA, Software, Phishing, Social Engineering, Keylogger, YubiKey, IDS, UBA.

В настоящее время вопрос кибербезопасности по-прежнему актуален. Одним из самых распространённых средств защиты является двухфакторная аутентификация (2FA), ставшая стандартом безопасности для значительного количества различных онлайн-сервисов, предоставляя дополнительный уровень защиты для пользователей. Однако, несмотря на её эффективность, злоумышленники продолжают разрабатывать методы обхода 2FA. Для создания должного уровня безопасности нужно понимать, как действуют механизмы обхода защиты. В данной статье мы рассмотрим современные техники обхода двухфакторной аутентификации и методы защиты от них [1].

В большинстве атак злоумышленником применяются однотипные техники обхода двухфакторной аутентификации. Одним из таких способов является Фишинг. Названый способ можно считать одной из самых распространённых техник обхода 2FA. Суть его заключается в следующем: необходимо заставить человека ввести свои учётные данные в подставную форму. Для реализации вышеизложенного создаются поддельные веб-сайты, устраивается рассылка фейковых электронных писем на личные адреса. Выглядит это примерно так: Пользователь получает электронное письмо, стилистически похожее на рассылку от его банка, с уведомлением о необходимости обновить сведения своей учетной записи. Открывает ссылку из письма и попадает на фальшивый сайт, идентичный оригинальному. А далее вводит данные учётной записи и код для 2FA, самостоятельно отдавая преступнику доступ к своей учетной записи.

Атаки с использованием вредоносного ПО. ПО, наносящее вред, как например, кейлоггеры и вирусы-трояны, злоумышленники используют для перехвата данных учётных записей и кодов 2FA. Такие программы записывают клавиши, нажатые пользователем,

делают скриншоты или даже перехватывают SMS-сообщения. Пример атаки: пользователь скачивает и устанавливает вредоносное ПО, замаскированное под легитимное приложение. Вредоносное ПО начинает записывать все нажатия клавиш и отправляет их злоумышленнику. Когда человек вводит свои данные для входа и код двухфакторной аутентификации, мошенник получает эти сведения и применяет их для входа в аккаунт.

Атаки, основанные на социальной инженерии. Социальная инженерия подразумевает манипуляцию людьми с целью получения их конфиденциальных данных. Преступники могут применять различные техники, включая телефонные звонки или обращения через социальные сети, чтобы обманным путем вынудить пользователей раскрыть свои коды двухфакторной аутентификации. [2]. Пример атаки: мошенник звонит клиенту, выдавая себя за работника службы технической поддержки. Он заявляет, что заметил подозрительную активность на учетной записи и запрашивает подтверждение личности, прося предоставить код двухфакторной аутентификации. Доверяя мошеннику, пользователь делится кодом, который затем используется для несанкционированного входа в его учетную запись.

Атаки на уязвимости в протоколах и системах. Некоторые недостатки в протоколах и системах двухфакторной аутентификации (2FA) могут быть использованы для обхода процесса аутентификации. К примеру, недостатки в реализации SMS-2FA способны предоставить злоумышленникам возможность перехвата кодов аутентификации. Пример атаки: Злоумышленник эксплуатирует уязвимость в системе телекоммуникационного оператора для перехвата SMS-сообщений. Когда пользователь получает код 2FA через SMS, злоумышленник перехватывает это сообщение и использует его для доступа к учетной записи.

Атаки на резервные коды и методы восстановления. Многие системы двухфакторной аутентификации (2FA) предлагают пользователям резервные коды или альтернативные методы восстановления на случай утраты доступа к устройству. Злоумышленники могут попытаться получить эти резервные коды или воспользоваться методами восстановления для обхода двухфакторной защиты. Один из примеров такой атаки выглядит так: злоумышленник получает доступ к электронной почте жертвы, в которой можно найти резервные коды 2FA. Вставляя эти коды, преступник обходит систему 2FA и получает несанкционированный доступ к учетной записи.

Методы защиты от обхода двухфакторной аутентификации. Обучение пользователей выявлению фишинговых атак и различных способов социальной инженерии представляет собой важный аспект безопасности. Нужно, чтобы пользователи понимали потенциальные угрозы и умели адекватно реагировать на подозрительные обращения. Рекомендации: не вводите свои логины и пароли на сомнительных веб-сайтах. Всегда проверяйте, точен ли URL-адрес перед тем, как предоставить какую-либо информацию. Не поддавайтесь на неожиданные запросы о предоставлении кодов двухфакторной аутентификации.

Применение аппаратных токенов. Устройства, такие как YubiKey, обеспечивают более высокий уровень безопасности по сравнению с SMS-сообщениями или аутентификационными приложениями. Эти токены создают одноразовые коды, которые невозможно перехватить или подделать. Основные преимущества: защита от фишинга и вредоносного программного обеспечения; независимость от услуг телекоммуникационных провайдеров; высокий уровень физической защиты.

Внедрение многофакторной аутентификации. Применение многофакторной аутентификации (MFA), которая включает в себя несколько уровней проверки, может значительно повысить безопасность. Например, сочетание биометрической аутентификации и аппаратного токена [3]. Преимущества: усложнение задачи взлома для

преступников; безопасность от различных видов атак; улучшенная степень доверия к идентичности пользователя.

Постоянное обновление и применение патчей для систем. Регулярное обновление и установка патчей в системах безопасности способствует защите от известных уязвимостей. Администраторы должны следить за обновлениями и своевременно применять их. Рекомендации: внедрите автоматические обновления для критических систем; регулярно проводите аудит безопасности; следите за новыми уязвимостями и реагируйте на них.

Мониторинг и анализ активности. Мониторинг и анализ активности пользователей могут помочь выявить подозрительное поведение и предотвратить атаки. Применение систем выявления вторжений (IDS) и анализа поведения пользователей (UBA) способно существенно улучшить уровень безопасности [4], [5]. Преимущества: раннее выявление ненормальной активности; способность оперативно реагировать на происшествия; улучшение общей безопасности системы.

Таким образом, можно сделать вывод, что двухфакторная аутентификация является важным элементом современной кибербезопасности, но она не является неприступной. Злоумышленники продолжают разрабатывать новые методы обхода 2FA, и пользователи должны быть осведомлены о рисках и методах защиты. Обучение пользователей, использование аппаратных токенов, внедрение многофакторной аутентификации, регулярное обновление систем и мониторинг активности являются ключевыми элементами защиты от обхода двухфакторной аутентификации.

**Список литературы:**

1. Что такое двухфакторная проверка подлинности? URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-two-factor-authentication-2fa (дата обращения: 10.11.24).
2. Возможности применения методов социальной инженерии в организации телефонного мошенничества. URL: https://cyberleninka.ru/article/n/vozmozhnosti-primeneniya-metodov-sotsialnoy-inzhenerii-v-organizatsii-telefonnogo-moshennichestva (дата обращения: 10.11.24).
3. Managing Multifactor Authentication. URL: https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/usingmfa.htm (дата обращения: 10.11.24).
4. IDS: Documentation. URL: https://ids.sourceforge.net/documentation.html (дата обращения: 10.11.24).
5. IBM QRadar User Behavior Analytics (UBA). URL: https://www.ibm.com/docs/en/SS42VS_SHR/pdf/b_Qapps_UBA.pdf (дата обращения: 10.11.24).

**References:**

1. What is two-factor authentication? URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-two-factor-authentication-2fa (accessed: 10.11.24).
2. The possibilities of using social engineering methods in the organization of telephone fraud. URL: https://cyberleninka.ru/article/n/vozmozhnosti-primeneniya-metodov-sotsialnoy-inzhenerii-v-organizatsii-telefonnogo-moshennichestva (accessed: 10.11.24).
3. Managing Multifactor Authentication. URL: https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/usingmfa.htm (accessed: 10.11.24).

4. IDS: Documentation. URL: https://ids.sourceforge.net/documentation.html (accessed: 10.11.24).
5. IBM QRadar User Behavior Analytics (UBA). URL: https://www.ibm.com/docs/en/SS42VS_SHR/pdf/b_Qapps_UBA.pdf (accessed: 10.11.24).