DOI 10.36622/VSTU.2022.25.4.015
УДК 004.056

АСПЕКТЫ ПРИМЕНЕНИЯ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ QR-КОДОВ ДЛЯ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК

П.А. Анцупов, М.А. Булычев, Е.А. Москалева

В современном мире в условиях повсеместной цифровизации информации вопросы безопасного доступа и работы с персональными данными стали основными и требующими постоянного внимания. Согласно статистике, начиная с 2018 года количество пользователей социальных сетей возрастает с каждым годом. Вследствие участившегося количества компьютерных атак, направленных на кражу конфиденциальных данных участников компьютерных сетей, все больше внимания уделяется безопасности данных. Одним из наиболее приоритетных методов обеспечения защищенности информации является применение алгоритмов двухфакторной аутентификации. В сложившейся ситуации немаловажным аспектом также выступает правильная конфигурация и внедрение механизмов защиты персональных данных. В данной статье рассматриваются вопросы организации безопасности информации пользователей социальных сетей и информационных систем, с использованием QR-кодов для противодействия компьютерным атакам.

Ключевые слова: цифровизация, компьютерные атаки, конфиденциальность, персональные данные, двухфакторная аутентификация, QR-код.

Введение

В настоящее время Интернет является неотъемлемой частью жизни большинства людей, где основную роль составляют социальные сети и информационные системы, аккумулирующие внутри себя информацию ограниченного пользования. В условиях цифровизации информации, когда персональные данные перешли из бумажного делопроизводства в электронное, количество компьютерных атак, направленных на кражу конфиденциальной информации, существенно увеличилось (рис. 1).

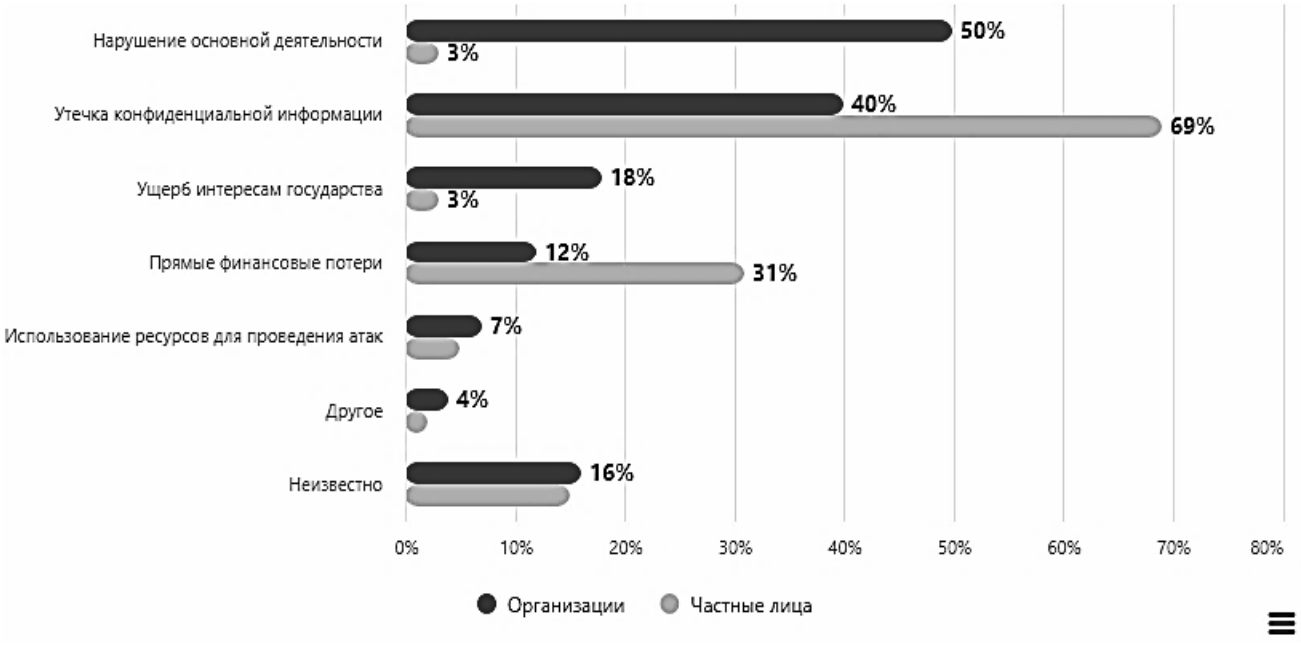

Рис. 1. Доля компьютерных атак по их типам [1].

Принимая во внимание вышеприведенную статистику, вопрос об обеспечении вариантов защиты компьютерной информации является крайне важным.

Особенно успешными для кражи конфиденциальных данных могут быть brute-force атаки, атаки с использованием ботов и атаки через посредника (MITM – man-in-the-millle). При brute-force атаках обычно применяются инструменты перебора для вскрытия паролей. На сегодняшний день существуют алгоритмы, позволяющие ускорять и оптимизировать процесс подбора комбинаций паролей, и простые пароли вскрывают очень быстро, от нескольких секунд до долей секунды, что и используется при brute-force атаках и атаках с применением ботов. Кроме того, бот, имитируя поведение пользователя осуществляют подбор с большой скоростью. При MITM-атаках киберпреступник или бот подключается к соединению пользователь-система и становится посредником, пропускающим через себя данные в обе стороны, считывая таким образом интересующие его данные. MITM-атака обычно направлена на обход аутентификации. При регистрации аккаунтов далеко не всегда обычные люди используют сложные пароли, поскольку требуется множество аккаунтов для входа в социальные сети, магазины, форумы, которые необходимо запоминать или записывать. Пользователи зачастую используют один пароль для всех аккаунтов, и этот пароль будет связан с датами рождения, именами и т.п. Такие пароли и могут легко вскрывать современные киберпреступники. Защита от ботов обычно основана на регистрации скорости ввода данных, но крупные компании и сети, например, Сбер, Google, ВКонтакте имеют такую защиту, а сайты магазинов могут не иметь и не будут отличать пользователя от бота. Таким образом, в современном информационном мире регистрация аккаунтов с помощью паролей становится неудобной для использования и опасной с точки зрения защиты конфиденциальных данных.

В связи с вышеизложенным в последнее время все больше вместо паролей при регистрации аккаунтов используют QR-коды и коды из SMS.

Для повышения защищенности пользователя применяют многофакторную аутентификацию. Основные способы аутентификации:

1) логин+пароль или e-mail+ пароль;
2) QR-код;
3) код из SMS или e-mail;
4) физический ключ безопасности (например, флэшка);
5) биометрия.

Двухфакторная аутентификация или 2FA предполагает применение двух различных способов аутентификации. Рассмотрим подробнее вопросы защиты конфиденциальной информации и определим модель двухфакторной защиты пользователя

Анализ компьютерных атак на ресурсы, содержащие конфиденциальную информацию

Исходя из информации агентства Kepios, занимающегося сбором и формированием визуализирующих панелей статистических данных пользователей сети Интернет, преобладающая доля населения использует социальные сети для вербальных и невербальных коммуникаций между собой.

Проводя анализ вышеприведенной статистики, можно прийти к выводу, что все большее число конфиденциальной информации размещается в открытых ресурсах компьютерных сетей [1]. Таким образом, подавляющее число хакерских атак на интернет-ресурсы производится с целью кражи персональных данных пользователей.

Наибольшее количество атак с заданным вектором используют методы социальной инженерии (рис. 2) [3]. Проблематика данного вопроса лежит в основе игнорирования пользователем методов защиты своих персональных данных (ПДн) с применением механизмов двухфакторной аутентификации (2ФА).

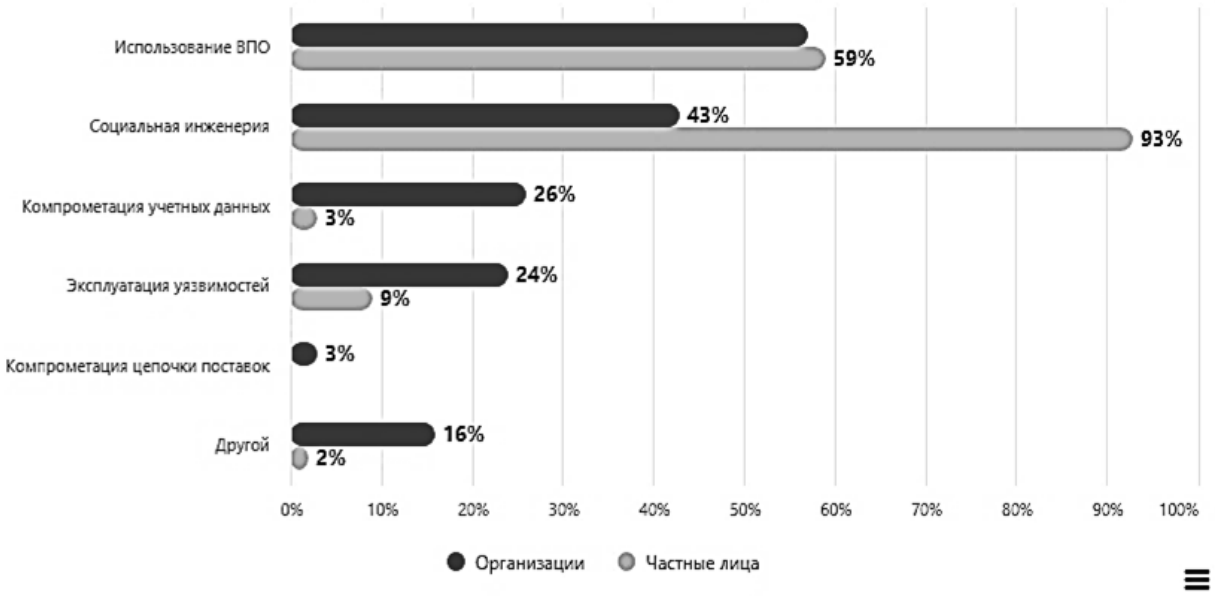

Рис. 2. Методы, применяемые в компьютерных атаках на интернет-ресурсы [1].

Оставшиеся виды деструктивного воздействия не рассматривают конечного пользователя как источник целевой информации. Они в большинстве случаев строят свой вектор атаки, исходя из технических аспектов, методов построения и защиты компьютерных сетей. Таким образом, социальная инженерия зачастую является наиболее эксплуатируемым способом для получения доступа к данным ограниченного пользования в социальных сетях и информационных системах.

Одним из ярких примеров подобных атак служит утечка ПДн из базы данных сети медицинских учреждений Baptist Health [2]. В рассматриваемом случае алгоритм негативного воздействия заключался в ненадлежащем внедрении и последующей эксплуатации системы обнаружения вторжений. Неавторизованный пользователь, подключившийся к системе хранения медицинских записей получил доступ к конфиденциальной информации пациентов данной организации.

Аналогичным образом следует рассмотреть инцидент, произошедший в группе компаний T-Mobile. Компьютерная атака, совершенная группировкой LAPSUS$, заключалась в краже конфиденциальной информации и ПДн пользователей компьютерной сети. Причинами данного деструктивного воздействия являлись недостаточность мер защиты при аутентификации клиентов системы с использованием технологии VPN и непосредственное использование методов социальной инженерии.

В контексте социальных сетей можно выделить случай кражи персональных данных платформы Yappy, случившийся 8 ноября 2022 года. В результате утечки учетных данных одного из администраторов системы были похищены конфиденциальные данные пользователей. Среди скомпрометированных данных содержатся более двух миллионов телефонов, также информация, включающая в себя имя пользователя, дату рождения, модель устройства, версию операционной системы смартфона, хэш пароля, ID профиля и информацию о привязанных аккаунтов иных социальных сетей [4].

Применение двухфакторной аутентификации с использованием QR-кодов для защиты конфиденциальных данных

С внедрением механизма аутентификации OpenID, предоставляющего возможность создания единого аккаунта несвязных между собой интернет-ресурсов, для доступа к конфиденциальной информации потребность в постоянном использовании учетных данных пользователей исчерпала себя [5]. Процесс аутентификации заключается в единоразовом использовании логина и пароля пользователя. В дальнейшем, при необходимости доступа в

защищенный сегмент информационной системы алгоритм автоматически строит цепочку сопоставления пользователя и доступа к требуемой информации.

Примерами интеграции данного механизма являются такие программно-прикладные средства, как:

– Google Authenticator.

– Яндекс Ключ.

Вышеописанные приложения используют в своей архитектуре систему доступа к конфиденциальным данным технологию генерации и считывания QR-кодов. При детальном рассмотрении приведенного метода аутентификации пользователь для доступа к необходимому контуру системы производит единоразовый ввод учетных данных. В дальнейшем используется только сканирование сгенерированного QR-кода, который устанавливает соответствие логина и пароля с системой защиты и предоставляет доступ к целевым данным.

Имитируя ситуацию использования подобной технологии, можно рассмотреть модель, состоящую из нижеприведенных взаимодействующих субъектов (рис. 3):

– Пользователь.

– Мобильное устройство.

– Приложение для авторизации.

– QR-код.

– База данных с аутентификационной информацией.

– Серверы предприятия.

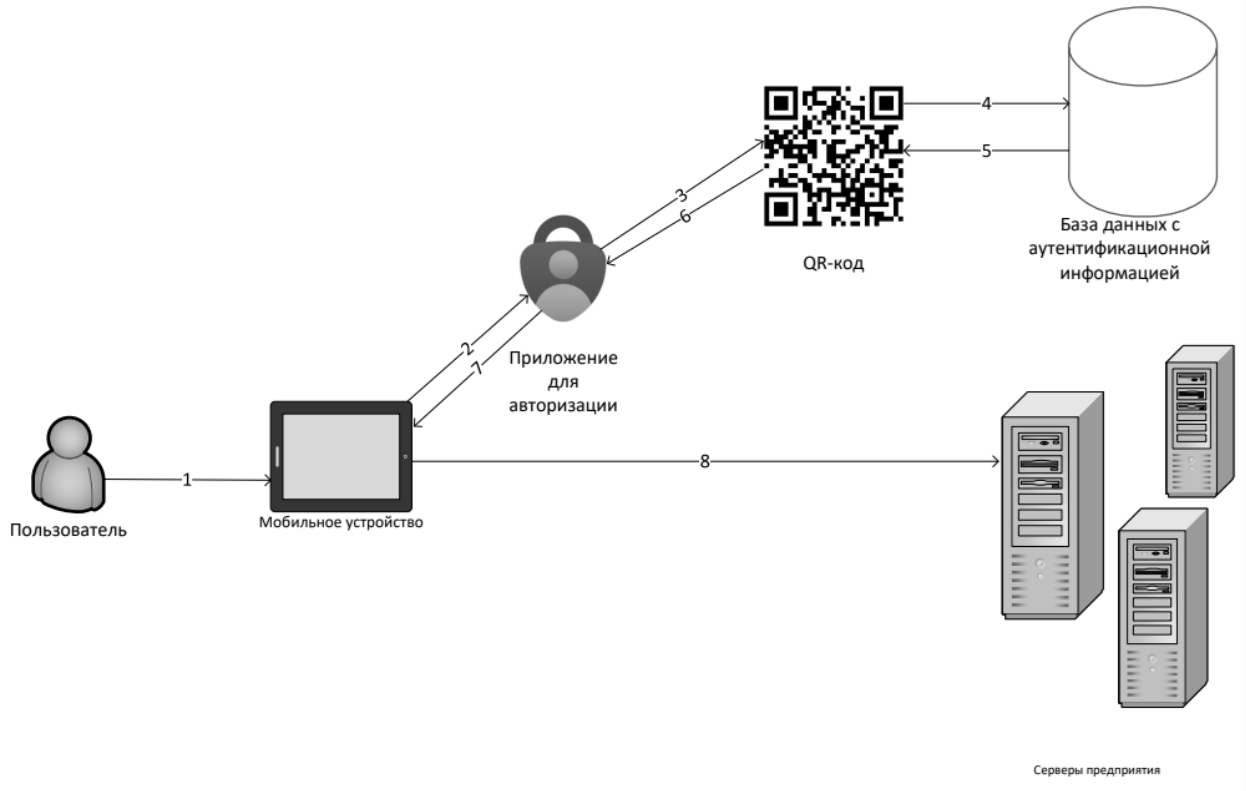

Рис. 3. Модель взаимодействия конечного пользователя с системой хранения информации ограниченного пользования в контексте использования технологии аутентификации с применением QR-кода

Конкретным примером может послужить деятельность инженера по защите информации. Специалист имеет необходимость, согласно своим должностным обязанностям, проводить проверку журнала обработки событий средства защиты информации (СЗИ) на удаленных участках компьютерной сети. Для оптимизации работы данного специалиста необходимой мерой является внедрение системы аутентификации с применением QR-кода. Посредством считывания

сгенерированного идентификатора, сотрудник получает доступ к необходимым данным для его трудовой деятельности.

Данный механизм решает следующие задачи:

– оптимизация рабочего процесса, посредством экономии времени на выполнение поставленных задач;

– повышение защищенности конечного ресурса от несанкционированного доступа.

Заключение

Таким образом, в данной статье рассмотрены вопросы повышения защищенности процесса аутентификации пользователя социальных сетей и Интернет-сайтов. Проведен анализ компьютерных атак с целью кражи конфиденциальной информации на примере атак на пользователей сетей медицинских учреждений Baptist Health, группы компаний T-Mobile и социальной сети Yappy. Необходимо выделить, что недостаточность мер защиты информации ограниченного пользования влечет за собой не только ущерб пользователя, но и материальный ущерб и технические сбои работы в распределенных компьютерных сетях. По результатам анализа принципов работы двухфакторной аутентификации и методов компьютерных атак отмечена необходимость применения двухфакторной аутентификации с использованием QR-кодов для повышения мер защиты доступа к конфиденциальным данным. По результатам аналитической деятельности была выработана модель взаимодействия конечного пользователя с системой хранения информации ограниченного пользования в контексте использования технологии аутентификации с применением QR-кода.

Список литературы

1. Актуальные киберугрозы: 2 квартал 2022 года / URL: https://www.ptsecurity.com/ruru/research /analytics/cybersecurity-threatscape/2022-q2 (дата обращения: 7.11.2022).

2. Texas Tech University Health Sciences Center and Baptist Health Report Data Breaches of Over 1.2 Million Records /URL: https://www.hipaajournal.com/ almost-1-3-million-patients-of-texas-tech-university-health-sciences-center-affected-by-eye-care-leaders-data-breach (Дата обращения: 24.10.2022).

3. Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code / URL: https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/ (дата обращения: 22.04.2022).

4. Yappy пошел по стопам Rutube / URL: https://www.kommersant.ru/doc/5653066 (дата обращения: 8.11.2022).

5. OpenID Connect простыми словами / URL: https://habr.com/ru/company/nixys/blog/566910 (дата обращения: 9.06.2021).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 15.11.2022

Информация об авторах

Анцупов Павел Андреевич – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Булычев Максим Александрович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

ASPECTS OF APPLYING TWO-FACTOR AUTHENTICATION USING QR CODES TO PROTECT AGAINST COMPUTER ATTACKS

P.A. Antsupov, M.A. Bulychev, E.A. Moskaleva

In the modern world, in the context of widespread digitalization of information, the issues of secure access and work with personal data have become basic and require constant attention. According to statistics, since 2018, the number of social network users has been increasing every year. Due to the increasing number of computer attacks aimed at stealing the confidential data of computer network participants, more and more attention is paid to data security. One of the highest priority methods for ensuring the security of information is the use of two-factor authentication algorithms. In the current situation, an important aspect is also the correct configuration and implementation of personal data protection mechanisms. This article discusses the issues of organizing the security of information for users of social networks and information systems, using QR codes to counter computer attacks.

Key words: digitalization, computer attacks, privacy, personal data, two-factor authentication, QR code.

Submitted 15.11.2022

Information about the authors

Pavel A. Antsupov – Graduate Student, Voronezh State Technical University, email: mnac@comch.ru
Maxim A. Bulychev – Student, Voronezh State Technical University, email: mnac@comch.ru
Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, email: mnac@comch.ru