УДК 004.056

Шамсутдинов Б.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

МЕТОДЫ ЗАЩИТЫ QR-КОДОВ ОТ ПОДДЕЛКИ

Аннотация. Для защиты QR-кодов от подделки важно использовать комплексный подход, основанный на использовании криптографических методов защиты информации, защищенные информационные платформы, двухфакторные аутентификацию. Применение этих методов защиты информации повышает сложность и стоимость использования QR-кодов, однако снижает риски использования их в целях фишинга и кражи данных. В докладе рассматривается пример генерации QR-кода и цифровой подписи.

Ключевые слова: QR-код, методы защиты, цифровая подпись.

Защита QR-кодов от подделки – актуальная задача в условиях активного их использования в системах логистики. Злоумышленники используют технологии копирования и замены QR-кодов для различных схем фишинга и кражи данных. Для защиты от этого можно использовать следующие методы [1–4]:

– использование защищенных цифровых платформ генерации QR-кодов. Для повышения безопасности следует создавать QR-коды с помощью специализированных цифровых сервиов, обеспечивающих дополнительную защиту подлинности QR-кода. Например, шифрование содержимого QR-кода, добавления цифровой подписи или проверки подлинности сканируемого адреса перед переходом по ссылке, полученной из QR-кода;

– шифрование данных. Использование криптографического алгоритма для шифрования информации внутри QR-кода помогает предотвратить несанкционированное чтение данных. Это значительно усложняет процесс подделки, поскольку сначала необходимо расшифровать данные, что требует занаие ключа;

– цифровая подпись. Применение цифровых подписей используется для подтверждения подлинности QR-кода. Когда пользователи сканируют код, специальное приложение проверяет цифровую подпись и подтверждает ее подлинность. Если подпись отсутствует или повреждена, то система предупреждает пользователей о возможной угрозе;

– контроль над распространением кода. Это ограничение распространение QR-кодов только через проверенные каналы распространения. В этом случае необходимо контролировать размещение QR-кода на открытых информационных платформах. Необходимо проводить мониторинг размещенных QR-кодов, чтобы убедиться в отсутствии подделок;

– обучение пользователей и персонала компаний. Необходимо информировать их о потенциальных рисках и правилах безопасного обмена информацией с помощью QR-кодов;

– использование двухфакторной аутентификации. Добавление второго уровня авторизации после сканирования QR-кода, содержащего ссылку на информационный ресурс снижает вероятность взлома злоумышленником аккаунта даже в случае успешной атаки. Пользователю при применении этого кода потребуется ввести дополнительный пароль или одноразовый код, отправленный на зарегистрированный номер телефона или электронную почту.

Пример применения цифровой подписи представлен на рис. 1.

	Информация из QR-кода: https://example.com Цифровая подпись включена в QR-код: 100680ad546ce6a577f42f5 2df33b4cfdca756859e664b 8d7de329b150d09ce9

Рис. 1. QR-код и цифровая подпись

Для защиты QR-кодов от подделки важно использовать комплексный подход, основанный на использовании криптографических методов защиты информации, защищенные информационные платформы, двухфакторные аутентификацию. Применение этих методов защиты информации повышает сложность и стоимость использования QR-кодов, однако снижает риски использования их в целях фишинга и кражи данных.

Список использованных источников:

1. Smith J. (2020). *The Security Risks of Barcode Systems. Journal of Information Security, 12(3), 45–58.

2. Jones A., Taylor, R. (2019). Best Practices for Secure Barcode Implementation. International Journal of Technology Management, 15(2), 123–134.

3. SO/IEC 15420:2009. Information technology – Automatic identification and data capture techniques – Bar code print quality test specification*. International Organization for Standardization.

4. National Institute of Standards and Technology (NIST). (2022). Guidelines for Securing Barcode Systems.

Shamsutdinov B.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

METHODS OF PROTECTING QR CODES FROM FORGERY

Abstarct: To protect QR codes from forgery, it is important to use an integrated approach based on the use of cryptographic information protection methods, secure information platforms, and two-factor authentication. The use of these information protection methods increases the complexity and cost of using QR codes, but reduces the risks of using them for phishing and data theft. The report examines an example of QR code generation and digital signature.

Keywords: QR code, security methods, digital signature.