УДК 004.056.53:004.7

І. О. Бондаренко
Х. А. Грищук

АНАЛІЗ БЕЗПЕКИ QR-КОДІВ ТА ДОСЛІДЖЕННЯ АТАК ТИПУ QR-ФІШИНГУ З ЕЛЕМЕНТАМИ ADVERSARY-IN-THE-MIDDLE

Вінницький національний технічний університет

Анотація

У роботі досліджено впровадження QR-кодів у сучасні інформаційні системи, що створює нові вектори кіберзагроз, пов'язаних із порушенням конфіденційних даних користувачів . Одним із найнебезпечніших методів реалізації цих загроз є квішинг (quishing), який поєднує методи соціальної інженерії з перенаправленням на шкідливі ресурси. Проаналізовано механізми атак «зловмисник посередині» (Adversary-in-the-Middle, AitM), в яких QR-коди використовуються для обходу багатофакторної автентифікації (MFA) та перехоплення сесійних файлів cookie. Розглянуто технічні засоби спуфінг-атак, зокрема використання вразливостей у відкритих системах перенаправлення та фільтрації трафіку (TDS). Систематизовано типові сценарії використання шкідливих QR-кодів у фінансових послуг та систем. Крім того, запропоновано рекомендації щодо підвищення безпеки мережевої інфраструктури та обізнаності користувачів.

Ключові слова: QR-коди, кібербезпека, квішинг, фішинг, Adversary-in-the-Middle (AitM), багатофакторна автентифікація (MFA), перехоплення сесії, соціальна інженерія.

Abstract

The paper examines the implementation of QR codes in modern information systems, which creates new vectors of cyber threats related to the violation of users' confidential data. One of the most dangerous methods of implementing these threats is quishing, which combines social engineering methods with redirection to malicious resources. The mechanisms of "Adversary-in-the-Middle" attacks (AitM) are analyzed, in which QR codes are used to bypass multi-factor authentication (MFA) and intercept session cookies. The technical means of spoofing attacks are considered, in particular, the use of vulnerabilities in open traffic redirection and filtering systems (TDS). Typical scenarios of the use of malicious QR codes in financial services and systems are systematized. In addition, recommendations are proposed for improving the security of network infrastructure and user awareness.

Keywords: QR codes, cybersecurity, quishing, phishing, Adversary-in-the-Middle (AitM), multi-factor authentication (MFA), session hijacking, social engineering.

Вступ

QR-коди набули значного поширення як один із найпопулярніших типів двовимірних штрихкодів завдяки своїй здатності зберігати великий обсяг інформації та стійкості до пошкоджень. Разом із активним розвитком смартфонів питання безпеки та конфіденційності користувачів стає все більш актуальним. Стрімке зростання використання мобільних пристроїв сприяло розширенню сфер застосування QR-кодів, однак водночас це призвело до появи нових загроз безпеці [1]. У цьому контексті скомпрометовані або підмінені QR-коди можуть використовуватися як ефективний інструмент для здійснення кібератак. Оскільки QR-коди широко розміщуються у публічних місцях, зловмисники можуть легко змінювати або підміняти їх, вводячи користувачів в оману.

Останнім часом організації все частіше страждають від поширених і дедалі складніших фішингових атак, що використовують методи «зловмисник посередині» (AitM). Фішингові набори AitM переважно призначені для викрадення сесійних файлів cookie з цільових сервісів, щоб обійти процес MFA під час наступних входів у систему. У 2023 році аналітики Sekoia виявили, що зловмисники широко застосовували тактику вбудовування QR-кодів у документи для перенаправлення користувачів на фішингові сторінки типу AitM. До середини 2025 року ця техніка залишалася поширеною, незважаючи на те, що засоби безпеки стали ефективніше виявляти фішингові посилання, що поширювалися через QR-коди [2].

Результати дослідження

Квішинг, або фішинг за допомогою QR-кодів – це швидкозростаюча кіберзагроза. Шкідливі QR-коди використовують небезпечні посилання для перенаправлення жертв на фальшиві вебсайти з метою викрадення їхніх облікових даних. Хоча Microsoft Defender для Office 365 і шлюзи безпечної електронної пошти (SEG) пропонують певний захист від цих атак, проте засоби захисту часто є неповними або ненадійними від складних методів крадіжки даних.

Що робить квішинг особливо ефективним, так це його здатність обходити як перевірку людиною, так і традиційні фільтри безпеки. На відміну від текстових фішингових листів, які користувачі навчилися ретельно перевіряти, QR-коди виглядають як нешкідливі чорно-білі візерунки, які нічого не розкривають про своє призначення, доки їх не просканувати. Деякі існуючі рішення з безпеки можуть виявляти прості QR-коди на основі зображень, але не справляються з просунутими методами маскування. Ця вразливість посилюється тим, що, хоча шкідливий код надходить через корпоративну електронну пошту з корпоративними засобами безпеки, користувачі зазвичай сканують ці коди за допомогою особистих мобільних пристроїв, які не мають корпоративних засобів контролю безпеки, фактично обходячи весь стек безпеки [3].

Існує два основні вектори атак для зловживання QR-кодами: зловмисник замінює весь QR-код. Ця атака є простою, але ефективною. Зловмисник створює новий QR-код із закодованим шкідливим посиланням і накладає його на вже існуючий, наприклад, на рекламному білборді. Зловмисник модифікує окремі модулі QR-коду. Основна ідея такої модифікації полягає в тому, що закодований вміст змінюється виключно шляхом зміни кольору певних модулів QR-коду, на який користувач буде перенаправлений після сканування коду [4].

В таблиці 1.1 описано сценарії атак, які ґрунтуються на дослідженнях сучасних загроз, пов’язаних із використанням QR-кодів як вектора кібератак [5].

Таблиця 1 – Приклади сценаріїв атак через QR-коди

Назва атаки	Тип deep link	Опис атаки	Приклад (вміст QR-коду)
Фінансове шахрайство	Платіжні застосунки	Надання доступу до платіжних сервісів із заздалегідь підставленими реквізитами отримувача	bitcoin:attackers_address
Захоплення акаунтів	Соціальні мережі та месенджери	Перенаправлення жертви для авторизації зловмисника в обліковому записі користувача	tg://login?token=xxxx
Вбудовування шкідливих URL	Пошта, інші застосунки	Вбудовування шкідливих посилань у повідомлення або файли, які надсилаються або зберігаються на пристрої	mailto:receive@mail.com ?subject=...&body=www. malicious-url.com
Календарне зараження	Системні утиліти	Додавання шкідливих подій у календар із фішинговими посиланнями	Подія календаря з www.phishing-meeting-link.com
Зараження контактів	Системні утиліти	Вбудовування шкідливих URL або фейкових контактів у телефонну книгу	URL:malicious-website.com у vCard
Підроблені Wi-Fi мережі	Системні налаштування	Автоматичне підключення до Wi-Fi мережі, контрольованої зловмисником	WIFI:T:WPA;S:attacker-network;P:password;H:false

Незалежно від того чи зловмисники використовують QR-коди, HTML-вкладення або посилання, вбудовані у документи, останнім кроком є перенаправлення користувача на фішингову сторінку. Для того щоб обійти фільтри електронної пошти та запобігти виявленню сканерами шкідливих доменів,

зловмисники часто використовують один або декілька етапів перенаправлення. Зазвичай вони виконуються з використанням легітимних доменів для формування довіри користувачів та уникнення виявлення автоматизованими системами безпеки.

Зокрема, зловмисники активно використовують такі вразливості, як «відкрите перенаправлення» (open redirect), вставляючи шкідливі URL-адреси в параметри запиту легітимних вебдодатків. Це дозволяє перенаправляти користувачів на будь-який зовнішній ресурс. Технічно, open redirect базується на використанні параметра URL-адреси, який визначає кінцеву адресу користувача. Сторінки перенаправлення, якими керують зловмисники, часто містять механізми фільтрації трафіку, які гарантують, що фішингова сторінка відображається лише потенційним жертвам. Така фільтрація може базуватися як на власних, так і на комерційних системах розподілу трафіку (Traffic Distribution Systems, TDS), або ж на аналізі характеристик пристрою користувача. Зазвичай перевіряється, чи належить IP-адреса користувача до діапазону резидентного інтернет-провайдера (ISP), а також чи відповідають операційна система та веббраузер типовим корпоративним середовищам.

Зрештою, більшість фішингових кампаній AitM захищають шкідливі сторінки за допомогою CAPTCHA, що вимагає взаємодії з людиною. Ці антибот-сторінки зазвичай надаються у складі PhaaS-платформ і інтегрують легітимні сервіси (наприклад, Cloudflare Turnstile, reCAPTCHA, hCaptcha), рішення з відкритим кодом (зокрема IconCaptcha) або власні реалізації CAPTCHA [2].

Висновки

QR-коди є ефективним інструментом для сучасних кібератак, зокрема для фішингових компаній, що використовують технології AitM. Ефективність цих атак значною мірою залежить від механізмів багатоетапного перенаправлення, зокрема використання таких вразливостей як open direct, а також систем виявлення трафіку (TDS) та CAPTCHA для уникнення виявлення.

В атаках типу «зловмисник посередині» QR-коди виступають у ролі першого вектора доступу, а подальша реєстрація сесій дозволяє обходити механізми MFA. Сценарії атак підтверджують універсальність QR-кодів як інструменту загроз у різних галузях – від фінансових до системних функцій для мобільних пристроїв. Основними факторами ризику є поведінка користувачів та неможливість попередньої перевірки вмісту QR-кодів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mavroeidis, Vasileios & Nicho, Mathew. (2017). Quick Response Code Secure: A Cryptographically Secure Anti-Phishing Tool for QR Code Attacks. 313-324. DOI: https://doi.org/10.1007/978-3-319-65127-9_25.

2. Global analysis of Adversary-in-the-Middle phishing threats URL: https://blog.sekoia.io/global-analysis-of-adversary-in-the-middle-phishing-threats/ (дата звернення: 11.04.2026).

3. The Evolution of Quishing: How QR Code Phishing Bypasses Modern Security URL: https://www.open-systems.com/blog/evolution-of-quishing/ (дата звернення: 11.04.2026).

4. QR Code Security: A Survey of Attacks and Challenges for Usable Security URL:https://publications.sba-research.org/publications/llncs.pdf (дата звернення: 11.04.2026)..

5. Phishing on the Edge of the Web and Mobile Using QR Codes URL: https://unit42.paloaltonetworks.com/qr-codes-as-attack-vector/ (дата звернення: 11.04.2026).

Бондаренко Ірина Олексіївна **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Грищук Христина Анатоліївна **–** студентка групи 2КІТС-23б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: krisgrishuk92@gmail.com

Bondarenko Iryna O. **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua

Hryshchuk Khrystyna A. – student of group 2KITS-23b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: krisgrishuk92@gmail.com