https://nure.ua/

The Ministry of Education and Science of Ukraine

Kharkiv National University of Radio Electronics

KITAM

2023

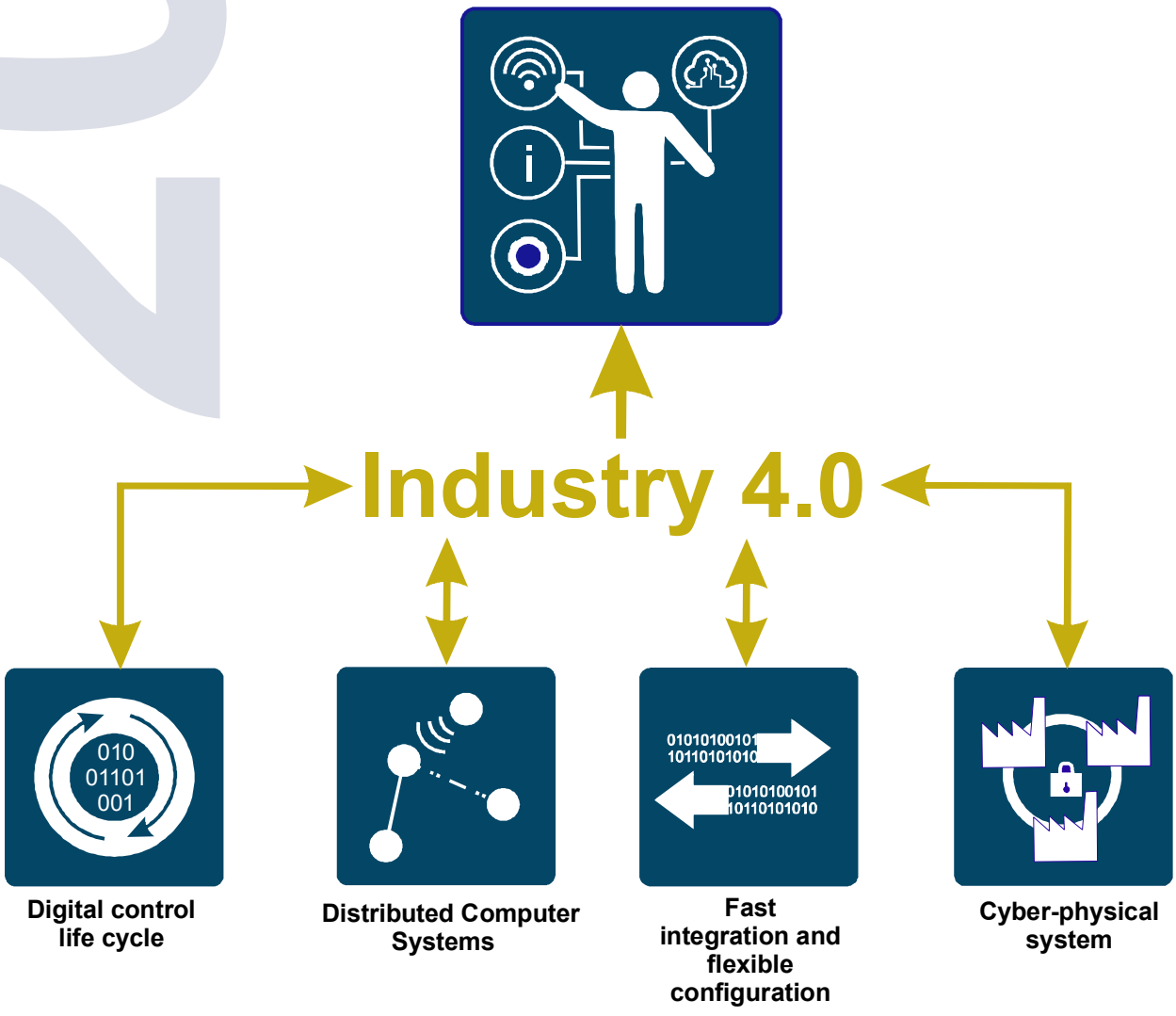
COLLECTION

OF STUDENTS' SCIENTIFIC PAPER

«Automation and Development of Electronic Devices»

ADED-2023

(Part 1)



https://nure.ua/

кафедра
Комп'ютерно-інтегрованих
технологій, автоматизації та мехатроніки

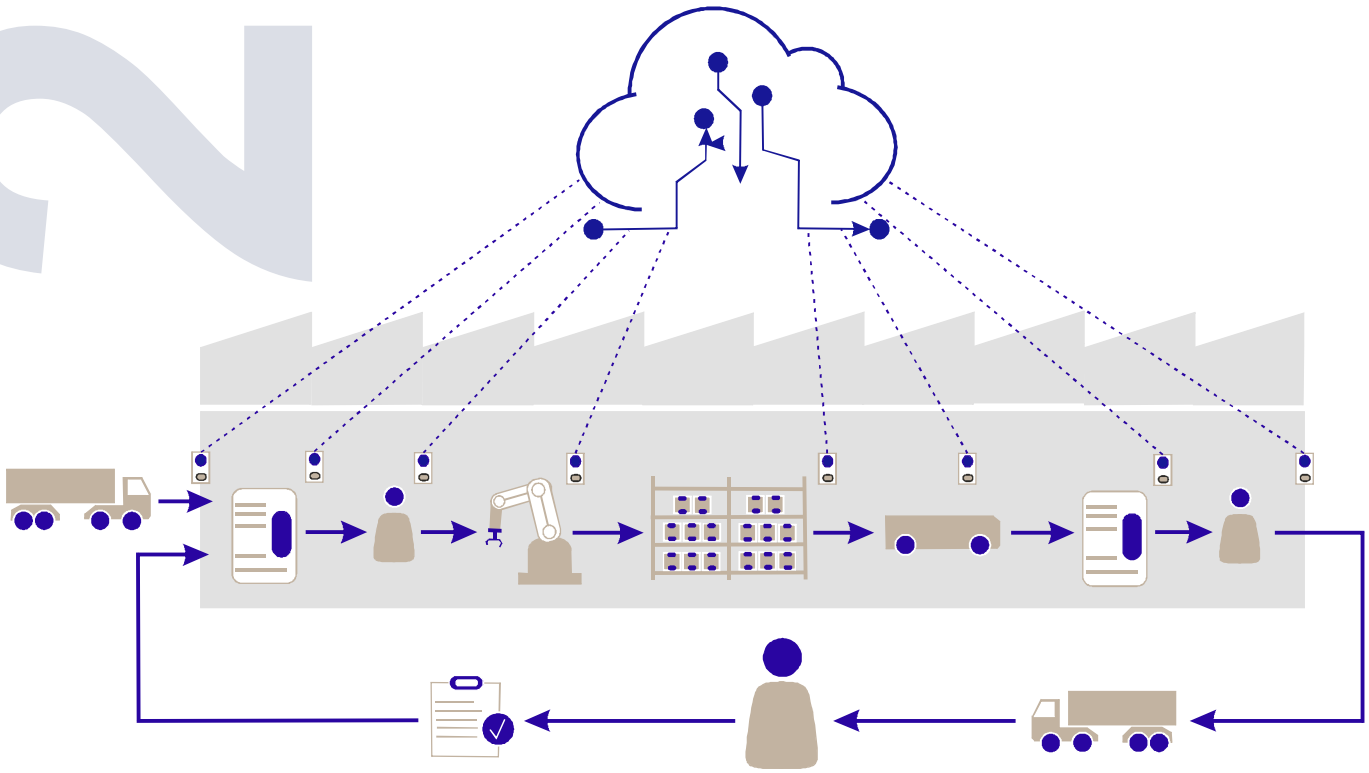
2023

ХНУРЕ

ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»
ADED-2023
(Випуск 1)
[електронне видання]



Industry 4.0

Автоматизація та Приладобудування («Automation and Development of Electronic Devices» ADED-2023) [Електронний ресурс] : збірник студентських наукових статей / Харківський національний університет радіоелектроніки ; [редкол.: І.Ш. Невлюдов та ін.]. – Харків : ХНУРЕ, 2023. – Вип. 1. – 336с.

Collection of Students' Scientific Paper «Automation and Development Of Electronic Devices» ADED-2023 Part 1 (Key infrastructure 2023) - Kharkiv/ The Editorial.: Nevlyudov I.Sh. (head), that all. Kharkiv: Kind of Kharkiv National Universitety of Radio Elektronics [electronic edition], 2023. – 336p with.

Рекомендовано рішенням
Науково-технічної ради
Харківського національного
університету радіоелектроніки
протокол №6 від 29.11.2018

Рекомендовано рішенням Вченої ради
факультету Автоматики і комп'ютеризованих технологій
Харківського національного
університету радіоелектроніки
протокол № 6 від 01.05.2023

Збірник містить наукові статті здобувачів першого (бакалаврського), другого (магістерського) рівнів вищої освіти кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки (КІТАМ) Харківського національного університету радіоелектроніки, кафедри Інформаційних технологій електронних засобів (ІТЕД) Запорізького національного технічного університету та кафедри Електронних апаратів (ЕА) Кременчуцького національного університету ім. М. Остроградського які навчаються за спеціальностями: 151 Автоматизація та комп'ютерно-інтегровані технології, 172 Телекомунікації та радіотехніка, 171 Електроніка та 163 Біомедична інженерія. Статті надані в авторській редакції.

ЗМІСТ

УДК 378.016

БЕЗПЕКА QR-КОДІВ ТА PHISHING АТАКИ

К. А. Поліканов
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки 14
Email: kyrylo.polikanov@nure.ua

Анотація: У даній статті розібрані основні різновиди QR-кодів, їх особливості та області використання, проблеми безпеки у використанні QR-кодів, дослідження такого явища як phishing й наведено існуючі засоби запобігання та протидії.

Ключові слова: QR-код, кібербезпека, phishing, атаки, метод передачі інформації.

QR CODE SECURITY AND PHISHING ATTACKS

K. A. Polikanov
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Prospect Nauki 14
Email: kyrylo.polikanov@nure.ua

Abstract: In this article, the main varieties of QR codes, their features and areas of use, security problems in the use of QR codes, the study of such a phenomenon as phishing are analyzed and existing means of prevention and counteraction are given.

Keywords: QR-code, cybersecurity, phishing, attacks, method of information transfer.

QR-коди – це швидкий та зручний спосіб передачі інформації, який знаходить все більш широке застосування в різних галузях життя. Однак, разом зі зростанням популярності QR-кодів, з'являються нові проблеми та загрози, зокрема проблема phishing. У цій статті ми розглянемо особливості QR-кодів та проблеми, пов'язані з phishing, а також розглянемо способи захисту від цієї загрози. Розуміння того, як QR-коди працюють та які ризики з ними пов'язані, може допомогти уникнути потенційних проблем з безпекою в Інтернеті та збереження ваших особистих даних.

QR-код (Quick Response Code) – це двовимірний штрих-код, що здатний зберігати багато інформації в компактному форматі. Він складається з чорних та білих квадратів, які утворюють візуальний код. Для зчитування QR-коду достатньо використати камеру смартфону та спеціальну програму [1 - 3].

QR-коди мають декілька основних характеристик:

1. Кодування інформації – QR-код може містити різну кількість інформації, залежно від розміру та складності коду. Він може кодувати текст, URL-адреси, контактні дані, календарні події, електронні візитки та інші дані
2. Швидкість зчитування – QR-коди зчитуються досить швидко, що дозволяє використовувати їх для швидкої передачі інформації.
3. Візуальний вигляд – QR-коди можуть мати різні кольори та стилі оформлення, що дозволяє їх використовувати для реклами та брендування.

Інформація та її властивості є об'єктом дослідження цілої низки наукових робіт [4 - 6]. QR-коди також використовуються для збереження та передачі різної інформації [7 - 9]. Наприклад, QR-коди можуть бути використані для:

1. Передачі URL-адреси – відсканувавши QR-код, користувач може швидко відкрити веб-сторінку, не вводячи адресу вручну.
2. Збереження контактних даних – QR-код може містити контактні дані, такі як ім'я, прізвище, телефон та електронну пошту, що дозволяє зберегти цю інформацію в адресну книгу без необхідності вводити її вручну.

3. Організації квитків та пропусків – QR-коди можуть містити інформацію про квитки та пропуски на захід, що дозволяє швидко та зручно перевіряти їх на вході.

4. Організації оплати – QR-коди можуть бути використані для швидкої та зручної оплати товарів та послуг через мобільний додаток.

QR-коди використовуються для збереження та передачі різних видів інформації, таких як веб-адреси, контактні дані, текстові повідомлення, географічні координати, номери телефонів та багато іншого. Для створення QR-коду можна використовувати спеціальні програми або онлайн-сервіси, які генерують код на основі введеної інформації.

QR-коди можуть бути роздруковані на різних матеріалах, таких як паперові листи, рекламні буклети, наліпки, товарні ярлики та інші матеріали. Також можна створювати QR-коди для відображення на екрані мобільних пристроїв, що дозволяє передавати інформацію швидко та зручно.

Для того, щоб отримати доступ до інформації, яка зберігається у QR-коді, необхідно відсканувати його за допомогою спеціальної програми або функції, яка доступна в багатьох сучасних мобільних пристроях. Після сканування QR-коду, інформація автоматично відображається на екрані пристрою. Таким чином, QR-коди дозволяють швидко та зручно обмінюватися різними видами інформації без необхідності вводити довгі адреси веб-сторінок або контактні дані вручну.

Існує декілька типів QR-кодів, кожен з яких має свої особливості та використовується для різних цілей. Ось декілька найпоширеніших типів QR-кодів:

1. QR-коди – це 2D-коди, які складаються з чорних і білих точок, що можуть бути зчитані за допомогою спеціальних сканерів або мобільних пристроїв з камерою. QR-коди використовуються для зберігання і передачі різної інформації, включаючи веб-адреси, контактну інформацію, текстові повідомлення, номери телефонів та інше.

2. Існує кілька різновидів QR-кодів, які відрізняються за своєю структурою та можливостями:

3. Стандартний QR-код: це найбільш поширений тип QR-коду. Він містить до 3 000 символів, включаючи латинські літери, цифри та спеціальні символи.

4. QR-код з розширенням: цей тип QR-коду дозволяє додавати до звичайного QR-коду додаткові функції, такі як зберігання картки візитів, веб-сторінок, інформації про події та інше.

5. Динамічний QR-код: це QR-код, який може змінювати свій вміст залежно від потреб користувача. Наприклад, якщо ви створюєте динамічний QR-код для веб-сайту, він може автоматично переадресувати користувача на іншу сторінку, якщо перша була замінена.

6. Колоровий QR-код: це QR-код, який має кольорову гаму замість чорних та білих точок. Він може бути використаний для створення дизайнерських QR-кодів, що відрізняються від звичайних.

7. QR-код з шифруванням: це QR-код, який містить зашифровану інформацію, яку можуть розкодувати лише особи з відповідними ключами. Він використовується для захищенного способу передачі інформації.

Крім того, існують QR-коди з різним розміром та складністю. Наприклад, QR-коди можуть містити різні види коригуючих кодів, що дозволяє їм зберігати інформацію навіть при деяких пошкодженнях. Також можуть використовуватися різні кольори та фони для QR-кодів, що дозволяє їх краще виділяти та привертати увагу.

Безпека інформації – це на сьогодні дуже важлива область бо вона забезпечує конфіденційність, цілісність і водночас доступність інформації [1]. Phishing (фішинг) – це вид шахрайства, коли зловмисник намагається отримати конфіденційну інформацію від людей, використовуючи підроблені Веб-сайти, електронні листи та інші електронні засоби комунікації.

Щодо QR-кодів, то phishing може відбуватися за допомогою підроблених QR-кодів, які ведуть до фішингових сайтів. Наприклад, зловмисник може створити QR-код, який містить

посилання на підроблений сайт банку. Коли користувач сканує такий QR-код за допомогою мобільного пристрою, він буде перенаправлений на підроблений сайт банку, де зловмисник може запросити у нього конфіденційну інформацію, таку як пароль, номер кредитної картки або іншу особисту інформацію.

Таким чином, зловмисники можуть використовувати QR-коди як інструмент для залучення жертв та здійснення фішинг-атак. Тому важливо бути обережними та перевіряти джерело QR-кодів, перед тим як сканувати їх. Також важливо користуватися захисними програмами та програмами-антивірусами для захисту від шахрайства та інших кіберзлочинів.

Існує декілька видів фішингу, які можуть бути небезпечними для користувачів:

1. Перехоплення інформації: цей вид фішингу полягає в тому, що зловмисник намагається перехопити конфіденційну інформацію, таку як паролі, номери кредитних карток або іншу особисту інформацію, коли користувач вводить її на підробленому сайті або через підроблений QR-код.
2. Фішинг за допомогою електронної пошти: цей вид фішингу полягає в тому, що зловмисник відправляє електронний лист, який маскується під лист від довіреної особи або організації, і запитує від користувача конфіденційну інформацію.
3. Фішинг за допомогою соціальних мереж: цей вид фішингу полягає в тому, що зловмисник створює підроблені профілі в соціальних мережах та використовує їх для надання шахрайських послуг, запитує від користувачів конфіденційну інформацію, таку як паролі або номери кредитних карток.
4. Фішинг за допомогою QR-кодів: цей вид фішингу полягає в тому, що зловмисник створює підроблені QR-коди, які містять посилання на підроблені сайти, де користувач може надати конфіденційну інформацію.

Ці види фішингу можуть бути небезпечними для користувачів, оскільки зловмисники можуть отримати доступ до їх конфіденційної інформації, що може призвести до фінансових втрат, крадіжки особистої інформації та інших негативних наслідків. Тому важливо бути обережним й свідомо використовувати QR-коди.

В ході наведених варіантів безпечних ситуацій з QR-кодами визначимо основні заходи для захисту від phishing з використанням QR-кодів:

1. Не відскановуйте QR-коди з невідомих джерел або невідомих вам осіб. Якщо QR-код приходить до вас по електронній пошті, SMS або месенджеру, перевірте, щоб він був відправлений відомою особою або організацією, якій ви довіряєте.
2. Перевірте URL-адресу, яка розкривається після сканування QR-коду, перед тим, як натиснути на неї. Якщо URL-адреса містить дивні символи або виглядає неправильно, це може бути ознакою phishing спроби.
3. Використовуйте програми сканування QR-кодів з вбудованими функціями захисту від phishing, такі як Norton Snap QR Code Reader, Kaspersky QR Scanner, QR Code Reader and Scanner або інші подібні програми.
4. Встановлюйте оновлення програм сканування QR-кодів та операційних систем своїх пристроїв, щоб забезпечити найбільшу безпеку та усунення вразливостей.
5. Не вводьте особисту інформацію на сторінках, які відкриваються після сканування QR-коду, якщо ви не довіряєте джерелу.
6. Використовуйте програми антивірусного захисту на своїх пристроях та перевіряйте їх регулярно на наявність шкідливих програм.
7. Якщо ви отримали QR-код від організації, з якою ви маєте стосунки, перевірте правильність та актуальність інформації, яка міститься в QR-коді, з надійним джерелом.

Існує кілька способів, які можна використовувати для захисту від phishing за допомогою QR-кодів:

1. Використання персоналізованих QR-кодів: При створенні QR-кодів для продуктів чи послуг можна включити в них інформацію про назву бренду, логотип, та інші візуальні елементи, які допоможуть відрізнити дійсний QR-код від фішингового.

2. Перевірка джерела QR-коду: Перш ніж сканувати QR-код, корисно перевірити джерело, з якого він отриманий. Наприклад, якщо QR-код розміщено на сайті, перевірте, чи це дійсно офіційний сайт компанії.

3. Використання безкоштовних мобільних застосунків для перевірки QR-кодів: Існує багато безкоштовних мобільних застосунків, які дозволяють перевірити QR-код на безпеку. Зокрема, вони можуть перевірити, чи містить QR-код небезпечні посилання.

4. Застосування двофакторної аутентифікації: При скануванні QR-коду, який містить небезпечні посилання, двофакторна аутентифікація може допомогти попередити атаку. Для цього на смартфоні можна налаштувати сповіщення, яке попереджатиме про потенційну небезпеку, та запитувати додаткові дані для підтвердження ідентичності користувача.

5. Надійність джерела: Крім QR-коду, на який потрібно сканувати, важливо враховувати джерело, з якого він був отриманий. Зверніть увагу на посилання, з якого ви отримали QR-код, і переконайтеся, що воно дійсне та надійне.

Отже, можна зробити деякі висновки про QR-коди та проблему phishing. QR-коди – це потужний інструмент для збереження та передачі інформації, який має різноманітні варіанти використання в бізнесі та особистому житті. Проте, phishing – це серйозна проблема, пов'язана з QR-кодами, що може призвести до крадіжки конфіденційних даних, таких як паролі та фінансова інформація. Щоб запобігти phishing, слід бути дуже обережними при скануванні QR-кодів та не забувати про необхідність перевірки посилань та джерел, з яких вони походять. Забезпечення безпеки QR-кодів може залежати від кількох чинників, таких як використання спеціальних програм та технологій шифрування, вибір надійних джерел та перевірка кодів перед скануванням.

Література:

1. Kapsalis I. security of QR codes / I. Kapsalis. – Institutt for telematikk, 2013. – 92 P.

2. Ardiansyah R. et al. Design of Prototype Information System for Tracking & Tracing Fish Distribution Based on Mobile Agent / R. Ardiansyah // IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2022. – Т. 1212. – №. 1. – С. 012045.

3. Pan J. S. et al. Robust digital watermarking with parallel compact sparrow search algorithm applied for QR code / J. S. Pan // Journal of Information Hiding and Multimedia Signal Processing. – 2022. – Vol. 13, Num. 2. – P. 124-144.

4. Sotnik S. Features of Database Types // International Journal of Engineering and Information Systems (IJEAIS) / S. Sotnik, Z. Deineko, O. Vovk, V. Lyashenko – 2021. – Т. 5. – №. 10. – С. 73-80.

5. Sotnik S., Lyashenko V. Agricultural Robotic Platforms / S. Sotnik, V. Lyashenko // International Journal of Engineering and Information Systems (IJEAIS). – 2022. – Vol. 6, Iss. 4. – P. 14-21.

6. Lyashenko V. Overview of Modern Accelerometers / V. Lyashenko, S. Sotnik // International Journal of Engineering and Information Systems (IJEAIS). – 2022. – Vol. 6, Iss. 1. – P. 57-64.

7. Sotnik, S. Usage and Application Prospects QR Codes / S. Sotnik, Zh. Deineko, V. Lyashenko // International Journal of Engineering and Information Systems. – 2022. – Vol. 6, Issue 7. – P. 40-48.

8. Lyashenko, V. Dynamic and Static QR Coding / Zh. Deineko, S. Sotnik, V. Lyashenko // International Journal of Academic Engineering Research (IJAER). – 2023. – Vol. 6, Iss. 11. – P. 1-6.

9. Sotnik, S. Confidentiality of Information when Using QR-Coding / S. Sotnik, Zh. Deineko, V. Lyashenko // International Journal of Academic Information Systems Research. – 2022. – Vol. 6, Iss. 9. – P. 10-15.