Рисунок 2 – Внешний вид стереокамеры

Анализ выражения (1) показывает, что при фиксированном ω одна и та же диспарантность может быть достигнута при $b*f = const$. Выбор этих параметров целиком определяется конкретными задачами измерения.

Литература

1. Патент РБ № 13744. Дальномер на цифровой стереофотокамере / В. С. Калинов, В. Л. Козлов, Д. Л. Яковлев; заявитель и патентообладатель [указать при наличии]. – № 20231111; опубл. 07.05.2025. – 5 с.

УДК 004.774

АТАКИ С ИСПОЛЬЗОВАНИЕМ QR-КОДОВ

Ковынев Н. В.

МГТУ имени Н.Э. Баумана, Москва, Россия

Аннотация. В данной статье рассматриваются распространенные атаки при помощи qr-кодов, а также некоторые способы противодействия данным атакам.
Ключевые слова: qr-код, фишинг, qr-фишинг, квишинг.

QR-CODE ATTACKS

Kovynyov N. V.

Bauman Moscow state technical university, Moscow, Russia

Abstract. This article applies mass measures using QR codes, as well as some methods to counter these attacks.
Keywords: QR code, fishing, QR-fishing, quishing.

Адрес для переписки: Ковынев Н. В., МГТУ имени Н.Э. Баумана, Москва, Россия
e-mail: nvkovynyov@bmstu.ru

Активное развитие информационных технологий, их внедрение в повседневную жизнь общества, позволяют злоумышленникам находить новые способы по обману граждан, используя различные уязвимости современных технологий. Высокий уровень популярности мобильных технологий позволяет реализовывать фишинговые атаки на новых направлениях. Одни из самых распространенных способов реализации фишинга – это поддельные ссылки на вредоносные сайты, поддельные электронные письма, ссылки, которые очень похожи на адреса популярных сайтов (магазины, информационные ресурсы, какие-либо площадки, торговые площадки).

С внедрением qr-кодов во многие отрасли современной жизни такие как: банковская, маркетинговая, логистическая, государственная, образовательная и другие, у злоумышленников появились новые возможности для обмана граждан. Атаки с использованием qr-кодов только набирают популярность, но уже имеют ряд неоспоримых преимуществ: легкие генерация и связывание с поддельным сайтом; широкая область применения qr-кодов; отсутствие каких-либо визуальных признаков, гарантирующих подлинность или наоборот; невозможность проверки информации, которую содержит qr-код, без сканирования; широкое распространение различных считывателей qr-кодов. Помимо этого, высокое распространение для таких атак играет огромное количество мобильных телефонов, потому что большинство настольных операционных систем компьютеров имеет защиту от фишинга, телефоны же гораздо более уязвимы к таким атакам.

Использование qr-кодов для фишинговых атак получило название «квишинг». Данный термин определяют следующим: квишинг или qr-фишинг – угроза информационной безопасности, при реализации которой злоумышленник использует qr-код, чтобы перенаправить жертву на вредоносный сайт, загрузки вредоносного контента, кражи персональных данных или несанкционированных финансовых операций. При получении нужных данных или если жертва переходит на нужный интернет-ресурс, злоумышленник при помощи различных способов психологического воздействия или методов социальной инженерии может получить персональные данные жертвы, конфиденциальную информацию, доступ к финансовым ресурсам жертвы.

Одними из распространенных способов использования qr-кодов являются: создание qr-кодов, содержащих ссылки на поддельные сайты; подмена физических или цифровых кодов крупных компаний, которые расположены в доверенных местах; маскирование под рекламные компании различных брендов; маскирование под официальные способы оплаты или просмотра различных товаров и услуг.

Использование qr-фишинга позволяет злоумышленнику обходить традиционные способы борьбы с фишингом. Данное преимущество достигается из-за того, что системы обнаружения вторжений, системы обнаружения вредоносного программного обеспечения и различные почтовые фильтры способны блокировать подозрительные сообщения только при наличии ссылок или каких-либо вложений. Данный способ фишинга же позволяет злоумышленнику встраивать поддельный qr-код в письма в виде изображений, добавить его в документы с безопасным расширением, интегрировать в различные файлы рассылок компаний, разослать через социальные сети, распространить через какие-либо печатные материалы рекламного или научно-популярного формата. Описанные способы

позволяют вредоносному письму избежать попадания в раздел «спам», в результате чего, пользователь остается один на один в борьбе со злоумышленником. Если жертва сканирует вредоносный qr-код со своего личного телефона, то она перенаправляется на вредоносный сайт, где могут быть предложены различные формы взаимодействия: ввод личной информации (персональные данные, финансовые реквизиты). В данном случае сайт может запросить: имя пользователя; адреса электронной почты; номер мобильного телефона, для высылки кода подтверждения; дату рождения или же какие-либо данные учетной записи; данные банковских карт для проведения тех или иных операций.

Для уменьшения вероятности реализации угрозы необходимо использовать технические способы противодействия. Одним из таковых способов является использование приложений (Kaspersky QR Scanner; Norton Snao QR Code Reader; Dr. Web Security Space) с функцией предварительного анализа содержимого qr-кода перед открытием ссылки в нем. Также не стоит забывать про организационные меры и работу с персоналом: проведение регулярного обучения и повышения квалификации персонала в данном вопросе; разработка и внедрение политики взаимодействия и использования qr-кодов внутри организации и при контактах с партнерами; регулярные проверки выполнения должностных инструкций и знаний у работников. Также стоит отметить проработку мер по установлению стандартов при использовании qr-кодов в коммерческих и государственных сервисах, усиление ответственности при использовании qr-кодов в мошеннических или незаконных целях.

Одной из главных задач является – безопасное взаимодействие с qr-кодами: проверка url адреса после сканирования qr-кода, чтобы убедиться, что это предполагаемый сайт, и он выглядит подлинным; соблюдение осторожности при вводе личной, финансовой информации, данных учетных записей, при входе на интернет-ресурсы доступ к которым осуществляется при помощи qr-кодов; внимательно смотреть на средства платежа с использованием qr-кодов для доступа на сайт оплаты, если данный сайт вызывает сомнения, то лучше собственноручно ввести самому сайт в браузере для завершения транзакции; проявление внимания и осторожности при работе со срочными запросами, особенно если они сопровождаются различными угрозами; крайне нежелательно загружать приложения на свои смартфоны через qr-коды, лучше найти его и загрузить через официальный магазин приложений на смартфоне.

В заключении стоит отметить: если вы считаете, что сообщение выглядит законным, то можно проверить подлинность отправителя при помощи номера телефона или сайта, подлинность которого подтверждена для проверки информации; законные компании всегда высылают инструкции для взаимодействия с их сервисами, также они не высылают qr-коды для подтверждения учетных записей, точно также sms сообщения с неизвестных номеров или непонятных источников могут содержать поддельные qr-коды, поэтому если нет уверенности в подлинности qr-кода, лучше его не сканировать; стоит внимательно изучать адреса, с которых приходит электронная почта; не стоит забывать про регулярное обновление программного обеспечения вашего устройства, использование надежных паролей и многофакторной аутентификации в ваших учетных записях; обязательно подтверждение url сайта, связанного с qr-кодом; стараться не пересылать личную информацию, не совершать платежи или загрузку приложений при помощи qr-кода, если не уверены в его подлинности, так как данный способ поможет злоумышленникам получить доступ к конфиденциальной информации или к ваши финансовым активам.

Литература

1. Копнин, А. А. QR-фишинг: современные угрозы в эпоху цифровизации / А. А. Копнин // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы XII Междунар. науч.-практ. конф. / Урал. гос. экон. ун-т. – Екатеринбург: УрГЭУ, 2025. – С. 18–21.

2. Кибербезопасность. Quishing – отличие от smishing и vishing / А. В. Аменицкий [и др.] // Наука, общество, технологии: актуальные вопросы, достижения и инновации: сб. ст. – Пенза: Наука и просвещение, 2024. – С. 181–192.

3. Кадыров, Р. Р. Защита личных данных при использовании QR-кодов / Р. Р. Кадыров // Инициативы молодых – науке и производству: сб. ст. VII Всерос. науч.-практ. конф. молодых ученых и студентов. – Пенза: Пензенский ГАУ, 2024. – С. 406–409.

УДК 615.47

ПРИМЕНЕНИЕ ДАТЧИКОВ В МЕДИЦИНСКИХ ДИАГНОСТИЧЕСКИХ СИСТЕМАХ

Кудина А. В.[1],Франко Е. П.[1], Габец В. Л.[2] , Ахмед Сохайб[1]

[1]Белорусский государственный университет информатики и радиоэлектроники
[2]Белорусский национальный технический университет
Минск, Беларусь

Аннотация. В данной работе рассматривается применение датчиков в медицинских диагностических системах, что становится ключевым аспектом современного здравоохранения. В условиях быстрого развития технологий, использование различных типов датчиков значительно улучшает процесс диагностики и