

РАЗБОР R08 · ЦИФРОВАЯ ШКОЛА

Покупка и доставка: ссылка, QR и чужая карта в телефоне



Учебная иллюстрация

Не путайте подтверждение посылки, код банковской операции и NFC-внесение денег. У каждого действия свой получатель и последствия.

- Различить легенду и подтверждаемое действие.
- Разобрать две разные практики на вымышленных примерах.
- Выбрать первые действия по уже случившемуся и заполнить рабочий лист.

Иван Юрьевич

learn.ivan-it.net

Версия 4.1 · Редакционная проверка: 2026-10-28

Можно читать без интернета, отмечать на бумаге и возвращаться к нужной ситуации.
Кликабельные ссылки и адреса ведут к материалам и официальным источникам.

Название проекта рабочее. Материал авторский, не государственная программа. Не вводите настоящие пароли и коды в учебные задания.

При риске денег - действуйте сейчас

Если деньги отправлены, наличные переданы или раскрыта карта, самостоятельно свяжитесь со своим банком сейчас. Не ждите конца документа. Далее используйте официальный порядок обращения; возврат не гарантирован.

Как складывается цепочка

1. **1. Контакт**

Посылка, заказ, оплата продавцу или возврат.

Выход: Открыть свой заказ самостоятельно.

2. **2. Доверие и давление**

Известное имя магазина, детали заказа.

Выход: Сведения о заказе не подтверждают оператора.

3. **3. Просьба**

Код, QR-подтверждение, установка или внесение наличных.

Выход: Определить точное действие и получателя.

4. **4. Действие**

Подтверждение входа, платежа или чужой карты.

Выход: Остановить дальнейшие подтверждения.

5. **5. Последствия**

Риск доступа и денежной потери.

Выход: Банк сейчас при денежных действиях; безопасное устройство.

Что подтверждено

Официальное предупреждение

МВД предупреждает о звонках от имени доставки с запросом кода авторизации под бытовым предлогом.

Публикация: 2026-02-19; событие: точная дата не указана; проверка: 2026-10-28

МВД России / МВД МЕДИА. Просьба курьера назвать код

Сообщение о расследовании

В историческом сообщении МВД продавцов переводили на фальшивую оплату и запрашивали банковские коды; вместо получения денег происходили списания.

Публикация: 2023-03-06; событие: точная дата не указана; проверка: 2026-10-28

МВД России / МВД МЕДИА. Расследование фальшивой оплаты продавцу

Сообщение о расследовании

В описанном МВД NFC-механизме программа загружала образы подконтрольных злоумышленникам карт. Внесённые в банкомат наличные поступали соучастникам.

Публикация: 2026-04-28; событие: точная дата не указана; проверка: 2026-10-28

МВД России / МВД МЕДИА. Расследование вредоносной программы и внесения денег через NFC

- Это три разных механизма, а не один подтверждённый эпизод. Источники февраля и апреля 2026 года и марта 2023 года старше 90 дней; не выдаём их за октябрьские новости.
- В NFC-материале не описано чтение карты жертвы через телефон. Не воспроизводите установку, прикладывание к банкомату и ввод присланного PIN ради практики.

Пример с объяснением

Вымышленная учебная адаптация; это не цитата и не дополнительные факты расследования.

«Заказ завис. Откройте форму возврата и подтвердите код. Если не работает, установите нашу программу: телефон с NFC нужно приложить к банкомату, а наличные внести для проверки». Это учебное объединение приманок.

1. Возврат требует кода другой операции

Название получения денег скрывает возможное подтверждение списания или входа.

Следующий шаг: Прочитать назначение уведомления, не передавая код.

2. Предлагают выйти за пределы известной площадки

Правила навязывает собеседник, а не самостоятельно открытый заказ.

Следующий шаг: Проверить заказ в официальном канале.

3. Новая программа и действия с банкоматом

Меняется платёжный инструмент и получатель наличных.

Следующий шаг: Не устанавливать и не проводить учебный тест на банкомате.

В учебном решении заказ проверяют отдельно. Никакой настоящий QR, программа, карта, PIN или банкомат в задании не используются.

Код определяется назначением, а не словом курьера

Код из уведомления о входе в Госуслуги не становится кодом посылки оттого, что собеседник знает ваш адрес. Равным образом «получение оплаты» в чате не доказывает зачисление. Проверяйте статус заказа и операции на самостоятельно открытых официальных ресурсах.

QR может содержать адрес или запускать другой процесс; само изображение не удостоверяет получателя. Важно, какое действие вы затем подтверждаете: открытие страницы, вход, разрешение или оплату. Не сканируйте настоящий код для выполнения учебной задачи.

Почему NFC-пример разобран отдельно

В опубликованном МВД механизме на телефон передавался образ чужой подконтрольной карты. При последующем внесении наличных через банкомат средства получал другой участник. Это отличается от утверждения, будто телефон просто считывает вашу карту; такую подмену объяснения нельзя делать в памятке.

Не исследуйте вредоносную программу самостоятельным запуском. Если установка или удалённый доступ уже произошли, прекратите их влияние и обращайтесь с безопасного устройства. Если деньги внесены или переведены, сразу сообщите своему банку и полиции фактическую последовательность. Удаление программы само по себе не гарантирует возврат средств.

Что уже произошло?

Только получил сообщение

1. Остановитесь: не отвечайте кодом, не звоните по навязанному номеру и не выполняйте денежную операцию.
2. Проверьте саму просьбу через заранее известный контакт или самостоятельно открытый официальный ресурс. Одно получение не доказывает захват аккаунта.

Открыл ссылку, ничего не вводил

1. Закройте сомнительную страницу. Уточните, были ли скачивание, запуск, выдача прав или подтверждение входа - это разные действия.
2. Не делайте вывод о заражении только по открытому адресу. Проверьте факты и не устанавливайте предложенную страницей «очистку».

Ввёл пароль

1. На безопасном устройстве самостоятельно откройте настоящий сервис. Сохраните полезный сеанс и проверьте доступные способы возврата.
2. Используйте официальную процедуру смены раскрытого секрета и проверки сеансов, контактов и связей. Если пароль повторялся, отдельно обработайте другие затронутые аккаунты.

Сообщил или ввёл код

1. Не сообщайте новые коды. Уточните назначение операции по настоящему уведомлению, не передавая значение кода школе или помощнику.
2. При банковском коде или риске денег свяжитесь со своим банком сейчас; при входе в сервис проверьте его устройства и официальный путь возврата. Смена пароля не всегда отзывает все другие полномочия.

Подтвердил QR-вход

1. Различите получение QR, открытие адреса и отдельное подтверждение. Не все QR являются входом, но любой подтверждаемый вход или платёж требует понимания назначения.
2. Прекратите подтверждения. Если QR выдавал вход, сохраните свой доступ и проверьте список авторизаций или связанных устройств нужного сервиса.
3. Отзовите нежелательный доступ предусмотренным способом и проверьте результат. Получение картинки QR не равно подтверждённому входу, а закрытие картинки не отзывает его.

Выдал разрешение приложению

1. Определите, личному аккаунту, серверу или устройству выдано разрешение. В официальном управлении подключениями проверьте назначение и объём прав.
2. Отзовите ненужную связь предусмотренным способом и проверьте зависимые функции. Закрытие вкладки и отзыв разрешения - разные действия.

Установил программу или дал удалённый доступ

1. При установленной программе с неизвестной платёжной функцией не проводите пробные операции и не прикладывайте телефон к банкомату по инструкции из чата.
2. Прекратите общение. При текущем удалённом управлении прекратите сетевой доступ подозрительного устройства; важные обращения и входы выполняйте с другого безопасного устройства.
3. При риске денег самостоятельно свяжитесь с банком. Сохраните названия и время действий без новых запусков; используйте официальную помощь по устройству. Удаление одного файла не доказывает устранение всех последствий.

Перевёл деньги, передал наличные или раскрыл карту

1. Если наличные внесены через NFC, сообщите банку именно это действие и известные обстоятельства; не описывайте случай как чтение вашей карты, если такого факта нет.
2. Сразу самостоятельно свяжитесь со своим банком по номеру с карты, официального сайта или из ранее установленного приложения. Сообщите о мошенничестве и выполните официальный порядок ограничения риска и обращения об операции. Не ждите конца урока.
3. Остановите новые переводы и обратитесь в полицию по официальному каналу. Сохраните сведения об операции и переписку для обращения, не публикуя секреты. Возврат денег не гарантирован; не платите посреднику за «разблокировку возврата».

Если это случилось с ребёнком

- Не используйте карту семьи, настоящий QR или банкомат для проверки посылки. Покажи просьбу безопасному взрослому.
- Если уже нажал или установил, расскажи последовательность без паролей. Помощь не требует продолжать тест.

Практика 1

Вымышленный новый пример для распознавания.

Найдите подмену: Покупка и доставка: ссылка, QR и чужая карта в телефоне

Сначала ответьте самостоятельно. Объяснения всех вариантов находятся в конце методички; к ним можно перейти по ссылке у вопроса.

1. В новом примере «курьер» знает адрес и просит код государственного входа. Что важнее?

Выберите один вариант.

- 1) Обещание курьера удалить код
- 2) Назначение кода, а не знание адреса
- 3) То, что имя магазина написано правильно

[Проверить ответ и объяснение](#)

2. Телефон загрузил чужой образ карты, затем через NFC внесли наличные. Как описать механизм?

Выберите один вариант.

- 1) Внесение по подконтрольному другому инструменту
- 2) Обычное чтение своей карты телефоном
- 3) Безопасный возврат наличных себе по умолчанию

[Проверить ответ и объяснение](#)

Практика 2

Вымышленный человек установил предложенную программу, но ещё не ходил к банкомату и не вносил наличные.

Выберите действия: Покупка и доставка: ссылка, QR и чужая карта в телефоне

Сначала ответьте самостоятельно. Объяснения всех вариантов находятся в конце методички; к ним можно перейти по ссылке у вопроса.

1. Нужен ли пробный визит к банкомату?

Выберите один вариант.

- 1) Да, если взять только немного наличных
- 2) Нет, не проводить навязанную операцию
- 3) Да, чтобы узнать владельца карты

[Проверить ответ и объяснение](#)

2. Где выполнять важные обращения после неизвестной установки?

Выберите один вариант.

- 1) С безопасного устройства
- 2) В установленной программе по её подсказкам
- 3) Через удалённое окно того же консультанта

[Проверить ответ и объяснение](#)

3. Что сообщить при риске денег?

Выберите один вариант.

- 1) Публичному чату все PIN и реквизиты
- 2) Курьеру новый код отмены
- 3) Банку фактические действия и время

[Проверить ответ и объяснение](#)

Что делает подтверждение?

Только бумажная схема. QR, банковские карты, программы и реальные реквизиты не нужны.

Как объяснили задачу?

Доставка, возврат, оплата продавцу.

Что на самом деле запрашивают?

Открытие, вход, код, разрешение, установка, деньги.

Кто контролирует получателя?

Площадка, банк или неизвестный собеседник.

Что уже было сделано?

Не смешивайте получение файла с установкой.

Безопасное продолжение

Остановить операцию, при риске денег обратиться в банк.

Проверьте решение

- Назначение кода отделено от легенды.
- NFC-механизм объяснён без выдуманного чтения карты жертвы.
- Нет реальной тестовой установки или операции.

Самопроверка

Восемь вопросов

Сначала ответьте самостоятельно. Объяснения всех вариантов находятся в конце методички; к ним можно перейти по ссылке у вопроса.

1. R08: курьер знает номер заказа. Можно назвать код входа в другой сервис?

Выберите один вариант.

- 1) Нет, назначение кода не изменилось
- 2) Да, адрес уже подтверждён
- 3) Да, если доставка действительно ожидается

[Проверить ответ и объяснение](#)

2. R08: что различать при QR из сообщения?

Выберите один вариант.

- 1) Только цвет квадратов
- 2) Только знакомый логотип рядом
- 3) Картинку и затем подтверждаемое действие

[Проверить ответ и объяснение](#)

3. R08: продавцу обещают оплату через форму с банковским кодом. Что проверить?

Выберите один вариант.

- 1) Только размер продаваемого товара
- 2) Реальное назначение операции независимо
- 3) Только подпись «безопасная сделка»

[Проверить ответ и объяснение](#)

4. R08: чей образ карты описан в источнике о NFC?

Выберите один вариант.

- 1) Подконтрольный злоумышленникам
- 2) Обязательно собственной карты жертвы
- 3) Любой карты, считанной автоматически

[Проверить ответ и объяснение](#)

5. R08: программа установлена, наличные ещё не внесены. Что выбрать?

Выберите один вариант.

- 1) Проверить на малой сумме
- 2) Попросить друга повторить на его телефоне
- 3) Не проводить предложенный тест

[Проверить ответ и объяснение](#)

6. R08: неизвестная программа удалённо управляет устройством. Где менять важные доступы?

Выберите один вариант.

- 1) На публичном экране в чате
- 2) На другом безопасном устройстве
- 3) В той же программе под его диктовку

[Проверить ответ и объяснение](#)

7. R08: деньги уже внесены через навязанный NFC-сценарий. Что первично?

Выберите один вариант.

- 1) Обратиться в свой банк и полицию
- 2) Удалить картинку и ждать возврата
- 3) Оплатить повторную синхронизацию

[Проверить ответ и объяснение](#)

8. R08: пример продавца опубликован в марте 2023 года. Как его показать?

Выберите один вариант.

- 1) Как происшествие текущей недели
- 2) Удалить дату и назвать свежим
- 3) Как исторический подтверждённый механизм

[Проверить ответ и объяснение](#)

Ответы и объяснения

Найдите подмену: Покупка и доставка: ссылка, QR и чужая карта в телефоне

1. В новом примере «курьер» знает адрес и просит код государственного входа. Что важнее?

Верные варианты: 2.

- 1) Обещание не меняет полномочия кода.
- 2) Данные доставки не дают права подтверждать вход в другой сервис.
- 3) Название можно использовать без полномочий.

2. Телефон загрузил чужой образ карты, затем через NFC внесли наличные. Как описать механизм?

Верные варианты: 1.

- 1) Это соответствует описанному источником различию получателя.
- 2) В источнике говорится о загруженных чужих образах.
- 3) Получатель требует проверки, а не предположения.

Выберите действия: Покупка и доставка: ссылка, QR и чужая карта в телефоне

1. Нужен ли пробный визит к банкомату?

Верные варианты: 2.

- 1) Малая сумма не устраняет риск.
- 2) Учебный разбор не требует реальной финансовой проверки.
- 3) Операция может уже передать деньги.

2. Где выполнять важные обращения после неизвестной установки?

Верные варианты: 1.

- 1) Не следует отдавать дальнейшие действия под контроль программы.
- 2) Программа не является независимым каналом помощи.
- 3) Консультант остаётся в прежней цепочке.

3. Что сообщить при риске денег?

Верные варианты: 3.

- 1) Публикация секретов создаёт новые риски.
- 2) Новый код может подтвердить новую операцию.
- 3) Банк задаёт официальный порядок ограничения риска.

Самопроверка

1. R08: курьер знает номер заказа. Можно назвать код входа в другой сервис?

Верные варианты: 1.

- 1) Детали заказа не дают полномочий на вход.
- 2) Адрес не удостоверяет запрос секрета.
- 3) Ожидание не обосновывает чужой вход.

Ключевой навык: прежде чем продолжать, разберите, почему это решение сохраняет контроль.

2. R08: что различать при QR из сообщения?

Верные варианты: 3.

- 1) Цвет не определяет получателя.
- 2) Логотип не удостоверяет операцию.
- 3) QR может вести к разным процессам.

3. R08: продавцу обещают оплату через форму с банковским кодом. Что проверить?

Верные варианты: 2.

- 1) Размер товара не меняет код.
- 2) Обещание получения не исключает списания.
- 3) Подпись на чужой форме не удостоверяет сервис.

4. R08: чей образ карты описан в источнике о NFC?

Верные варианты: 1.

- 1) На телефон загружали чужой платёжный инструмент.
- 2) Это подменяет механизм источника.
- 3) Такой общий механизм не описан.

5. R08: программа установлена, наличные ещё не внесены. Что выбрать?

Верные варианты: 3.

- 1) Тест уже может передать деньги.
- 2) Это переносит риск на другого человека.
- 3) Можно остановиться до денежного действия.

Ключевой навык: прежде чем продолжать, разберите, почему это решение сохраняет контроль.

6. R08: неизвестная программа удалённо управляет устройством. Где менять важные доступы?

Верные варианты: 2.

- 1) Публикация раскрывает новые секреты.
- 2) Дальнейшие действия не должны оставаться видны оператору.
- 3) Это сохраняет чужой контроль.

7. R08: деньги уже внесены через навязанный NFC-сценарий. Что первично?

Верные варианты: 1.

- 1) Финансовое обращение не ждёт конца обучения.
- 2) Скрытие не возвращает деньги.
- 3) Новый платёж может увеличить потери.

Ключевой навык: прежде чем продолжать, разберите, почему это решение сохраняет контроль.

8. R08: пример продавца опубликован в марте 2023 года. Как его показать?

Верные варианты: 3.

- 1) Это придуманная дата события.
- 2) Отсутствие даты вводит в заблуждение.
- 3) Дата проверки не делает старый эпизод новой новостью.

Версия и связанные материалы

Редакция 4.1 опубликована 2026-10-28. Источники повторно проверены 2026-10-28. Даты источников не заменяют даты событий.

История: 4.1 - самостоятельный разбор, две практики, восемь вопросов, рабочий лист и ветки после ошибки.

Разбор на сайте

- Проверьте сообщение о Госуслугах без спешки - <https://learn.ivan-it.net/courses/gosuslugi/lessons/recognize>
- Ссылка, QR-вход и вложение - разные действия - <https://learn.ivan-it.net/courses/telegram/lessons/links-qr-files>
- WhatsApp: просьба о коде, чужая привязка и знакомое имя - <https://learn.ivan-it.net/courses/whatsapp/lessons/recognize>

ИСТОЧНИКИ И РЕДАКЦИОННЫЕ ОГРАНИЧЕНИЯ

Проверяйте по первоисточнику

Каналы, возможности и названия разделов могут изменяться. Материалы помогают выбрать действие, но не гарантируют восстановление аккаунта, возврат денег или отсутствие риска. При денежном происшествии обращайтесь в банк сразу.

1. МВД России / МВД МЕДИА. Просьба курьера назвать код

<https://mvdmedia.ru/news/ofitsialnyy-predstavitel/mvd-rossii-preduprezhdaet-v-predprazdnichnye-dni-moshenniki-predstavlyayutsya-sotrudnikami-sluzhby-d/>

Содержание проверено · 2026-10-28 · Публикация: 2026-02-19

Описаны звонки от имени доставки с запросом кода авторизации под предлогом посылки, ошибки заказа или подтверждения.

Ограничения: Базовый материал февраля, не свежая новость. Учебная проверка различает назначение конкретного кода и не требует сообщать его школе.

2. МВД России / МВД МЕДИА. Расследование фальшивой оплаты продавцу

<https://mvdmedia.ru/news/ofitsialnyy-predstavitel/irina-volk-v-sankt-peterburge-politseyskie-presekli-seriyu-khishcheniy-s-bankovskikh-schetov-prodavts/>

Содержание проверено · 2026-10-28 · Публикация: 2023-03-06

По сообщению полиции, продавцов переводили с площадки в мессенджер и на фальшивый платёжный сайт; запрошенные банковские коды приводили к списаниям вместо оплаты.

Ограничения: Исторический пример 2023 года, не новость 2026 года. Статус расследования относится к публикации; дальнейший результат дела не проверялся.

3. МВД России / МВД МЕДИА. Расследование вредоносной программы и внесения денег через NFC

<https://mvdmedia.ru/news/ofitsialnyy-predstavitel/irina-volk-v-sledstvennom-departamente-mvd-rossii-rassleduetsya-ugolovnoe-delo-o-khishcheniyakh-dene/>

Содержание проверено · 2026-10-28 · Публикация: 2026-04-28

По предварительным данным МВД, программа передавала на телефон образы подконтрольных злоумышленникам карт. Внесённые через NFC-банкомат деньги попадали соучастникам.

Ограничения: Старый материал о продолжающемся расследовании. Это не описание чтения карты жертвы: в описанном механизме загружается чужой образ карты. Точные даты эпизодов не приведены.

4. Банк России. Что делать при раскрытии карты и спорной операции

https://www.cbr.ru/faq/information_security/

Содержание проверено · 2026-10-28

В FAQ описаны самостоятельное обращение в банк, блокировка скомпрометированной карты и оформление обращения об операции.

Ограничения: Даты у ответов разные; не присваиваем всему FAQ дату одного ответа. Конкретные сроки, основания возмещения и результат зависят от случая. Здесь даётся порядок первого обращения без обещания возврата.