

АЛЕКСЕЙ ДОВГУН

ЦИФРОВОЙ РОБИНЗОН

КАК ЗАЩИТИТЬ
СЕБЯ И СВОИ ДАННЫЕ
ПРИ ОБРУШЕНИИ
ИНФРАСТРУКТУРЫ



СВЯЗЬ



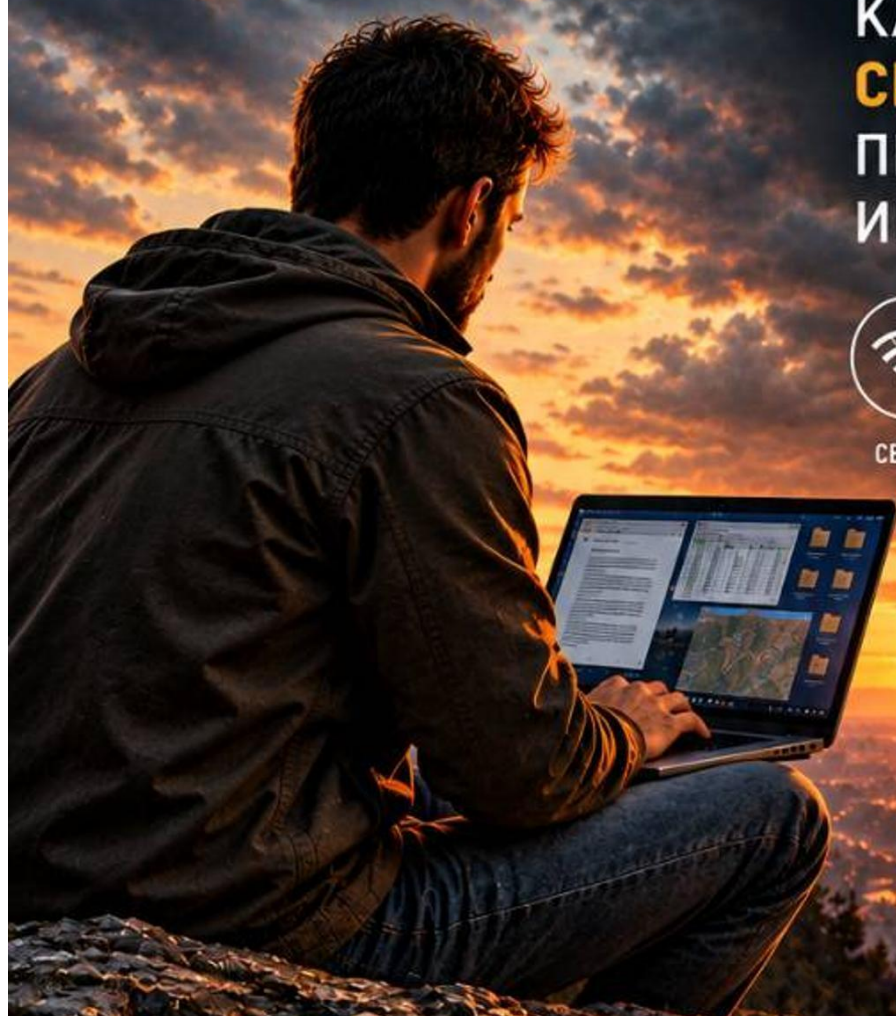
ФИНАНСЫ



ДОКУМЕНТЫ



БЛИЗКИЕ



Алексей Довгун

Цифровой робинзон

«Автор»

2026

Довгун А.

Цифровой робинзон / А. Довгун — «Автор», 2026

Мы привыкли полагаться на смартфоны, банковские приложения, облачные хранилища и государственные онлайн-сервисы. Но что произойдёт, если привычная цифровая инфраструктура внезапно перестанет работать? Эта книга объясняет, как подготовиться к масштабным сбоям, сохранить важные документы и данные, обеспечить резервный доступ к деньгам и информации, поддерживать связь с близкими и распознавать мошенничество в условиях кризиса. На основе реальных происшествий и практических рекомендаций она поможет выявить уязвимые места в повседневной жизни и создать собственный план цифровой автономности. Цель не в том, чтобы отказаться от технологий, а в том, чтобы не зависеть от единственной точки отказа.

© Довгун А., 2026

© Автор, 2026

Содержание

Введение	5
Глава 1. Мир, который перестал отвечать	7
Глава 2. Невидимые зависимости	10
Глава 3. Когда отказ становится системным	13
Конец ознакомительного фрагмента.	14

Алексей Довгун

Цифровой робинзон

Введение

Эта книга посвящена личной цифровой устойчивости: способности сохранить доступ к необходимой информации, деньгам, документам и связи, когда отдельные цифровые сервисы или поддерживающая их инфраструктура перестают работать. Она не обещает полной независимости от внешних систем. Ни один набор устройств, файлов и инструкций не может гарантировать работу банков, мобильных сетей, электроснабжения или государственных сервисов при любом развитии событий.

Рекомендации общего характера следует соотносить с конкретной ситуацией. При непосредственной угрозе жизни, эвакуации, пожаре, аварии или иной чрезвычайной ситуации приоритет имеют указания экстренных служб и компетентных органов. Процедуры банков, операторов связи и государственных платформ меняются; перед применением проверяйте их актуальные официальные инструкции. Не сообщайте третьим лицам пароли, одноразовые коды и данные, позволяющие распоряжаться вашими деньгами.

В тексте различаются факты, прямо подтверждённые источниками, сообщения конкретных организаций и аналитические выводы автора. Корпоративное заявление об инциденте не равнозначно независимому расследованию. Там, где причины или масштабы последствий не установлены, это обозначено отдельно.

Человек, который зависит от сети

В обычный день цифровая инфраструктура почти незаметна. Телефон подтверждает личность, банковское приложение показывает остаток на счёте, карта прокладывает маршрут, почта хранит билеты, облачный сервис синхронизирует фотографии, а рабочие документы открываются на ноутбуке из любой точки. Пользователь видит интерфейсы, кнопки и уведомления. За ними находятся сети связи, центры обработки данных, системы электроснабжения, программные компоненты, базы данных, договоры между организациями и процедуры подтверждения доступа.

Большую часть времени эта сложность работает в нашу пользу. Она снижает издержки, ускоряет расчёты, позволяет хранить документы без папок и поддерживать отношения на расстоянии. Проблема возникает не из-за самой цифровизации, а из-за незаметности зависимости. Мы начинаем считать доступность сервиса постоянным свойством мира, хотя на деле это результат работы множества систем, каждая из которых может отказать отдельно или вместе с другими.

Потеря доступа не всегда означает потерю данных. Если приложение банка не открывается, деньги на счёте могут оставаться на месте. Если исчезла мобильная связь, телефон может продолжать показывать сохранённые документы. Если не работает облачный сервис, локальная копия файла может быть доступна. Но обратное также верно: привычный значок приложения на экране не гарантирует, что данные хранятся на устройстве, а резервная копия не гарантирует, что пользователь сможет её расшифровать или восстановить.

Именно это различие составляет предмет книги. Цифровая устойчивость — не умение обходиться без технологий вообще. Это способность не зависеть критически от одного устройства, одного канала связи, одного пароля, одного сервиса или одного способа подтверждения

личности. Устойчивость начинается там, где у критически важной функции есть проверенная альтернатива.

Представим человека, которому нужно купить лекарства, связаться с родственником и подтвердить бронь. Если смартфон разрядился, у него может быть записан номер родственника на бумаге, немного наличных и адрес аптеки. Если пропал мобильный интернет, на телефоне могут остаться офлайн-карта и сохранённый документ. Если заблокирован основной аккаунт, резервный адрес электронной почты и актуальные способы восстановления позволят начать процедуру без паники. Ни один из этих резервов не универсален, но каждый снимает одну точку отказа.

Книга рассматривает четыре уровня подготовки.

Первый — понимание системы. Нужно отличать локальную проблему от массового сбоя, отказ приложения от потери связи, а техническую ошибку — от атаки. Без этого человек тратит силы на неподходящие действия: многократно переустанавливает приложение, хотя не работает сеть, или вводит пароль на поддельном сайте, потому что ищет «альтернативный вход».

Второй — сохранение важного. Речь идёт не о том, чтобы копировать всё подряд. Нужно определить, какие сведения действительно необходимы в первые часы и дни: контакты, документы, адреса, данные о лекарствах, подтверждения поездок, рабочие материалы, сведения о счетах и контакты организаций. Для каждого набора следует выбрать способ хранения, учитывающий конфиденциальность и доступность.

Третий — альтернативы. Важные действия должны по возможности иметь несколько независимых путей. Это может быть не второй смартфон, а бумажный список телефонов; не ещё один облачный сервис, а зашифрованная копия на отключаемом носителе; не запасная банковская карта того же банка, а небольшая сумма наличных. Разные варианты решают разные задачи. Два приложения, зависящие от одного дата-центра или одного номера телефона, могут оказаться не двумя независимыми каналами, а двумя окнами в одну и ту же систему.

Четвёртый — проверка. Подготовка, которую никогда не испытывали, часто существует только на бумаге. Резервный адрес может оказаться недоступным; зарядное устройство — несовместимым; пароль — забытым; копия — повреждённой; офлайн-карта — не покрывать нужный район. Поэтому готовность требует не только создания запасов, но и периодического тестирования.

В книге используются реальные инциденты, чтобы объяснить механизмы отказов. Они не служат доказательством того, что аналогичный сценарий обязательно повторится в каждом городе или у каждого пользователя. Например, сбой программного обновления и физическое повреждение дата-центра имеют разные причины и требуют разных мер устойчивости. Общим может быть лишь то, что зависимые сервисы одновременно становятся недоступны и пользователю приходится действовать при неполной информации.

Географический фокус книги — Россия. Поэтому практические разделы учитывают российские банковские и государственные сервисы, но не пытаются заменить инструкции конкретного банка, оператора или ведомства. Данные и правила могут меняться быстрее, чем выходит печатное издание. Для этого в конце приведены источники, а в ключевых местах обозначено, что именно необходимо перепроверять перед применением.

Главная мысль проста: личная цифровая автономность — это не отказ от удобств, не покупка дорогого оборудования и не подготовка к фантастическому концу света. Это разумное управление зависимостями. Необходимо знать, что нельзя потерять, понимать, от чего зависит доступ к этому, иметь подходящий резерв и однажды убедиться, что он работает.

Глава 1. Мир, который перестал отвечать

Один симптом — разные причины

Сообщение «не удалось подключиться» мало говорит о том, что именно произошло. Проблема может находиться в самом телефоне, домашнем роутере, сети оператора, DNS-сервисе, приложении, сервере поставщика или системе авторизации. Пользователь видит одинаковый результат — экран не обновляется, — но правильные действия зависят от причины.

Для практики полезно разделять четыре уровня отказа.

Локальный отказ затрагивает конкретное устройство или программу. Телефон перегрелся, приложение зависло, закончилась память, отключён режим передачи данных, повреждён файл. Другие устройства и сервисы могут работать нормально. Начинать стоит с простых проверок, не уничтожающих данные: заряд, режим полёта, подключение к сети, перезапуск приложения, свободное место и сообщения об ошибках. Сбрасывать устройство к заводским настройкам без резервной копии — плохой первый шаг: он может удалить данные, не решив внешнюю проблему.

Отказ канала связи означает, что устройство не может получить доступ к сети обычным способом. Это может быть неисправность домашнего маршрутизатора, проблема у оператора, отсутствие покрытия, ограничение конкретного типа трафика или повреждение линии. При этом локальные файлы, камера, заметки и некоторые приложения могут продолжать работать. Отсутствие интернета не равно полной потере функциональности телефона.

Отказ отдельного сервиса возникает, когда сеть в целом доступна, но определённый сайт или приложение не отвечает. Причиной могут быть сбой сервера, ошибка обновления, проблема базы данных, перегрузка, истечение сертификата, неисправность системы авторизации или зависимость от внешнего поставщика. Если десятки сайтов открываются, а один нет, это полезный диагностический признак, но не окончательное доказательство: часть сервисов использует общую инфраструктуру и может отказывать одновременно.

Инфраструктурный кризис затрагивает несколько зависимых систем: например, электроснабжение и мобильную связь, несколько дата-центров или региональные каналы связи. Здесь привычный сценарий «перезагрузить и попробовать снова» перестаёт быть достаточным. Нужно оценивать масштаб, сохранять энергию, искать независимую информацию и переходить к заранее подготовленным альтернативам.

Между этими уровнями нет жёстких границ. Локальный сбой может быть следствием общей проблемы, а крупный инцидент может проявляться у пользователей не одновременно. Поэтому первый принцип — не путать симптом с диагнозом.

Диагностика без лишнего риска

В первые минуты полезно задать несколько вопросов:

1. Не работает только одно приложение или сразу несколько независимых сервисов?
2. Работает ли обычная телефонная связь или SMS, если они доступны в данном месте?
3. Есть ли доступ к интернету через другой канал, например домашнюю сеть вместо мобильной, — если это безопасно и реально?
4. Сообщают ли об инциденте официальный сайт организации, оператор или надёжные средства массовой информации?
5. Не появилось ли необычное требование срочно ввести пароль, установить «исправление» или назвать код подтверждения?

Проверка должна быть ограниченной. Не нужно многократно менять настройки, переустанавливать приложения и сбрасывать пароль в каждой системе подряд. Каждое лишнее действие способно ухудшить ситуацию: пользователь может заблокировать аккаунт попытками входа, потерять локальные данные или попасть на поддельный ресурс.

Официальные статусы сервисов полезны, но не всегда доступны именно тогда, когда нужны. Кроме того, сообщение «проблема устранена» может означать, что восстановлен сервер, а не все пользовательские данные или функции. Поэтому важно различать три состояния: поставщик сообщил о восстановлении; конкретная функция снова доступна; пользователь проверил, что его данные и операции в порядке.

Не всякий отказ — кибератака

Слово «хакеры» часто становится универсальным объяснением любого цифрового сбоя. Это удобно для короткого заголовка, но плохо помогает действовать. Причиной может быть ошибка программного обеспечения, неудачное обновление, поломка оборудования, потеря электропитания, ошибка маршрутизации, человеческий просчёт, атака или сочетание факторов.

Различать причины важно не только ради точности. При подозрении на компрометацию аккаунта необходимо защищать учётные данные, проверять операции и обращаться в организацию по официальному каналу. При массовой технической аварии смена пароля обычно не восстановит доступ, а многократные попытки могут только усложнить его. Если причина неизвестна, безопасная тактика — не совершать необратимых действий и следить за подтверждённой информацией.

Не следует и обратная ошибка: считать отсутствие признаков атаки доказательством полной безопасности. Массовый сбой может использоваться мошенниками как повод для фишинга. На фоне новостей об отключениях появляются поддельные страницы «проверки аккаунта», сообщения якобы от поддержки и предложения скачать утилиту восстановления. Техническая авария и мошенничество могут существовать одновременно, хотя первое не обязательно вызвано вторым.

Когда ждать, а когда действовать

Если сервис не работает, а критической задачи прямо сейчас нет, часто разумно подождать официального сообщения и не менять ничего в аккаунте. Если же от доступа зависят лекарства, поездка, безопасность ребёнка или срочная финансовая операция, следует переключаться на заранее предусмотренный резервный путь: телефон организации, бумажные данные, наличные, физический офис или помощь близкого — в зависимости от ситуации.

Подготовка нужна именно для того, чтобы не принимать все решения в момент сбоя. Если человек заранее записал адрес ближайшего отделения банка и номер контактного центра с официального сайта, он меньше зависит от поиска в сети. Если он знает, какие документы хранятся локально, не тратит время на бесполезные попытки войти в облако.

Полезно запомнить простую последовательность: определить масштаб — сохранить работоспособность устройства — проверить надёжный источник информации — выбрать альтернативу — перепроверить результат. Это не универсальный алгоритм для любой аварии, но хорошая отправная точка для цифрового отказа, когда непосредственной физической опасности нет.

Если одновременно происходят пожар, эвакуация, отключение жизненно важного оборудования или иная угроза людям, цифровая диагностика отходит на второй план. Приоритетом становится безопасность, выполнение указаний экстренных служб и перемещение в безопасное место. Данные можно пытаться восстановить позже; человеческая жизнь не должна зависеть от сохранения телефона или ноутбука.

Вывод главы

Одинаковый экран ошибки может скрывать разные причины. Пользователь не обязан самостоятельно устанавливать техническую первопричину, но должен уметь отличить вероятный локальный сбой от более широкой проблемы, не предпринимать разрушительных дей-

ствий и знать, когда переходить к резервному плану. Устойчивость начинается с диагностики без паники и без самоуверенных догадок.

Глава 2. Невидимые зависимости

Сервис — это не значок на экране

Цифровой сервис воспринимается как единый объект: «банк», «почта», «карта», «государственный портал». На деле это цепочка компонентов. Пользовательское приложение должно запуститься, установить соединение, найти нужный сервер, пройти аутентификацию, получить данные, обработать запрос и показать результат. Для платежа могут дополнительно понадобиться банк, платёжная система, процессинг, связь с торговой точкой и подтверждение операции. Отказ любого критического элемента способен прервать действие.

Цепочка не всегда линейна. Крупные поставщики используют резервные серверы, распределённые сети и несколько площадок. Это повышает устойчивость, но не устраняет все общие зависимости. Разные сервисы могут пользоваться одной облачной платформой, системой авторизации, оператором связи, библиотекой программного обеспечения или поставщиком обновлений. Если общий компонент отказывает, последствия распространяются за пределы одной компании.

В инженерии это называют общей точкой отказа. Она не обязательно выглядит как один физический сервер. Общей точкой может быть учётная запись администратора, ключ шифрования, единственный номер телефона для восстановления, одна SIM-карта, один почтовый ящик или единая система идентификации. Человек может иметь десять приложений, но если все они восстанавливаются через один недоступный адрес электронной почты, его фактический резерв невелик.

Электричество и связь

Электроснабжение поддерживает не только домашний роутер и зарядку телефона. Оно необходимо базовым станциям, сетевому оборудованию, центрам обработки данных, офисам и кассовым терминалам. На критических объектах могут быть аккумуляторы и резервные генераторы, но их автономность конечна, а работоспособность зависит от обслуживания, топлива, охлаждения и доступности персонала.

Мобильная сеть состоит из множества элементов: радиодоступа, транспортных каналов, ядра сети, систем управления и соединений с другими сетями. Телефон может показывать уровень сигнала, но это не гарантирует доступность интернета или конкретного сервиса. И наоборот, мобильная передача данных может быть ограничена, а обычные голосовые вызовы или SMS — работать, если архитектура сети и текущие ограничения это допускают. Нельзя предполагать, что любой канал сохранится или исчезнет во всех обстоятельствах одинаково.

Домашний Wi-Fi также не является интернетом. Роутер может продолжать создавать беспроводную сеть, но если его внешний канал отключён, доступ к сайтам исчезнет. Локальные устройства при определённой конфигурации всё ещё смогут обмениваться данными, однако большинство пользователей не настроили такую автономную сеть и не должны рассчитывать на неё без предварительной проверки.

Данные и вычисления

Дата-центр — это не просто помещение с компьютерами. Он объединяет серверы, хранилища, сетевые соединения, электропитание, охлаждение, пожарную защиту, физическую охрану и процессы эксплуатации. Географически разнесённые площадки могут обеспечивать резервирование, но только если данные и функции действительно реплицируются, приложения умеют переключаться, а резерв не зависит от того же повреждённого компонента.

Копия данных не равна работающему сервису. Чтобы восстановить сервис, нужны вычислительные ресурсы, конфигурации, ключи, доступы, совместимые версии программ и персонал, который умеет провести восстановление. Иногда данные сохранены, но приложение вре-

менно недоступно. Иногда сервер работает, но часть данных повреждена. Иногда пользователь видит сайт, однако его учётная запись заблокирована отдельной системой безопасности.

Это различие важно для личной подготовки. Пользователь не может обеспечить резервирование чужого дата-центра, но может снизить последствия его отказа. Если расписание, адрес и билет доступны только через один онлайн-аккаунт, отказ сервиса создаёт непосредственную проблему. Если важные сведения сохранены локально и в разумной бумажной форме, внешняя авария не лишает человека всей информации.

Идентификация как скрытая зависимость

Многие системы требуют не только интернет, но и подтверждение личности. Код приходит по SMS, push-уведомлению, электронной почте или генерируется приложением-аутентификатором. Каждый способ имеет свои ограничения.

SMS зависит от доступности телефонного номера и сети, а также от защиты SIM-карты. Push-подтверждение может зависеть от интернета, работы приложения и сервера поставщика. Почта требует доступа к отдельному аккаунту, который сам может быть защищён тем же номером телефона. Приложение-аутентификатор может работать без сети, но пользователь должен заранее перенести его на новое устройство или сохранить предусмотренный способ восстановления. Аппаратный ключ не зависит от SMS, но его можно потерять или оставить дома.

Ни один фактор не идеален. Практическая задача — не собрать максимально возможное количество факторов, а настроить безопасные и доступные варианты восстановления. Резервный способ должен быть независимым настолько, насколько это реально, и защищённым от злоумышленника. Записать пароль на листе, который лежит рядом с телефоном, — не то же самое, что хранить его в защищённом месте отдельно от устройства.

Платежи и иллюзия единого кошелька

Оплата картой кажется простой: приложить пластик или телефон к терминалу. Но успешная операция зависит от нескольких участников. Для бесконтактной оплаты телефоном может понадобиться заряженное устройство и доступная функция кошелька; для обычной карты — рабочий терминал, связь торговой точки и инфраструктура банка или платёжной системы. Некоторые операции могут обрабатываться по специальным режимам, но их доступность зависит от оборудования и правил конкретной системы. Нельзя строить план на предположении, что «карта всегда работает офлайн».

Наличные не требуют связи для самой передачи денег, но не решают все задачи. Они могут быть потеряны или украдены, не подходят для всех покупок и не гарантируют наличие товаров. Снятие наличных, в свою очередь, может зависеть от банкомата, электричества, его подключения, запасов купюр и доступности банковской инфраструктуры. Резерв лучше строить из нескольких инструментов, а не противопоставлять один идеальный способ всем остальным.

Банк России сообщал о мерах адаптации части банкоматов к отключениям мобильного интернета, включая использование проводного подключения или Wi-Fi, и о развитии сервиса выдачи наличных на кассах. Это показывает, что отказ мобильной передачи данных не тождественен полному отказу платежей. Но подобные меры не гарантируют работу каждого банкомата или кассы при любом сценарии: остаются зависимость от электричества, связи, оборудования и конкретной организации.

Как составить карту зависимостей

Выберите пять функций, потеря которых создаст наибольшую проблему: доступ к деньгам, связь с близкими, документы, работа, медицинская информация. Для каждой функции запишите:

- основной способ доступа;
- что должно работать, чтобы он сработал;
- что будет, если основной способ недоступен;

- есть ли независимая альтернатива;
- когда вы последний раз проверяли её.

Пример: «Связаться с матерью — смартфон и мессенджер». Зависимости: заряд, устройство, интернет, аккаунт и приложение у обоих участников. Альтернативы: обычный звонок, SMS, записанный номер, договорённость о месте встречи. Если все альтернативы существуют только в том же телефоне, независимость условная.

Карта не обязана описывать всю цифровую жизнь. Её задача — выявить критические цепочки. Слишком подробная карта быстро устареет; слишком общая не поможет. Начните с того, что действительно необходимо в первые сутки после сбоя.

Вывод главы

Устойчивость зависит не от числа приложений, а от независимости путей доступа. Нужно искать общие точки отказа: один телефон, один номер, один аккаунт, одна облачная копия, один способ оплаты. Подготовка эффективна, когда резерв работает через иной путь и проверен заранее.

Глава 3. Когда отказ становится системным

Ошибка, которая прошла через множество компьютеров

19 июля 2024 года многие организации по всему миру столкнулись с серьёзным сбоем компьютеров под Windows. Компания CrowdStrike сообщила, что причиной стало обновление конфигурационного содержимого для сенсора Falcon, используемого в системах киберзащиты. Это не было объявлено кибератакой: проблема возникла из-за дефекта обновления. Компания опубликовала предварительный разбор 24 июля и более подробный анализ первопричины 6 августа 2024 года.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.