В 2020 году Павел Жовнер с командой удивили интернет своим проектом Flipper Zero — карманного мультитула для хакеров. Тогда, вместо запрошенных $60 тысяч на разработку, ребята собрали почти $5 млн, после чего решили делать всё по-взрослому — с компанией в Делавере и массовым производством в Китае. Павел рассказывал, что идея Флиппера родилась когда он игрался с системами контроля доступа — чтением карточек «Тройка», ключей от домофонов, копировании RFID, и прочего. Они у себя в хакспейсе «Нейрон» (ныне закрытом) собрали свою собственную систему, которая пускала людей внутрь хоть по «Тройке» хоть по Apple Pay. В комплекте есть: ИК-порт, чтобы выключать телевизоры в Макдональдсе. USB-C для зарядки и обновлений, а так же запуска Bad USB -скриптов. Читалка и писалка ключей от домофонов, довольно прикольно задизайненая. Набор GPIO пинов для программирования и подключения сторонних плат расширения. NFC/RFID, чтобы читать всякие карточки. Радио-антенна, чтобы читать и посылать радиосигналы, например открывать Теслам лючки зарядки (будет ниже). Блютус, но я пока не нашел для чего он мог бы пригодиться. Неочевидные плюшки: спикер-пищалка как на старых Nokia, под который даже можно писать мелодии, и вибромоторчик, применения которому я пока не придумал. Батарейка на 2000 mAh, которая держит неделю. Управляет всем этим добром маленький STM32-микроконтроллер, под который написана своя операционка. По сути это Arduino, оно даже совместимо с Arduino IDE. Теперь по больному: у флиппера нет WiFi. Скорее всего его просто невозможно было хорошо туда засунуть, не убив энергопотребление и не раздув размеры корпуса до неприятных. Вроде как скоро будет WiFi-модуль аддоном, вставляющийся сверху в GPIO-пины, но это, конечно, не то. Как по мне, будь у Флиппера WiFi, идею с «тамагочи» можно было бы повернуть прям на порядок круче. Например, для Pi Zero есть проект Pwnagotchi (которым явно где-то под капотом вдохновлялись), у которого одна из главных идей геймификации состоит в том, что ты должен «кормить» своего тамагочи новыми WiFi-сетями. Ходишь по городу, собираешь хендшейки, а потом дома он автоматически пытается их для тебя взломать. Такого тамагочи правда хочется носить с собой по улицам и кормить хендшейками, не только потому что он иначе грустит и жалуется, а еще и потому что бонусом он приносит тебе карту взломанных WiFi сетей с паролями. Кайф же. Думаю, команде Флиппера можно подумать об отдельной версии Flipper WiFi, из которой можно спокойно выпилить всё остальное, но усилить геймификацию с «кормёжкой» дельфина. Когда выпускаешь «хакерский» девайс на массовый рынок, естественно, встаёт вопрос регуляций, сертификации и законности использования частот в разных странах. Как можно догадаться, это полнейший цирк и зоопарк. Не знаю каким чудом ребятам удалось разобраться во всех необходимых сертификациях и получить комплаенс для импорта почти во все страны мира. Без потерь не обошлось. В разных странах Флипперу пришлось программно зарезать некоторые частоты — в США запрещены одни, в ЕС другие, в России третьи. Хорошая же новость в том, что на Github лежит целый набор «альтернативных» прошивок, где все эти ограничения удобно выпилены. Самая популярная — от RogueMaster. В этом видео будет полный обзор, практика, модификации и прошики.