

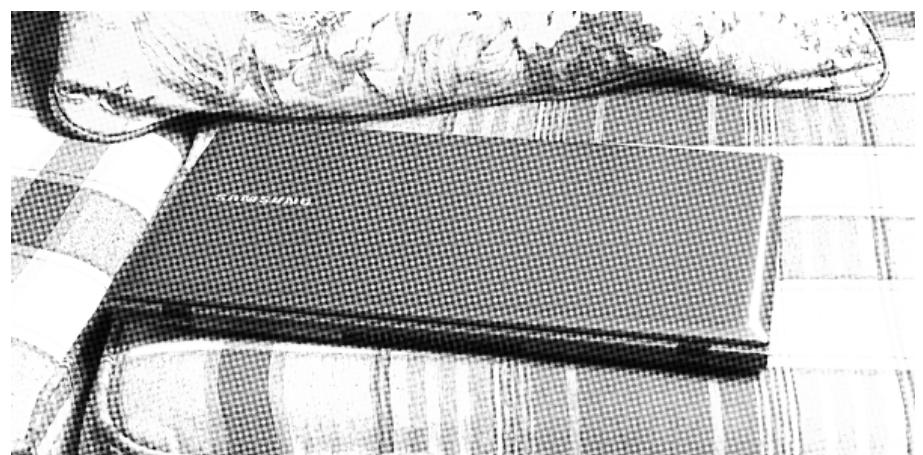
В политически нестабильных странах очень часто прессуют журналистов, правозащитников и простых активистов. Порой приходят с обысками, изымают технику – и через определённое время, как правило, возвращают. Многие из-за паранойи вынуждены впоследствии её продавать и покупать новое железо, так как не исключают вживления в устройства аппаратных бекдоров. Особенно напрягает менять устройства, когда такая практика их изъятия – систематическая. Но к сожалению, это вынужденная и правильная мера. Хочу рассказать почему.



No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.

Что делать с компьютерной техникой после обыска, изъятия и возврата



Что делать с компьютерной техникой после обыска, изъятия и возврата

Original text in Russian

2021

[cryptopunks.org/
article/actions_after_the_search_and_seizure_of_computers](https://cryptopunks.org/article/actions_after_the_search_and_seizure_of_computers)

Layout

No Trace Project

notrace.how/resources/ru/#kompiuternoi-obyska

В политически нестабильных странах очень часто прессуют журналистов, правозащитников и простых активистов. Порой приходят с обысками, изымают технику—и через определённое время, как правило, возвращают. Многие из-за паранойи вынуждены впоследствии её продавать и покупать новое железо, так как не исключают вживления в устройства аппаратных бекдоров. Особенно напрягает менять устройства, когда такая практика их изъятия—систематическая. Но к сожалению, это вынужденная и правильная мера. Хочу рассказать почему.

Аппаратные и программные бекдоры

Прошли те времена, когда спецслужбы в компьютеры внедряли аппаратные бекдоры. Раньше можно было обойтись переодлическим взвешиванием устройства до обыска/изъятия и после его возврата. Сейчас же эта схема не сработает. А всё потому что появились более изящные способы взять тебя на карандаш и следить за твоими действиями. Теперь же могут модифицировать биос на материнской плате, либо вообще прошить микрокод в винчестере, и после подключения он может, например, слить пароль от твоего LUKS-контейнера майору на почту (ну а копия твоего винта у него уже есть, не сомневайся в этом). Не исключено также, что и в

сам софт тебе что-то внедрили, и что скорее всего не сразу увидит антивирус.

Поэтому лучше всего сменить устройство на новое. И не менее важно ответственно подойти к копированию информации со старого устройства на новое!

Если же ты решил оставить устройство, то как минимум снеси всё к чертям, установив всё с нуля (но, повторюсь еще раз, это не гарантированное решение—ты просто чуть минимизируешь риски).

Как правильно копировать информацию с устройства, которое вернули

Поскольку старое устройство может быть заражено, то как только ты подключишься к интернету—твои конфиденциальные данные могут утечь в сеть. Причём может не спасти даже то, что раздел с ОС был зашифрован, потому что ПЗУ биоса или накопителя могло быть модифицировано для этой задачи. Поэтому необходим как минимум еще один компьютер. В этом компьютере ты отключаешь интернет, подключаешь запоминающее устройство, проверяешь файлы на вирусы и делаешь бекап необходимых данных, после чего отключаешь накопительное устройство—и только потом подключаешься к интернету.

В идеале вообще загрузиться с какого нибудь Tails¹ (с флешки, с загрузкой в ОЗУ без какой-либо записи на винт, без сети), подключить накопитель с которого будем копировать (!) **по USB** (т.к. через системную шину он может выполнять некоторые команды CPU в основной системе, если заражен микрокод) и скопировать с него файлы на дополнительный накопитель. После чего не забыть прогнать антивирусом все файлы (при условии что твое устройство попало не в те руки не в зашифрованном состоянии).

В безопасности можно копать до бесконечности, поэтому выбирай, какой из способов и какая степень тебе необходимы. Моя задача лишь представить и оговорить возможные варианты.

¹<https://tails.net/index.ru.html>