# Источник: Что известно про «киберпартизан Беларуси»? Поговорили со специалистами по инфобезопасности

[16 сентября 2020 в 11:25](https://42.tut.by/archive/16.09.2020.html)  
[Тамара Колос](https://news.tut.by/author/2643.html) / [42.TUT.BY  
Читать полностью:](https://42.tut.by/) <https://42.tut.by/700656>

**В начале сентября на некоторые государственные интернет-ресурсы Беларуси были предприняты атаки — в частности, на сайты МВД, Академии МВД, Белорусской торгово-промышленной палаты, «Белорусских лотерей». На них размещались послания от неких «киберпартизан Беларуси». В то же время в Telegram появился** [**одноименный канал**](http://(https:/t.me/cyberpartisan)**, где утверждалось, что если 13 сентября в Минске будут задержания, следующей целью станет сайт Министерства по налогам и сборам. Однако в понедельник, 14 сентября, ресурс все еще** [**работал**](https://finance.tut.by/news700354.html) **в штатном режиме. 42.TUT.BY поговорил с людьми, которые занимаются инфобезопасностью в Беларуси, на тему, кем могут быть эти «киберпартизаны» и способны ли они «сломать» сайт налоговой.**

**Что уже сделали «киберпартизаны»?**

Первым сигналом о деятельности «киберпартизан» стал сайт МВД — вечером 3 сентября, по сообщениям издания «[Наша Нива](http://t.me/nashaniva/13356)» и телеканала «[Белсат](http://t.me/belsat/17086" \t "_blank)», неизвестные изменили список разыскиваемых лиц, а именно разместили объявления о розыске президента Александра Лукашенко и министра внутренних дел Юрия Караева. После этого МВД приняло решение временно отключить внешнюю работу сайта, чтобы «сохранить все размещенные на нем материалы».

В пресс-службе МВД тогда [сообщили](https://42.tut.by/699360), что «была предпринята попытка внедрения вредоносных программ, блокирующих или вносящих изменения в работу ряда информационных ресурсов МВД. В настоящее время специалисты ведомства занимаются устранением выявленных проблем».

По данному факту [проводится проверка](https://42.tut.by/699287) в рамках уголовно-процессуального законодательства по ч. 1 ст. 349 «Несанкционированный доступ к компьютерной информации», которая предусматривает наказание в виде штрафа или ареста на срок до 3 месяцев. Сайт по-прежнему был недоступен утром 16 сентября.

Также вечером 5 сентября перестал открываться и официальный сайт Белорусской торгово-промышленной палаты — но до того на нем разместили сообщение от «киберпартизан Беларуси». Такое [появилось](https://42.tut.by/699914) 9 сентября и на сайте Академии МВД.

Скриншот с сайта Академии МВД

Позже, 12 сентября, на сайте «Белорусских лотерей» неизвестные разместили поздравление Светлане Тихановской с днем рождения. И в тот же день в телеграм-канале «Кибер Партизаны» [появилось](https://t.me/cyberpartisan/53) заявление, что на налоговые сервисы могут совершить кибератаки, если 13 сентября будут задержания участников акций протестов.

Однако назавтра, 14 сентября, Министерство по налогам и сборам [сообщило](https://finance.tut.by/news700354.html), что сайт ведомства и электронные сервисы работают в штатном режиме. То, что атаки действительно совершались, в ведомстве не отрицают, но акцентируют внимание на том, что сбоев в работе сервисов для пользователей нет. Также в ведомстве подчеркнули, что не видят предпосылок для сбоев в работе электронных сервисов, так как «они имеют достаточную защищенность».

И 15 сентября в телеграм-канале «партизан» [появился](https://t.me/cyberpartisan/68) опрос: «Открываются ли у вас сайты butb.by, goszakupki.by?» (это ресурс Белорусской универсальной товарной биржи и сайт госзакупок). Позже в канале «киберпартизан» добавили, что «нечего броники в мирной стране закупать», скорее всего, подразумевая запрос на сайте госзакупок от Мингорисполкома — учреждение [планирует](https://42.tut.by/700520) закупить партию бронежилетов на сумму 240 тысяч рублей.

Спустя какое-то время ресурсы вновь начали открываться. В пресс-службе Белорусской универсальной товарной биржи 42.TUT.BY пояснили, что 15 сентября шло «тестирование сайта на уязвимость», поэтому десктопная версия могла быть недоступна.

Также вечером 15-го числа «киберпартизаны» предприняли попытку атаки на сайт президента РБ, но были вынуждены [признать](https://t.me/cyberpartisan/73), что ресурс поднялся, «„крэпкi арэшак“ оказался».

Разумеется, это не первые случаи, когда на сайты белорусских госпредприятий предпринимались атаки. Так, в феврале — начале марта мы [писали](https://42.tut.by/674726), что с почтового ящика Минского зонального центра гигиены и эпидемиологии, а также учреждения «Республиканский научно-практический центр пульмонологии и фтизиатрии» были разосланы письма с ложным сообщением, будто в Беларуси зафиксировано шесть случаев коронавируса. Причем в «теле» письма содержалась ссылка, которая вела к скачиванию вируса.

И в 2018-м хакеры [взломали](https://interfax.by/news/policy/raznoe/1243441/) аккаунты белорусских госорганов и чиновников в соцсетях и опубликовали заявления на тему отношений с Москвой.

**Сложно ли взломать государственный сайт и можно ли в принципе «сломать» сайт МНС?**

Чтобы найти ответ на этот вопрос, 42.TUT.BY побеседовал с различными специалистами, которые занимаются вопросами инфобезопасности в Беларуси. Если кратко — нет, не сложно.

Так, специалист по информационной безопасности Руслан Наркевич считает, что действия «киберпартизан» — «не взлом в чистом виде» и высокой квалификации не требует.

По мнению некоторых наших собеседников, неизвестные «киберпартизаны» применили дефейс — это тип хакерской атаки, когда страница сайта заменяется другой, чаще всего содержащей рекламу, угрозы или вызывающие предупреждения. Вдобавок злоумышленники либо блокируют доступ к остальным сегментам сайта, либо вообще удаляют прежнее содержимое ресурса.

Это не самое сложное действие для хакеров — как сказал один из специалистов, «сегодня такое умеют даже 15-летние». Например, известная хакерская группа Anonymous не проводит атаки подобного рода — их профиль скорее DDoS-атаки и деанонимизация.

Так, в 2011 году хакеры Anonymous [заявили](https://www.dw.com/ru/%D0%B1%D0%B5%D0%BB%D0%B0%D1%80%D1%83%D1%81%D1%8C-%D0%BE%D1%82%D0%B2%D0%B5%D1%80%D0%B3%D0%B0%D0%B5%D1%82-%D0%BE%D0%B1%D0%B2%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B2-%D0%BF%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B0%D1%85-%D0%BE%D1%80%D1%83%D0%B6%D0%B8%D1%8F-%D1%82%D0%B5%D1%80%D1%80%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BC/a-15307259), что взломали серверы итальянской киберполиции и выяснили, что Беларусь осуществляет поставки оружия двум базирующимся в Пакистане террористическим группам. Позже пресс-секретарь МИД заявил, что «появившиеся публикации являются полной дезинформацией», а для достоверности были применены «электронные технологии фальсификации текста для подтасовки содержания».

Другой наш собеседник, попросивший не указывать его имя, считает, что сайты были взломаны с применением «человеческого фактора».

— Самый простой вариант — это социальная инженерия, фишинг, — говорит он. —  Я сам два года проработал в кибербезопасности в государственной структуре, и сплошь и рядом мы сталкивались с подобными ситуациями: какому-нибудь главному бухгалтеру приходит письмо, где написано, к примеру, «у вас задолженность по платежам». 99% людей машинально открывают прикрепленный файл, а там уже работает какой-то эксплойт (компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. — Прим. TUT.BY) — либо троян, либо какой-нибудь стилер, который будет воровать вашу личную информацию.

Повесить картинку на сайт МВД или «Белорусских лотерей» несложно, особенно когда на многих сайтах госструктур при переборе пароля нет ограничений. Есть такое понятие, как брутфорс — когда запускается робот, который просто перебирает пароли на протяжении дня, часа или месяца — в зависимости от сложности задачи.

На вопрос, могут ли «киберпартизаны» сломать сайт МНС, собеседник ответил, что пока сложно сказать: сейчас непонятно, связаны ли периодические проблемы с электронной цифровой подписью с атаками или это просто сбои в системе. Кроме того, он считает сайт налоговой довольно странным выбором — ведь это может ударить по тем же ипэшникам, которые не смогут вовремя заплатить налоги.

— Посмотрим, что получится, — добавил он. — Возможно, они еще не доделали обещанное, и, может, мы еще увидим какой-то результат.

Еще один спикер, который занимается предотвращением и расследованием преступлений в сфере высоких технологий, ответил так:

— Взломать могут — если даже NASA взламывали, то что говорить про сайт МНС. Другой вопрос — какая у них цель.

**Кем могут быть «киберпартизаны»?**

Фото: Michael Geiger / Unsplash

В одном из сообществ, объединяющем специалистов по информационной безопасности, пришли к выводу, что «киберпартизаны» — это так называемый Honeypot (англ. «горшочек с медом») — ресурс, представляющий собой приманку.

Идея в том, чтобы Honeypot-ресурс подвергся атаке или несанкционированному исследованию, что впоследствии позволит изучить стратегию злоумышленника и определить перечень средств, с помощью которых могут быть нанесены удары по реально существующим объектам безопасности.

Однако когда мы написали боту «киберпартизан» с вопросом, можно ли побеседовать с кем-либо из них, чтобы убедиться, что они не условный honeypot, нам ответили следующее: «Привет, сотрудник tut.by, лучше скажите кто так считает, чтобы он убедился в обратном)» (орфография и пунктуация сохранены). После этого собеседник не выходил с нами на связь.

Наше письмо на зашифрованную почту «киберпартизан» также осталось без ответа, и заявка на вступление в их сообщество на Keybase не была одобрена.

В целом по результатам бесед с экспертами можно выделить три основные версии. Первая, что «киберпартизаны» — это провокация, возможно, со стороны властей, которая или должна изменить информационную повестку, или послужить поводом для ужесточения контроля за действиями пользователей в Сети.

Вторая — что на деле «партизаны» не профессиональные хакеры и не структурированное объединение, а обычные айтишники, программисты или пентестеры, которые делают то, на что хватает их сил и умений. Об этом косвенно свидетельствует снижение уровня их активности. Либо же эти неизвестные люди просто хотят отвлечь внимание правоохранительных органов на мелочи и измотать их «партизанщиной», или не желают переходить некую грань и «ломать» действительно серьезные ресурсы.

— Лично я не знаком с «киберпартизанами», но я на 300% уверен, что эти люди существуют. Единственное, я не уверен, насколько они работают как команда, возможно, это отдельно взятые энтузиасты, — отметил один из опрошенных нами специалистов. — Это не какие-то японские хакеры, как показывают в фильмах, нет, скорее это продвинутые айтишники, которые очень неплохо «волокут» в кибербезопасности.

И третий, самый маловероятный вариант, — что это некая команда «профи», которая финансируется из-за рубежа. Но если бы это было действительно так, то «киберпартизаны» действовали бы активнее и более масштабно.

Есть ли практический смысл в действиях «партизан»? На этот вопрос можно ответить по-разному. Один из наших собеседников считает, что это закономерная реакция на действия властей и активность «киберпартизан» будет только расти. Другой же считает это ребячеством.

— Нападения и атаки были всегда, и в них есть смысл — конкурентная борьба для блокировки ресурсов, политический манифест, рейдерская атака на бизнес (озвучить могут как угодно). Смысл появляется, если знать цели и задачи атакующей группы в глобальном видении, — считает Руслан Наркевич. — Но в текущей ситуации смысла нет — так как власть прекрасно оперирует силовыми единицами для навязывания видения ситуации протестующим, и такие действия скорее вызывают раздражение односторонностью исполнения и этической стороной посыла. Это как поведение обиженных мальчишек, которых не пустили в сад, и поэтому они на заборе нарисовали матерное слово, при этом сам сад в неприкосновенности.

При этом «партизаны», примеряя на себя рубашку борцов, забывают, что точка их зрения примитивно-оскорбительная в части, касающейся толерантности взглядов на ситуацию — позиционирование с флагом в руках человека на митинге вызывает искреннее уважение к его взглядам в отличие от безликих поделок в духе мемов низкого пошиба. Это мое личное мнение и не имеет отношения к мнению компании, в которой я работаю.  
Читать полностью:  <https://42.tut.by/700656>