**Феміда на швидкості 150 км/год: чому в Україні статус нардепа став «ліцензією на вбивство»**

**Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка**

**РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення**

# Тотальная безответственность. Кибератака на Украину: как это стало возможным и последствия

КІБЕРЗЛОЧИННІСТЬ | СБ, 2022-01-15 09:32

Версия для печати


Госспецсвязи не контролирует ситуацию с безопасностью "государственного" киберпространства.

В ночь с 13 на 14 января десятки правительственных сайтов стали жертвами хакерского удара, а на страницах отдельных взломанных ресурсов появились угрозы в адрес украинцев. Как это произошло и что удалось совершить киберпреступникам, віясняли в издании **Экономическая правда**.

**Хакерская атака в ночь с 13 на 14 января более 15 государственных веб-сайтов** произошла из-за уязвимости системы управления содержимым сайта, о которой было известно еще с мая 2021 года.

Вероятно, атака произошла централизованно через одну частную IT-компанию, которая создавала все эти сайты. Сценарий нападения на государственные информационные ресурсы напоминает кибератаку 2017 года через ПО "**MEDoc**".

> На эту тему: **Как заражали Украину: хронология крупнейшей в истории кибератаки**

## Кибератака

Сайты украинских организаций в очередной раз стали жертвой хакерских атак. На этот раз злоумышленники ударили по правительственным учреждениям.

В ночь с 13 на 14 января, когда празднуют так называемый Старый Новый год (по юлианскому календарю), были сломаны сайты "**Дія**", Государственной службы чрезвычайных ситуаций, Министерства иностранных дел, Министерства здравоохранения, Минобразования, Министерства молодежи и спорта, Минэнерго, Минагрополитики, непосредственно Кабинета Министров, Государственной казначейской службы и других органов. Атаковали и сайт Национального банка, однако как убеждают в регуляторе, все попытки удалось "нейтрализовать".

НОВИНИ

13:01 **2500 гектарів лісу палає на Чернігівщині через російські обстріли**

12:19 **Підозрювана у хабарництві: ВРП звільнила львівську суддю Ірину Малех**

11:50 **УПЦ МП має повернути державі споруди Богоявленського монастиря у Кременці - суд**

10:53 **Біля Ормузької протоки застрягли 1600 суден**

09:59 **Сергій Гнезділов: Згаяний шанс на встановлення справедливих термінів служби**

08:00 **Доба на Сумщині: п’ятеро вбитих та 11 поранених**

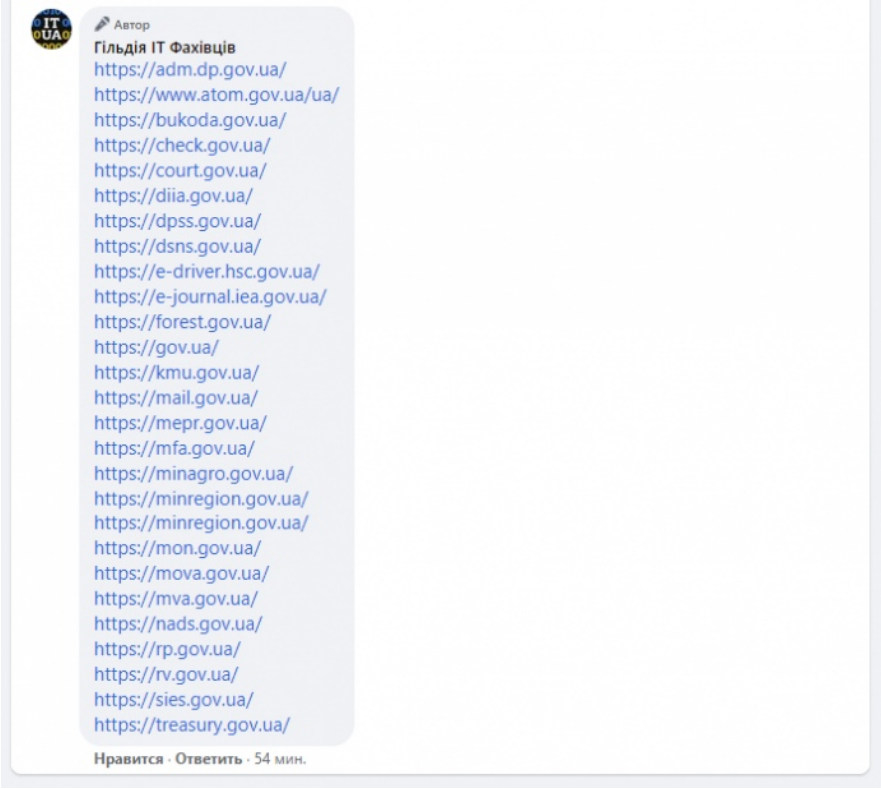
20:00 **Прогноз погоди в Україні на 7 – 10 травня 2026 року**

19:04 **Бутусов: Про іноземців у ЗСУ, СЗЧ і плани ворога (ВІДЕО)**

18:05 **Чернігів, Полтава та Харків серед аутсайдерів у рейтингу прозорості фінансів — дослідження TI Ukraine**

17:08 **Виконавча служба: з гривні боргу вдається стягнути лише 1,5 копійки**

ПІДПИСКА НА КАНАЛ




Перечень веб-адресов государственных информационных ресурсов, пострадавших в результате кибератаки. FACEBOOK **ГИЛЬДИЯ IT СПЕЦИАЛИСТОВ**

Хакерская атака не отразилась на работе государственных органов. По крайней мере, официально. Некоторые учреждения разместили на своих страницах в социальных сетях **сообщения** о том, что актуальную информацию до момента восстановления IT-систем можно получить на их страницах в соцсетях.

"Актуальная информация о работе Казначейства и обновлении сайта будет обнародована на официальном Facebook странице Казначейства. Счета для уплаты платежей доступны на официальном сайте Государственной налоговой службы Украины", – говорится в **сообщении** Госказначейства.

Примечательно, что на странице Министерства иностранных дел злоумышленники разместили сообщения на украинском, русском и польском языках, в котором хакеры запугивают пользователей: "Все данные на компьютере уничтожаются, восстановить их невозможно. Вся информация о вас стала публичной, бойтесь и ждите худшего".


Послание было сделано на трех языках: украинском, русском и польском

В "послании" украинцам, которое хакеры оставили на сайте Министерства иностранных дел, версия на польском языке выдает, что те, кто его писал, не являются носителями языка – несмотря на то, что содержание сообщения намекает на "польский след".

На это обратили внимание журналисты польского издания **Wprost**.

В Министерстве цифровой трансформации **успокаивают** граждан: "Работа большей части атакованных государственных ресурсов уже восстановлена. Контент сайтов при этом остался без изменений, и утечка персональных данных не состоялась. Другие сайты возобновят работу в ближайшее время."

Расследованием инцидента уже занялись Служба безопасности Украины, **Госспецсвязи** и **департамент киберполиции**. Сейчас они собирают цифровые подтверждения.

"Работа большей части атакованных государственных ресурсов уже возобновлена, другие будут доступны в ближайшее время. Решается вопрос об открытии уголовного производства по статье 361 (Несанкционированное вмешательство в работу компьютеров, автоматизированных систем, компьютерных сетей или сетей электросвязи) Уголовного кодекса" , – **сообщили** в департаменте киберполиции.

> На эту тему: **President.gov.ua? gov.Ze? gov.no!**

## Как хакеры атаковали Украину ранее

### Декабрь 2015

С помощью троянского программного обеспечения BlackEnergy 3 неустановленные хакеры 23 декабря 2015 года вывели из строя часть энергосистемы Украины.

Они успешно атаковали компьютерные системы управления в диспетчерской "Прикарпатьеоблэнерго". В результате этого было выключено около 30 подстанций, а около 230 тысяч граждан в течение одного-шести часов остались без электроэнергии.

### Декабрь 2016

Организованная группа хакеров проникла во внутренние телекоммуникационные сети Министерства финансов, Государственной казначейской службы, Пенсионного фонда и вывела из строя ряд компьютеров, а также уничтожила важные базы данных, касающиеся работы Госказначейства и Пенсионного фонда.

В результате 7 декабря 2016 года было заблокировано проведение обязательных платежей на сотни миллионов гривен Госказначейством и Пенсионным фондом. Платежи проходили с задержками или вообще не проходили, не работали сайты Министерства финансов и Госказначейства.

### Декабрь 2016

17 декабря 2016 года в результате атаки на часть электросети Украины пятая часть киевской агломерации вместе с Киевской ГАЭС была обесточена. Отключение части киевской сети продолжалось один час.

### Июнь 2017

В канун Дня Конституции произошла самая большая за всю историю Украины кибератака на компьютерные системы финансовых учреждений, энергетических предприятий, средств массовой информации, объектов транспорта и инфраструктуры, телекоммуникационных сетей и других крупных организаций.

Попадая в компьютер, вирус-требитель Petya.A зашифровывал все данные и потребовал заплатить 300 долларов в криптовалюте Bitcoin. После перечисления средств злоумышленники обещали послать ключ для расшифровки.

От этой кибератаки пострадали более 100 компаний по всей Украине. Среди них "Ощадбанк", "Укрпочта", "Новая почта", "Укрэнерго", "Укртелеком", Министерство инфраструктуры, Минэнергоуголь, 24 канал, Интер, Первый национальный и многие другие.

## Как атаковали Украину атаковали: старый новый хак

Первые догадки о том, как хакерам удалось реализовать кибератаку, обнародовала американская журналистка Ким Зеттер. В своем твиттер-аккаунте она **обнародовала** ссылку на уязвимость системы управления содержимым веб-сайтов October CMS, обнаруженной еще в мае 2021 года.

Через несколько часов на официальном сайте Службы безопасности Украины появилось сообщение о кибератаке с рекомендациями правоохранителей по пути устранения уязвимости. Специалисты спецслужбы предлагают "Обновить OctoberCMS до последней версии (минимум до 472)".

October – это система управления содержимым сайта (CMS) с открытым исходным кодом. Первый релиз системы прошел 15 мая 2014 года. Эту систему используют такие компании как Toyota, KFC и Nestle. October особенно популярен среди пользователей в США и России, а также в Европе: Швейцарии, Польше, Нидерландах, Великобритании и других странах.

Предварительно известно, что атакованные государственные вебсайты были построены на CMS October киевской IT-компанией Kitsoft (ООО "Компьютерные информационные технологии"), специализирующейся на создании IT-продуктов для государственных органов и бизнеса.

В ноябре 2021 года стало **известно**, что компания выиграла тендер на разработку Единого государственного вебпортала электронных услуг по заказу ГП "Дія" стоимостью 38,4 млн грн. Предмет торгов – разработка новых и модернизация существующих компонентов "Дії" с расширением программ-аппаратных возможностей и унификацией комплекса в рамках обеспечения цифровизации paperless.

Часть средств, а именно 12,7 млн. грн., направленных на разработку портала, в прошлом году выделили из государственного бюджета. Все работы по реализации задачи Kitsoft должны быть закончены до конца 2022 года.

Сайт Kitsoft, как и других государственных органов, также не работает.

Кэширование страницы компании в Google показало, что ТОВ "Комп'ютерні інформаційні технології" создавало интернет-ресурсы для почти 40 государственных органов, учреждений и организаций. Среди них, например:

- Будівельні послуги СС1 в Дія;
- новий дизайн сайту для Верховної ради України;
- "Дія" – платформа державних послуг онлайн;
- страховий поліс в застосунку "Дія";
- "Допомога по безробіттю" на порталі "Дія";
- "е-Гавань" (електронний кабінет моряка);
- "єМалятко";
- Фонд соціального захисту інвалідів;
- Міністерство закордонних справ;
- КП "Київтеплоенерго";
- Антимонопольний комітет;
- Донецька обласна державна адміністрація;
- Національний комітет спорту інвалідів;
- Міністерство аграрної політики та продовольства;
- Державна служба морського та річкового транспорту;
- Державна казначейська служба;
- Міністерство у справах ветеранів;
- Урядовий портал;

- Дизайн-система державних сайтів України;
- Український державний центр радіочастот;
- Міністерство освіти і науки;
- Міністерство екології та природних ресурсів.

По данным из открытых реестров, в октябре-ноябре 2021 года Kitsoft выиграла три тендера государственного КП "Головний інформаційно-обчислювальний центр" стоимостью от 1,3 млн грн до 4,4 млн грн. Именно эта компания разрабатывала и программное обеспечение "Киев Цифровой".

Kitsoft работает в сфере компьютерного программирования с 2007 года с руководителем и основным из двух ее бенефициаров Александром Ефремовым.

Комментарии специалистов в сфере кибербезопасности

### Андрей Баранович, Sean Brian Townsend

– По какому принципу были выбраны сайты для атаки?

– Принцип очень прост: они все работали на одной и той же НЕ ОБНОВЛЕННОЙ ВЕРСИИ программного обеспечения. В нем была найдена уязвимость еще в мае прошлого года, и за семь месяцев, прошедших с мая, никто в ни одном из подвергшихся атакам министерств и ведомств не сумел обновить ПО.

Более того, если бы сам софт был настроен правильно, тогда можно было даже не обновлять ПО, потому что уязвимость не подействовала бы. Но ПО было не настроено и не обновлено.

– Кто должен был настраивать и обновлять веб-сайты?

– Все зависит от того, как у госорганов заключены договоры. Я подозреваю, что министерство заказывает себе сайт, фирма подрядчик создает сайт, устанавливает его, настраивает, и на этом работа завершена, за поддержку веб-сайта просто не платят.

Подозреваю, что все было именно так. Я не могу найти другую причину, почему в центральных органах власти семь месяцев не обновляется софт, когда известно, что в нем есть дыра.

– Почему атака имела успех?

– Потому что список уязвимостей October CMS публично доступен. Информация о том, какие уязвимости существуют в том сборнике (версии программного обеспечения – ЭП), и как ими можно пользоваться – открыта.

– Как в будущем следует предупреждать такие атаки?

– Такие атаки происходят из-за тотальной безответственности. До сих пор наши законодатели и исполнительная власть летают в облаках, мечтают о кибервойсках, придумывают какие-то совершенно неосуществимые кибер-стратегии. Все, что нужно делать – это выполнять элементарные обязанности, то есть обслуживать все эти информационные системы.

Если эти обязанности выполнять некому, тогда эти IT-системы нужно просто выключить и перейти на бумажное делопроизводство. Потому что компьютерная система в неуправляемом виде существовать не может. Пусть нанимают администраторов, пусть ищут подрядчиков, которые эти системы будут обслуживать.

А если просто один раз установить, а дальше будет как будет – все кончится катастрофой.

– Как вы оцениваете информационный эффект от публикации провокационной информации на сломанных ресурсах?

– Мотивы взломщиков понятны. Они стремятся поссорить Украину с Польшей, потому что текст переведен на польский язык, написано об исконных галицких землях. Здесь все зависит от реакции министерств иностранных дел Украины и Польши. Для всех очевидно, что это вряд ли польские хакеры. Это могут быть хакеры из России или Беларуси.

Лично мне стыдно за то, что половину правительства завалили публичной уязвимостью полугодичной давности. Это значит, что в кибербезопасности у нас конь не валялся, несмотря на все заявления властей.

### Никита Кныш, Founder и CEO HackControl

- Взлом веб-ресуров произошел из-за уязвимости в CMS, о которой было известно еще с мая 2021 года. Но у нас в Министерстве цифровой трансформации считают, что вопрос кибербезопасности несколько переоценен, и результаты мы теперь видим.

С точки зрения безопасности дефейс (изменение содержимого главной страницы) сайта не предполагает каких-либо критических проблем. Если хакер хотел бы добиться другого эффекта, то он мог бы изменить файлы внутри системы. Но сайт выполняет только ознакомительную функцию.

Эта кибератака лишь в очередной раз полностью дискредитирует систему кибербезопасности Украины. Хочу сказать людям, которые это сделали, спасибо большое, что в очередной раз показали, насколько у нас все "дырявое".

Когда к нам приходила киберполиция, мы говорили, что есть большие проблемы с кибербезопасностью государственных ресурсов, мы предлагали бесплатно их протестировать. Мы предупреждали, что в случае начала войны таким же образом будут идти сообщения о минировании учреждений, организаций, объектов критической инфраструктуры.

> На эту тему: **О вирусе-вымогателе Petya, и о телеметрии Microsoft, которая говорит, что задействован в заражении и MEDOC (обновлено)**

Все происходит четко по сценарию, о котором адекватные люди предупреждали все министерства заранее. Сначала идет атака, цель которой – исчерпать все ресурсы силовых ведомств в Киеве, то есть фейковые минирования. Следующим шагом является распространение паники, то есть проведение специальных информационных операций. Все это – часть гибридной войны.

Сегодня, вероятно, состоялась вторая часть специальной информационной операции. Ее цель – показать, что ваша кибербезопасность на нуле. И треть – это обычно полномасштабное вторжение. Во всяком случае, так было в 2014 году. Это стандартная методология, согласно которой действуют россияне и белорусы.

Я подчеркиваю, что это просто публичное унижение. Затрагивает ли она критическую инфраструктуру? Нет. Сайт можно восстановить с резервной копии и исправить уязвимость за 15 минут.

Как обеспечить защиту? Поскольку у нас все централизовано, нужно децентрализовать управление IT-системами.

—

**Всеволод Некрасов, опубликовано в издании** **Экономическая правда**

---

**На эту тему:**

- **Константин Корсун: «Существующая система кибербезопасности - живой труп»**
- **"Мониторили интернет по запросу "порно"»**
- **Госпецсвязью руководит взяточник и жулик**
- **Украинские спецслужбы выложили на Prozorro документы с грифом «Секретно» и «Для служебного пользования»**
- **Фиктивная система "Рада": электронное шулерство должно покрывать коррупцию?**
- **82% програмного забезпечення в Україні не ліцензоване, — Business Software Alliance**
- **Увы, это не паранойя: за нами следят**
- **GDPR: мифы и реальность**
- **Как российские хакеры взламывали избирательную систему США. Секретный отчет АНБ**



Читайте «Аргумент» в **Facebook** и **Twitter**

*Если вы заметили ошибку, выделите ее мышкой и нажмите* ***Ctrl+Enter.***

**Коментарі**