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

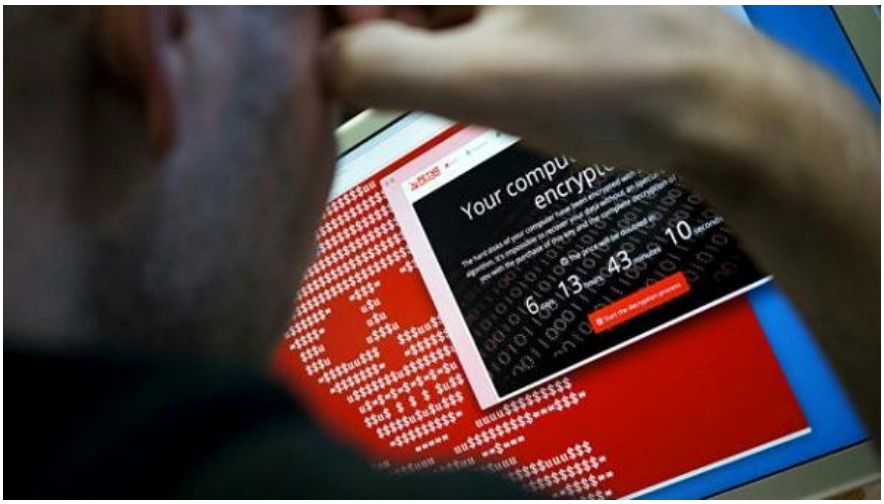
Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка

РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення

Глава киберполиции Сергей Демедюк: Инструкции к вирусу Petya.A писали на русском языке

КІБЕРЗЛОЧИННІСТЬ | СБ, 2017-08-05 08:26

Версия для печати



Начальник киберполиции Украины объяснил, откуда взялся Petya.A, почему к этому может быть причастна Россия, и что действительно было целью черных хакеров, проверявших на прочность киберсистему Украины.

«Если я англоязычный, я не буду писать инструкции для программистов на русском языке». Накануне Дня конституции, 27 июня, страна едва ли не впервые почувствовала, что такое кибервойна. Финансовые учреждения, компании, государственные органы атаковал вирус-вымогатель Petya.A. Жертвами хакерской атаки стали Кабинет министров, Министерство инфраструктуры Ощадбанк, Укргазбанк, Укрсоцбанк, «ОТР Банк», Укрпочта, «Новая почта», аэропорт «Борисполь», сети WOG, KLO, гипермаркеты «Эпицентр», Чернобыльская АЭС и ряд СМИ.

Вирус-вымогатель шифровал данные на компьютере и требовал выкуп — около $300. Специалисты по компьютерной безопасности советовали ничего не платить. И действительно, никаких ключей после выплаты денег владельцы зараженных компьютеров так и не получили. И здесь есть вполне логичное объяснение: по информации СБУ, настоящая цель Petya.A — это отнюдь не заработать денег, а прежде всего, дестабилизировать ситуацию в стране.

Надо признать, что вирус распространился и в других странах Европы и Азии. Как утверждают эксперты, убытки от деятельности вируса по всему миру достигли отметки в $8 млрд. Некоторым пострадавшим структурам для того, чтобы вернуться к нормальной работе, понадобилось три дня.

Впоследствии был найден и канал распространения вируса — «заражение» происходило через обновление бухгалтерского программного обеспечения MEDoc украинского производства. В компании-розработчике программы причастность к распространению Petya.A сначала опровергли, а позже признали, что действительно кто-то вмешивался в работу серверов.

Так или иначе, во время массированной хакерской атаки в Украине были инфицированы более 12 500 компьютеров. И это только вершина айсберга. Часть пораженной техники до сих пор просто себя не обнаружила, и вирус может возобновить атаку в любое время.

> В тему: **NYT: Хакеры атаковали Украину оружием, разработанным АНБ США**

В интервью «Главкому» глава киберполиции Украины Сергей Демедюк объяснил, откуда взялся Petya.A, почему к этому может быть причастна Россия, и что

НОВИНИ

20:00 **Погода в Україні на 8 травня: місцями короткочасні дощі та грози**

19:09 **Павло Казарін: Пастка безстроковості**

18:04 **Олег Чеславський: ЦПК і розкрадання стратегічних активів**

17:10 **Геннадій Левітас: Піхота - рід військ, який зникає**

16:04 **Касьянов: Вони крадуть 4 млн доларів на добу**

15:10 **Батьки очільника столичної прокуратури Сергія Ходаківського та судді Соборного суду Дніпра Максима Ходаківського у 2020 році придбали квартиру в Москві**

14:59 **ВАКС засудив заступника голови Рівненської облради за хабар до 9 років позбавлення волі**

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**

ПІДПИСКА НА КАНАЛ

действительно было целью черных хакеров, проверявших на прочность киберсистему Украины.

— На каком этапе расследования относительно распространения Petya.A? Причастной к распространению вируса была названа компания MEDoc. Экспертиза должна установить, было ли это умышленное действие компании, или она стала только каналом распространения. Сейчас уже есть подтверждение первой или второй версии?

— Вы правильно сказали, точно уже известно, что именно каналом распространения вируса было программное обеспечение MEDoc, здесь уже без исключения. О причастности персонала и должностных лиц компании-разработчика — пока не доказано. Нами также установлено, что их серверы были сломаны еще заранее до самой атаки, очень давно. Сейчас наша задача состоит в том, чтобы мы могли выявить все вредные программные обеспечения, которые использовались с помощью этого канала. Мы уже сообщали, что одной из главных целей распространения вируса Petya.A была затирка следов предварительной преступной деятельности. Поэтому сейчас наша главная задача — не один вирус исследовать, нас теперь интересуют вредные программные обеспечения, которые были установлены с помощью этого канала задолго до вируса Petya.A. Поэтому сейчас назначено много экспертиз.

— Экспертизы касаются компании-разработчика?

— Мы изъяли практически все их оборудования, так как знали, что 4 июля состоялось уже повторное распространение вируса с помощью программного обеспечения MEDoc. Поясню, что произошло: должностные лица компании не отреагировали на наши устные предупреждения, хотя мы сотрудничали уже с 29-го июня (взяли все копии серверов и начали их исследовать). На наши предостережения компания-разработчик не отреагировала. То есть она не закрыла доступ к обновлению. Напротив, они продолжили работу, еще и начали себя пиарить, что они чистые и произошла подмена серверов. Хотя это не так. И когда полицейские пришли к ним и рассказали, каким образом это происходит, они же признали, что заражение произошло.

> В тему: **О вирусе-вымогателе Petya, и о телеметрии Microsoft, которая говорит, что задействован в заражении и MEDOC**

— Компания MEDoc идет вам на встречу?

— Да, каждый день мы работаем вместе. Мы распаковываем оборудование только в присутствии их специалистов.

— Сразу после того, как произошла атака, киберполиция давала рекомендации отказаться от продуктов этой компании. Вы до сих пор убеждены в полезности этих советов?

— Да, потому что мы не исследовали до сих пор их патча обновления (патчем или обновлением называется программный продукт, который используется для устранения проблем в программном обеспечении или изменения его функциональности -«Главком»). Но киберполиция — не учреждение по исследованию антивирусных программ, это не входит в наши функции. Однако мы взяли на себя добровольное обязательство исследовать патчи, но учитывая то, что их исходный код программного обеспечения очень большой и писался некачественно, исследовать и сказать в кратчайшие сроки, что их обновление является действительно безопасным, мы не имеем возможности. Сейчас мы в процессе исследования. Даже те международные компании, которые с нами сотрудничают, они также не готовы предоставить свои предварительные выводы относительно этих обновлений.

Опять же, непорядочно поступают в компании MEDoc — они объявили, что уже разработали исследования, закрывают те уязвимости, которые были раньше. У нас возникает вопрос: какие уязвимости, если даже мы не обнаружили до конца всех уязвимостей?

— В конце концов, если будет доказано, что они знали о вирусе, но ничего не сделали, каким будет наказание?

— Конечно, будем ходатайствовать перед прокуратурой, чтобы должностных лиц привлечь к уголовной ответственности за служебную халатность.

— Какое наказание может их ждать?

— Небольшое, но уголовная ответственность может быть. До 5 лет лишения свободы, не больше.

— В одном из своих интервью Вы говорили, что распространение Petya.A было лишь прикрытием успешной кибероперации хакеров, собиравших информацию. Какая все же была конкретная цель у преступников?

— Еще 15 мая из-за процедуры обновления MEDoc было установлено вредоносное программное обеспечение, так называемый backdoor (основной целью backdoor является тайное и быстрое получение доступа к данным, в большинстве случаев — к зашифрованным и защищенным — "Главком«).Человек, который удерживал этот канал, мог получать данные, которые находились на пораженном компьютере.

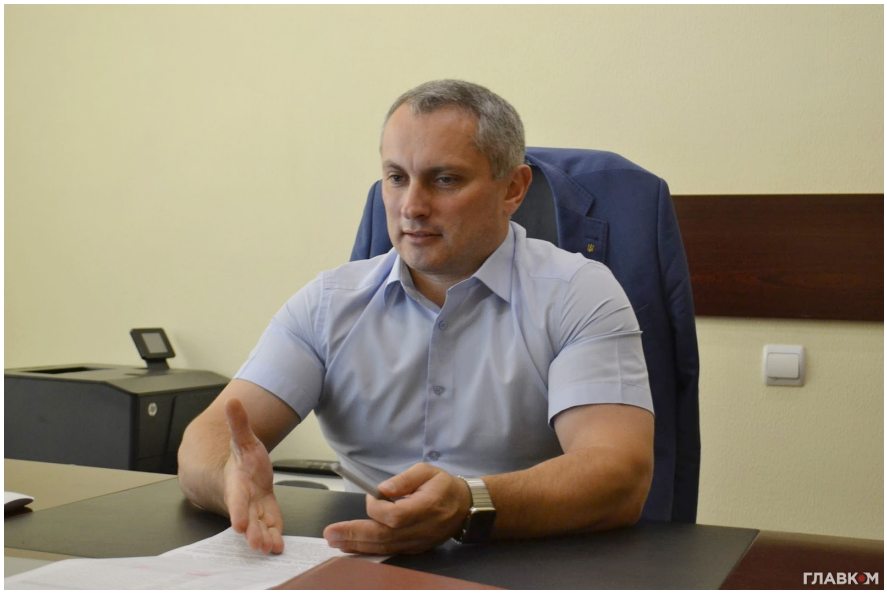
— Готовы ли Вы сегодня признать, что можно было действовать на опережение, предотвратить кибератаку?

— Превентивные меры нами были осуществлены еще после мировой атаки вирусом WannaCry в мае. Мы говорили везде, что необходимо закрыть уязвимости в компьютерах. Есть соответствующие патчи разработчиков Microsoft, других программ, которые были использованы в данных вирусах, но у нас никто не выполнил этих рекомендаций. Даже после последней кибератаки лишь 10% предприятий, как государственных, так и частного сектора, среагировали. Все остальные не предприняли никаких мер безопасности. Никто не учится на своих ошибках.

> В тему: **«Белые» хакеры из Украины признаны лучшими в мире по итогам 2016 года**

— Возможно, стоит делать специальные предупреждения и заявления на уровне правительства.

На уровне правительства и СНБО это все проговаривается и принимаются решения, однако заключительное слово — за Верховной Радой. Парламент даже после таких атак, которые состоялись, не смог принять закон «Об основных принципах кибербезопасности». О чем мы дальше можем говорить?



Глава киберполиции Сергей Демедюк

— Чего именно вам не хватает сегодня?

— Законодательство Украины в этой сфере не сформировано на достаточном уровне. До этого времени у нас в стране неопределенные конкретные профессиональные термины — что такое «киберпреступление», что значит «киберпространство» и так далее — все слова с приставкой «кибер».

— Как же в таких условиях работает киберполиция?

— Мы работаем на понятиях, предусмотренных в Конвенции, н о которую Украина ратифицировала, правда, не в полном объеме. Наша основная цель — добиться от Верховной Рады, чтобы они все-таки имплементировали на 100% эту конвенцию. Она предусматривает азы борьбы с киберпреступностью — это взаимодействие между бизнесом и правоохранительными органами, кто что делает в конкретных случаях при совершении преступления. Сейчас мы работаем на взаимных договоренностях с бизнесом.

> В тему: **Bloomberg: Лабораторія Касперського тісно співпрацювала з ФСБ Росії**

— А законопроект «Об основных принципах кибербезопасности», разработанный депутатами, внесен, зарегистрирован, но они не успели за него проголосовать.

— Вас устраивает этот проект?

— Понимаете, он об основах. Он не может не устраивать, он конкретно определяет: чем занимается СБУ, Госспецсвязь, Нацполиция, НБУ, разведка, Минобороны и другие. Там четко для всех прописаны функции. Чтобы каждый мог под эти основы разработать свои ведомственные акты.

Единственное, что у нас принято, это — Стратегия кибербезопасности Украины, утвержденная указом президента в марте прошлого года. Этой стратегией был создан Центр кибербезопасности при СНБО. Это помогло нам 27-го июня экстренно собраться и вместе — Госспецсвязи, СБУ и Нацполиции — противодействовать атаке.

— По словам президента Петра Порошенко, последняя атака была организована РФ. Еще какие-то данные подтверждают, что хакеры были из России, кроме того, что в ней были задействованы русскоязычные специалисты?

— Каждый вирус пишется на определенном языке программирования. Однако для того, чтобы сделать какие-то поправки, прописываются определенные инструкции. Мы обнаружили, что как раз в доработке в этом коде были такие инструкции на русском языке. В качестве примера, если я англоязычный, я не буду инструкции писать на русском языке.

— Но и в Украине есть много специалистов, использующих русский язык ...

— Я говорил только о русскоязычных, я не говорил о Российской Федерации. Основная из версий — это вмешательство спецслужб РФ, но я пока этого не утверждаю.

— То есть, никаких новых деталей расследования относительно связи с Россией хакеров вы не можете сегодня обнародовать?

— К сожалению, пока не могу. У нас очень много наработок, но нам бы не хотелось, чтобы лица, причастные к определенным этапам атаки, об этом узнали и могли

уничтожить свои следы. Поэтому мы лишь информируем бизнес и население, даем рекомендации по защите их техники. Мы точно знаем о том, что было запущено много вредоносного программного обеспечения с помощью M.E.Doc и не все компьютеры были выведены из строя Petya.A. Мы должны всех, кто уцелел, предупредить, рассказать, каким образом найти вредоносное программное обеспечение, которое уже установилось на их технику. Все рекомендации, которые мы дали, сегодня действуют. Их просто никто не выполняет. В Украине очень много профессиональных специалистов по администрированию сетей, а вот специалистов по киберзащите и отражению киберугроз вообще нет.

— В чем проблема? Мы же постоянно слышим, что наши it-специалисты ценятся во всем мире ...

— Никто не хочет оплачивать труд отделов кибербезопасности. В подавляющем большинстве руководители наших компаний не воспринимают всерьез киберугрозы. Даже случай, который мы испытали на своей шкуре 27-го июня, нечему никого не научил. Только те компании, которые пострадали больше и почувствовали потерю своей информации, сейчас вкладывают средства.

— В Украине немало объектов критической инфраструктуры находятся в частной собственности, но вопрос их кибербезопасности затем становится проблемой государства?

— Вы верно и четко подметили. До сих пор не принят перечень объектов критической инфраструктуры. СБУ и мы настояли на том, чтобы в этот перечень включить и частные структуры, например, компании мобильной связи. Но обо всем списке я не могу вам говорить. Это компетенция Госспецсвязи. Некоторые объекты будут открыты, некоторые закрыты. Это уже они определяют.

— Когда возможна следующая кибератака в Украине?

— Мы предупреждаем, что это будет 24 августа, на День Независимости. Мы видим, что такие атаки происходят накануне или в день каких-то больших праздников для Украины.

Во вредоносном программном обеспечении MEDoc было много элементов, которые до сих пор не активированы. Мы еще не знаем в полной мере, какие свойства имеет вирус. У нас только около 1,3 тыс. официальных заявлений, где начаты уголовные производства. Мы должны учитывать: если преступники уничтожили такой важный для них канал получения информации, то они оставили резервы. Очень мощные резервы. Сейчас мы пытаемся найти еще один канал. Мне хочется надеяться, Petya.A случайно поразил канал и сжег их сеть, но это не так. Потому что мы четко знаем, основная цель киберпреступников — уничтожить следы вмешательства в уязвимые критические объекты.

— Объясните, как работают оперативники и спецагенты во время кибератак?

— Специалист приезжает на место киберинцидента и начинает исследовать. Наша основная задача — выявить вредоносное программное обеспечение и немедленно его отдать в лабораторию для реверса, то есть установить, кто им управляет, каким образом, каковы его функции. В данном случае с Petya.A под вечер мы уже всем объявили, что каналом распространения является MEDoc — для того, чтобы те, кто еще не заразился, могли отключиться и не делать обновления программы. И это спасло очень многих. Нас упрекали, что мы не должны были этого делать.

— Специалисты говорят, что ключ от Petya.A найти крайне сложно. Что вам известно?

— Обычно после заражения вирус-вымогатель сообщает хозяину адрес компьютера, который он заблокировал, и на этот компьютер должен прийти после оплаты код декриптования. Но в этом случае мы не нашли подходящего канала связи вируса со своим хозяином. Это означает, что намеренно все криптовалось без возможности восстановления. Второй вариант — есть уязвимость, о которой мы еще не знаем, она будет фактическим ключом ко всем пораженным компьютерам.

— В киберполиции есть версии, почему именно Petya и откуда такое название?

— Petya.A потому, что был использован ранее запущенный вирус Petya. Это же модифицированный вирус. Кто придумал раньше — это надо только догадываться. Он был зафиксирован еще в начале 2016-го года.

— То есть, Вы не видите никакого политического подтекста?

— Я думаю, нет. Но, возможно, разработчики хотели этим что-то сказать, так как он был распространен на территории Украины.

— Чтобы обезопасить себя, специалисты рекомендовали компаниям перейти вместо Windows на другие операционные системы. Если частные структуры решают этот вопрос в индивидуальном порядке, то на государственных предприятиях нужно какое-то правительственное решение?

— К сожалению, не определено, кто должен этим заниматься в государственных предприятиях. В определенных правительственных учреждениях этим занимается Госспецсвязь. Она дает рекомендации, обеспечивает полностью внутренней сетью, осуществляет проверку всех поступлений контента в их закрытое поле.

Кибербезопасность других учреждений лежит на плечах ответственного должностного лица этой структуры. Оно обязано обеспечить надлежащую безопасность, нанять специалистов, закупить программное обеспечение. К большому сожалению, в настоящее время никто не собирается этого делать.

— В киберполиции сегодня много вакансий?

— Около 60. В ближайшее время мы объявим донабир спецагентов — около 10 человек и около 50 человек — это инспекторы. Их места освободились, потому что, к сожалению, специалисты оставили наши ряды. Они не ожидали такой работы. В большинстве случаев люди думали, что будут находиться на рабочих местах, в очень хороших кабинетах, думали, что им дадут такие программы, которые сами

будут искать преступников. Они не понимали, что надо будет учиться каждый день. Не смогли, потому что надо и в засадах сидеть, и преступников на улице искать, осуществлять вербовку агентуры, и так далее ...

— Элементы разведки в вашей работе есть также?

— Есть, но только в киберпространстве. Наши преступники скрываются за вымышленными аккаунтами в даркнете (darknet — высшей степени анонимности сегмент интернета, к которому невозможно подключиться через обычный браузер — «Главком») и на закрытых форумах. У нас есть специальное подразделение, которое совершает погружение в среду хакеров и именно там происходит разведка.

— Боты в Facebook — не ваши агенты?

Facebook — это не наш профиль. Я говорю о специализированных форумах, куда простому пользователю трудно зайти. Там очень четко преступники определяют, кто чужой, кто свой. Это как классическая разведка среди воров, только наша в киберпространстве, и здесь даже на волосок неправильно сказанный термин ставит агента в режим большого знака вопроса. Тебя могут сослать в карантин и присматриваться к тебе, если подозрения подтверждаются, то тебя выбрасывают из форума, и ты больше не имеешь возможности туда попасть.

— Среди вашего персонала есть бывшие хакеры, которые теперь стали борцами с киберпреступниками?

— Когда мы набирали спецагентов, часть таких людей как раз и пришла. Это — чистые патриоты, которые хотят помочь. Но есть и другая категория, хакеры, которые не являются сотрудниками. Они помогают в зависимости от того, какой подход к ним найти.

— Кроме Petya.A, какие еще большие киберпреступления сейчас расследуете?

— Например, однон из последних. Во время скачивания видео-контента на каналах Youtube идет распространение «интересного» программного обеспечения. Вы переходите по ссылке, чтобы посмотреть фильм, и в это время у вируса есть полтора часа установиться, похитить информацию, дать сигнал командному центру, и все — вы или в бот сети, или у вас похитили полностью все данные, которые были на этом компьютере. Это реальный случай. Это действует, даже если не скачивать фильм, а только смотреть онлайн. Ваша задача лишь нажать на клавишу play.

> В тему: **АЭС США подверглись кибератаке**

— Как себя обезопасить?

— Пользоваться теми ресурсами, которые уже себя зарекомендовали, как надежный источник и имеют определенную репутацию. Фильм в хорошем качестве и бесплатный — это уже должно насторожить. Просто так никто не распространяет контент в сети.

Порносайты, сайты с пиратским софтом используются для того, чтобы установить вредоносное программное обеспечение. Например, порносайты используются разработчиками блокирующих программ, потому что они знают, на что давить — в каждой стране порнография обычно — запрещенная деятельность. Человек заходит на сайт, а там выскакивает окно с объявлением «это киберполиция УМВД, вас оштрафовали, заплатите» и т. д. И кто-то действительно может заплатить «штраф», потому что человек был на таком сайте и уже стесняется сказать об этом жене, или ребенок — своим родителям.

— Вы находили людей, которые занимаются этим?

— В большинстве этим занимаются россияне, мы даже установили фамилии этих людей. Это в основном начинающие, которые берут где-то на закрытых форумах вирусы, переделывают под себя и распространяют на незащищенных сайтах.

Если этот ресурс легитимный, это не значит, что он не сломан, и от его имени не распространяется вредоносное программное обеспечение. Даже от наших партнеров получаем сведения о взломе государственных сайтов, где распространяются вредоносные программы. К государственным сайтам доверие, человек не подозревает, что пользуясь этим сайтом, получает себе такой «подарок».

— Кражи с банковских карточек: какие здесь новые тенденции?

— Да, у нас кардерство очень распространено. Понимаете, сайты, которые занимаются пополнением мобильных телефонов, являются фишинговыми (фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинов и паролей, номеров кредитных карт, электронной почты — «Главком»). Мало того, что вы сообщаете номер своего мобильного телефона, так еще и свои координаты банковских карточек.

Сейчас мошенничество уже дошло до того, что аферисты не используют большие накладки в банкоматах, а только маленькую ленту и микроскопическую камеру. Таким образом снимается пин-код с вашей карты и при вставке ее в картоприемник считывается вся информация. Затем преступники продают эти данные на черном рынке, так как хакеры никогда в жизни не будут использовать то, что воруют.

Стоит сказать, что украинцы очень бедны по сравнению с европейцами, американцами, канадцами и австралийцами. Украина интересна только для начинающих киберпреступников. Преступники из Румынии к нам приезжают, но их объект — это очень крутые магазины или аэропорты, где бывают иностранцы. Преступники знают, что когда иностранец выезжает за границу, он полностью разблокирует доступ к карте.

— В Киеве на фасадах зданий пишут номера телефонов, по которым можно найти группу, в которой продают наркотики. Что касаемо использования соцсетей, например, каналов в Телеграмм для распространения наркотиков?

— Это парафия подразделения по борьбе с наркопреступностью, мы им помогаем установить тех, кто стоит за тем или иным ресурсом.

— Что из новых видов киберпреступлений в ближайшем будущем будет распространяться?

— Опять пошла активная фаза вмешательства мошенников в отдаленный клиентский банковский софт, в основном похищения средств. Также была старая схема, которая возобновилась — взлом почты бухгалтеров и перехват платежных инструментов.

— Несанкционированное вмешательство в государственные реестры — тоже ваша парафия. Ряд рейдерских захватов сельскохозяйственных предприятий осуществлены именно этим способом.

— Мы возвращаемся к тому вопросу, что произошло с MEDoc. У нас не предусмотрена и до сих пор нет процедуры допуска к коммерческим структурам, которые разрабатывают определенный софт для государства. Все разработчики — это частные компании, которые не несут ответственность. Теперь и Кабмин, и Верховная Рада инициируют сертификацию такой продукции каким-то органом, который бы осуществлял контроль.

— Когда ГФС сделает нормальное программное обеспечение для обмена и регистрации налоговых накладных? Кто саботирует этот процесс?

— Никто там не саботирует. В связи с тем, что люди перешли и пользовались частным продуктом, не было стимула для ГФС разработать собственный продукт. Сейчас, знаю, они работают над этим. Другие структуры поняли, что должна быть альтернатива для клиента. Наша инициатива — обязать государство предоставлять альтернативный продукт для граждан.

—

Юлія Тунік, Микола Підвезяний, опубликовано в издании Главком

Перевод: Аргумент

В тему:

- **Carderplanet и убийство Дмитрия Завгороднего: дело российских спецслужб?**
- **Carderplanet и убийство Дмитрия Завгороднего: дело российских спецслужб? Часть 2**
- **Взлет и падение CarderPlanet глазами участника движения**
- **Пол Грэм: Слово «хакер»**
- **Как российские хакеры взламывали избирательную систему США. Секретный отчет АНБ**
- **Кибервойна: зачем государствам армии хакеров?**
- **Кибер-война: в атаку идут только хакеры и боты**

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

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

Коментарі