ЦИФРОВЫЕ МОНСТРЫ

МЕЖДУНАРОДНЫЕ IT-КОРПОРАЦИИ ГОТОВЫ К ВОЙНЕ С РОССИЕЙ

Окончание. Начало — на стр. 1

ТРЕТИЙ ПОДАРОК из коробки под новогодней ёлкой — подготовка сокрушительной глобальной кибервойны. Речь идёт не о войнушке где-то на периферии из-за какого-нибудь гористого клочка земли, а о войне тотальной. Речь не идёт о кибератаке где-то в сети, когда пользователи сталкиваются с некоторыми неудобствами. На кону жизнь и смерть инфраструктуры и всех систем жизнедеятельности целых стран и народов. Война, первые киберзалпы которой звучали и раньше, в декабре вышла на поверхность и стала мощным и долгоиграющим фактором информационного поля, а в будущем году может стать ощутимой в жизни каждого. Война эта, надо понимать, ведётся на полное подчинение не только нашей России, но и всего мира воле того самого цифрового Левиафана.

В декабре случилась разведка боем, подлинное происхождение которой вызывает много вопросов, но вполне вероятно, именно так и проявляет себя Левиафан. Один из эпизодов этого боя, похожего на психическую атаку из фильма "Чапаев", — это объявление компанией "Майкрософт" войны Российской Федерации. Майкрософт является важной составляющей Левиафана, входя в пятёрку ведущих технологических компаний западной части мира.

"МАЛОЙ КРОВЬЮ И НА ЧУЖОЙ ТЕРРИТОРИИ"

Что такое кибератака? Это, если грубо, захват контроля над удалённой вычислительной системой, захват, который может выражаться в отказе обслуживания либо в такой дестабилизации работы, которая делает невозможной полноценное исполнение системой её функций.

Кибератака — это нападение нового типа, для него не нужны танки и самолёты, наоборот, оно может отключить ваши танки или самолёты или направить их против вас же. Когда вырубятся системы жизнеобеспечения, управляемые сегодня компьютерами, соединёнными в сети, то в городах погаснет свет, отключатся газ и вода, остановятся автомобили и поезда, самолёты не смогут взлететь или сесть, люди не получат доступа к своим банковским счетам и карточкам, что в отсутствие наличных приведёт к полному параличу финансовой системы.

Кстати, волею Центробанка РФ мы переходим от пластиковых денег к полностью цифровым — и вся эта система открыта для кибератаки и полностью окажется парализованной. Это как если бы мы полностью отдали всю свою память внешним устройствам, а те бы внезапно отключились — и мы бы забыли, как нас зовут, где живём, кто мы и откуда. Мировые центробанки, ведомые ФРС, торопят всех в новый дивный мир бесконтактных платежей, рассматривая ковид как возможность пришпорить в их понимании технологическую революцию, но вместо предполагаемых неудобств, связанных с пользованием наличностью, нам готовят киберболезнь Альцгеймера. И возможно, только те, кто её устроил, будут знать, как её лечить. В грядущей кибервойне банки более всего открыты для атаки, информация на их серверах может быть безнадёжно утрачена, и в условиях тотального финансового дефолта мир может вернуться к наличности и бартерным отношениям.

Готова ли Россия к такому сценарию, не говоря уже о предотвращении такого исхода? А ведь для этого нужно больше ресурсов и умения, чем для организации жизни в условиях отказа систем жизнеобеспечения. Располагает ли страна сегодня такими ресурсами и умениями? В 1938 году на экраны СССР вышел фильм "Если завтра война", в котором описывалось, как Красная армия малой кровью и на чужой территории побеждает войска европейского агрессора. Реальность, как мы знаем, оказалась совсем другой. В первый же день войны фашисты нанесли по СССР настолько сильный удар, что Гитлер был уверен: победа в кармане. Напав внезапно и мощно, по всем фронтам, немцы помешали стратегическому развёртыванию советских войск. Германское командование создало огромные оперативные группировки от Баренцева до Чёрного моря, а на направлениях главного удара сосредоточило элитные части. Застав нас, по сути, врасплох, в первые недели войны они полностью овладели стратегической инициативой и добились больших успехов. СССР оказался на волоске от полного разгрома.

Не находится ли Россия сегодня в ещё более худшем положении — как в том, что касается подготовки к будущей войне, так и в самом осознании её неотвратимости? При том, что многие представители верхушки государства и бизнеса говорят в терминах технологического детерминизма, эта предопределённость почему-то не распространяется на древнейшее человеческое занятие, для которого, по сути, и создаются в первую очередь новые технологии, — на войну. Насколько Россия готова сегодня к масштабной кибератаке, которая может быть молниеносной в исполнении, пусть и длительной по подготовке и информационному сопровождению? Кибервзлом ведь сначала незаметен, здесь его можно сравнить с взломом сознания, и кибернандемию сперва можно принять за информационный шум — но его результаты будут разрушительнейшие.

ПСИХИЧЕСКАЯ АТАКА ИЛИ?

Но давайте сначала оценим вероятность такой мощной глобальной кибератаки. Прежде всего, обратимся к первоисточнику — к Клаусу Швабу, главе и основателю Всемирного экономического форума, этого штаба глобалистов, куда так любят ездить наши министры и олигархи. Клаус Шваб подарил свою книжку о четвёртой промышленной революции Владимиру Путину, и тот с благодарностью её принял. Интересно, что ещё год назад эксперты поговаривали об открытии в Москве офиса ВЭФ. Это планировалось сделать в Сколково при участии Сбера, тогда ещё Сбербанка.

Вот что публично заявил Шваб 8 июля 2020 года: "Мы уделяем недостаточное внимание устрашающему сценарию полномасштабной кибератаки, которая приведёт к полной остановке энергообеспечения, транспорта, работы больниц, всего общества в целом. Кризис ковида-19 в сравнении покажется небольшим недоразумением".

Имеем ли мы здесь дело с предупреждением — или скорее с планом действий, планом, обнародованным и в целях психологического давления, и для открытой координации? Ведь в 2020 году практически все события происходят удивительно открыто. Если посмотреть на временну́ю линию событий, создаётся впечатление, что сразу после этого выступления началась информационная подготовка к кибератаке, о которой говорил Шваб. А 18 ноября 2020 года первая проверка того, как это будет работать, прошла на примере компании Americold, которая первой сообщила о кибератаке.

Americold — это крупнейшие кондиционируемые склады по всем США и своя логистика. За этой американской компанией стоит более ста лет истории. Её склады используются, например, для доставки вакцины от ковида, то есть компания эта имеет стратегическое значение. В случае кибератаки все её холодильники с вакциной от ковида могут быть разморожены и вакцинация будет сорвана. Защита этой компании была взломана неведомыми хакерами, хотя власти США в таких случаях привыкли показывать пальцем на Россию. Выяснилось, что Americold является клиентом компаний SolarWinds и FireEye, через софт которых, по утверждениям властей США, и произошла атака.

FireEye — компания кибербезопасности, которая занимается мониторингом киберугроз через программу "Орион". Хакеры компании, так называемая "красная команда", занимались инсценировкой кибератак на инфраструктуру клиентов. Утверждается, что наработки "красной команды" были украдены и через компанию кибербезопасности SolarWinds сотни тысяч клиентов по всему миру — в основном, на 80 процентов, в США — были взломаны. То есть им были разосланы трояны — коды, которые посылают своему хозяину информацию о системах взломанной структуры и выполняют его команды. Фактически сервер клиента переходит под контроль хозяина трояна, который может активизировать нужную программу в любой момент и, например, вызвать отключение города от электричества. Список тех, кто является клиентами FireEye и SolarWinds, опубликованный американскими СМИ, впечатляет сам по себе.

Это Пентагон, Федеральная резервная система, Госдеп, Агентство национальной безопасности США, НАСА, Минфин, Почтовая служба, Минюст, администрация президента США, ведущие американские консалтинговые компании, практически все компании верхнего списка Форбс, крупнейшие города страны, инвестиционные компании и банки, оборонные предприятия — например, Локхид Мартин, Космический центр Кеннеди, Университет Джонса Хопкинса, на котором стоило бы остановиться отдельно. Этот частный американский университет, расположенный в Балтиморе, между Нью-Йорком и Вашингтоном, сегодня управляет ковидом, определяя политику чуть ли не всех стран мира, за весомым исключением Китая. Формально Университет Джонса Хопкинса является ведущим мировым центром по статистике, прогнозам и анализу, но это тот самый анализ, исходя из которого, власти принимают решения по закрытию стран и городов, ограничению конституционных прав и свобод, уничтожению "аналоговой" экономики в пользу цифровой. Не стоит строить иллюзий: этим командам подчиняется в том числе и глава Роспотребнадзора Анна Юрьевна Попова.

Кроме того, в списке потенциально "хакнутых" пользователей — американская сеть управления умными городами, ведущие СМИ страны типа газеты "Нью-Йорк Таймс", телевизионные кабельные сети, фонд Билла и Мелинды Гейтс, Мастеркард и Виза, ВВС США, системы управления атомными станциями, сотни университетов и колледжей. Даже сеть Макдоналдс в этом списке, и её могут отключить по команде неведомого врага!

Получается, что хакеры внедрились в системы управления и через обновления разослали трояны по сотням тысяч адресов, что позволяет им держать под полным своим контролем системы компьютерной безопасности этих организаций и структур. В случае кибератаки все они безоружны — ведь, по сути, все их системы безопасности обойдены.

Осознав масштаб происшедшего — так об этом пишет большая американская пресса — и после обнаружения троянов на серверах прежде всего Пентагона, Агентство кибербезопасности и инфраструктурной безопасности США (CISA) впервые за свою историю опубликовало чрезвычайную директиву, обращённую ко всем организациям и компаниям, в том числе гражданским. Там говорилось — дословно, — что "все агентства, оперирующие продуктами SolarWinds, должны предоставить об этом отчёт CISA".

Директива была выпущена 13 декабря, в воскресенье, а отчёт требовалось доставить к полудню понедельника 14 декабря по времени восточного побережья.

При этом замечу, что ничего внешне не произошло. Программа не запущена, самолёты летают, поезда ходят. Но при этом кибератака, о которой летом говорил Шваб, стала потенциальной реальностью. Она может случиться через месяц, через неделю, через год или уже завтра. При этом она может прийти, откуда не ждали — то есть через те самые компании и структуры, которые занимаются кибербезопасностью и у которых есть доступ, по сути, к оружию кибернетического массового поражения.

Кому же выгодна такая кибератака? В ней тут же обвинили удобного врага — Россию, удобного, потому что безответного. Но это обвинение — далеко не только предлог для каких-то новых санкций. Это надо понимать, прежде всего, в контексте так называемого ответного удара. А ответный удар американцев планируется полномасштабный: из контекста того, как характеризовалась атака на США. Понятно, что за цели собираются атаковать сами американцы. Они собираются отключить у своего вероятного противника спецслужбы, армию, ВВС, космические силы, Центробанк и финансовую систему, госрезервы, крупнейшие инфраструктурные компании, системы обеспечения городов, транспортную систему. Этим противником — и это очень чётко обозначено — является Россия.

Госсекретарь Майк Помпео заявил в интервью на консервативном ток-шоу, что "мы совершенно чётко можем сказать, что это были русские". И хотя Трамп вначале отшутился в Твиттере, написав, что, вероятно, целью атаки была одна из этих смешных машин для голосования, глубинное государство дало понять всем серьёзным игрокам в поле, что шуткам не место. Байден высказал уверенность, что за кибернападением стоят русские, и он убеждён, что нужен ответный удар. "Хорошая защита недостаточна", — сказал Байден. Он пообещал сделать так, что виновные в атаке серьёзно за это заплатят.

"Нью-Йорк таймс", орган ЦК Демократической партии США, американская газета в роли "Правды", пишет о происшедшем следующее: "Русская атака была тщательно откалибрована так, чтобы избежать кибероборонны. Они получили доступ к софту SolarWinds — это всё равно как если получить доступ к обновлениям Apple и других производителей телефонов, — и при этом они рассчитывали, что небольшие изменения кодов не будут заметны".

На базе Форт-Мид под Вашингтоном, где расположен новый совместный командный центр АНБ и киберкомандования, эту кибератаку никто не заметил, пишет "Нью-Йорк таймс". Датчики не сработали, и командир кибернетических сил опытный генерал Пол Накасоне не сказал об этом пока ни слова. Но вот что по горячим следам заявил генеральный директор той самой компании FireEye Кевин Мандиа: "Мы являемся свидетелями атаки нации, обладающей высочайшими наступательными возможностями".

Можно не сомневаться, что американцы готовят то, что они воспринимают как ответный удар, по этой самой нации. И нужно отметить, что эта нация — не китайцы, ибо на карте атаки, оперативно опубликованной компанией Майкрософт, Китай также обозначен как жертва атаки в отличие от России, одной из немногих стран, этой атакой не затронутых.

МАЙКРОСОФТ ПРОТИВ РОССИИ

В связи с происходящим огромный интерес представляет официальное заявление компании Майкрософт, которое её президент Брэд Смит выпустил 17 декабря. Этот программный документ доступен на сайте компании — лучшего друга Сбера и правительства Российской Федерации. В нём Брэд Смит объявляет Россию ответственной за кибератаку и не только призывает к её наказанию, но и предлагает, как это сделать эффективнее, так, чтобы противник уже не встал.

В этом заявлении Майкрософт не только объявляет войну России, не только фактически признаёт связь с американскими секретными службами, не только косвенно намекает на свой собственный опыт создания оружия массового киберпоражения, но и чётко говорит о планах постановки под контроль американцев глобальной системы кибербезопасности целиком. Судя по фактам, раскрытым на ноябрьских слушаниях в Сенате США, компании "Фейсбук", "Твиттер" и "Гугл" на оперативном уровне координируют свои действия, фактически представляя собой единую, хотя и трёхголовую структуру. Есть основания полагать, что и в стратегии эти корпорации выступают единым фронтом, во всяком случае, в отношениях с Белым домом и Конгрессом, не говоря уже о внешних рынках. Интересно, что на сенатские слушания последних лет, где между государственными мужами и культовыми фигурами бизнеса устраивается борьба нанайских мальчиков, не приглашают руководителей Майкрософта, — видимо, эта компания считается уже "старыми деньгами" и освобождена от ритуальных отчётов. Тем не менее можно не сомневаться, что и эта компания, и Амазон участвуют в цифровом картеле.

Майкрософт, получивший в 2019 году 20-миллиардный контракт от Пентагона на разработку программного обеспечения театра боевых действий, просто стоит ближе всех к правительству и занимается сейчас весьма успешным лоббированием интересов всего картеля. Вот и теперь именно представитель Майкрософта доносит до политиков единое мнение цифровых олигархов. Во-первых, подчёркивается, что жертвами кибератаки русских стали США и их ближайшие союзники:

"Хотя примерно 80% (жертв атак. — **И.Ш.**) находятся в Соединённых Штатах, выявлены жертвы ещё в семи странах. Сюда входят Канада и Мексика в Северной Америке; Бельгия, Испания и Великобритания в Европе; Израиль и ОАЭ на Ближнем Востоке. Несомненно, число и местонахождение жертв будут расти. Мы все должны быть готовы к рассказам о дополнительных жертвах в государственном секторе и на других предприятиях и в организациях. К сожалению, атака представляет собой широкое и успешное нападение как на конфиденциальную информацию правительства США, так и на технические инструменты, используемые компаниями для их защиты. Атака продолжается, активно расследуется и решается группами кибербезопасности в государственном и частном секторах, включая Microsoft. …Атака отличается своим масштабом, изощрённостью и воздействием. Есть и широкие её разветвления, которые ещё больше сбивают с толку".

Майкрософт оперативно опубликовал карту кибератаки, которая основана на телеметрии Microsoft Defender, антивирусного программного обеспечения для последней версии Windows. На этой карте Россия и другие страны СНГ представлены белыми пятнами, что подводит к выводу, что они в атаке не пострадали, зато остальные страны, включая не только США, но и Японию, Китай, страны Европы, оказались жертвами кибернападения.

"Карта позволяет идентифицировать клиентов, которые используют Defender и установили версии программного обеспечения SolarWinds Orion, содержащие вредоносное программное обеспечение злоумышленников, — пишет Смит. — Этот аспект атаки создал уязвимость цепочки поставок почти глобального значения, достигнув многих национальных столиц за пределами России. Это также свидетельствует о повышенном уровне уязвимости в Соединённых Штатах".

Президент Майкрософта практически открытым текстом говорит об экзистенциальной вине русских инженеров, которые виноваты уже в том, что не уступают американским:

"Это не "обычный шпионаж" даже в эпоху цифровых технологий. Напротив, он представляет собой акт безрассудства, который показал серьёзную технологическую уязвимость для Соединённых Штатов и всего мира. По сути, это не просто атака на конкретные цели, но и на доверие и надёжность критически важной мировой инфраструктуры с целью продвижения разведывательной службы некоей одной страны (речь, очевидно, о стране, где так любят водку и балалайку. — **И.Ш.**). Как мы уже неоднократно видели, Кремниевая долина — не единственный дом для гениальных разработчиков программного обеспечения. В 2016 году российские инженеры выявили слабые места в защите социальных сетей, проникли в американские политические кампании и использовали дезинформацию, чтобы посеять разногласия среди электората. Они повторили это упражнение во время президентской кампании во Франции 2017 года. По данным Центра анализа угроз и отдела цифровых преступлений Microsoft, эти методы затронули жертвы более чем в 70 странах, включая большинство демократических стран мира".

Если аналитики Майкрософта делают такие выводы, то очевидно, они мониторят политическую активность по всему миру.

Особую обеспокоенность Смита вызывает возможность использования русскими хакерами искусственного интеллекта: "Одним из наиболее пугающих событий этого года стали новые шаги по использованию ИИ для вооружения больших украденных наборов данных о людях и распространения целевой дезинформации с помощью текстовых сообщений и приложений для обмена зашифрованными сообщениями. Мы все должны исходить из того, что, как и изощрённые атаки из России, это тоже станет постоянной частью ландшафта угроз".

Но погодите: не тот ли это искусственный интеллект, который Майкрософт помогает разрабатывать Сберу, — а Сбер расплачивается за услугу тем, что продвигает базирующиеся на ИИ продукты Майкрософта в России? Как можно продвигать ИИ в России и одновременно выражать обеспокоенность именно по этому пункту? Не в том ли дело, что Майкрософт продвигает в России "правильную версию" ИИ?

Далее в тексте обращения появляются тревожные нотки: под угрозой главный план глобалистов — использовать ковид для резкого продвижения своей повестки:

"Кибератаки нацелились на больницы и органы здравоохранения, от местных органов власти до Всемирной организации здравоохранения, — бьёт в колокола Смит и делает вброс о том, что винить в этом нужно всё тех же русских. — Пока человечество стремилось разработать вакцины, группы безопасности Microsoft обнаружили трёх субъектов в некоем национальном государстве, нацеленных на семь известных компаний, непосредственно участвующих в исследованиях вакцин и методов лечения COVID-19. В мире, где авторитарные страны совершают кибератаки против мировых демократий, для демократических правительств как никогда важно работать вместе".

Смит видит выход в сращивании государства с технологическими монополиями: "В отличие от прошлых атак угрозы кибербезопасности также требуют уникального уровня сотрудничества между государственным и частным секторами. Современная технологическая инфраструктура, от центров обработки данных до волоконно-оптических кабелей, чаще всего принадлежит и управляется частными компаниями. …Для эффективной киберзащиты требуется не просто коалиция мировых демократий, но коалиция с ведущими технологическими компаниями".

При этом партия "большого тека" начинает диктовать правительству свои условия, что для США достаточно необычно. Начинается всё с обвинений в адрес администрации Трампа: "Слишком часто кажется, что федеральные агентства в настоящее время не действуют скоординированно или в соответствии с чётко определённой национальной стратегией кибербезопасности".

Смит призывает к объединению разведданных корпораций и государства, "объединению стратегической разведки" и "переходу от "необходимости знать" к "необходимости делиться".

Чем делиться? Правительство может делиться в первую очередь данными, а компании — продуктами, произведёнными из этих данных: "Даже в такой крупной компании, как Microsoft, мы узнали, что для нашего центра анализа угроз критически важно агрегировать и анализировать данные из наших центров обработки данных и служб. А когда возникает серьёзная угроза, нам нужно делиться информацией и коллективными оценками с другими технологическими компаниями".

Таким образом, исподволь компании в отношениях с государством резервируют для себя место более высокого уровня: государство поставляет сырьё — человеческие данные, а компании находят им применение.

Интересно, что то же самое — и гораздо успешнее, чем в США — пролоббировали в российском правительстве наши "цифровики". Я не думаю, что российским цифровикам под силу поставить российских чиновников под контроль, но соответствующие законы-то приняты и продолжают приниматься. Именно эти законы могут послужить тараном для своего рода "международных кибервойск быстрого реагирования".

По сути, речь идёт о более активной, чем прежде, форме глобального контроля США над миром. Смит пишет, что нападение русских хакеров "требует коллективного ответа, который показывает, что серьёзные нарушения имеют последствия": "Защита демократии требует, чтобы правительства и технологические компании работали вместе в новых и важных направлениях — для обмена информацией, усиления защиты и реагирования на атаки. Поскольку мы оставляем 2020 год позади, новый год даёт новую возможность продвинуться вперёд по всем этим направлениям".

Отмечая, что "международное сообщество движется в этом направлении", Смит выделяет такой орган, как Глобальная комиссия по стабильности киберпространства (GCSC).

Как американцы хотели бы управлять глобальным рынком кибербезопасности? Прежде всего через знакомый приём — санкции. Вот что пишет Смит:

"Это необходимо для обеспечения того, чтобы внутреннее законодательство чётко и строго запрещало компаниям помогать правительствам участвовать в незаконных и наступательных кибератаках, а инвесторам — сознательно финансировать их… Нам нужны шаги, чтобы гарантировать, что американские и другие инвесторы сознательно не подпитывают рост этого вида незаконной деятельности. И Соединённым Штатам следует активно проводить обсуждения с другими странами, которые создают эти компании, в том числе с Израилем, который имеет сильную экосистему кибербезопасности, которая может быть использована для опасной поддержки авторитарных режимов".

Может получиться, что правила игры по глобальным системам кибербезопасности будут писать в Вашингтоне, а России придётся сдать то, что ещё осталось от нашего национального суверенитета, поставив свои системы под контроль цифрового Левиафана.

АТАКУЯ, ЗАРАБАТЫВАЙ

Итак, Майкрософт может атаковать Россию и напрямую, и одновременно косвенно, через санкции. Через контроль над инвестициями им довольно легко будет поставить под контроль российские частные экосистемы Ай-Ти и искусственного интеллекта — в том числе экосистему Сбера и Яндекса.

Но как это возможно, если Майкрософт — один из главных партнёров Сбера, активно работает с правительством РФ, имеет здесь своё представительство и извлекает из России десятки миллиардов рублей прибыли? По официальным данным, Майкрософт Рус зарабатывает в России около 6-7 миллиардов рублей в год. Однако большая часть российских предприятий и организаций платит Майкрософту непосредственно через европейское подразделение компании в Ирландии, Microsoft Ireland Operations Limited, MIOL, которое российским налоговикам неподконтрольно и данных о своих денежных потоках из России не раскрывает.

Чем занимается Майкрософт в России? Это отнюдь не только обновления MS Windows, которые стоят во всех компьютерах и через которые компания может постоянно собирать информацию на пользователей.

На официальном сайте Майкрософт Рус первой главной целью компании значится помощь российским компаниям в решении вопросов цифровой трансформации. А это сегодня, как мы знаем и как постоянно подчёркивает господин Мишустин, — дело государственное. Второе направление — участие в развитии российской ИТ-экосистемы через стратегические коалиции, с фокусом "на индустриальные решения и помощь российским партнёрам в глобальном продвижении". Третье — "поддержка российских стартапов" и четвёртое — "содействие росту числа высококвалифицированных ИТ-кадров". То есть Майкрософт обращает особое внимание на талантливую молодёжь.

Очень важным направлением работы Майкрософта в России как раз является развитие стратегических партнёрств. Особенное внимание американцы уделяют телеком-операторам: ведь именно туда стекаются основные объёмы данных. Именно эти объёмы, согласно принятым в 2020 году законам и концепциям правительства РФ, предполагается широко продавать и покупать, в том числе и иностранным компаниям. Понятно, что и тут Россия выступает поставщиком сырья — своеобразной новой "нефти человеческого поведения", из которой будут изготовлены продукты человеческого управления.

"Трансформация партнёрской экосистемы — один из приоритетов новой стратегии, — говорится на сайте Майкрософт Рус. — Одни из самых ярких примеров — разворачивание стэка Microsoft Azure в центрах обработки данных МТС и программа совместных со Сбербанком исследований в сфере искусственного интеллекта и робототехники". Именно облачные технологии являются ключевыми в развитии ИИ-сектора, и Сбер делает всё, чтобы это развитие в России происходило именно в облаках Microsoft Azure.

Также в качестве примеров применения технологий Майкрософта в России называется разработка ChemTech (программное обеспечение для нефтегазовых и химических компаний), "Робот Вера" (чат-бот для собеседований при подборе персонала), Bright Box (решение для "подключённых автомобилей").

ТЕМ ВРЕМЕНЕМ ШВАБ

Не хочется даже думать о том, что случится, если миллионы людей в Северном полушарии уже в 2021 году на месяцы останутся без энергии, а заодно и без пищи, воды, отопления, наконец, без Интернета. И всё же, кто стоит за той самой кибератакой на США, которая может стать прологом вполне реальной войны? Может ли это быть операцией ложного флага, когда русских просто подставили? Может ли такая атака быть организована частными игроками, и что о таких возможностях может знать Шваб? Американцы отрицают такую возможность, но не является ли такое торопливое отрицание подозрительным? И возможно, главный вопрос: может ли цифровой Левиафан атаковать Интернет, не рискуя таким образом потерять контроль над человечеством? Какие ещё стратегии и технологии контроля мы увидим в ближайшее время?

Вернёмся на Всемирный экономический форум. С его активным участием недавно была создана организация Cyber Polygon. Как написано на сайте организации, в ней состоят 120 организаций из 29 стран. Список этих организаций, вывешенный у них на сайте, впечатляет, хотя многие из них, как там написано, пожелали остаться анонимными. Среди них очень важное место занимают российские структуры, такие как Сбер, часть его экосистемы Работа.ру, МТС, Мейл.ру, Почта-банк, Центр данных Ростелеком, тюменский фонд ЦИТТО и так далее.

Cyber Polygon продвигает "Цифровую идентификацию ООН" — то есть перед тем, как зайти в Интернет в любой точке земного шара, вы должны будете идентифицировать себя. Доступ будет привязан к идентификации, а она, в свою очередь, например, к вакцинации, а потом и к чипизации.

Ведущую роль в Cyber Polygon играет компания IBM, о которой написано больше книг, чем о Майкрософте. IBM на сегодняшний день — также один из лидеров разработок ИИ на собственных платформах корпорации.

Возможно, Cyber Polygon — объединение компаний, созданное ВЭФ для аккуратного продвижения продуктов американской компании IBM. Каковы же эти продукты? IBM объявила, что разрабатывает сервис по сопряжению Интернета, вышек 5G, транспортных систем, всяческой логистики с системами искусственного интеллекта. Этот сервис будет представлять собой блокчейн, сообщает компания, хотя это весьма сомнительно — ведь блокчейн по определению децентрализован, а тут контроль за транзакциями сохранит за собой центральная структура. В этом так называемом блокчейне любая транзакция, любое действие записывается навечно, может быть отслежено и восстановлено. Этот продукт, утверждает IBM, способен решить проблему с кибербезопасностью.

Не получится ли так, что в предполагаемом пессимистическом сценарии человечество (или значительная его часть) подвергнется кибератаке и будет вынуждено провести дни, недели или даже месяцы без элементарных удобств, в результате чего в народе созреет запрос на решение вопроса кибербезопасности любой ценой?

И тогда IBM сможет предложить миру свое решение проблемы — свой блокчейн. Те, кто создал проблему, лучше всех смогут её решить — и получить власть над миром.

Игорь ШНУРЕНКО

Рисунок Василия ПРОХАНОВА

Газета "ЗАВТРА" зарегистрирована Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия. Свидетельство ПИ № ФС 77-22122 от 24 октября 2005 года.

Учредитель и издатель — ООО "Редакция газеты-еженедельника "Завтра" (119146, г.Москва, Фрунзенская наб., 18, пом. VII).

Адрес редакции: 119146, г. Москва, Фрунзенская наб., 18, пом. VII.
E-mail: **zavtra@zavtra.ru** Электронная версия: **http://zavtra.ru/**
Служба распространения: (499) 246-88-52 (т/ф). Служба рекламы: (903) 131-53-97.
Отпечатано в АО "Красная Звезда" (125284, г. Москва, Хорошевское шоссе, 38, тел.: (495) 941-32-09, (495) 941-34-72, (495) 941-31-62, http://www.redstarprint.ru, e-mail: kr_zvezda@mail.ru.

Главный редактор Александр ПРОХАНОВ

Тел. редакции: (916) 502-49-86. **Тираж 27 850** Заказ № 5989-2020 Дата выхода в свет — 29.12.2020 г. Подписано в печать 28.12.2020 г. в 15.00, по графику — в 15.00