ВЛИЯНИЕ КИБЕР-БЕЗОПАСНОСТИ НА СУВЕРЕНИТЕТ СТРАНЫ

и перспективы российско-вьетнамского сотрудничества

С.Довгий, руководитель направления СОРМ ООО "Ноябрьскнефтегазсвязь",
В.Колотов, д.и.н., заведующий кафедрой истории стран Дальнего Востока СПбГУ,
директор Института Хо Ши Мина СПбГУ,
Н.Сторожук, к.т.н., генеральный директор АО НПП "КОМЕТЕХ"

DOI: 10.22184/2070-8963.2019.83.6.42.48

Рассматривается влияние кибербезопасности на уровень суверенитета в современном мире; предлагается перечень первоочередных мер, применение которых может повысить уровень суверенитета страны. Проблемы рассматриваются на примере Вьетнама, который в последние годы показал очень высокую эффективность управления экономикой, однако в области сетевой и кибербезопасности до сих пор находится в зоне опасной уязвимости. Авторы полагают, что активизация сотрудничества в данной области с Россией позволит Вьетнаму оперативно снизить риски на наиболее опасных направлениях.

Постановка задачи

В настоящее время большинство стран – это пользователи современных технологий, управление которыми в случае необходимости может осуществляться удаленно, без ведома операторов, что может нанести ущерб критической инфраструктуре и национальной безопасности тех стран, руководство которых проявило преступную небрежность, а профильные ведомства показали свою профнепригодность.

В современном мире информационные технологии с каждым днем все больше меняют нашу жизнь, проникая практически во все сферы образования, производства, логистики, финансов, а также обороны и безопасности. Как это неоднократно происходило в истории человечества, наиболее развитые державы стремятся применить разработанные ими передовые технологии против отстающих, чтобы за их счет укрепить собственное геополитическое и экономическое положение. Увеличивающаяся разница в уровне цифрового развития ведет к тому, что останутся государства суверенные, которые смогут контролировать и защищать свое цифровое пространство, и все остальные, которым придется или смириться с рисками давления и грабежа, или идти на поклон к тем, кто может взять над ними "шефство" [1].

В наши дни киберпространство представляет собой сферу, над которой может быть либо установлен национальный суверенитет так же, как и над территорией, воздушным или морским пространством, либо власти страны могут принять решение передать контроль над своим киберпространством другой державе или вообще оставить

эту сферу на самотек (в такой стране уже не государство будет управлять процессами, а инициированные извне процессы).

Однако основная проблема цифровой безопасности – это не кибермошенничество, а кибервойна. В США и других странах полным ходом идет подготовка кибервойск. Предыдущий американский президент Барак Обама открыто угрожал атакой на российскую критическую инфраструктуру. Документы WikiLeaks показывают, как разрабатываются инструменты для кибератак. Думать, что они не будут применены, особенно в условиях все увеличивающейся напряженности, – наивно. Раньше, чтобы принудить противника сдаться, осаждали крепости и бомбили города. Теперь будут ломать платежные системы и индустриальные цифровые платформы [2].

Кибератака США на Венесуэлу, которая началась 7 марта 2019 года, свидетельствует о том, что эксперты не напрасно призывали к бдительности: мир практически вступил в новую эпоху кибервойн, где более развитые страны применяют современные кибертехнологии для подчинения более слабых стран.

Еще одним примером боевых кибердействий может служить решение президента США Дональда Трампа объявить чрезвычайное положение в телекоммуникационной сфере, закрывающее китайской компании Huawei доступ на рынок США. И это не сиюминутная прихоть. В сентябре 2018 года, когда была утверждена стратегия кибербезопасности США, помощник президента по нацбезопасности Джон Болтон заявил: "Мы идентифицируем и сдерживаем такое поведение в киберпространстве, которое противоречит международным интересам, но стараемся при этом обеспечить США сохранение преимущества в киберпространстве". Другими словами, американское правительство считает себя вправе запретить использование информационных технологий любой страны или компании, если они угрожают доминированию США в той или иной области. Нынешние санкции по отношению к Huawei вызваны не столько угрозами безопасности от закладок в оборудовании китайской компании, сколько возможным технологическим отставанием США [16].

Вьетнамская киберситуация

В Социалистической республике Вьетнам (СРВ) знают, что кибербезопасность является одним из наиболее слабых мест в стране, и вполне резонно полагают, что данный вопрос следует решать при поддержке России. Официальный визит Генерального секретаря Центрального комитета коммунистической партии Вьетнама Нгуен Фу Чонга в Российскую Федерацию в сентябре 2018 года активизировал сотрудничество двух стран в сфере кибербезопасности.

По информации вьетнамского Центра реагирования на компьютерные угрозы (ЦРКУ), в 2017 году было зафиксировано свыше 40 тыс. кибератак с совокупным ущербом более 400 млн долл. Только в Агрибанке киберпреступники взломали более 400 счетов [3]. Злоумышленники постоянно совершенствуют способы и инструменты атак. В группу риска в первую очередь попадают объекты государственной, банковской и промышленной инфраструктуры. Нападение может быть выражено заражением программами-вирусами, позволяющими киберпреступникам удаленно контролировать пораженные ресурсы. Подобные атаки могут иметь весьма тяжелые последствия для финансовых учреждений и компаний, занимающихся онлайн-платежами, поэтому таким структурам следует обратить особое внимание на защиту своих баз данных, предупреждают специалисты ЦРКУ.

По оценкам экспертов центра, сегодня уязвимость Вьетнама в области киберпреступности достигла высокого уровня. Часто злоумышленники получают через интернет доступ к интеллектуальной собственности, личным данным или денежным средствам. По данным специализирующейся на обеспечении информационной и сетевой безопасности вьетнамской компании BKAV, число случаев взлома и заражения вирусами локальных сетей и персональных компьютеров во Вьетнаме ежегодно увеличивается примерно на 10% [4].

В свою очередь, специалисты Ассоциации информационной безопасности (АИБ) Вьетнама отмечают, что большая часть интернет-страниц вьетнамских государственных учреждений и структур не имеют должной защиты от кибератак и могут быть взломаны в любую минуту. Так, в октябре 2014 года была проведена целенаправленная атака на крупнейшего хостинг-провайдера Vietnam Communications, когда несколько сайтов, размещенных на площадках компании, были выведены из строя. В 2019 году, по данным "Лаборатории Касперского", "вьетнамские пользователи сталкиваются более чем с 800 тыс. атак со стороны вредоносного кода, и 21,5% интернет-пользователей Вьетнама подвержены риску стать жертвами кибератаки" [5]. Одновременно с этим вьетнамские хакеры инициировали около миллиона кибератак только за последний квартал 2018 года [5].

Некоторые кибернападения синхронизированы со знаковыми геополитическими событиями. Например, в 2016 году вердикт Гаагского Третейского суда, признавшего юридическую несостоятельность претензий Пекина на единоличный контроль над островами в Южно-Китайском море, был широко поддержан правительствами и общественностью США, Японии и Филиппин. Во Вьетнаме также с одобрением отнеслись к решению суда, но подчеркнули, что выступают исключительно за мирное решение территориальных споров [6]. После этого хакеры группы 1937CN на несколько минут сумели заблокировать системы оповещения в международных аэропортах Ханоя и Хошимина и запустить на мониторах видеоролики со своей символикой и заявлением, что эти острова принадлежат КНР. Одновременно по системе звукового оповещения звучал мужской голос, который на английском языке критиковал позицию вьетнамских властей по спорным островам. Затем был взломан интернет-сайт авиакомпании Vietnam Airlines, национального авиаперевозчика Вьетнама, и на его главную страницу было выведено изображение, которое ранее демонстрировалось на мониторах аэропортов [7].

Дипломатические представительства Вьетнама в США, согласно информации Эдварда Сноудена, находятся под полным "киберколпаком" американских спецслужб [8].

Попытка правительства страны принять закон о сетевой информационной безопасности и разместить на своей территории сервер с данными, касающимися Вьетнама, стала одной из причин инспирированных извне беспорядков летом 2018 года, которые имели целью помешать принятию закона о сетевой безопасности и сохранить уязвимость. Однако об этом прямо не говорилось, и демонстранты выступали под лозунгами защиты свободы прав на информацию. Тем не менее с первого января 2019 года в СРВ этот закон вступил в силу, а его принятие, по заявлениям вьетнамских экспертов, связано с усилением подрывной деятельности иностранных спецслужб с целью расшатать политический режим. Кроме того, правительство СРВ озабочено нападениями хакеров, которые наносят существенный экономический ущерб.

Закон и вокруг закона

Закон о сетевой информационной безопасности предусматривает государственное регулирование деятельности по обеспечению информационной безопасности телекоммуникационных сетей, права и обязанности учреждений, организаций и частных лиц в ее обеспечении, подготовку соответствующих специалистов; построение сетей связи и управление ими с учетом требований информационной безопасности.

В законе продекларированы следующие принципы обеспечения информационной безопасности телекоммуникационных сетей [9]: обеспечивать информационную безопасность сети должны все государственные органы, организации и частные лица, а проводимые ими сетевые мероприятия должны соответствовать положениям законодательства, обеспечивающего национальную безопасность, сохранение государственной тайны, поддержание политической стабильности, порядка и безопасности; организации и частные лица не должны нарушать безопасность сетевой информации других организаций и частных лиц; обработка сетевых инцидентов информационной безопасности должна обеспечивать законные права и интересы организаций и отдельных лиц, не нарушать личную жизнь, отдельных лиц и не угрожать информации организаций; сетевые мероприятия по информационной безопасности должны проводиться регулярно, непрерывно, своевременно и эффективно [9].

Что касается вопросов на тему "вокруг закона", то в период его разработки и обсуждения вьетнамские власти оказались под давлением со стороны США и общественного мнения в стране. Эти две силы объединились "против режима и в защиту свободы слова и прав человека", что спровоцировало массовые беспорядки, демонстрации с нападениями на представителей органов власти и сил общественной безопасности. Протесты ориентирующихся на Вашингтон сил были не в последнюю очередь обусловлены тем, что этот закон поставил под угрозу деятельность американской агентуры во Вьетнаме (однако она по обыкновению прикрылась демагогией и протестами обманутых пропагандой народных масс).

Роль Сети в беспорядках

При организации массовых беспорядков во Вьетнаме (как и во многих других странах) активно использовалась сеть Интернет и социальные сети. Такая сетевая активность, предшествующая беспорядкам, имеет свою специфику, – и при должном уровне развития систем законного перехвата трафика у специальных служб легко отслеживается и блокируется, чего в 2018 году в СРВ сделано не было.

Опасения спецслужб США относительно усиления сил, обеспечивающих информационную безопасность стран, в которых они ведут активную работу, вполне оправданы. Например, китайская контрразведка смогла проникнуть в сеть, используемую ЦРУ для связи с завербованными в Китае агентами, что привело к разгрому агентурной сети в 2011–2012 годах. Из просочившихся в СМИ сведений стало известно, что для управления агентурой ЦРУ использовало секретную систему связи Covcom, которая имела слабую защиту и работала через сеть Интернет. Она во многом копировала аналогичную ближневосточную систему, где киберпротиводействие со стороны местных спецслужб менее активно. Контрразведка КНР смогла проникнуть в эту систему и, используя встроенные уязвимости, получила доступ к более широкой системе секретной связи с агентурной сетью ЦРУ в иных регионах мира. На Ближнем Востоке такая примитивная сеть без проблем выполняла свои функции, так как ближневосточные страны в области кибербезопасности имеют слабые позиции, а кибервойска КНР смогли взломать эту сеть и пресечь деятельность враждебной агентуры [10].

Москва и Ханой – за кибербезопасность

Руководство СРВ прекрасно понимает, что многие внутренние угрозы государству спровоцированы извне, что "эффективно противостоять внешнему давлению можно только сохраняя порядок внутри страны" [11, 9]. "Цель этой инспирированной извне нестабильности понятна: оказать давление на власти с целью консервации зависимости и отсталости Вьетнама в области защиты критической информационной инфраструктуры и национальной безопасности. Согласно законам жанра удары наносятся по самым слабым местам противника" [11, 9]. Поэтому для повышения внутренней стабильности страны перед лицом возможного усиления давления извне "необходима активизация сотрудничества с рядом зарубежных стран, в первую очередь с Российской Федерацией. Развитие отношений с Ханоем также отвечает интересам Москвы, особенно в период усиления западных санкций" [11, 10].

Как отмечено в [10–11], "Москва и Ханой заплатили высокую цену за сохранение своего суверенитета, поэтому его поддержание представляется первостепенной задачей. Россия и СРВ также имеют богатый опыт в области защиты национальных интересов и пользуются заслуженным авторитетом в сфере обеспечения своей безопасности".

Изучение вопросов кибербезопасности в целом и "анализ ситуации вокруг РФ и СРВ позволяют сделать вывод о том, что против этих стран по ряду направлений ведется классическая гибридная война, однако характер и интенсивность воздействия существенно различаются. При сравнении основных угроз в сфере национальной безопасности перед РФ и СРВ стоят следующие общие проблемы и задачи" [11–14]:

- "противодействие западной стратегии смены режимов" [11];
- "мониторинг ситуации при выявлении каналов оказания внешней финансовой и технологической поддержки оппозиционных сил" [11];
- "обеспечение территориальной целостности и противодействие сепаратистским проектам" [11];
- "противодействие международному терроризму" [11];
- "преодоление происходящего в последние годы ослабления торгово-экономических связей между нашими странами" [11];
- "противодействие информационным войнам! [11, 12] и фальсификации истории;
- "противодействие иным проявлениям "мягкой силы" противников российско-вьетнамского сотрудничества" [11, 12];
- "противодействие различным видам организованной преступности" [11, 13];
- "противодействие высокотехнологичным угрозам, в том числе профессиональной киберпреступности, а также кибернападениям на критическую инфраструктуру" [11, 13];
- "преодоление тенденции к снижению уровня научного и культурного сотрудничества между нашими странами" [11, 13];
- постепенное вытеснение из сетей связи и государственных информационных систем иностранного оборудования, произведенного большей частью в США и КНР, имеющего незадекларированные возможности тайного перехвата информации и внешнего управления средствами связи;
- "повышение качества управления на всех уровнях, которое в некоторых областях принимает критический характер" [11, 14].

В решении проблем кибербезопасности Россия в сравнении с Вьетнамом достигла на сегодняшний день лучших результатов. Правительством СВР поставлена задача в ближайшие годы укрепить позиции в сфере информационной безопасности, что может быть оперативно сделано с опорой на внедрение российского опыта и технологий в СРВ.

В свое время использование советских политтехнологий и военно-техническое сотрудничество позволили восстановить суверенитет Вьетнама [12] и завоевать подлинную независимость. В настоящее время можно сказать, что Вьетнам находится в положении "между молотом и наковальней", когда Пекин и Вашингтон, используя свое глобальное доминирование в области кибербезопасности и информационной безопасности, могут угрожать Ханою, и такие прецеденты с обеих сторон уже имели место. Укрепление сотрудничества с Москвой, которая не угрожает интересам Ханоя, в данных условиях стало бы полезным шагом на пути решения этой задачи, выгодным обеим странам. "Образ России как державы, которая успешно решает проблемы – как свои, так и чужие, – позволит выйти на качественно иной виток развития" [1]. Однако во Вьетнаме есть влиятельные силы, выступающие против укрепления сотрудничества с Россией в оборонной сфере; их представители полагают, что в нынешних условиях следует ориентироваться на Вашингтон [13]. Так, один из авторов данной статьи вскоре после конференции Валдайского клуба "Международное сотрудничество в неспокойном мире", которая прошла в Хошимине 25–26 февраля 2019 года, написал на вьетнамском языке для вьетнамской прессы статью о современных угрозах в области кибербезопасности, но вьетнамское издание не рискнуло печатать этот материал, полагая, что эксперт сгущает краски, и таких высокотехнологичных угроз реально не существует. Через два дня было совершено кибернападение на Венесуэлу. "Стратегия страуса", которая предполагает уход от реальных проблем в мир политкорректных иллюзий, не позволяет адекватно видеть и решать реальные проблемы в области национальной безопасности. Как показывает опыт Югославии, Ирака, Ливии, Венесуэлы и других, это сильно вредит самосохранению региональных стран на новом этапе "Большой игры".

Столпы суверенитета и опыт России

Опыт России и других государств, находящихся на верхних позициях в области обеспечения информационной безопасности, показывает, что любое государство для обеспечения собственного суверенитета должно иметь и эффективно управлять следующими информационно изолированными системами:

- сетью правительственной связи, подконтрольной исключительно высшему политическому руководству;
- сетью военной и специальной связи в интересах обороны, безопасности и обеспечения правопорядка;
- системой контроля безопасности критической информационной инфраструктуры, независимой от номинальных и реальных собственников такой инфраструктуры;
- системой законного перехвата, обеспечивающей поступление необходимой информации о пользователях сетей связи и информационных систем в интересах правоохранительных, следственных органов и специальных служб;
- системой контроля трансграничного трафика;
- системой радиоконтроля;
- системой управления сетями связи и критическими информационными системами в периоды чрезвычайных ситуаций, угрожаемый и военный периоды.

Российская Федерация обладает компетенциями, разработками и заделами, позволяющими предложить странам Юго-Восточной Азии экспорт как готовых решений (аппаратно-программных комплексов), так и компетенций для собственных разработок по всем перечисленным выше системам, а также для других задач кибербезопасности и противодействия иностранным техническим разведкам. Такие компетенции, разработки и заделы сложились на основе достижений фундаментальной и прикладной науки России и проверены в условиях реального противостояния с военными и специальными структурами коллективного Запада.

Накопленный в Российской Федерации опыт позволяет утверждать, что национальные сети связи, обеспечивающие взаимодействие органов государственной власти, объектов и субъектов критической информационной инфраструктуры, должны соответствовать следующим принципам:

- изолированности (такие сети связи должны быть информационно и физически изолированы от сетей связи общего пользования);
- интеграции (создание единой выделенной транспортной среды в интересах всех специальных и государственных потребителей с возможностью их информационного взаимодействия);
- централизации управления (применение единых административных, технических и правовых механизмов предоставления услуг связи специальным и государственным потребителям);
- максимальной сетевой разветвленности (заблаговременное создание и поддержание

функционирования единой транспортной среды с заданными параметрами целостности и устойчивости функционирования, обеспечивающей доступность услуг связи всем потребителям в условиях мирного времени, особого периода, чрезвычайного и военного положения).

Последние события в Венесуэле наглядно показали уязвимость стран, использующих в своей критической информационной инфраструктуре решения, в отношении которых по тем или иным причинам государственные структуры не убедились в невозможности их несанкционированного злонамеренного использования. Выполнить такую проверку могут только специально подготовленные национальные кадры в области информационной безопасности. Государства, которые не создадут систему подготовки таких кадров на собственной национальной территории, а также систему постоянного и эффективного контроля лояльности таких кадров, обречены на повторение сценариев, аналогичных блэкауту в Венесуэле.

В настоящее время в России приступили к созданию закрытой системы обмена цифровой информацией. Проект получил название "Мультисервисная транспортная сеть связи" (МТСС). Завершение первого этапа запланировано на конец 2019 года. Проект должен быть полностью готов через два года. Сеть строится на основе отечественного телекоммуникационного оборудования. МТСС будет изолирована от глобальной сети Интернет, а серверы хранения данных – располагаться на национальной территории. Сеть будет иметь собственные волоконно-оптические линии, поделенные на зональные магистральные каналы, электронный журнал идентификации пользователей и учета их действий. В "военном интернете" появится свой поисковик. Безопасность передачи данных обеспечит система мониторинга состояния оборудования и качества каналов, а также управления сетью под названием "Единый контур информационной безопасности" [14].

В построении подобной системы обмена цифровой информацией заинтересованы вьетнамские государственные структуры и силовые ведомства. Такая система может быть построена с учетом российского опыта и с применением российских технологий, технических решений и оборудования. Производство последнего имеет смысл развернуть на вьетнамской территории с параллельной организацией обучения специалистов.

Заключение

В последние годы между Россией и Вьетнамом подписан ряд межправительственных соглашений по вопросам сотрудничества в сфере информационной безопасности, целостности и устойчивости функционирования информационной инфраструктуры, в том числе сетей связи специального назначения. Сотрудничество в данной области взаимовыгодно: Вьетнам сможет существенно улучшить ситуацию с информационной безопасностью, а Россия – нарастить экспорт технологий и оборудования.

У руководства СРВ есть понимание: "проблемы в области безопасности могут быть решены только при поддержке РФ, но не КНР и США. Однако Москва на вьетнамском направлении действует менее активно, чем Пекин и Вашингтон, и поэтому постепенно сдает позиции более активным и амбициозным конкурентам" [11, 14]. "Активизация российско-вьетнамского сотрудничества может способствовать решению выявленных проблем в области безопасности, и это полностью соответствует долгосрочным национальным интересам обеих стран" [11, 14]. "Фактическое же ослабление связей между Москвой и Ханоем препятствует реализации политики "Поворота на Восток" в России и политики Обновления в СРВ. Данный процесс не только торпедирует решение как частных, так и общих проблем в области безопасности обеих стран, но и способствует ослаблению их позиций на международной арене" [11, 15].

В современном мире ни одна страна не в состоянии в одиночку справиться с нарастанием цифрового неравенства и киберугрозами, а также со связанными с этим угрозами суверенитету. Развитие сотрудничества в области противодействия современным киберугрозам между Москвой и Ханоем будет способствовать укреплению позиций наших стран в условиях уже начавшихся технологических войн и все более нарастающей кибертурбулентностью.

ЛИТЕРАТУРА

1. **Безруков А.О.** Спасти и сохранить. Россия как экспортер безопасности // Россия в глобальной политике. 2017. № 1. [Электронный ресурс] https://globalaffairs.ru/number/Spasti-i-sokhranit-18557
2. **Безруков А.О.** Мировое поле боя [Электронный ресурс] http://svop.ru/main/25438/
3. Более 400 счетов в крупном вьетнамском банке взломаны хакерами [Электронный ресурс] https://tass.ru/ekonomika/5162969
4. Во Вьетнаме зафиксирован высокий уровень угрозы кибератак на сайты банков [Электронный ресурс] https://densegodnya.ru/glavnye-sobytiya/article_post/vo-vyetname-zafiksirovan-vysokiy-uroven-ugrozy-kiberatak-na-sayty-bankov
5. Число кибератак на Вьетнам уступает лишь числу кибератак на Россию [Электронный ресурс] https://regnum.ru/news/2559489.html
6. Спор о Южно-Китайском море: суд в Гааге отверг права Пекина // РИА Новости [Электронный ресурс] https://ria.ru/20160712/1464640532.html
7. Китайские хакеры взломали систему оповещения в аэропортах Вьетнама [Электронный ресурс] http://biang.ru/ru/soczialnyie-seti/kitajskie-xakeryi-vzlomali-sistemu-opoveshheniya-v-aeroportax-vetnama.html
8. **Гринвальд Г.** Негде спрятаться. Эдвард Сноуден и зоркий глаз Дядюшки Сэма. – СПб: Питер, 2015. 320 с.
9. Закон СРВ о информационной безопасности сетей, № 86/2015/QH13 от 19 ноября 2015 г.
10. **Ардаев В.** Китай разгромил американскую разведку. США не могут понять, почему [Электронный ресурс] https://ria.ru/20180826/1527183366.html
11. **Колотов В.Н.** SWOT-анализ политики обновления во Вьетнаме и проблемы российско-вьетнамских отношений // Вьетнамские исследования. 2018. № 4. С. 5–18.
12. **Колотов В.Н.** Идеология Хо Ши Мина – духовный фундамент современной системы политической власти Вьетнама // Вьетнамские исследования. Вып. 7. – М.: ИД Форум, 2017 (в). С. 57–68.
13. **Ле Ван Банг**. США могут помочь сбалансировать силы в Южно-Китайском море [Электронный ресурс] http://viettimes.vn/viet-nam/cuu-dai-su-le-van-bang-my-co-the-giup-can-bang-luc-luong-bien-dong-55649.html
14. **Рябов К.** "Мультисервисная транспортная сеть связи" для Минобороны [Электронный ресурс] https://army-news.ru/2019/03/multiservisnaya-transportnaya-set-svyazi-dlya-minoborony/
15. **Колотов В.Н.** Навстречу XII съезду КПВ: анализ внутриполитической ситуации и международной обстановки. Вьетнамские исследования. Вып. 6. Вьетнам: 70 лет независимости. – М.: ИД Форум, 2016. С. 107–122.
16. **Комиссаров Д.** Ловушка глобализации: какие выводы следуют из санкций США против Huawei [Электронный ресурс] https://www.rbc.ru/opinions/business/ 24/05/2019/5ce6a8a09a79471c2317044a.


При поддержке:
Минкомсвязь России
НАТ
АТРП
NAT
EXPO
2019
5-7 НОЯБРЯ, 2019
МОСКВА, ВДНХ
www.natexpo.ru
www.facebook.com/groups/NATEXPO