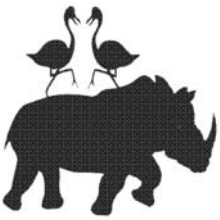

Андрей Колесников:

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РФ: СЛОЖНОСТИ И ПЕРСПЕКТИВЫ

Проблемы отражения киберугроз, защиты критической инфраструктуры, развития доменного пространства и обеспечения безопасности в интернете выходят на первый план в российской повестке дня. Эксперты, бизнес-лидеры и дипломаты стремятся понять, что ждет кириллическую доменную зону, требуется ли России новый доктринальный базис для обеспечения эффективной политики кибербезопасности и достигают ли своей цели недавние новации в отечественном законодательстве о безопасном интернете. Каковы приоритеты в перечисленных областях у администратора национальных доменов верхнего уровня .ru и .рф — Координационного центра национального домена сети Интернет (КЦ НДСИ)? Об этом мы побеседовали с директором КЦ НДСИ Андреем Колесниковым.

ИНДЕКС БЕЗОПАСНОСТИ: Координационный центр принимает активное участие в продвижении ряда сюжетов в области развития информационных технологий в РФ. Попадают ли в повестку КЦ НДСИ вопросы информационной безопасности, и если да, то в каком ключе? В частности, видит ли Координационный центр перед собой задачу участия в совершенствовании национального законодательства в области информационной безопасности, безопасного интернета?

КОЛЕСНИКОВ: Действительно, Координационный центр исторически принимает активное участие в обсуждении и решении вопросов обеспечения безопасности как в области интернет-инфраструктуры, так и в сфере информационной безопасности, хотя некоторые из этих функций и не вытекают напрямую из названия и уставных документов нашей организации. Однако все эти вопросы являются неотъемлемой частью обеспечения функционирования интернета, а наша непосредственная обязанность прежде всего состоит в обеспечении непрерывности оказания услуг доменной адресации, а также функционирования сети DNS российского сегмента интернета. Установленный показатель — 100% работоспособности разрешения доменных имен в зонах *.ru* и *.рф* вне зависимости от внешних и внутренних ситуаций. Второй важной областью деятельности КЦ НДСИ является анализ использования доменных имен в незаконных целях и борьба со *зловредами* (буквальный перевод англ. *malware*, вредоносные зловредные программы. — *Ред.*). К числу основных видов деятельности, предполагающей использование программного кода в злонамеренных целях, сегодня относится создание ботнетов, вирусов, а также фишинг и кибермошенничество. Координационный центр постоянно участвует в различных инициативах, в том числе законодательных, для повышения общего уровня кибербезопасности в Российской Федерации и противодействия данной деятельности.

ИНДЕКС БЕЗОПАСНОСТИ: Какие проекты и инициативы, связанные с повесткой информационной безопасности, развивает или планирует развивать в ближайшем будущем Координационный центр? Ведется ли сотрудничество Координационного центра с госорганами и экспертным сообществом, и если да, то по каким направлениям и каковы его результаты на сегодняшний день?

КОЛЕСНИКОВ: Одной из самых первых инициатив Координационного центра в области информационной безопасности был *День безопасного Интернета*, который впоследствии превратился в *Год безопасного Интернета*. Эта инициатива, которую мы начали совместно с Фондом Развития Интернет (ФРИ) в 2008 г., была поддержана многими компаниями-операторами и *хостерами*. По сути, именно она стала основой для множества других общественных инициатив, включая создание такой организации, как *Лига безопасного интернета*. КЦ НДСИ впервые предложил серьезные поправки в понятийный аппарат российских нормативно-правовых актов, так или иначе затрагивающих проблематику интернета, три года назад, в 2009 г. Однако на тот момент в силу различных обстоятельств предложенные поправки так и не были приняты.

Сегодня эксперты КЦ входят в различные рабочие группы, задействованные в работе по повышению качества законодательной базы в сфере информационной безопасности. Последний пример — принятие 139-ФЗ от 28 июля 2012 г.[1] и наши конкретные предложения касаются переноса фокуса фильтрации контента в соответствии с положениями закона с *уровня кабелей* на уровень интернет-приложений. В текущие поправки, которые были разработаны Российской ассоциаций электронных коммуникаций (РАЭК) и которые были поддержаны Координационным центром, наши предложения не вошли, так как они требуют расширения фактуры закона. Но рано или поздно методы и технологии приведут нас к подобным решениям — ведь речь идет о неизбежной эволюции интернета.

В части взаимодействия с правоохранительными органами нашим главным государственным партнером является Министерство связи и массовых коммуникаций РФ. КЦ НДСИ играет роль *центра компетенций* по многим вопросам, связанным с обеспечением безопасного функционирования сети интернет. Другим направлением в рамках деятельности Координационного центра является сотрудничество с МВД РФ и другими правоохранительными органами в рамках борьбы с киберпреступностью.

ИНДЕКС БЕЗОПАСНОСТИ: Видите ли Вы потребность в обновлении или пересмотре российской нормативной и доктринальной базы в области информационной безопасности на сегодняшний день? Если да, какие подходы и решения должны составлять основу такого документа? Предпринимает ли КЦ НДСИ какие-то действия в этом направлении?

КОЛЕСНИКОВ: С точки зрения экспертов Координационного центра, в России на сегодняшний день отсутствует сформулированный и закрепленный в каком-либо доктринальном или нормативно-правовом акте целостный подход к национальной проблематике кибербезопасности. Существует лишь ряд разрозненных документов, в которых просматриваются интересы различных ведомств в получении контроля над той или иной областью деятельности, такой как защита критической инфраструктуры, лицензирование операторов и т.д. Что касается Доктрины информационной безопасности Российской Федерации от 2000 г., добавить к ней что-либо и провести ее *модернизацию* не представляется возможным, так как документ морально устарел. В России не существует формального списка угроз безопасности киберпространства и матрицы приоритетов, необходимой для адекватной оценки этих угроз и управления ими.

Мы изучили опыт 11 ведущих *кибердержав* и пришли к неутешительному выводу: Российская Федерация серьезно отстала в области разработки и внедрения единых методов и стандартов обеспечения кибербезопасности. В Стратегии национальной безопасности Российской Федерации до 2020 г. и упомянутой Доктрине

повестке кибербезопасности практически не нашлось места. В частности, не урегулированы и нормативно не закреплены проблемы оперативной реакции на инциденты в информационных сетях, использование интернета в криминальных целях и т.д. Подход к этой проблематике должен принципиально отличаться от традиционных для России практик с выраженным приоритетом роли специальных служб и вооруженных сил. Например, в вышеупомянутой Стратегии определено, что национальную безопасность обеспечивают именно армия и силовые структуры; практически идентичный посыл несет Доктрина.

Нам нужен другой подход, близкий к тем, которые сегодня используются в Великобритании и других странах Евросоюза, в США, Китае, Японии, Бразилии и многих других странах. Кибербезопасность должны обеспечивать все участники национальных интернет-отношений сообща — от рядовых пользователей до руководителей страны. Что особенно важно, в обеспечении кибербезопасности должен принимать активное участие бизнес.

В этой связи России необходима прежде всего *Стратегия кибербезопасности* верхнего, национального уровня, в которую будет входить список из конечного и конкретного списка задач, которые необходимо решать, а также сроки, к которым их надо решить. Нужны не общие слова, а конкретика. И исполнителями этой стратегии должны быть не только государственные органы и органы власти, а все задействованные и заинтересованные стороны, включая граждан в частном качестве. Зачатки этого подхода можно увидеть в недавнем документе по вопросам защиты объектов критической инфраструктуры[2]. Хотя и в нем, опять-таки, *торчат уши* вполне конкретных ведомств, а указанные ориентиры по срокам вызывают удивление. Так, появление в России системы обнаружения кибератак на критическую информационную инфраструктуру запланировано только в период с 2017 до 2020 г., то есть через пять-восемь лет! Между тем уже два года назад вирус *Stuxnet* показал, какой ущерб может быть нанесен критической инфраструктуре лишь при помощи компьютерного кода. Следует помнить о том, что за прошедшее время арсенал кибероружия лишь увеличился и обогатился еще более сложными разработками. В то же время российская критическая инфраструктура сложнее и *разветвленнее* иранской, и уже поэтому нам следует быть готовыми к отражению подобных угроз сейчас, а не в среднесрочной перспективе.

ИНДЕКС БЕЗОПАСНОСТИ: 12 июля 2012 г. на сайте Совета безопасности РФ был опубликован очередной документ[1], посвященный вопросам защиты критической инфраструктуры в РФ. Входят ли вопросы безопасности критической инфраструктуры, включая инфраструктуру глобальной сети и ее российского сегмента, в круг приоритетов КЦ НДСИ? Какие угрозы безопасности инфраструктуры интернета существуют в РФ в настоящее время?

КОЛЕСНИКОВ: Координационный центр обеспечивает работоспособность одного из главных критических элементов инфраструктуры Сети — системы доменной адресации. При этом специалисты КЦ стабильно демонстрируют стопроцентную доступность сервиса, что является одним из наших ключевых приоритетов. Используя передовые технологические и методические подходы к построению географически распределенного сервиса, мы полностью исключили возможность злонамеренного влияния на сети извне и изнутри. В ближайшее время мы поднимем уровень доверия и защиты от подмены доменных ресурсов внедрением протокола DNSSEC [Domain Name System Security Extensions], обеспечивающего цепочки доверия между серверами DNS. Хотелось бы выразить надежду, что основные стратегические инфокоммуникационные системы в Российской Федерации используют столь же надежные методы и подходы.

Мы считаем, что проблематика кибербезопасности выходит далеко за пределы вопросов регламентирования доступности государственных служб и структур через интернет, равно как и сетевого обмена для обеспечения информационного взаимодействия госструктур. Напротив, доступность и безопасность электронных коммуникаций потребителей с банками и другими финансовыми учреждениями,

системами интернет-торговли, системами электронных платежей, ведущими СМИ, социальными сетями, мультимедийными порталами и другими интернет-сервисами вызывает бо́льшую озабоченность у общества, чем недоступность, например, сайта органа федеральной или муниципальной власти.

Оценивая актуальность тех или иных проблем в российской повестке кибербезопасности, мы бы предложили следующую иерархическую шкалу:

- во-первых, отсутствие стратегических планов решения проблем кибербезопасности, отсутствие единой политики кибербезопасности России и опасность внутриведомственной борьбы в этой области;
- во-вторых, отсутствие единого механизма управления вопросами кибербезопасности в России
- в-третьих, низкая грамотность в области безопасного использования интернета, как дома, так и на работе;
- в-четвертых, отсутствие законодательно закрепленных требований по обеспечению безопасности информационной инфраструктуры бизнеса, в том числе в критически важных областях, например в сфере инфокоммуникаций;
- наконец, как следствие вышеперечисленного, отсутствие последовательной и *прагматичной* внешней политики в области управления интернетом, направленной на защиту конкретных интересов Российской Федерации в трансграничном киберпространстве.

ИНДЕКС БЕЗОПАСНОСТИ: Насколько успешным и оправданным Вы считаете опыт внедрения и использования кириллической доменной зоны *.рф*? Каковы перспективы дальнейшего развития кириллического сегмента Рунета? Считаете ли Вы повсеместное развитие локальных алфавитных доменных зон, таких как кириллическая, арабская и иероглифическая — фундаментальной тенденцией развития интернета, и если да, не повлечет ли она фрагментацию и потерю единства глобальной сети?

КОЛЕСНИКОВ: Запуск домена *.рф* для Российской Федерации, а также иероглифической доменной зоны. 中国 для КНР, арабской доменной зоны и других корневых доменов на национальных языках, а точнее алфавитах, отражает естественный процесс эволюции адресного пространства интернета. При этом данный процесс не несет в себе фундаментальной тенденции потери единства глобальной сети. Мы сталкиваемся с действием своеобразного *фактора Вавилона,* перенесенного в виртуальное пространство. Здесь важно помнить, что Рунет говорит по-русски со времен своего появления, и появление кириллических доменов лишь закрепляет языковую специфику российского сегмента Сети, не придавая ему каких-либо фундаментально новых качеств.

Домен *.рф* с момента запуска является одним из наиболее успешных среди, с одной стороны, проектов интернационализированных нелатинских доменов верхнего уровня, а с другой стороны — проектов развития Рунета, к воплощению которых был непосредственно причастен КЦ НДСИ. Главная проблема интернет-компаний, госструктур и пользователей в странах, работающих с интернационализированными нелатинскими доменами верхнего уровня, заключается в опыте использования программ и приложений, задействованных в интернете, таких как электронная почта, поисковые машины, приложения социальных сетей и т.д. Такая проблема характерна не только для Рунета, но и для интернет-сегментов КНР и арабских стран. Однако я считаю, что это всего лишь вопрос времени и уже через два-три года никто не заметит разницы в обработке названий доменов на латинице и на нелатинских алфавитах.

ИНДЕКС БЕЗОПАСНОСТИ: Какова позиция Координационного центра в отношении недавно принятого закона 139-ФЗ? Какое техническое решение в отношении

блокировки контента, подпадающего под запрет в соответствии с положениями закона, Вы считаете оптимальным? В частности, как Вы оцениваете организационную, финансовую и техническую готовность российского интернет-сектора к широкому применению технологии DPI (deep packet inspection) с целью соблюдения положений 139-ФЗ?

КОЛЕСНИКОВ: *Во-первых*, мы считаем появление закона в отношении защиты детей воплощением закономерного *социального заказа* граждан России. Формирование такого заказа является знаком того, что интернет стал частью повседневной жизнь большинства граждан России. *Во-вторых,* имплементация этого заказа в букве закона в разделе, регламентирующем доступ к онлайн материалам, представляется Координационному центру неверной в части выбора алгоритма ограничения доступа к материалам, подпадающим под запретительные нормы законодательства. Мы считаем, что появление фильтров-посредников между *источник*ом и *потребителем,* логически, технологически и юридически не связанных ни с первым, ни со вторым, может повлечь труднопредсказуемые последствия с точки зрения организации и функционирования интернет-связи. Кроме того, подобный способ ограничения доступа абсолютно неэффективен в отношении организации связи с использованием защищенных протоколов и *туннелей* HTTPS/SSL и других подобных средств.

Но самой главной логической ошибкой в выборе метода блокировки мы считаем игнорирование того факта, что сегодняшняя Сеть предоставляет практически неограниченные возможности для бесплатного воспроизведения и тиражирования (репликации) контента, доступ к которому предполагается блокировать по тому или иному конкретному адресу в интернете. При этом в законе полностью отсутствуют какие-либо методы борьбы с *первоисточником*, то есть непосредственным производителем подобного рода материалов. Мы полагаем, что 139-ФЗ должен эволюционировать, чтобы превратиться в эффективное орудие защиты детей от ненадлежащего контента в Сети. Чтобы закон мог исполнять такую функцию, в само его *тело*, равно как и в подзаконные акты, в дальнейшем необходимо будет вносить определенные коррективы. Такие коррективы должны быть направлены прежде всего на использование фильтрации на абонентских устройствах и на уровне интернет-приложений, обеспечивающих потребителя информацией: поисковых машин, интернет-браузеров, семейных фильтров, встроенных в операционные системы, и т.д. При этом фильтрация контента должна быть максимально *смысловой* и в минимальной степени зависеть от инфраструктуры и места размещения незаконного контента. Мы активно сотрудничаем с Лигой безопасного интернета в выборе наиболее действенных методов смысловой категоризации информации в интернете и ведем достаточно активную лабораторную деятельность по изучению новых методов определения тематической составляющей с такими учеными, как Симон Кордонский и Валерий Бардин.

Думаю, что техническая готовность к исполнению закона будет обеспечена без особых проблем, так как у операторов есть возможность выбора методов фильтрации. Злоупотребления и неточность исполнения будут видны моментально. Но неблагодарное дело строить предположения, пока не появилась практика исполнения этого закона. В любом случае необходимо будет смотреть на конкретные случаи применения закона в течение достаточно длительного времени, как минимум одного года. Очевидно, что оператором так называемого реестра *черного списка* будет Лига безопасного интернета, так как именно эта организация выступает локомотивом внесения ограничений в интернете для детей. И, по всей видимости, тема *списков* будет развиваться и, как мне кажется, следующий логичный шаг — это переоценка методов, используемых в *школьной* фильтрации.

Подход, который предписывает операторам *закрывать* доступ к ресурсам, предполагает использование оборудования, необходимого для глубокой проверки информационных пакетов (DPI) и обещает быть весьма затратным. Очевидно, что закон и его разработчики нуждаются в постоянной *обратной связи* с представителями интернет-сектора и экспертного сообщества, для корректировки слабых мест

в тексте закона и повышения эффективности методов фильтрации. Необходимо также следить за случаями неизбирательного применения. Крайним примером здесь мог бы служить принцип блокировки противоправного контента по доменному имени. В случае с ФЗ-139 речь шла бы о полной остановке деятельности таких крупных сервисов и ресурсов, как *LiveJournal, YouTube, Facebook, Twitter* на территории Российской Федерации из-за единственной записи в аккаунтах кого-либо их пользователя, которая нарушала бы положения закона и не была бы удалена вовремя. Мы с интересом следим за развитием сюжета, связанного с размещением фильма *Невинность мусульман* на *YouTube*.

К сожалению, в России имеются прецеденты временной блокировки подобных ресурсов из-за несоответствия контента, загруженного пользователями, нормам российского законодательства. И хотя до сих пор такие случаи не были связаны с действием 139-ФЗ, каждый из них наносил определенный ущерб интернет-сектору. Даже сутки блокировки *LiveJournal* в отдельно взятом регионе чреваты для сервиса значительными репутационными и финансовыми рисками. В этом смысле чрезвычайно важно уточнить нормы 139-ФЗ на уровне подзаконных актов, чтобы свести к минимуму *сопутствующий ущерб* от применения закона и *неизбирательную* блокировку крупных сервисов, не несущих ответственности за действия пользователей. В этой связи Координационный центр поддерживает разработанные РАЭК и компанией *Яндекс* поправки к 139-ФЗ, так как их цель состоит в сокращении неизбежного ущерба от подобного применения 139-ФЗ.

Примечания

[1] Федеральный закон Российской Федерации от 28.06.2012. № 139-ФЗ «О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации».

[2] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Информационная безопасность, Национальная безопасность России. Совет Безопасности Российской Федерации, http://www.scrf.gov.ru/documents/6/113.html (последнее посещение — 11 сентября 2012 г.).