Издаётся с 1924 года

РАДИО®

10•2024

МАССОВЫЙ ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

"Радиолюбитель"—"Радиофронт"—"Радио"

"Radio" is monthly publication on audio, video, computers, home electronics and telecommunication

12+

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ:
АНО «РЕДАКЦИЯ ЖУРНАЛА «РАДИО»
Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.
Регистрационный ПИ № ФС77-82030

Главный редактор В. К. ЧУДНОВ
Редакционная коллегия:
А. В. ГОЛЫШКО, А. Н. КОРОТОНОШКО, К. В. МУСАТОВ,
И. А. НЕЧАЕВ (зам. гл. редактора), Л. В. МИХАЛЕВСКИЙ,
С. Л. МИШЕНКОВ

Выпускающий редактор: С. Н. ГЛИБИН
Обложка: В. М. МУСИЯКА
Вёрстка: Е. А. ГЕРАСИМОВА
Корректор: Т. А. ВАСИЛЬЕВА

Адрес редакции: 129090, Москва, Протопоповский пер., 25, к. Б
Тел.: (495) 607-31-18.
E-mail: **ref@radio.ru**
Приём статей — e-mail: **mail@radio.ru**
Отдел рекламы — (495) 607-31-18; e-mail: **advert@radio.ru**
Распространение — (495) 607-31-18; e-mail: **sale@radio.ru**
Подписка и продажа — (495) 607-87-39
Бухгалтерия — (495) 607-87-39

Наши платёжные реквизиты:
получатель — АНО "Редакция журнала "Радио", ИНН 7708187140,
р/сч. 40703810538090108833
Банк получателя — ПАО Сбербанк г. Москва
корр. счёт 30101810400000000225 БИК 044525225
Подписано к печати 24.09.2024 г. Формат 60×84 1/8. Печать офсетная.
Объём 8 физ. печ. л., 4 бум. л., 10,5 уч.-изд. л.
В розницу — цена договорная.

Подписной индекс:
Официальный каталог ПОЧТА РОССИИ — П4014;
КАТАЛОГ РОССИЙСКОЙ ПРЕССЫ — 89032.

Отпечатано в ОАО «Подольская фабрика офсетной печати»
142100, Моск. обл., г. Подольск, Революционный проспект, д. 80/42.
Зак. 03572-24 .

О суверенном Интернете

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Первый шаг — установить, что нечто возможно, затем появится вероятность".

Илон Маск

Казалось бы, Интернет и суверенный — это слишком разные и даже вполне себе взаимоисключающие понятия. Тем более, что поверх него существует и работает практически всё, что основано на информационных технологиях (ИТ) — от простых ИТ-сервисов на госуслугах до сетей связи и всей мировой цифровой валюты. И всё было бы хорошо, если бы современные войны не стали гибридными и не превратили Интернет в ещё одно поле боя, причём практически полностью в поле зарубежное. И это является сегодня для нашей страны одним из серьёзнейших рисков с точки зрения функционирования хотя бы экономики.

В рамках международного военно-технического форума "Армия-2024" телерадиокомпания "Звезда" проводила круглый стол на тему "Информационное противоборство в условиях СВО: борьба за коллективное сознание общества с использованием передовых технологий и цифровых СМИ". На этом мероприятии президент ГК InfoWatch Наталья Касперская, в частности, заявила: "К сожалению, мы очень сильно зависим от западных технологий, и та ситуация с импортозамещением, которая у нас началась в 2015 г., не доведена до конца. Поэтому во многих системах, особенно в оборудовании, мы очень сильно зависим от Запада. Если бы Запад хотел нам объявить кибервойну, то нет ничего проще, эту инфраструктуру выключить, и у нас бы почти всё перестало работать совсем. Например, смартфоны и операторы связи. Это самый простой способ".

К сожалению, Интернет не является безопасной средой. Это не парк с освещением, лавочками, мощёными дорожками и охраной на входе. Интернет, по мнению Натальи Касперской, не раз озвученному в ходе её выступлений, скорее, напоминает дикий лес с кровожадными зверями, где от любой опасности (деструктивные группы, наркотики, вовлечение в противоправную деятельность) — всего один шаг. По её словам, сейчас агрессия против России ограничивается кибератаками и киберпреступлениями. Сейчас доля страны в мировом объёме конфиденциальных данных составляет 10 %. К 2023 г. были зарегистрированы 1024 крупные утечки данных, каждая из которых включает не менее 1 млн записей.

Согласно прогнозам компании Positive Technologies, специализирующейся на разработке решений в сфере информационной безопасности, в наступившем году многие отечественные компании будут отдавать приоритет устранению уязвимостей. Будет расти общее количество инцидентов за счёт роста эксплуатации этих уязвимостей. Уязвимости в ИТ-отрасли будут влиять на киберустойчивость многих других отраслей, от государственных организаций до сферы услуг, через которую можно атаковать и всю цепочку поставок. Очевидно, что и национальная критическая информационная инфраструктура также ощутит на себе рост угроз. В общем, прогноз во многом ожидаемый.

Да и за мошенниками во время информационной войны ожидаемо могут скрываться сами знаете кто.

Впрочем, Интернет был небезопасен и просто по рождению. Новые компьютерные технологии, использующие стек протоколов TCP/IP, были разработаны для межкомпьютерных связей. Однако на рубеже тысячелетий именно ими всемирная телекоммуникационная индустрия окончательно заменила технологии телекоммуникационные, потому что думать о том, как всё это будет работать в условиях тяжёлого трафика, соблюдения норм качества (QoS), фрода и многомиллионной абонентской базы, было некогда и особо некому — хотелось денег, и побыстрее. Ранее весьма продолжительное время это развитие ограничивали "неуклюжие" в части передачи данных телефонные сети и системы на базе коммутации каналов. Это серьёзно тормозило процесс, потому что люди попросту не могли мыслить за пределами небогатого набора услуг, предоставляемых телефонными компаниями. Отчасти сетевая "революция" на базе интернет-технологий заключалась в смене "телефонного" мышления на цифровое мышление и коммутацию пакетов. Тут и выросли "крылья" у Интернета, WWW и социальных сетей.

Сама идея, что устройства могут быть связаны между собой, появилась в конце 50-х годов прошлого века, причём идеи создания огромной межкомпьютерной сети возникали отнюдь не только на родине Интернета. В 1959 г. кибернетик Анатолий Китов представил Хрущёву свой план по созданию в СССР общей вычислительной сети. Кибернетик разработал план "Красная книга" по созданию ЕГСВЦ — единой государственной сети вычислительных центров. Вычислительные машины в Советском Союзе должны были объединиться в единую компьютерную сеть с высокой (для того времени) производительностью. В военное время мощности ЕГСВЦ могли использоваться для военных нужд, а в мирное работали бы как система управления национальной экономикой и различными хозяйственными подразделениями.

В 1962 г. математик и кибернетик Виктор Глушков представил Хрущёву свой проект по созданию национальной сети, вдохновившись проектом Китова. Общегосударственная автоматизированная система учёта и обработки информации (ОГАС) должна была стать "мыслящей" сетью. С помощью воплощённого в жизнь проекта Глушкова можно было бы управлять в режиме реального времени экономикой СССР.

Оба проекта, к сожалению, завершились ничем и, тем не менее, заслуживают отдельной статьи. Ну, а в конце 60-х было создано первое соединение между узлами сети ARPANET, и приложившая к этому свою "руку" DARPA (Defense Advanced Research Projects Agency или Управление перспективных исследовательских проектов Министерства обороны США) стала той организацией, в недрах которой была создана сеть Интернет. В начале 80-х в Интернете стала использоваться связка TCP/IP, а в начале 90-х Тимоти Джон Бернерс-Ли предложил идею всемирной паутины — World Wide Web. Потом Элон Ганор сделал первый шлюз из телефонной сети в IP-сеть. И понеслось...

Однако с тех пор проблемы новых сетей лишь накапливались и усиливались, их латали и затыкали. К примеру, транспортный протокол TCP, который согласно своему алгоритму при потере какого-либо пакета из общего кадра во имя поддержки качества передачи осуществляет повторную передачу всех пакетов, отнюдь не идеален. Это как если с грузовика, гружённого коробками, упала одна коробка, потребителю везли бы новый грузовик. Прошли годы, объёмы и скорости передаваемого сегодня трафика вряд ли ожидал кто-нибудь 20 лет назад. И вот там, где эти огромные потоки сталкиваются, к примеру, в ЦОДах, закономерно возникают проблемы пропуска трафика, потому что тот самый алгоритм TCP банально тормозит работу этих центров управления "инфокоммуникационной вселенной". Впрочем, дадим слово профильным специалистам.

В финальном техническом отчёте "Архитектура Интернета будущего поколения", выпущенном Исследовательской лабораторией BBC Рим, Нью-Йорк, за авторством Дэвида Кларка (один из отцов Интернета), Карен Соллинс, Джона Вроцлавски и др., включая специалистов Лаборатории компьютерных наук и ИИ Массачусетского технологического института и др. научных учреждений от конца 2003 г., сказано следующее: "Мы считаем, что наибольший прогресс сегодня обусловлен краткосрочным мышлением. Множество мелких изменений, которые предлагается внести в Интернете для исправления конкретных сиюминутных проблем, предлагаются без общего видения того, какой должна быть сеть в будущем. Первоначальный дизайн Интернета появился почти 30 лет назад во времена, которые предшествовали персональному компьютеру и локальным сетям. Волоконная оптика ещё не вышла из лаборатории, самая быстрая коммерчески доступная линия связи имела скорость около 50 кбит/с, а компьютеры не были массовыми. Индустрия связи была определена ролью оператора AT&T как регулируемого монопольного поставщика телефонных услуг. Очевидно, что с тех пор многое изменилось с точки зрения технологий, компьютерного контекста, в котором находится Интернет, и более широкого социального воздействия, которое оказывают компьютеры и сети".

"Первоначальный дизайн Интернета был описан как прозрачный: то, что входит, то и выходит. Сеть не отслеживает, не фильтрует и не преобразует передаваемые ею данные; она не обращает внимания на содержимое пакетов. Эта прозрачность, возможно, была единственным наиболее важным фактором успеха Интернета, потому что прозрачность позволяет развёртывать новое приложение без необходимости изменять ядро сети. С другой стороны, прозрачность также облегчает доставку атак безопасности, вирусов и других нежелательных данных. Когда сеть была небольшой, а между пользователями существовала высокая степень доверия, сила прозрачности перевешивала связанные с ней риски. Сегодня развёрнуты такие устройства, как брандмауэры (межсетевые экраны), чтобы разрушить прозрачность путём блокирования неизвестного трафика. И сегодня мы видим как пользу, так и опасность таких устройств, как брандмауэры, потому что становится намного сложнее развёртывать новые приложения в Интернете из-за того, что брандмауэры могут блокировать их. Мы пришли к выводу, что интернет-сервис должен быть более регулируемым, чем-то, что мы имеем сегодня: прозрачным среди пользователей, которые предпочитают доверять друг другу, но крайне ограниченным среди пользователей, которые этого не делают. Эта прозрачность, основанная на доверии, должна стать базовой службой доставки нового Интернета".

"Когда Интернет только зарождался, предполагалось, что интересы большинства пользователей совпадают. Различные группы пользователей хотели бы общаться и делали бы это на основе взаимного желания. Но сегодня мы видим, что заинтересованные стороны в интернет-пространстве часто имеют интересы, которые являются неблагоприятными или конфликтующими. Пользователи хотят вести приватный разговор, в то время как правоохранительные органы хотят иметь возможность осуществлять законный перехват. Пользователи хотят защиты от спама, а спамеры пытаются обойти их средства защиты. Пользователи, вступившие в сговор, делятся музыкой; правообладатели пытаются предотвратить это. Борьба между этими различными интересами происходит по-разному: в дискуссии по протоколу, в законодательстве и регулировании, в технических решениях различных групп пользователей и поставщиков и т. д. Эти конфликты могут помешать повышению безопасности сети".

"В оригинальном Интернете каждый пакет полностью самоопределяется. Он содержит полные адреса источника и получателя и может быть переадресован без какой-либо настройки или сигнализации. Этот режим работы не должен быть утрачен, иначе мы потеряем возможность обмениваться пакетами с небольшими накладными расходами. Однако цели прозрачности, регулируемой доверием, и другие аспекты безопасности, наряду с целью обеспечения качества обслуживания и другими аспектами обслуживания, предполагают, что при некоторых обстоятельствах в сети будет больше состояний, связанных с конкретными потоками пакетов. Интернет должен иметь возможность плавно переключаться между различными режимами доставки с различным уровнем контроля в сети".

"Первоначальный Интернет предполагал наличие единого глобального адресного пространства. Адреса служат двум целям — они предоставляют как указание на местоположение

конечной точки, так и указание на её идентичность. Мы пришли к выводу (как и многие другие), что эти предположения необходимо переосмыслить. Проект новой схемы местонахождения и личности является важнейшим архитектурным требованием вопросам безопасности, мобильности, маршрутизации и региональной автономии... Мы провели исследования... Мы утверждаем, что можно разделить идеи местоположения и идентификации, обе из которых представлены IP-адресом в современном Интернете и что результирующая архитектура облегчает мобильность, а также решает другие проблемы, связанные с современной сетью".

"По соображениям управления и безопасности Интернет отказался от единого глобального адресного пространства, хотя формального признания этого в архитектуре не было. Мы пришли к выводу, что на самом деле нет принципиальной необходимости в таком глобальном адресном пространстве, хотя следствием отказа от него является большая сложность в установлении сеанса приложения и меньшая однородность в управлении сетью и диагностике неисправностей. Однако сеть без единого глобального адресного пространства вполне осуществима, и она отвечает практическим потребностям. Будущий Интернет должен проектироваться без требования глобального адресного пространства".

В общем, многое было понятно уже сравнительно давно. В 2007 г. во время выступления перед национальным научным обществом США Дэвид Кларк сказал, что "архитектура сети, созданная 30 лет назад, имеет фундаментальные проблемы дизайна, и эти проблемы неизбежно будут накапливаться со временем. Поэтому нужно создавать новую архитектуру с нуля".

По словам Бернерса-Ли, список назревших проблем включает наметившийся отказ от защиты принципов "сетевого нейтралитета", поддельные новости, наметившиеся успехи пропаганды и растущая поляризация сетевого общества. Сетевой нейтралитет (Net Neutrality) — принцип, согласно которому провайдеры интернет-услуг не должны отдавать предпочтений какому-то одному классу интернет-приложений или задач — сообщению от бабушки, сериалу или банковскому переводу. В США в своё время её окрестили как "первая поправка Интернета", не дающая привилегий никому. Тимоти Бернерс-Ли никогда не скрывал своего мнения о том, что его детище — Мировая Сеть, всегда являлась прямым отражением человечества и в хорошем смысле, и в плохом, и даже в ужасном. Тем не менее, его восприятие Сети в качестве "открытой платформы, позволяющей всем и каждому открыто делиться информацией, обеспечивающей доступ и возможности сотрудничества без географических границ", в последнее время всё больше подвергается испытаниям ввиду возросшей мощи крупных провайдеров, всё чаще вооружённых разрушительными алгоритмами манипуляции.

Учитывая изложенное выше, специалисты разрабатывают свои решения Интернета будущего (FI — Future Internet). Такие проекты есть в ЕС, в США, в Японии, в Индии и других странах. В частности, КНР активно участвует в будущих исследованиях архитектуры Интернета, уделяя особое внимание тестовым стендам, связанным с IPv6. Китай построил крупнейшую инфраструктуру тестирования будущего Интернета (FI) для поддержки эволюции будущего Интернета с участием ИИ и сетей мобильной связи 5G. В целом США, Европа, Япония, Корея и КНР имеют программы, в рамках которых выполняются от 5 до 20 проектов FI. Индия, Бразилия, Пакистан, ЮАР и ещё порядка 70 стран объявили о наличии проектов в этом направлении.

Ну, хорошо, люди во многих странах работают над улучшением Интернета с самых разных сторон, защищают, развивают, дополняют. А что у нас? Что произошло в этой сфере с тех пор, как во времена Хрущёва сгинули упомянутые выше проекты, неоспоримые преимущества которых, будь они реализованы, явственно видны из дня сегодняшнего?

Прошло 60 лет. В результате всеобщей цифровизации и последующей цифровой трансформации на базе созданного у нас появились мультисервисные сети, информационное общество, цифровые двойники, всевозможные роботы, ИИ и пр. Информация стала основой всего, вплоть до экономики и обороны. А кто владеет информацией, тот... Ну, вы понимаете. Впрочем, сегодня он может её поток и прервать. И кто-то только думает, что чем-то владеет.

Исследование лаборатории Citizen Lab на базе университета Торонто говорит, что в Китае даже есть, чем ответить на информационные атаки с помощью так называемой "Великой пушки" для совершения DDoS-атак. И речь идёт не только о "китайском" Интернете, потому что она позволяет атаковать любые сайты, расположенные в любой точке мира. Таким образом, мы видим, что Китай прошёл огромный путь в попытках взять Интернет под свой контроль и определённо добился определённых успехов, используя ИТ-инфраструктуру, созданную когда-то DARPA.

К примеру, в КНР существует проект "Золотой щит" (The Golden Shield Project), имеющий неофициальное название "Великий Китайский файрвол" (Firewall — межсетевой экран/брандмауэр), который не позволяет спокойно посмотреть на территории КНР YouTube, а также использовать Telegram, Twitter и др. Это многоуровневая система защиты национальной информационной инфраструктуры.

На первом уровне осуществляются блокировка IP-адресов и перехват DNS (примерно с 2002 г.) с помощью "чёрных списков". Файрвол перехватывает ответ от DNS (Domain Name System — система доменных имён Интернета) и отправляет его далее пустым, в результате чего зайти на сайт не удаётся.

На втором уровне производятся проверка пакетов и фильтрация ключевых слов (примерно с 2007 г.). Весь интернет-трафик в Китае дублируется и анализируется специальной системой IDS (Intrusion Detection System) или Системой обнаружения вторжений, которая в случае необходимости инициирует процесс сброса соединения. Если же автоматическая система не справляется, ей на помощь приходит специальное подразделение интернет-полиции, насчитывающее несколько десятков тысяч сотрудников.

На третьем уровне осуществляется блокировка способов обхода (примерно с 2008 г.), а именно прокси-серверов, VPN и Тора. При этом история Китайского файрвола и, к примеру, постоянно модифицирующегося Тора, это как Инь и Ян или история вечной борьбы снаряда и брони. Говорят, что уже к 2020 г. в Китае было заблокировано около 311 тысяч сайтов (при этом около 10 % ошибочно — "лес рубят, щепки летят").

А пока интенсифицируются информационные войны, в том числе и против нашей страны. Казалось бы, теперь уже у России есть шансы на собственные разработки в области FI, решающие вопросы сетевого ускорения, нагрузки, информационной безопасности, адресации и пр. Но кто-нибудь слышал о чём-либо подобном в части каких-нибудь госпрограмм? А в части столь активно развивающегося импортозамещения? Нелишне заметить, что импортозамещение касается не только оборудования и программного обеспечения, но и алгоритмов, по которым, к примеру, осуществляется соединение или передача информации.

А если в ИТ-инфраструктуре что-нибудь изменить в рамках движения к FI, чтобы попытки тех же DDoS-атак в рамках сетевых войн стали попросту бессмысленными, потому что в сети принципиально другая адресация, другой значительно более эффективный транспортный протокол, а выход в обычный Интернет осуществляется через межсетевые шлюзы? Чтобы туда — свободно, а оттуда — под контролем. Очевидно, тут многое можно придумать с дифференциацией по пакетам, по адресам, по принципам взаимодействия и пр., если серьёзно заняться этим вопросом. Интересно, а кто-нибудь у нас занимается FI? К сожалению, если что и есть, то оно всё равно играет на "чужом поле" и существует поверх чужой инфраструктуры.

Однако есть предположение, что главным препятствием для подобных разработок будет преодоление нежелания ими заниматься несмотря на очевидные в текущей ситуации вещи. Как рассказывали коллеги, посещавшие в своё время калифорнийскую Кремниевую долину, местные ИТ-специалисты на вопрос о необходимости модернизации Интернета для "заделки" всех обнаруженных в нём "дыр" отвечали, что хорошо понимают это, что вопрос назрел, что над ним надо обязательно работать и менять IP-инфраструктуру. Напротив, разговаривая о том же с отечественными интернетчиками, они получали ответ, что всё замечательно, что ничего менять не

надо, всё же работает и пр. Вы что, хотите балканизации Интернета (термин придуман на фоне распада Югославии)? Создавалось впечатление, будто вот эта Сеть дарована нам богом (американским, разумеется), и наше дело лишь уметь с ней обращаться. Не зря же мы подготовили за много лет именно для этого выпускников различных вузов. Всё это очень созвучно недавним решениям из прошлого по необходимости наличия отечественных заводов, самолётов, продуктов, различного оборудования и пр. — мол, мы всё купим! Ну, а когда гром грянул и пришло осознание, что не всё можно решить за деньги, поняли, что это было банальным предательством, спохватились и занялись-таки импортозамещением. И небезуспешно, между прочим.

Конечно, кое-какие опасения существуют, и не зря же в РФ проводились учения на случай отключения нашего сегмента сети от Интернета. С другой стороны, скорее всего, никто пока "из-за бугра" не собирается этого делать. А зачем? Когда вся наша ИТ-инфраструктура построена на базе разработок вероятного (впрочем, уже реального) противника, этому противнику должно всё нравиться. А не нападает он, возможно, просто потому, что время не пришло включать какую-нибудь очередную "пушку". Все агенты влияния, шпионы, номерные колонны и пр. на связи. Да и американская система "Эшелон" (как и другие подобные системы), работающая уже более 70 лет по глобальному перехвату информации, сегодня наверняка использует интернет-ресурсы.

А вы развиваете Интернет Вещей? — Отлично! Значит, скоро будет доступ и ко всем этим вещам. Говорят, они будут исчисляться миллиардами...

Почему наши танкисты не используют танковую платформу "Леопард" или "Абрамс"? Почему наши лётчики не летают на базовых решениях корпорации "Локхид"? Почему вместо автомата Калашникова не используем "Узи"? Ответ очевиден даже не военным и даже не инженерам. Почему, к примеру, разработан целый комплекс отечественных операционных систем типа AstraLinux и пр., несмотря на столь замечательный Windows? Почему приснопамятная проблема 2000 (кто помнит) была максимально эффективно решена в РВСН? Потому, что там ничего управляющего не было подключено к Интернету, а самая эффективная защита — это рубильник или смена правил игры.

А почему тогда базовая инфраструктура связи, без которой сегодня уже практически ничего в стране не работает, остаётся полностью на импортных идеях и алгоритмах? Мы её уже купили в таком виде навсегда? Ждём, когда нам свой FI предложит действующий противник? А ведь он предложит, будучи уверен — а куда мы денемся?

Пока же из каждого утюга мы слышим, что ИТ и цифровизация — это наше всё. Но достаточно отключить связь, как не будет ни ИТ, ни "цифры". А потому пора уже думать об отечественном суверенном Интернете, чтобы ни одна... Ну, вы понимаете.

Как выразился однажды Илон Маск, историю пишут победители, а проигравшие редактируют Википедию. И не выбрасывайте раньше времени бумажные справки.

По материалам

Валов С. Г., Голышко А. В. Инфокоммуникационные сети будущего: общие принципы. — Вестник связи, 2003, № 2, с. 52—61;

https://dzen.ru/a/YN8xnbr0tDnTU9Yf?ysclid=m00vac15wy97496326;

https://www.isi.edu/newarch/iDOCS/final.finalreport.pdf;

https://www.cnews.ru/news/top/2017-11-20_otets_vsemirnoj_pautiny_o_ee_budushchem_sistema?ysclid=lqxlecsfrk700498728;

https://www.mdpi.com/1999-5903/15/5/166

Приём статей: mail@radio.ru
Вопросы: consult@radio.ru