Введение

От цифровой экономики никуда не спрячешься, как от кубинской игуаны: она видит и днем, и ночью.

- ☑ Программа «Цифровая экономика» как новый План ГОЭЛРО
- ☑ Промышленность средств связи в России разрушена
- ☑ Сеть IP/MPLS — главные линии связи страны: а если это кибербомба?
- ☑ Наступает кибервойна
- ☑ Отсутствие системных исследований по телекоммуникациям
- ☑ О чем эта книга?

Программа «Цифровая экономика» как новый План ГОЭЛРО

Когда-то словосочетание «План ГОЭЛРО» было известно каждому школьнику. Государственный план электрификации России — это детище Октябрьской революции и лично В.И. Ленина. План был разработан в декабре 1920 г. и ставил задачи ускоренного развития народного хозяйства.

Сегодня судьба ставит перед Россией новый вызов. 3 апреля 2017 г. Президент Российской Федерации Владимир Путин утвердил рабочую группу Экономического совета по направлению «Цифровая экономика». Цифровая экономика — это грандиозное, по замыслу, государственное движение, предполагающее разработку своего рода «нового плана ГОЭЛРО». Станет ли это движение базой модернизации России — покажет ближайшее будущее. Цифровая экономика в мире развивается быстрыми темпами — 10 % в год, что более чем в три раза выше показателя глобального экономического роста. Многие понимают, что цифровая экономика может способствовать экономическому росту и устойчивому развитию. Корпорация Huawei составила Индекс глобальной связанности 2016 г., который показывает уровень цифровой экономики по странам* . Страны были рас-

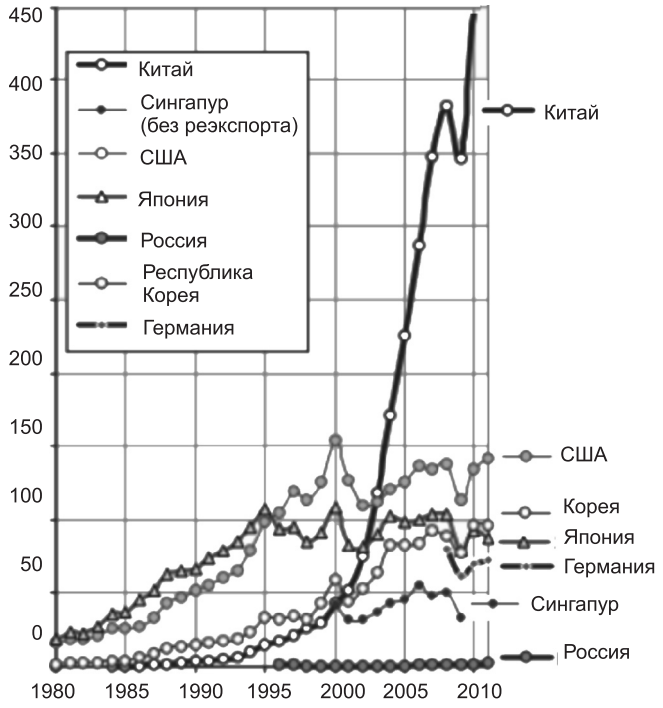
* Цифровая экономика для устойчивого экономического роста //Мосты, Volume 9, Number 4, 20 June 2016 www.ictsd.org/

пределены по трем группам: лидирующие, проходящие адаптацию и начинающие. Первую группу возглавили США, Сингапур и Швеция. В середине второй группы расположились Китай (23-е место), Россия (26-е место) и Бразилия (30-е место).

Задача правительства России — войти в группу лидирующих стран по цифровой экономике. Удастся ли это сделать в ближайшем будущем — не ясно. Пока «новый план ГОЭЛРО» не составлен.

Промышленность средств связи в России разрушена

В настоящее время подавляющее большинство средств связи в России имеют иностранное происхождение. Действительно, на базе лучшего иностранного оборудования можно строить современные сети. Но, к сожалению, эта стратегия приводит к зависимости от этих компаний на необозримое будущее. И как быть с безопасностью страны, как преодолеть международные санкции?



Объемы экспорта офисного и телекоммуникационного оборудования в мире, млрд долл.*

* http://kaivg.narod.ru/exp.pdf/ Retrieved: Mar, 2018.

Например, сети «Ростелекома» недавно были ареной борьбы «за сферы влияния» двух американских компаний — Cisco и Juniper. С ними конкурирует китайская компания Huawei. Рисунок раскрывает состояние мирового рынка телекоммуникационного оборудования. Участие России тут близко к нулю. В последнее десятилетие лидирует Китай — и в большой мере за счет того, что производство этого оборудования США перенесли в Китай. А ведь в советское время было мощное Министерство промышленности средств связи.

Вчитываясь в текст Программы цифровой экономики (ЦЭ), естественно, возникает чрезвычайно важный вопрос: обеспечит ли она возрождение отечественной промышленности средств связи?

Сеть IP/MPLS — главные линии связи страны: а если это кибербомба?

Важнейшим проектом компании «Ростелеком» является высокоскоростная IP-магистраль, которая построена полностью на изделиях американской компании Juniper. IP-магистраль построена на базе первичной сети по технологии MPLS (Multi-protocol Label Switching) и обеспечивает конвергенцию услуг по передаче видео, речи и данных. IP/MPLS-инфраструктура имеет свыше 350 точек доступа на всей территории России, десять опорных и около 150 региональных узлов в регионах РФ. Использованы магистральные маршрутизаторы Juniper T1600 производительностью до 1,6 Тбит/с и менее мощные пограничные маршрутизаторы. Общая протяженность магистральной сети составляет более 40 тыс. км, пропускная способность достигает 1 Тбит/с, емкость внешних каналов составляет 200 Гбит/с. Компания присутствует как на зарубежных узлах (в Стокгольме, Лондоне, Гонконге, Франкфурте, Амстердаме), так и имеет сеть собственных дата-центров в Москве, Казани, Екатеринбурге, Новосибирске, Хабаровске.

Компания, конечно, имеет необходимые сертификаты информационной безопасности на используемое оборудование, тем не менее использование импортных систем для критических приложений всегда будет вызывать, по крайней мере, настороженность.

Наступает кибервойна

Разоблачения Сноудена. Благодаря разоблачениям Э. Сноудена (Washington Post, 30.98.2013), стало известно о шпионской программе GENIE, разработанной Агентством национальной безопасности (АНБ), которая проникает в зарубежные сети и ставит их под контроль США. Точнее, речь идет об отделе TAO (Tailored Access

Сеть IP/MPLS — гордость «Ростелекома»

Operations, Отдел специализированного доступа). К концу 2013 г. было заражено как минимум 85 тыс. стратегических серверов. Сейчас АНБ внедряет более мощную систему — TURBINE, которая будет управлять имплантами для сбора разведывательной информации в автоматическом режиме. К началу 2014 г. она заразила до 100 тыс. серверов*. Система TURBINE составляет основу крупнейшей программы кибервойны Quantum, которую АНБ реализует в содружестве с телефонными операторами и пользуясь услугами мощной серверной сети. Головной офис Quantum находится в штаб-квартире АНБ (Форт Мид, штат Мэриленд), а отделения — в Японии и Великобритании.

Пентагон взломал командную систему России**. Такое сенсационное сообщение недавно появилось в прессе. Пентагон получил доступ в командную систему армии и спецслужб России и довольно уверенно там себя чувствует. Об этом сообщил неназванный источник в американском военном ведомстве. Как сообщают из Пентагона, — это ответ на взлом правительственных серверов российскими хакерами в США. «Военные хакеры США внедрились в электросети и телекоммуникации России, а также в командную систему Кремля, сделав их уязвимыми для атаки с помощью секретного американского кибероружия, если США сочтут это необходимым.» Об этом сообщил высокопоставленный представитель разведки.

Пятый театр военных действий. Под таким названием американский журналист написал книгу о кибервойне***, собрал в ней множество тревожных сведений. В качестве простейшего примера приводится взлом сотовых телефонов. Во время иракской войны армейские операторы взламывали сотовые телефоны повстанцев и отправляли им дезинформирующие сообщения, поскольку воевали с повстанцами на поле боя именно сухопутные войска. Однако у кибервоинов из военно-воздушных сил тоже имеются навыки проведения подобного рода дезинформации, и нет никаких причин, которые бы помешали им вступить в игру в случае, когда армейские

---

* From Turbine to Quantum: Implants in the Arsenal of the NSA // GENERAL SECURITY, MARCH 24, 2014. http://resources.infosecinstitute.com/turbine-quantum-implants-arsenal-nsa/

** Пентагон взломал командную систему России — СМИ. Ноябрь 5, 2016. http://rusjev.net/2016/11/05/pentagon-vzlomal-komandnuyu-sistemu-rossii-smi/ Retrieved: Mar, 2018.

*** Шейн Харрис. Кибервойна. Пятый театр военных действий. — М.: Альпина нон-фикшн, 2016. https://e.rutlib4.com/book/17272/p/6

были бы заняты в других сражениях. Аналогично военно-морской киберсолдат, обученный тому, как взломать навигационную систему вражеской подводной лодки или «поджарить» корабельный радар, может произвести разрушения и в коммерческой телекоммуникационной сети.

Внедрение вирусов в самолеты. Китайцы разработали метод внедрения компьютерных вирусов по беспроводной связи в системы трех моделей самолетов, которые ВВС США используют для ведения наблюдения и разведки. Атака осуществляется посредством электромагнитных волн и направлена на бортовые системы наблюдения, которые их излучают. Это очень изобретательная тактика и потенциально крайне разрушительная: такой удар может вывести из строя системы управления самолетом, что приведет к его падению.

Северная Корея недосягаема. Единственной задачей, с которой хакеры из ТАО не могут справиться, является шпионаж в странах, ограничивающих выход в Интернет. Именно поэтому Северная Корея оказалась за пределами досягаемости этого элитного подразделения.

Кибервойна с Китаем. Китай — это одна из наиболее важных целей АНБ для слежки и планирования кибервойны. И хотя китайские власти пошли на все, чтобы контролировать доступ в Интернет и активность пользователей в Сети в пределах страны, Китай все же огромная, технологически развивающаяся страна, и это делает ее уязвимой.

ТАО успешно проник в китайские компьютерные и телекоммуникационные сети почти 15 лет назад. Секретные документы АНБ показывают, что агентство выбрало целью сети компании Huawei, крупнейшего в мире производителя телекоммуникационного оборудования. Руководители разведки и законодатели в США подозревают, что Huawei работает в интересах военных и разведывательных служб Китая. Поэтому контролирующие органы США запретили установку телекоммуникационного оборудования Huawei, включая коммутаторы и маршрутизаторы: из-за опасения, что оно будет использовано в качестве каналов связи для кибершпионажа.

Кибервойна в Ливии. Во время американской военной операции в Ливии в 2011 г., которая привела к отстранению от власти Муаммара Каддафи, АНБ сотрудничало с киберсолдатами ВМС для поиска целей в Ливии и оказания помощи в создании «ударных пакетов». Хакеры находили цели в реальном мире с помощью радиосигналов электронных устройств, а затем передавали координаты

ударной группе ВМС, находившейся на американском военном корабле Enterprise.

Siemens — посредник в кибервойне США. Работа компьютерного червя Stuxnet, который уничтожил центрифуги на иранском ядерном производстве, была построена на неизвестной ранее уязвимости в системе управления, используемой компанией Siemens. Эксперты по компьютерной безопасности задавались вопросом: может быть, производитель знал об этой уязвимости и согласился оставить ее неисправленной? В любом случае АНБ, несомненно, обладало какой-то детальной информацией о слабых местах и использовало ее при создании червя Stuxnet.

Цель кибервойны — глобальные сети. В рамках программы SIGINT Enabling Project АНБ платило телефонным и Интернет-компаниям, чтобы они при строительстве своих сетей оставляли лазейки для агентства или, если использовать менее понятный язык секретного документа, «обеспечивали непрерывное сотрудничество с основными поставщиками телекоммуникационных услуг для формирования глобальной сети с целью приобретения набора доступов».

Вся эта секретная работа подчеркивает степень зависимости АНБ от корпораций, которые производят программное и аппаратное обеспечение, а также владеют сегментами глобальной сети и обслуживают их. Без кооперации с такими компаниями агентство, в общем-то, не смогло бы вести шпионскую и кибервоенную деятельность. Однако попытки агентства занять доминирующее положение на «пятом театре» военных действий не ограничивались только заключением сделок с частными корпорациями.

Отсутствие системных исследований по телекоммуникациям

Телекоммуникации представляют собой яркий пример технологий двойного применения. В мирное время телекоммуникации входят в сферу ответственности сил гражданской обороны и, по идее, должны обеспечивать мобилизационную готовность населения на случай чрезвычайных ситуаций. В военное же время системы связи могут перейти под полный контроль военного ведомства. По крайней мере службы Ростелекома как федерального оператора должны иметь двойное подчинение и, например, при крупных чрезвычайных мероприятиях Центры обслуживания вызовов Ростелекома, а также сети мобильных операторов должны работать на нужды МЧС.

Чем характерен текущий момент в российской отрасли связи, в отрасли народного хозяйства, важнейшей как для гражданских,

так и специальных нужд*:

- полноценные системные исследования путей модернизации сетей связи не ведутся в России, как минимум, два десятилетия;
- операторы связи и Поставщики услуг копируют решения, принятые в других странах, без адекватной оценки их положительных и отрицательных сторон;
- не учитывается приемлемость иностранных решений для различных групп пользователей, прежде всего сетей специального назначения.

О чем эта книга?

В программе «Цифровая экономика Российской Федерации» определены цели и задачи в рамках пяти базовых направлений развития народного хозяйства на период до 2024 г.:

- нормативное регулирование;
- кадры и образование;
- формирование исследовательских компетенций и технических заделов;
- информационная инфраструктура и
- информационная безопасность.

Мы ограничимся в основном обсуждением одного из пяти направлений Программы — «Информационная инфраструктура». Но так как информационная инфраструктура охватывает все народное хозяйство, то, в определенном смысле, она является решающим звеном всей цифровой экономики, т. е. затрагивает и остальные четыре раздела Программы.

В Главе 1 рассмотрена суть программы «Цифровая экономика», подробно перечислены ближайшие задачи информационной инфраструктуры и указано на головную роль «Ростелекома» в создании информационной инфраструктуры. Так как в Программе основной упор делается на доступ к сети Интернет и ориентация идет на использование двух новейших технологий: мобильной связи пятого поколения 5G и сети LPWAN, то они описаны подробнее.

Глава 2 посвящена критике программы «Цифровая экономика», в том числе необходимости разработки новой версии закона «О связи» (что относится к разделу «Нормативное регулирование»), необходимости введения открытых интерфейсов для реализации воз-

---

* *Соколов Н.А.* Системные аспекты построения и развития сетей электросвязи специального назначения // International Journal of Open Information Technologies. 2014. Т. 2, № 9. С. 4–8.

можностей технологии Bigdata. Указывается на отставание по элементной базе, что препятствует реализации проекта «Промышленная Россия 4.0» и созданию технических средств информационной инфраструктуры (что относится к разделу «Формирование исследовательских компетенций и технических заделов»).

Программа «Цифровая экономика» ориентируется на развитие сети Интернет, т. е. на всестороннее развитие сети пакетной коммутации. Но существующие сети связи до сих пор в значительной мере сохраняют средства коммутации каналов. В Главе 3 анализируется российский опыт перехода от коммутации каналов к коммутации пакетов. Изложены исторические факты о создании Единой автоматизированной сети связи СССР (ЕАСС), о началах АСУ в СССР, о разработках АТС в советское время. Изложен опыт цифровизации сетей: как внедряли ОКС-7 в постсоветской России, указано на неиспользованные особенности российской интеллектуальной сети (можно было обойтись без протокола INAP, что существенно упростило бы разработку новых услуг). Указано на важнейший факт в мире связи: «Ростелеком» переходит на пакетную коммутацию, хотя, конечно, средства коммутации каналов еще сохранятся на долгое время.

Глава 4 посвящена отдельным фактам цифровой трансформации сетей связи в мире, что важно учесть при создании информационной инфраструктуры цифровой экономики — особенно из-за чрезмерного увлечения сетью Интернет. Показаны тенденции развития коммутационной техники, проведено сравнение маршрутизаторов и электронных АТС по стоимости (разработка маршрутизаторов обходится почти в 10 раз больше стоимости электронных АТС, в то же время маршрутизаторы бесспорно упрощают сети доступа). На примере анализа капитальных затрат новой архитектуры IP-сети американского оператора AT&T показано, что на магистральной сети (в случае России — это связь между УАК) выгодно сохранить режим коммутации каналов.

Глава 5 посвящена развитию информационных сетей Пентагона. В силу открытости документов Пентагона, с одной стороны, и учитывая практическую неограниченность финансовых ресурсов, с другой, опыт развития информационных сетей Пентагона может оказаться чревычайно поучительным при создании информационной инфраструктуры цифровой экономики. В 1996 г. было принято решение о построении информационных сетей на основе изделий Bell Labs, т. е. применять каналы ISDN, сеть SS7 и строить интеллектуальную сеть. Ныне — через 20 лет после тех судьбоносных

решений — удивительно, что сеть SS7 сохраняет роль «нервной» системы информационных сетей Пентагона.

Глава 6 посвящена важнейшей программе модернизации информационных сетей Пентагона — переходу на IP-протокол (этот опыт может оказаться весьма поучительным для строителей информационной инфраструктуры цифровой экономики, ориентированной полностью на пакетную коммутацию). Перечислены пять ключевых информационных сетей Пентагона. Рассказано об отличиях между сигнализацией SIP и новой сигнализацией AS-SIP, разработанной специально по заказу Пентагона. Подробно рассказано о многофункциональном софтсвиче MFSS как основе перехода от TDM к IP, о ведущей роли комплекса Session Controller, который обеспечивает как все имеющиеся ранее «старые» услуги, так и запланированные «новые» информационные услуги. Описана целевая архитектура единой информационной сети Пентагона и указано на одно досадное обстоятельство: не удается полностью уйти от коммутации каналов, так как на правительственной сети DRSN сохраняются каналы ISDN — как средство подключения так называемых «красных» телефонов. Отсюда следует важная мораль для программы «Цифровая экономика»: вряд ли все средства связи в России удастся перевести в область Интернета.

Глава 7 посвящена конкретной области цифровой экономики — экстренной службы, точнее, разбору опыта создания службы 112 и аппаратно-программного комплекса «Безопасный город»в России и сетей NG911 и FirstNet в США. Характерно, что все они испытывают похожие трудности. Подробно анализируется мировой опыт по обеспечению кибербезопасности критической инфраструктуры (что относится к разделу «Информационная безопасность»).

Книга завершается главой 8 «Цифровая экономика: чему учить?» и относится к разделу «Кадры и образование» программы «Цифровая экономика Российской Федерации». Рассмотрены предложения для учебного курса по M2M и IoT, дан обзор существующих в мире учебных курсов, подробно рассмотрена Программа MIT и высказаны предложения по ее усовершенствованию в области технологий программирования. Рассказано о содержании первой в России программе MBA по специализации «Цифровая экономика», предложенной институтами МГИМО и МФТИ.