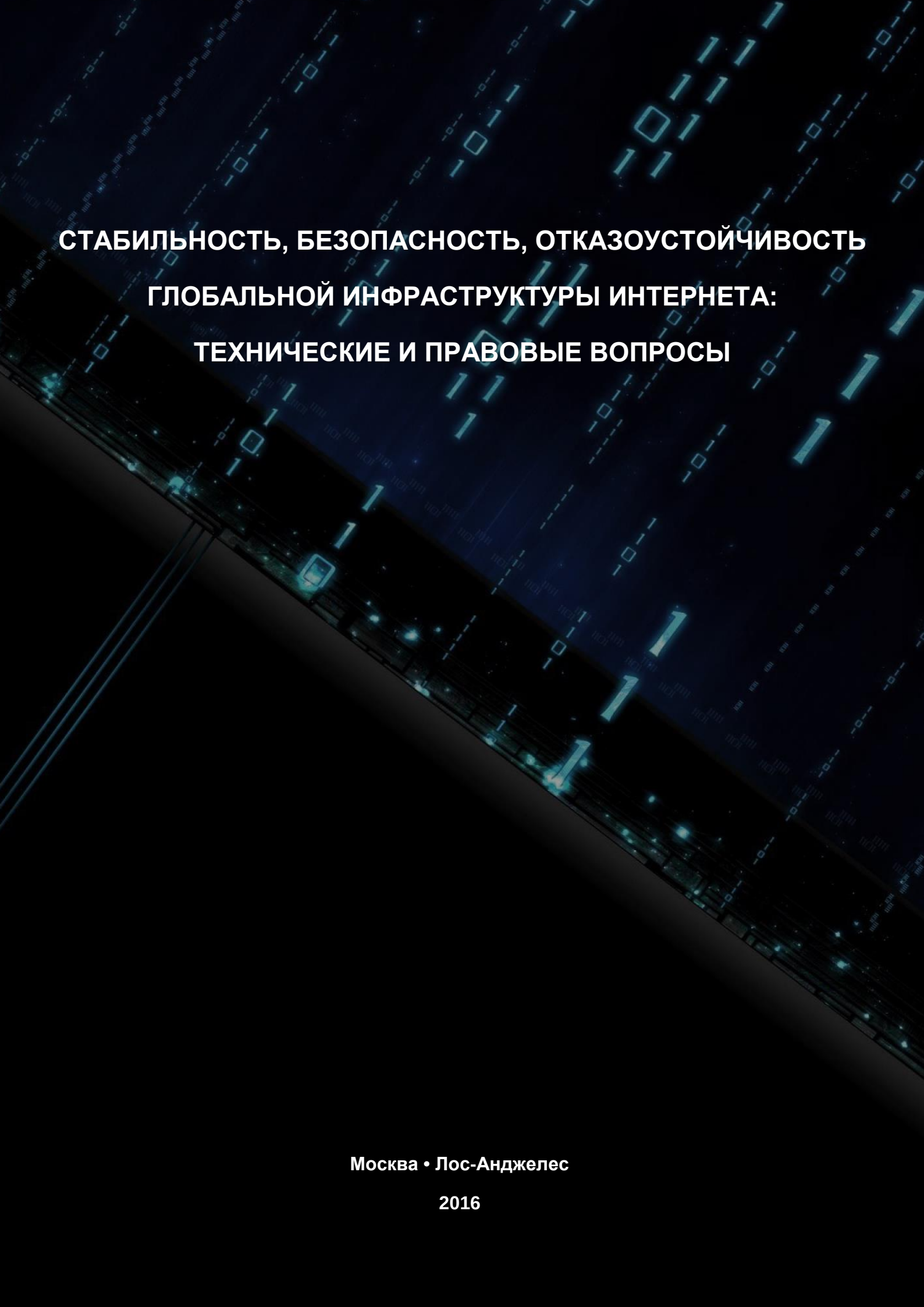


СТАБИЛЬНОСТЬ, БЕЗОПАСНОСТЬ, ОТКАЗОУСТОЙЧИВОСТЬ ГЛОБАЛЬНОЙ ИНФРАСТРУКТУРЫ ИНТЕРНЕТА: ТЕХНИЧЕСКИЕ И ПРАВОВЫЕ ВОПРОСЫ

Москва • Лос-Анджелес

2016

Доклад «Стабильность, безопасность, отказоустойчивость глобальной инфраструктуры Интернета: технические и правовые вопросы» был подготовлен в 2015-2016 гг. инициативным экспертным коллективом с участием российских и американских представителей. Доклад адресован российскому и международному техническому и отраслевому сообществу, а также исследователям и экспертам, чья сфера профессиональных интересов охватывает организационно-правовые и технические аспекты функционирования и управления системой уникальных идентификаторов Интернета.

В работе над докладом в составе экспертного коллектива приняли участие:

- М.А.Медриш, директор Фонда поддержки интернет (координатор экспертного коллектива, редактор доклада);
- О.В.Демидов, консультант ПИР-Центра;
- А.А.Кульпин, старший научный сотрудник Института проблем информационной безопасности МГУ имени М.В.Ломоносова;
- П.Л.Пилюгин, старший научный сотрудник Института проблем информационной безопасности МГУ имени М.В.Ломоносова;
- А.А.Сальников, старший научный сотрудник Института проблем информационной безопасности МГУ имени М.В.Ломоносова;
- Санджай Гоел, старший доцент Университета штата Нью-Йорк в Олбани (SUNY);
- Пол Мора, партнер Hunton & Williams LLP.

Экспертный коллектив также выражает признательность за участие в редакторской работе над докладом, предоставлении рецензий и отзывов:

- Е.А.Валовой, менеджеру проектов Фонда поддержки интернет;
- В.В.Ященко, заместителю директора Института проблем информационной безопасности МГУ имени М.В.Ломоносова;
- Патрику Джонсу, старшему директору по глобальному взаимодействию с заинтересованными сторонами Корпорации Интернета по распределению имен и адресов (ICANN);
- Дэвиду Сатола, ведущему советнику по вопросам ИКТ Всемирного Банка;
- Ли Хиббарду, координатору по вопросам интернет-политики Совета Европы;
- Джорджу Шаркову, национальному координатору по кибербезопасности при правительстве Республики Болгария;
- Джонатану Эскин, директору Brooklyn Law Incubator & Policy Clinic.

Все должности членов экспертного коллектива и иных упомянутых участников работы над докладом указаны на момент участия в работе над докладом.

Оглавление

Сокращения и аббревиатуры:

BGP – Border Gateway Protocol (Протокол граничного шлюза)
ccTLDs – Country-code Top Level Domains (страновые домены верхнего уровня)
CIR – Critical Internet Resources (критические ресурсы Интернета)
DNS – Domain Name System (система доменных имен)
ICANN – Internet Corporation for Assigned Names and Numbers (Корпорация Интернета по распределению имен и адресов)
IAB – Internet Architecture Board (Совет по архитектуре Интернета)
IEEE – Institute of Electrical and Electronics Engineers (Институт инженеров по электротехнике и электронике)
IETF – Internet Engineering Task Force (Рабочая группа по проектированию Интернет)
IP – Internet Protocol (интернет-протокол; IP-протокол)
ISOC – Internet Society (Общество Интернета)
ISO – International Standardization Organization (Международная организация по стандартизации)
ISP – Internet Service Provider (интернет-провайдер)
ITU – International Telecommunications Union (Международный Союз электросвязи)
gTLDs – Generic Top-Level Domains (домены верхнего уровня общего назначения)
MSU (MGU) – Lomonosov Moscow State University (Московский государственный университет имени М.В.Ломоносова)
NATO – North Atlantic Treaty Organization (Организация Североатлантического договора, НАТО)
NIST – National Institute of Standards and Technology (Национальный институт стандартов и технологий)
NTIA – National Telecommunications and Information Administration (Национальная администрация по телекоммуникациям и информации)
OSCE – Organization for Security and Co-operation in Europe (Организация по безопасности и сотрудничеству в Европе)
RFC – Request For Comments (Запрос комментариев)
RIR – Regional Internet Registry (Региональная регистратура Интернет)
SCO – Shanghai Cooperation Organization (Шанхайская организация сотрудничества)
SSR – Stability, Security and Resiliency (стабильность, безопасность и отказоустойчивость (СБО))
TCP/IP – Transmission Control Protocol / Internet Protocol (Протокол управления передачей/Интернет-протокол; набор сетевых протоколов передачи данных TCP/IP)
TSIG – Transaction SIGnature protocol (протокол Подписи транзакции)
UN – United Nations (Организация Объединенных Наций, ООН)
W3C – World Wide Web Consortium (Консорциум Всемирной Сети)
WIPO – World Intellectual Property Organization (Всемирная организация интеллектуальной собственности)
WSIS – World Summit on the Information Society (Всемирная встреча на высшем уровне по вопросам информационного общества)
UII – Unique Identifiers of the Internet (уникальные идентификаторы Интернета)

Примечание:

Текст доклада отражает ситуацию в рассматриваемой области по состоянию на **1 марта 2016 г.** и может не отражать последующих изменений в части практик и политик, правовых и административных механизмов, технических стандартов и институциональных преобразований в области обеспечения безопасности, стабильности и отказоустойчивости глобальной системы уникальных идентификаторов Интернета. В том числе в докладе не рассматривается развитие процесса передачи ответственного управления функциями Администрации адресного пространства Интернет (IANA) от правительства США глобальному сообществу заинтересованных сторон с момента и после направления итоговых Предложений Координационной группы по передаче координирующей роли в осуществлении функций IANA (ICG) Национальной администрации по телекоммуникациям и информации (NTIA) США в марте 2016 г.

Раздел 1. Введение

Интернет как глобальная сеть сетей, устройств и информации, в начале XXI века стал одним из ключевых факторов развития человеческой цивилизации. С учетом этого важную роль приобрело обеспечение стабильного и устойчивого развития инфраструктуры Интернета.

Наряду со многими важными участниками, обеспечивающими и поддерживающими функционирование инфраструктуры Сети (на физическом уровне – интернет-провайдеры, Рабочая группа по проектированию Интернета (IETF), Институт инженеров по электротехнике и электронике (IEEE), Международный союз электросвязи (МСЭ), национальные министерства информационных и коммуникационных технологий (ИКТ); на логическом уровне – Региональные регистратуры Интернет (РРИ), Общество Интернета (ISOC), Консорциум Всемирной Сети (W3C), Международная организация по стандартизации (ИСО), операторы доменов верхнего уровня и проч.) особую важность с точки зрения целей этого исследования имеет исполнение координирующих функций Корпорации Интернета по распределению имен и адресов (ICANN), чья миссия включает в себя координацию работы системы Уникальных Идентификаторов Интернета (здесь и далее по тексту – система УИИ). Согласно Уставу ICANN, Корпорация выполняет следующие конкретные функции:[1]

1. Управляет назначением и передачей следующих трех типов уникальных идентификаторов Интернета:
- доменные имена (формирующие систему, называемую «DNS»);
- адреса интернет-протокола («IP-адреса») и номера Автономной Системы («AS»);
- номера портов и параметров протоколов Интернета.

2. Координирует работу и развитие корневой системы серверов имен DNS.

3. Управляет разработкой политики, имеющей непосредственное отношение к этим техническим функциям.

Участники сегодняшних дискуссий по вопросам глобального управления Интернетом акцентируют внимание на двух типах идентификаторов (доменные имена и сетевые адреса). Надежное функционирование этих идентификаторов является главной задачей в рамках той роли, которую ICANN играет для глобального Интернета. В своей работе Корпорация Интернета, согласно своему Уставу, руководствуется принципами сохранения и повышения эксплуатационной стабильности, надежности, безопасности и мировой функциональной совместимости Интернета.

В отношении ключевых функций ICANN упор делается на последовательное соблюдение требований в части обеспечения стабильности, безопасности и отказоустойчивости Интернета как глобальной сети. Такая постановка задачи

[1] См.: https://www.icann.org/resources/pages/governance/bylaws-en (последнее посещение 1 марта 2016 г.).(последнее посещение 1 марта 2016 г.).

влечет за собой ряд теоретических, технологических, политических, правовых и социальных вопросов.
К числу *теоретических* вопросов, выходящих за рамки непосредственного процесса координации уникальных идентификаторов, относятся проблемы обеспечения гарантированной передачи информации по существующим (и будущим) коммуникационным сетям вне зависимости от географического местонахождения отправителя и получателя такой информации. Дискуссия развивается и по многим другим вопросам, например таким как хранение информации и регулирующие его законы, право на цифровое забвение и т.д. В целом, обсуждение этих вопросов пока носит разнородный характер и протекает в различных юрисдикциях.

Технологические вопросы, сопряженные с развитием и внедрением технических стандартов Интернета, затрагивают изменение самой среды, в которой происходит развитие информационных технологий, а также появление новых возможностей.

Вопросы политического характера связаны, к примеру, с тем обстоятельством, что технологическое развитие Интернета осуществлялось инженерами и изначально не было вписано в какие-либо глобальные процессы выработки и согласования политик. На заре своего существования Интернет развивался для обеспечения возможности обмена данными между компьютерами различных научно-исследовательских организаций. Вследствие этого, любые топологии сетей и принципы построения сетевой инфраструктуры в общем и целом не учитывали трансграничную природу Интернета, которая в полной мере проявилась в будущем, и соответствующие геополитические реалии. Спустя несколько десятилетий, когда количество пользователей по всему миру измеряется миллиардами, все чаще звучит призыв заняться решением международных проблем, которые формулируются по-разному, но могут быть обобщенно обозначены как вопросы «глобального управления Интернетом».

В рамках Всемирной встречи на высшем уровне по вопросам информационного общества, организованной ООН, была создана Рабочая группа по вопросам управления Интернетом, предложившая определение понятия управления Интернетом. Определение получило широкое распространение среди всех заинтересованных сторон (включая правительства, представителей частного сектора, гражданское общество, академическое сообщество и проч.).[2] Необходимо помнить, что ряд технических решений (таких как система распределения IP-адресов, развитие системы DNS, потребность в идентификации владельцев доменов по базе WHOIS) были разработаны без оглядки на какие-либо политические соображения. Кроме того, развитие Интернета, по словам одного из его создателей, Винтона Серфа, пошло по пути лабораторного эксперимента, который необратимо вышел за рамки лаборатории.[3] Многие

[2] «Управление Интернетом представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета» (Доклад рабочей группы по управлению Интернетом. Шато де Босси. Июнь 2005 года, сайт ВВУИО).
[3] См.: См.: http://fortune.com/2015/09/24/we-are-out-of-ipv4-addresses/ (последнее посещение 1 марта 2016 г.).

сегодняшние проблемы невозможно было представить в 1970-х гг., и потому в течение какого-то времени для них не искали должных технологических решений.

Правовые вопросы тесно связаны с политическими. В целом они могут быть сведены к проблеме признания прав национальных государств (одной из заинтересованных сторон в глобальной экосистеме Интернета), изначально не участвовавших в разработке стандартов Интернета, которой занималась Рабочая группа по проектированию Интернет (IETF). На сегодняшний день не существует международных договоров или соглашений, которые регулировали бы развитие Интернета. Интернет опирается на глобально связную инфраструктуру, составляющие которой подпадают под лицензирование и/или регулирование в соответствии с национальным законодательством или международными нормами. Поэтому попытки правительств регулировать и контролировать развитие Интернета не встречают достаточной поддержки у отрасли и ни разу не получили развития. В некоторых случаях такие инициативы встречают активное сопротивление. К примеру, попытка ввести в 1998 г. в Болгарии механизм лицензирования интернет-провайдеров встретила противодействие со стороны болгарского Общества Интернета. В результате разбирательства в Верховном административном суде Республики стороны пришли к соглашению во внесудебном порядке, которое включало полный отказ от идеи регулирования, лицензирования и даже регистрации болгарских интернет-провайдеров.[4] В то же время, некоторые государства в рамках МСЭ и на других международных площадках высказывались о необходимости регулирования Интернета на международном уровне, в рамках ООН в целом или конкретно МСЭ.[5]

Существует много других, в том числе социальных, экономических, гуманитарных и лингвистических вопросов, связанных с развитием Интернета, которые становятся предметом обсуждения в рамках различных площадок и форматов.[6] Однако один из наиболее важных вопросов, пожалуй, связан с обеспечением стабильности, безопасности и отказоустойчивости (СБО) глобальной сетевой инфраструктуры. В отсутствие проработки этого вопроса и поиска путей обеспечения СБО остальные проблемы не имеют первостепенного значения. Сохранение уверенности в безопасности Интернета является залогом успеха для всех сервисов, предоставляющих свои услуги миллиардам пользователей.

Более того, обеспечение СБО Интернета, оставаясь технологическим вызовом по своей природе, также ставит вопросы правового характера. Необходимо достичь общего понимания в вопросе о том, должно ли обеспечение и поддержание СБО Интернета опираться на какую-либо форму нормативно-правового регулирования.

Таким образом, в настоящем исследовании можно выделить несколько взаимосвязанных структурных блоков:

---

[4]См.: См.: http://isoc.bg/kpd (последнее посещение 1 марта 2016 г.).

[5]См., например, публикацию в Газете Коммерсантъ: См.: http://www.kommersant.ru/doc/2749679 (последнее посещение 1 марта 2016 г.).

[6] См. например, на сайте Форума по вопросам управления Интернет (IGF) или на сайте форума NetMundial.

1) Теоретическое – включая определения и терминологию – понимание СБО критической инфраструктуры Интернета;
2) Определение источников административных норм и технологических стандартов регулирования критических ресурсов Интернета, оценка их эффективности и уровня развития;
3) Выявление возможностей, форматов и правовых аспектов признания режимов регулирования, действующих в различных юрисдикциях (а также на глобальном уровне, в случае выявления таковых);
4) Описание вызовов и поиск решений, приемлемых для всех заинтересованных сторон.

Раздел 2. Терминология и основные факты

2.1. Глобальный Интернет

Интернет представляет собой глобальную трансграничную сеть компьютерных сетей, связанных набором протоколов TCP/IP. Одним из ключевых свойств Интернета является полностью децентрализованный контроль над потоками данных. Такой подход к контролю реализован за счет координации глобальных функций, связанных с распределением уникальных идентификаторов, маршрутов и протоколов.

Последовательное функционирование в такой системе взаимосвязанных сетей может быть обеспечено лишь за счет использования общих технологических стандартов, а также организационных и технических решений. Стандартизация такого подхода была достигнута в 1978 г. с разработкой протоколов, описанных в 1981 году в Запросах комментариев (RFC) 791 (IP) и 793 (TCP). Нужно отметить, что появление этих стандартов стало результатом многолетнего труда большого количества специалистов. Основа этих документов была заложена в 1974 г. с публикацией RFC 675. Реализация TCP/IP завершилась к концу 1982 г., а с 1 января 1983 г. набор протоколов стал использоваться в сети ARPANET. С тех пор, набор сетевых протоколов TCP/IP составляет фундамент Интернета. Одна из главных особенностей TCP/IP – полное отсутствие центральной точки, в которой осуществляется управление.. Каждое отдельное сетевое соединение независимо. За счет этого свойства обеспечивается почти бесконечная масштабируемость Интернета, иллюстрацией которой сегодня служат миллиарды существующих одновременно отдельных независимых сессий.

Однако отсутствие центра управления процессом передачи данных не означает отсутствия централизованных функций в рамках организационной и технической координации глобальной сети. Необходимость централизованной структуры для решения вопросов распределения IP-адресов между сетевыми операторами, равно как и поддержание базы данных присвоенных адресов, стала очевидна с началом развития глобального Интернета. Такая необходимость стала естественным следствием потребности обеспечить уникальными адресами все устройства, подсоединенные к сети, а также потребности в бесперебойной маршрутизации сетевых пакетов к каждому IP-адресу.

Между 1983 и 1984 гг. опубликованы RFC 881, RFC 882, RFC 883 и RFC 980, в которых была оформлена концепция доменных имен и их использования для адресации интернет-ресурсов. Потребность в системе доменных имен (Domain Names System – DNS) возрастала по мере роста числа онлайн-пользователей. Параллельно с внедрением доменных имен решалась группа организационных и технических задач по поддержанию DNS. В частности, работа над этими задачами включала в себя составление, поддержание и координация базы данных доменов верхнего уровня (TLDs), а также текущую работу, поддержание и координацию деятельности операторов корневых серверов системы доменных имен.

Разрастание Интернета и деятельности интернет-провайдеров, в том числе растущее количество используемых ими IP-адресов, привело к появлению идеи

агрегирования сетевых адресов для целей маршрутизации (Автономные Системы), т.е. объединения всех адресов, используемых сетевым оператором, в единые адресные блоки и организации маршрутизации между такими блоками через границы сетей, составляющих Интернет. Этот подход описан в RFC 1126, опубликованном в октябре 1989 г. Реализация идеи использования Автономных Систем (АС) потребовала создания и поддержания механизма, который позволял бы управлять номерами АС, чтобы обеспечить их уникальность. Администрация адресного пространства Интернет (IANA) ведет запись блоков номеров АС, которые она распределяет между Региональными регистратурами Интернет (РРИ), которые, в свою очередь, распределяют отдельные номера АС между своими клиентами, поддерживая уникальность этих идентификаторов.

Идеи интернационализации некоторых административных функций, связанных с уникальными идентификаторами, были сформулированы в RFC 1174 в августе 1990 г. В рамках воплощения этой идеи в 1992 г. в Нидерландах была зарегистрирована некоммерческая организация – Координационный Центр распределения ресурсов сети Интернет в Европейском регионе (RIPE NCC), которая стала первой из пяти Региональных регистратур Интернет. Эти организации получают блоки IP-адресов и номеров АС от Администрации адресного пространства Интернет (IANA) и осуществляют их дальнейшее распределение в пределах соответствующих географических регионов. Региональные регистратуры Интернет (РРИ) распределяют ресурсы нумерации между операторами услуг и коммерческими компаниями, зарегистрированными в качестве Локальных регистратур Интернет (LIRs). Сегодня, когда национальному интернет-провайдеру необходимы IP-адреса или номера АС, он запрашивает их у РРИ. РРИ действуют в соответствии со своей открытой политиками, известной под названием ICP-2[7].

Вместе с тем, глобальный Интернет представляет собой не только сеть взаимосвязанных сетей, которые обеспечивают сквозной пропуск потоков данных при помощи общих протоколов. Интернет является также средой, через которую различные сервисы предоставляют услуги своим пользователям.

Назовем лишь немногие из них, которые широко используются сегодня: поисковые системы такие как Google, Яндекс и другие, социальные медиа такие как Facebook, Вконтакте, Twitter и проч., сервисы распространения мультимедийного контента такие как YouTube, Instagram, площадки онлайн-торговли такие как e-Bay, Alibaba, онлайн-платформы для оказания банковских или иных специализированных услуг, облачные сервисы виртуальных игр и облачного хранения данных и т.д. Стабильная работа таких сервисов крайне важна, поскольку ими пользуются сотни миллионов, а иногда и миллиарды интернет-пользователей.

Глобальный Интернет также использует аппаратное обеспечение и физическую инфраструктуру – волоконно-оптические кабели, национальные, континентальные и трансконтинентальные опорные сети, необходимые для передачи больших объемов данных между компьютерными сетями.

[7] См.: https://www.icann.org/resources/pages/new-rirs-criteria-2012-02-25-en (последнее посещение 1 марта 2016 г.).

Представленная выше классификация сервисов Интернета условна, однако она дает представление об их разнообразии и важности стабильного функционирования систем уникальных идентификаторов. Ключевой причиной для такой важности, на наш взгляд, служит то, что эти сервисы сегодня используются половиной населения планеты.

2.2. Глобальная инфраструктура Интернета

Интернет, будучи объектом настоящего исследования, представляет собой достаточно сложную, многомерную и многоуровневую сущность, поэтому для его описания обычно используются различные способы и определения.

Для целей настоящего исследования необходимо определить (а) основные архитектурные элементы Интернета как глобальной сети и описать их функциональные свойства, и (б) их характеристики с точки зрения правового статуса в рамках соответствующих юрисдикций. Кроме того, необходимо также определить, какие именно составляющие инфраструктуры Интернета можно называть *глобальными* – то есть уникальными в плане их роли для поддержания связности различных сетей. И наконец, не следует забывать о том, что Интернет представляет собой архитектурно открытую систему, основанную на стандартах, созданных в рамках открытого процесса и преимущественно определяемых на площадке Рабочей группы по проектированию Интернет (IETF).

На основе специфических характеристик Интернета, а именно передачи информации в соответствии с набором протоколов TCP/IP, описание его ключевой инфраструктуры можно начать, используя концепцию уровней, определенных в базовой эталонной модели взаимодействия открытых систем (сетевая модель OSI), разработанной Международной организацией по стандартизации (ISO).

Обычно базовая эталонная модель взаимодействия открытых систем включает в себя семь уровней:

- (7) уровень приложения (Application layer);
- (6) уровень презентации (Presentation layer);
- (5) сеансовый уровень (Session layer);
- (4) транспортный (Transport layer);
- (3) сетевой уровень (Network layer);
- (2) канальный уровень (Channel layer, Data link layer);
- (1) физический уровень (Physical layer).

Для описания сети Интернет используется четырехуровневая модель, в которой по сути объединены первые два, а также последние три уровня из семиуровневой модели:

- (4) прикладной уровень (Application layer).
- (3) транспортный уровень (Transport layer),
- (2) сетевой уровень (Internet layer),

- (1) канальный уровень (Link layer).

К каждому из этих уровней применимы соответствующие протоколы, разработанные IETF и другими структурами. Каждый уровень имеет критическое значение для функционирования Интернета и приложений, которые работают на его основе.

На самом нижнем уровне взаимодействия (канальный уровень) находится собственно передача сигналов и физические носители (лини связи и физические каналы).

На сетевом уровне находится протокол IP – интернет-протокол, который определяет уникальность сети Интернет.

Транспортный уровень обеспечивает возможность надежной передачи данных между конечными устройствами, подключенными к сети, Основным протоколом транспортного уровня является Протокол управления передачей (TCP).

Наконец, на прикладном уровне обеспечивается доступ к ресурсам и сервисам. Именно на этом уровне происходит взаимодействие с конечными пользователями Интернета, для чего необходимо наличие интерфейса между приложением и человеком или прикладными программами. В модели OSI-ISO также существует уровень презентации, на котором определяется, какие протоколы используются для того или иного взаимодействия (протокол передачи файлов, FTP, гипертекстовый протокол http / https, протокол электронной почты POP3).

Необходимо отметить различия в статусе телекоммуникационных операторов, интернет-провайдеров и других поставщиков услуг в сфере телекоммуникаций.[8] Можно выделить по крайней мере три уровня таких операторов, среди которых ключевую позицию занимают операторы первого уровня – т.н. сетевые операторы Tier 1. Другие виды интернет-провайдеров либо имеют лишь частичный доступ к Интернету через пиринговые соединения (Tier 2), либо используют для доступа к Интернету только те каналы, которые они покупают или арендуют у других операторов (Tier 3).

Таким образом, можно сказать, что для телекоммуникационной инфраструктуры Интернета по-настоящему незаменимы лишь сетевые операторы первого уровня (Tier 1) (AT&T, TeliaSonera и проч.), которые формируют глобальную опорную сетевую инфраструктуру Интернета. Остается открытым вопрос о том, может ли телекоммуникационная инфраструктура каждого из этих операторов может быть причислена к «глобальной». Скорее всего, сугубо положительный ответ на этот вопрос будет преждевременным: сеть каждого такого оператора дополняет сети первого уровня других операторов на этом же самом уровне, но никто из них по отдельности не является единственным глобальным, поэтому критически важно поддерживать функционирование мирового Интернета как единого целого.

[8] – в отношении места в иерархии телекоммуникационной системы, обеспечивающей передачу данных в Интернете.

С регуляторной точки зрения, техническая инфраструктура Интернета вмещает всех сетевых и коммуникационных провайдеров, включая физические каналы и линии связи, инфраструктуру коммутации соединений и прочее сетевое оборудование, а также другие компоненты, обеспечивающие стабильную работу сетей. Владельцами этой инфраструктуры выступают частные и государственные структуры, она принадлежит компаниям и организациям, ведущим деятельность в соответствии с требованиями тех или иных национальных законодательств. В некоторых случаях (например, с подводными морскими кабелями, спутниковыми каналами и т.д.) использование такой инфраструктуры осуществляется в соответствии с нормами международных соглашений, например в области морского или космического права или права международных телекоммуникаций.

В отношении инфраструктуры собственно Интернета, за счет которой обеспечивается переход сетевых взаимодействий от канального уровня к прикладному и обратно, можно вычленить следующие функциональные процессы:

1) Распределение сетевых (IP) адресов и номеров АС через пять Региональных регистратур Интернет. Так, для Европы, России и Ближнего Востока компетентной структурой является RIPE NCC, которая выделяет диапазоны IP-адресов своим членам (телекоммуникационным операторам из стран региона). Неправительственная организация ARIN (зарегистрирована в Шантильи, штат Вирджиния, США) выполняет сходные функции для США и Канады; Латинскую Америку обслуживает LACNIC (зарегистрирована в Монтевидео, Уругвай), тогда как обслуживанием провайдеров из стран Африки занимается AfriNIC (базируется в Маврикии). Для Азиатско-Тихоокеанского региона эти функции выполняет APNIC (базируется в Брисбене, Австралия).

2) Обеспечение бесперебойного функционирования корневых серверов системы доменных имен.[9] Операторами этих серверов являются: корпорация Verisign, Университет Южной Калифорнии (ISI), Cogent Communications, Университет Мэриленда, Национальное управление по воздухоплаванию и исследованию космического пространства США (NASA), Internet System Consortium, Центр сетевой информации при Министерстве обороны США, Исследовательская лаборатория Армии США, компания Netnod, RIPE NCC, Корпорация Интернета по распределению имен и адресов (ICANN), WIDE Project. **Это не означает, что серверных машин в прямом смысле слова 13**. Каждый такой сервер является надёжной системой из нескольких компьютеров, часть которых находится в горячем резерве. Большинство корневых серверов имеют так называемые «зеркала». Таким образом, общее количество корневых серверов DNS по всему миру превышает 460. Несмотря на то, что каждый корневой сервер (и связанные с ним «зеркала») существует и функционирует в рамках того или иного национального законодательства, общее их количество таково, что делает это обстоятельство не критичным с точки зрения надёжности функционирования всей системы корневых серверов в целом.

[9] См. определение (англ.): https://en.wikipedia.org/wiki/Root_name_server.
См. полный список корневых серверов DNS: См.: http://root-servers.org/

3) Ключевым элементом в процессе работы системы доменных имен являются обновления файла корневой зоны DNS, которые периодически выполняет Администрация адресного пространства Интернет (IANA). С марта 2014 г. продолжается обсуждение с участием всех заинтересованных сторон вопроса передачи правительством США ответственного управления функциями IANA. Процесс стартовал 14 марта 2014 г. с публикацией объявления NTIA.[10]

Правовые вопросы, связанные с инфраструктурой уровня приложения, охватывают сервисы, предназначенные для конечных пользователей, и доступ к информационным ресурсам; решение таких вопросов находится в плоскости национального законодательства и регулирования. Использование интернет-сервисов обычно осуществляется на основе т.н. договоров на типовых условиях (договоры присоединения). Вступая в такие договоры, пользователь подпадает под ту или иную юрисдикцию, в рамках которой, как указывается в условиях договора, осуществляется регулирование вопросов, связанных с использованием сервиса, производится разрешение споров и т.д. В некоторых случаях это может повлечь конфликт с законодательством того государства, резидентом которого является пользователь – например, в отношении защиты прав потребителя, распространения контента и т.д.

В этой связи, роль Корпорации Интернета заслуживает некоторого пояснения.

Как уже отмечалось в Разделе 1, ICANN координирует назначение и передачу трех типов уникальных идентификаторов Интернета, а именно: а) доменных имен (формирующих систему, называемую «DNS»); б) распределение адресов интернет-протокола (IP-адреса) и номеров Автономной Системы («AS»); и с) распределение и ведение записей номеров портов и параметров протоколов Интернета. Корпорация также осуществляет координацию функционирования и развития системы корневых серверов DNS, а также разработки политик, связанных с выполнением этих технических функций.

Сказанное означает, что за рамками исполнения функций IANA Корпорация не осуществляет никакой контроль над корневыми серверами DNS, равно как и над организациями, которые выполняют роль операторов этих корневых серверов или их «зеркал».

ICANN является участником сложной многоуровневой системы организаций, которые координируют работу и принимают решения. Также Корпорация Интернета через Консультативные комитеты и Поддерживающие организации предоставляет площадку, позволяющую всем желающим участвовать в обсуждениях и выработке политик. Одной из структур, выполняющих такую роль, является Консультативный комитет системы корневых серверов (RSSAC), который отвечает за консультирование Правления и сообщества ICANN по вопросам, связанным с функционированием, администрированием, обеспечением безопасности и целостности системы корневых серверов Интернета.

[10] См. подробнее: http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (последнее посещение 1 марта 2016 г.).

Правление ICANN утверждает политики, разработанные Поддерживающими организациями и Консультативными Комитетами. В состав Правления входит 21 член: 15 из них имеют право голоса, а оставшиеся шесть является координаторами без права голоса. Из числа директоров восемь человек избираются независимым Комитета по назначениям, а остальные утверждаются на свои посты поддерживающими организациями (двое утверждаются Организацией поддержки адресов (ASO), двое – Организацией поддержки доменов общего пользования (gNSO), еще двое – Организацией поддержки страновых доменов (ccNSO), один человек – Расширенным консультативным комитетом (ALAC) и, наконец, в силу занимаемой должности членом Правления с правом голоса является Президент ICANN.

Развитие глобальной инфраструктуры Интернета ведется на основе технических документов (Запросы комментариев (RFC), Запросы предложений (RFP)), которые разрабатываются на площадках Рабочей группы по проектированию Интернет (IETF) и Совета по архитектуре Интернета (IAB). Принимая решения, Корпорация Интернета учитывает эти технические стандарты в той мере, в которой они связаны с функционированием IP-адресов и DNS. Обычно разработку технических политики инициируют участники Технического комитета, с которыми взаимодействуют Консультативные комитеты Корпорации (SSAC, RSSAC). Затем следует многоэтапное обсуждение предлагаемых решений, которое включает в себя консультации с сообществом, в том числе в формате процесса публичных комментариев, после чего одобренная сообществом политика выносится на рассмотрение Правления. Поскольку мандат организации достаточно узко определен в ее Уставе, и ограничен лишь системой УИИ, принимаемые ICANN решения не могут затрагивать никакие вопросы, относящиеся к более низким уровням Интернета (например, регулирование телекоммуникационных компаний и т.п.) или напротив к уровню приложения, включая те или иные требования к передаче данных, которые рассматриваются в рамках национального законодательства каждого государства.

В итоге, следует принять тот факт, что вопрос «вычленения» (выключения) тех или иных компонентов из глобальной инфраструктуры Интернета остается весьма противоречивым. Этот вопрос зависит от определения Интернета как информационной системы, и, кроме того, на него по-разному могут отвечать различные правительства, в зависимости от:

- принятой модели регулирования критической инфраструктуры – или отсутствия таковой;
- признания государствами возможности (или, напротив, отсутствия таковой) повлиять на работу определенных элементов инфраструктуры, которые географически (или логически) находятся за пределами их действенного контроля.

К основополагающим элементам глобальной инфраструктуры Интернета относятся (а) параметры протоколов, технические стандарты и спецификации, обеспечивающие связность и передачу информации через Интернет; (б) базы данных (файлы корневой зоны) и сходные с ними информационные ресурсы, которые обеспечивают связность Интернета на уровне приложения и

уникальность сетевых идентификаторов. Координацию работы глобальной инфраструктуры в отношении первой из ее названных составляющих ведут такие организации как Рабочая группа по проектированию Интернет, Общество Интернета МСЭ, ИСО, IEEE, 3GPP, GSMA, 3WC и прочие организации, вовлеченные в процесс разработки и принятия технических стандартов. Для второй составляющей в роли координаторов выступают участники сетевой адресации и пространства доменных имен, включая ICANN, включая Администрацию адресного пространства Интернет (IANA), а также Региональные регистратуры Интернет.

В настоящем исследовании не обсуждается национальная инфраструктура страновых (ccTLDs) и общих (gTLDs) доменов верхнего уровня; таким образом, мы не рассматриваем и администраторов таких доменов, равно как и телекоммуникационных операторов, интернет-провайдеров, или провайдеров сервисов и интернет-приложений (поисковых систем, социальных сетей и прочих).

Значение провайдеров интернет-приложений для Интернета как глобальной сети информационного контента будет постоянно расти. Однако обеспечение связанности различных сетей, предоставляющих информационные сервисы, слабо влияет на инфраструктуру, которая обеспечивает связность сетей на нижних уровнях. Таким образом, работа сервисов прикладного уровня в меньшей степени зависит от физических и технологических характеристик используемого сетевого оборудования и его расположения. В то же время, шансы достичь консенсуса по подходам к регулированию работы сервисов прикладного уровня существенно ниже, чем в отношении сервисов на других уровнях сетевой инфраструктуры.

2.3. Стабильность, безопасность и отказоустойчивость инфраструктуры глобального Интернета

Предметом настоящего исследования являются вопросы безопасности, стабильности и отказоустойчивости глобальной инфраструктуры сети интернет. При этом область исследования ограничена только теми вопросами, которые определены Уставом ICANN. Поэтому, прежде всего, приведем определения понятий «безопасность», «стабильность» и «отказоустойчивость» в том виде, как их определяет сама корпорация ICANN.[11]

Безопасность – способность предотвращать и ограждать от неправильного использования уникальных идентификаторов сети интернет.
(*Security – the capacity to protect and prevent misuse of Internet unique identifiers*).

Стабильность – возможность гарантировать, что система функционирует в соответствии со своим регламентом, а также способность обеспечить уверенность пользователей системы уникальных идентификаторов в том, что это именно так.

[11] См.: ICANN's FY 14 Security, Stability and Resiliency Framework; https://www.icann.org/public-comments/ssr-fy14-2013-03-06-en (последнее посещение 1 марта 2016 г.).

(*Stability – the capacity to ensure that the system operates as expected and users of the unique identifiers have confidence that the system operates as expected*).

Отказоустойчивость – способность системы уникальных идентификаторов эффективно противостоять/выдерживать/переживать злонамеренные атаки и другие разрушающие события без ущерба и без прекращения выполняемых системой функций.
(*Resiliency – the capacity of the unique identifier system to effectively withstand/tolerate/survive malicious attacks and other disruptive events without disruption or cessation of service*).

Перечисленные выше три понятия имеют фундаментальное значение, но приведенные определения требуют уточнений, во-первых, для того чтобы они соответствовали их современному значению (в понимании экспертов), а, во-вторых, для того, чтобы не возникали смысловые противоречия с существующими международными и национальными нормативными документами и стандартами, использующими эти понятия.

Основными причинами необходимости уточнения этих определений являются:

1. Неоднозначность толкования этих понятий. Во многих работах «стабильность» и «отказоустойчивость» рассматриваются как составные части общего понятия «безопасность» и, вследствие этого, явно или неявно входят в это общее определение. Более того, понятия «стабильность» и «отказоустойчивость» часто связывают с обобщающим понятием «надежность». Толкование термина «безопасность» через «неправильное использование» допускает очень широкую интерпретацию (защита от целенаправленной атаки или защита «от дурака» и пр.).

2. Проблемы лингвистического характера. При переводе с/на английский язык часто теряются или возникают новые, дополнительные коннотации. Базовое понятие «безопасность» в русском языке (и, что в данном случае даже более важно – в российских документах) прежде всего, означает «состояние защищенности», в то время как клише английского перевода «security» кроме этого подразумевает и совокупность средств, обеспечивающих это состояние защищенности. Попытка использовать для перевода английское слово «safety» также не слишком удачно, т.к. в оно несет оттенок «*внутреннее ощущение защищенности*», что вообще говоря, отсутствует в русском эквиваленте.[12] Непонимание этих нюансов часто приводит к долгим (и бессмысленным!) спорам при обсуждении конкретных вопросов на международных площадках.

3. Область применения понятий. Приведенные выше определения ограничены понятиями безопасности (стабильности и отказоустойчивости) в части функций, исполняемых ICANN (может быть, даже более точно – IANA), а именно в части системы распределения

[12] См.: Critical Terminology Foundations . Russia-U.S. Bilateral on Cybersecurity policy report 2/2014; James B.Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko (Chief Editors); https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf (последнее посещение 1 марта 2016 г.).

уникальных идентификаторов, номеров и параметров. В тоже время, как отмечено в разделах 2.1, 2.2 настоящего отчета, к критически важной инфраструктуре глобального Интернета относятся также а) инфраструктура магистральных сетей передачи данных (оптических, спутниковых) и б) сервисные платформы, обеспечивающие пользователям предоставление базовых услуг. Для них также должны быть определены соответствующие им понятия «безопасности» и «устойчивости», но в настоящем отчете эти вопросы не рассматриваются.

4. Условия применимости понятий. Кроме приведенных выше замечаний в отношении определения этих понятий необходимо учитывать условия, в которых эти понятия сохраняют свои значение. Описанная выше инфраструктура сети Интернет сохраняет свою работоспособность в условиях «нормальной» работы сети. Между тем ряд исследований (например, материалы Объединенный центр передовых практик в области кибероборонь (CCD COE) НАТО в Таллинне)[13] рассматривают условия функционирования сети как в случае «нормальных», так и в случае «экстремальных» (читай, в случае военных конфликтов) условий ее функционирования, что также требует соответствующего уточнения значения этих фундаментальных понятий.

5. Соответствие международным и национальным нормативным документам. Существует целый пул международных (ISO), национальных (NIST, ГОСТ и пр.) и ведомственных стандартов в области безопасности и надежности, относящихся не только к информационным системам,[14] в которых зафиксирована терминология, соответствующая этой предметной области. Помимо вынесенных в заголовок терминов «стабильность» (stability) и «отказоустойчивость» (resiliency), используются близкие понятия «надежность» (dependability), «безотказность» (reliability), «живучесть», ремонтопригодность и пр. Отдельный блок стандартов относится к вопросам управления рисками (см. ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения»; ISO/МЭК 73:2002 «Управление риском. Словарь. Руководящие указания по использованию в стандартах»). Терминология, зафиксированная в этих стандартах также имеет серьезные пересечения с определениями, приведенными в Уставе ICANN.

Для иллюстрации приведем несколько формулировок Национального института стандартов США NIST.[15]

---

[13] См.: The Tallinn Manual on the International Law Applicable to Cyber Warfare, http://www.cambridge.org/ca/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare (последнее посещение 1 марта 2016 г.).
Также см.: NATO Cooperative Cyber Defense Centre of Excellence “Peacetime Regime for State Activities in Cyberspace”. https://ccdcoe.org/multimedia/peacetime-regime-state-activities-cyberspace.html (последнее посещение 1 марта 2016 г.).

[14] См.: Струков А.В., Анализ международных и российских стандартов в области надежности, риска и безопасности, http://szma.com/standarts_analysis.pdf (последнее посещение 1 марта 2016 г.).

[15] См.: NISTIR 7298 Revision 2 Glossary of Key Information Security Terms; Richard Kissel, Editor; Computer Security Division Information Technology Laboratory; May 2013, http://dx.doi.org/106028/NIST.IR.7298r2 (последнее посещение 1 марта 2016 г.).

Безопасность – состояние, являющиеся результатом внедрения и поддержания работоспособности защитных мер, которые позволяют системе выполнять свои функции, несмотря на риски реализации угроз ее работоспособности. Защитные меры могут включать совокупность мер сдерживания, избегания, предотвращения, отслеживания, восстановления и исправления. В совокупности эти меры являются частью системы управления рисками.

Security *- A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach*.

Отказоустойчивость – способность быстро адаптироваться и восстанавливаться после любых известных или неизвестных изменений в окружающей систему обстановке путем комплексного применения системы управления рисками и непрерывного планирования. Речь идет о способности (а) продолжать функционировать и выполнять ключевые функции во враждебных условиях и воздействиях даже при частичном разрушении самой системы и (б) восстанавливаться до состояния, позволяющего выполнять предписанные функции за время, определяемое миссией системы.

Resilience *- The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.*

Все выше сказанное относится лишь к отдельным элементам глобальной информационной системы Интернет. Понятия «безопасность», «стабильность» и «отказоустойчивость» как системы уникальных идентификаторов, так и сервисных платформ и инфраструктуры магистральных сетей входят в общее понятие «информационной (кибер-) безопасности». Таксономия понятий «информационная безопасность», «кибербезопасность», «безопасность информации», «безопасность информационно-коммуникационных технологий» и т.д. является предметом обсуждения многих международных конференций, как академических, так и политических.[16] В силу самых разных причин (включая, конечно, и политические) до консенсуса в этом вопросе еще очень далеко. Приведем компромиссную формулировка понятия «кибербезопасность», выработанную в ходе выполнения совместного проекта Института проблем

[16] Например, Пятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействия терроризму», 25-28 апреля 2011 г., Гармиш-Партенкирхен, Германия, см.: http://www.iisi.msu.ru/events/news50/ (последнее посещение 1 марта 2016 г.).

информационной безопасности (ИПИБ) МГУ и Института Восток-Запад (EWI) США.[17]

Кибербезопасность – свойство киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз.

Cybersecurity *is a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover.*

Полезно отметить, что в том же проекте ИПИБ МГУ – EWI изложено соотношения понятий с приставкой «кибер-» и «инфо-».[18]

В Российской Федерации первоисточником трактовки понятий, связанных с вопросами безопасности, следует считать Закон Российской Федерации «О безопасности» № 2446-I:[19]

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Определения всех остальных видов безопасности (военно-политической, экономической, экологической, и пр.), включая понятие информационной безопасности, строятся на основе этого общего определения путем уточнения, о какой сфере общественных отношений идет речь. Для иллюстрации приведем определение информационной безопасности в том виде, как это сформулировано в ряде международных документов, подписанных Российской Федерацией:[20]

Информационная безопасность – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

Отметим два методически важных момента, связанных с последними определениями:

---

[17] См.: Critical Terminology Foundations…; https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf (последнее посещение 1 марта 2016 г.).

[18] Там же.

[19] Закон Российской Федерации «О безопасности» № 2446-I (с учетом изменений от 25 декабря 1992 г., 24 декабря 1993 г., 25 июля 2002 г., 7 марта 2005 г., 25 июля 2006 г., 2 марта 2007 г.); http://www.scrf.gov.ru/documents/20.html (последнее посещение 1 марта 2016 г.).

[20] См.: Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности; 16 июня 2009 г., NATO Cooperative Cyber Defense Center of Excellence, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf (последнее посещение 1 марта 2016 г.).

Также см.: Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной безопасности; 14 мая 2010 г. Правовой департамент МИД РФ, http://archive.mid.ru/bdomp/spd_md.nsf/0/92945909DDDE3EEE43257F770047770E (последнее посещение 1 марта 2016 г.).

- Содержание понятия «безопасность» раскрывается только (а) в привязке к конкретным интересам пользователей и (б) в отношении конкретных угроз этим интересам.

- Понятие «безопасность» увязано с интересами субъектов – пользователей информационной системой. Такая увязка на уровне базовых определений ведет к определенным методическим проблемам при оценке безопасности сложных (а тем более глобальных) систем. Проблема заключается в том, что у различных пользователей системы могут быть взаимоисключающие, противоречащие друг другу интересы (без привязки к анализируемой информационной системе). Поэтому при оценке защищенности их интересов в связи с анализируемой системой возникнут противоречия не связанные с функциями/услугами, выполняемыми системой.

Принципиально важно разделить угрозы на два класса: (1) угрозы, возникающие в силу случайных обстоятельств, непреднамеренных ошибок, перегрузок системы, стихийных бедствий, аппаратных сбоев, аварий и т.п., и (2) угрозы, сознательно планируемые, разрабатываемые и реализуемые одними пользователями системы в отношении других пользователей.

Именно последний тип угроз определяет принципиальную разницу двух понятий: «**безопасность**» и «**надежность**». Когда речь идет о **безопасности**, то предполагается наличие субъекта, порождающего угрозы. В то время, когда говорят о **надежности**, то наличие такого субъекта либо вообще не предполагается, либо он рассматривается неявно – т. е. источником угрозы являются естественные причины (например, перегрузки, сбои, старение материалов и т.д.), природные явления (ураганы, наводнения и т. п.) или неумышленные ошибки (прежде всего ошибки проектирования или написания программных кодов). При этом, как правило, стремятся уйти от рассмотрения **сценариев** и свести обсуждение только к выявлению (абстрактных, не увязанных с их источником) **уязвимостей**. В этом подходе есть определенная доля лукавства и/или проявление методологической ошибки. Для иллюстрации, приведем определение понятия «уязвимость»:[21]

Уязвимость – слабость информационной системы, процедур безопасности системы, процедур внутреннего контроля или их реализации, которые могут быть использованы **источником угрозы**.

Vulnerability – weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Таким образом, в самом определении появляется этот самый субъект – источник угроз (определение согласно стандарту NISTIR 7298):

Источник угроз – замысел и метод, имеющие целью намеренное использование уязвимости или сложившейся ситуации, а также метод, который может непреднамеренно активировать уязвимость.

[21] NISTIR 7298 Revision 2…, http://dx.doi.org/106028/NIST.IR.7298r2

Threat Source – the intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger vulnerability.

При оценке безопасности системы в отношении преднамеренных угроз методически точнее использовать хорошо известную в *Theory of Computer Science* схему математической криптологии.[22]

Описывается сама *Система*, т.е. перечисляют функции и услуги, оказываемые *Системой*. Декларируют, какие при этом качества, свойства функций/услуг должна обеспечить *Система*, и какие меры/механизмы безопасности она реализует.

1. Определяются *Участники*: а) Пользователь системы, на кого нападают (*Пользователь-жертва*); б) Пользователь системы, который нападает (*Нападающий*).
2. Формулируют *Цели атаки (угрозы)*, которых хочет достичь *Нападающий* (каким именно интересам *Пользователя-жертвы* он стремиться нанести ущерб). В данной трактовке *Цель атаки* – это нарушение какой-либо функции или качества услуги *Системы*, используемой *Пользователем-жертвой*.
3. Определяют, какими *Ресурсами* располагает *Нападающий* для достижения *Цели атаки* – к каким элементам *Системы* он имеет доступ, что он может при этом делать и т.п.

Важно подчеркнуть, что при этом изучается только качество механизмов и мер безопасности, реализуемых *Системой*. Мотивы атаки (политические, экономические, религиозные и т.д.) здесь не рассматриваются. Здесь отсутствуют эмоциональные (политические) оценки типа *Пользователь-жертва* – «хороший», а *Нападающий* – «плохой»: в качестве *Пользователя-жертвы* при анализе, вообще говоря, можно рассматривать и «Плохого парня» (Bad Guy), интересы которого (например, сохранение анонимности) стремятся нарушить *Нападающие* – «Хорошие парни», например правоохранительные органы.

Перечисленные выше четыре позиции являются исходными данными для оценки степени/уровня безопасности *Системы*. В ходе анализа рассматривают все возможные (гипотетически вообразимые) способы реализации *Нападающим* данной *Атаки*. Если при этом выясняется, что для достижения своих *Целей* при любом вообразимом способе реализации атаки *Нападающему* требуются ресурсы (финансовые, временные, организационные), превышающие разумные параметры, то *Система* признается безопасной в отношении данной *Атаки*. Для оценки безопасности *Системы* **в целом** необходимо проделать такой анализ для всех пар (*Пользователь-жертва – Нападающий*) и всех *Атак*. Обратим здесь внимание, что при оценке безопасности системы в целом, вообще говоря, каждый пользователь системы должен рассматриваться и как потенциальная жертва, и как потенциальный Нападающий!

Применение такого формального (и в определенном смысле «нудного») подхода к оценке безопасности глобальной инфраструктуры Интернета, на наш взгляд,

[22] См., например: Математическая криптография, http://www.cryptography.ru (последнее посещение 1 марта 2016 г.).

позволит во многом расставить точки над i в международных дискуссиях и при наличии доброй воли (заинтересованности) всех участников политического процесса перевести эти дискуссии в конструктивное русло.

В заключительной части этого раздела рассмотрим, к чему приводит применение данной методики в отношении оценки безопасности глобальной инфраструктуры распределения уникальных идентификаторов, номеров и параметров сети Интернет.

1. **Система (глобальная инфраструктура)** распределения уникальных идентификаторов, номеров и параметров сети Интернет является, прежде всего, информационной системой. Причем следует считать, что таких информационных систем несколько, так как в соответствии с многоуровневым представлением инфраструктуры для уровня приложений речь идет о системе доменных имен, а для сетевого и транспортного уровней – о номерах автономных систем, IP-адресах и номерах портов и параметров протокола. Как и всякая информационная система, система УИИ предоставляет возможность реализации следующего набора функций:

- формирование и накопление информации;
- хранение информации;
- передача информации;
- обработка информации;
- предоставление информации;
- поиск информации;
- распространение информации
- уничтожение информации.

В нашем случае, под «информацией» понимаются данные об уникальных идентификаторах, номерах и параметрах сети Интернет, а также вся сервисная (вспомогательная) информация, необходимая для выполнения перечисленных выше функций. В определении «безопасности», даваемом в уставе ICANN, понятие «неправильное использование» следует отнести к *каждой* из этих функций.

Элементы системы включают в себя инфраструктуру Корпорации Интернета ICANN и Администрации адресного пространства Интернет (IANA), структуру 13 корневых серверов DNS и их «зеркал», включая набор функций, выполняемых Verisign, пять Региональных регистратур Интернет (РРИ), национальных и местных интернет-регистраторов (NIR, LIR), интернет-провайдеров и т.д. В рамках настоящего отчета ограничимся только «верхним» уровнем, т.е. только рассмотрением функций ICANN и системы корневых серверов DNS. Описание элементов системы включает в себя:

- назначение по обработке того или иного вида информации (доменные имена, номера автономных систем, IP-адреса и номера портов);
- описание технических средств, реализующих функции системы (hardware, firmware, software);

- совокупность технических и организационных стандартов, регламентов и процедур;
- юрисдикцию, в рамках которой функционируют перечисленные выше элементы системы.

Подробно вся система рассматривается в Разделе 3.

2. **Пользователи** – все, кто входит в состав «заинтересованных сторон» (stakeholders) именно так, как это принято понимать в текущих дискуссиях:
   - субъекты международного права: государства, коалиции и союзы государств, негосударственные автономии и т.п.;
   - бизнес (национальный, транснациональный и т.п.), в том числе бизнес «вокруг» инфраструктуры сети Интернет;
   - субъекты гражданского общества: политические партии, отдельные Церкви, религии и их течения (причем, возможно, с экстремистскими целями), организационно оформленные общественные движения, неформальные союзы и объединения ученых и инженеров, и пр.;
   - неформальные виртуальные группы пользователей интернет, объединенные совместными интересами (“Anonymous”, аудитория виртуальных сетевых игр, участники «клубов по интересам» и проч.);
   - в отдельный блок следует выделить формальные и неформальные объединения разработчиков, инженеров, формирующих облик Интернета (ISOC, IETF и т.д.);
   - граждане и частные лица (в число которых неизбежно входят и граждане, имеющие преступные намерения).

3. **Угрозы безопасности** в отношении информационной системы в «классическом» понимании включают угрозы в отношении «триады» свойств – C.I.A.:
   - Confidentiality – конфиденциальность;
   - Integrity – целостность;
   - Availability – доступность.

В нашем случае может показаться, что первая из угроз – угроза нарушения конфиденциальности – не актуальна, по крайней мере, в отношении уникальных идентификаторов, номеров и параметров сети Интернет (так как сложно представить причину, по которой кому-либо потребуется «засекретить» IP-адрес или имя хоста). Однако сервисная информация, используемая в этих системах, может содержать информацию, составляющую коммерческую тайну или персональные данные физических лиц. Поэтому в рассматриваемом случае требуется обеспечить все три свойства – конфиденциальность, целостность и доступность.

При этом необходимо учитывать, что, во-первых, эти угрозы необходимо соотносить с уровнями модели инфраструктуры Интернета. Если на уровне приложений речь идет о безопасности системы доменных имен и работы всех серверов доменных имен (DNS), то на сетевом и транспортном уровне наиболее актуальны задачи обеспечения маршрутизации как в локальных сетях, так и на уровне взаимодействия автономных систем.

Также здесь следует обратить внимание еще на один аспект. Большинство операторов рассматриваемой инфраструктуры являются коммерческими организациями, основной мотив деятельности которых заключается в извлечении прибыли. Поэтому следует иметь в виду угрозы (риски) в отношении доступности и целостности в результате «выпадение» из системы (прекращение или ограничение деятельности) отдельных ее частей в силу самых разнообразных внешних (банкротство, решение суда, санкции, революции и т.п.) и внутренних (низкая рентабельность, смена сферы деятельности, политические или моральные мотивы и т.п.) причин.

Раздел 3. Технические стандарты и требования в части обеспечения стабильности, безопасности и отказоустойчивости системы Уникальных Идентификаторов

3.1. Техническая инфраструктура и стандарты, обеспечивающие ее стабильность, безопасность и отказоустойчивость

Интернет предоставляет собой, вероятно, самую сложную и многомерную технологическую рукотворную экосистему, когда-либо созданную в истории человечества. Хотя система УИИ является основным объектом исследования, инфраструктура Интернета не ограничивается системой УИИ и ее компонентов (DNS, IP адреса, номера АС, номера портов и параметры протоколов). Совокупность технической инфраструктуры Интернета не укладывается ни в одну универсальную классификацию, в то время как сам Интернет не имеет общепринятого определения. Однако для целей настоящей главы мы примем определение из Раздела 2.1.

Исходя из этого, в настоящем разделе вопросы технической инфраструктуры Интернета рассматриваются в двух различных плоскостях.

Первая, более широкая плоскость охватывает всю совокупность технической инфраструктуры, которая составляет Интернет. Сюда включается огромный спектр оборудования, программного обеспечения и протоколов, основанных на технических стандартах и бизнес-процессах, разработанных и реализованных на всех уровнях инфраструктуры Интернета. Одной из концепций, призванных обеспечить всеобъемлющую систематизацию информационных систем и их инфраструктуры на функциональном уровне, является Базовая эталонная модель взаимодействия открытых систем (сетевая модель OSI), значительный вклад в разработку которой внесло правительство США и техническое сообщество.[23]

Семь уровней модели OSI, которые иногда обобщаются в более крупные уровни (исходный уровень (Host layer) и уровень медиа (Media layer)), составляют приблизительную архитектурную концепцию инфраструктуры Интернета с точки зрения протоколов как специфического вида программного обеспечения, обеспечивающего функционирование Интернета на том или ином уровне. Тем не менее, каждый уровень сетевой модели OSI на физическом и техническом уровне представлен огромным и постоянно расширяющимся спектром инфраструктуры и программного обеспечения, начиная от магистральной инфраструктуры, волоконно-оптических кабелей, спутников, проводов, коммутаторов и маршрутизаторов, систем кабельных модемов, установок и оборудования для передачи, хранения и обработки данных в Интернете, и продолжая всевозможными серверами, устройствами и инфраструктурой конечных пользователей, программными приложениями, и т.д.

Важно отметить, что подавляющее большинство инфраструктуры ИКТ входит в состав инфраструктуры Интернета только когда такая инфраструктура тем или иным образом подключена или соединена с Интернетом, и, следовательно,

[23] См.: On OSI and its differences from the TCP/IP architecture concept http://electronicdesign.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip (последнее посещение 1 марта 2016 г.).

является частью глобальной сети. Как следствие, стандарты, технические политики и бизнес-процессы, связанные с инфраструктурой Интернета, в значительной степени являются неотъемлемым, хотя обособленным сегментом более широкой совокупности стандартов, политик и бизнес-процессов, разработанных и действующих в отношении информационных систем и ИКТ-инфраструктуры в целом.

Стандартизация и бизнес-процессы, которые определяют развитие и жизненный цикл перечисленных компонентов инфраструктуры, являются основной темой этого раздела, так как они определяют технические политики СБО для технической инфраструктуры Интернета. Общие стандарты для инфраструктуры ИКТ и информационных систем формировались в течение многих десятилетий с участием страновых технических регуляторов, межправительственных организаций, представителей частного сектора и технического сообщества.

Из числа стандартов, имеющих отношение к безопасности, стабильности и отказоустойчивости технической инфраструктуры, одним из наиболее известных являются Стандарты управления информационной безопасностью, разработанные негосударственным актором - Международной организацией по стандартизации (ИСО). В частности, Организация разработала ISO 17799 "Кодекс практики для управления информационной безопасностью", который позже был переиздан как ISO 27002 в новом семействе стандартов безопасности ISO 27000. Эта публикация содержит широкий перечень управленческих норм, включающий передовые практики в области информационной безопасности, и по-прежнему сохраняет важное значение как международно признанный общий стандарт информационной безопасности. Другим краеугольным камнем процесса стандартизации в области информационной безопасности являются Общие критерии оценки безопасности информационных технологий (Common Criteria), в разработку которых внесли вклад многочисленные национальные организации по стандартизации и правительственные учреждения, в том числе американский Национальный институт стандартов и технологии (NIST) и Агентство национальной безопасности США (NSA).

Главным достижением стандарта стала выработка системы ИТ-требований с известной областью применения, которые могут быть использованы при установлении требований безопасности для будущих продуктов и систем .[24] Еще один важным вкладом в стандартизацию в сфере ИБ стал Стандарт рекомендуемых норм по информационной безопасности, разработанный в рамках Форума по информационной безопасности (ISF), независимой неправительственной организации.[25] Кроме того, значимые разработки в области информационной безопасности и стандартизации инфраструктуры велись на площадках негосударственной Международной электротехнической комиссии (МЭК), американского Института инженеров по электротехнике и электронике (IEEE) и Рабочей группы по проектированию Интернет (IETF).

[24] Подробнее по стандартам ISO в области информационной безопасности и Общим критериям…. см..: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_standards.html (последнее посещение 1 марта 2016 г.).
[25] См.: https://www.securityforum.org/tools/sogp/ (последнее посещение 1 марта 2016 г.).

Вместе с тем, некоторые из числа стандартов, выступающих в качестве руководства для бизнес-процессов по обеспечению СБО, не ограничиваются техническими вопросами безопасности. Например, к таким стандартам относятся Стандарты управления непрерывностью бизнеса, разработка которых велась как на национальном, так и на международном уровне. Из числа внутристрановых стандартов одним из наиболее известных является американский Стандарт по регулированию реагирования на стихийные бедствия и чрезвычайные ситуации и программы непрерывной хозяйственной деятельности (NFPA 1600).[26] Положения стандарта охватывают развитие, внедрение, оценку и поддержание программ по предотвращению, минимизации последствий, обеспечению подготовленности, реагированию, обеспечению непрерывности и восстановления процессов. Национальная комиссия по террористическим атакам против США (Комиссия 9/11) признала NFPA 1600 в качестве Национального стандарта США по обеспечению готовности к чрезвычайным ситуациям.

Среди международных стандартов по обеспечению непрерывности бизнес-процессов наиболее известны стандарты Международной организации по стандартизации (ISO), включая ISO/PAS 22399, ISO 22301 and ISO/IEC 27031.

Стандарт ISO/PAS 22399 Общественная безопасность. Руководство по аварийной готовности и менеджмент постоянной готовности[27] предлагает общее руководство для частных, государственных и неправительственных организаций в части разработки ими собственных критериев оценки готовности к инцидентам и непрерывности процессов, а также в части разработки соответствующей системы управления. Последнее издание стандарта было опубликовано в 2007 г. Стандарт основан на обобщении лучших практик из пяти национальных стандартов: Австралии, Израиля, Японии, Великобритании и США, и актуален в том числе для инцидентов технологического характера наряду с другими видами инцидентов.

Стандарт ISO 22301 «Системы управления непрерывностью бизнеса (BCSMS) – Требования2[28] опубликован в 2012 г. является международным стандартом обеспечения непрерывности бизнес-процессов. Стандарт основан на модели, известной как цикл Деминга (планирование-действие-проверка-корректировка, 'Plan-Do-Check-Act'), и устанавливает требования для систем управления непрерывностью бизнеса (BCMS). К их числу относятся требования по планированию, организации, внедрению, использованию, мониторингу, поддержанию и последовательному улучшению документируемой системы управления. Задачи такой системы включают защиту от инцидентов, сокращение их вероятности, подготовку и реагирование, а также восстановление после наносящих ущерб инцидентов.

Наконец, в стандарте ISO/IEC 27031 Информационные технологии – Методы обеспечения защиты – Руководящие указания по готовности информационно-

[26] См.: См.: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600 (последнее посещение 1 марта 2016 г.).
[27] См.: http://www.iso.org/iso/catalogue_detail?csnumber=50295 (последнее посещение 1 марта 2016 г.).
[28] См.: http://www.iso.org/iso/catalogue_detail?csnumber=50038 (последнее посещение 1 марта 2016 г.).

коммуникационных технологий для ведения бизнеса[29] от 2011 г. посвящен конкретно вопросам непрерывности бизнеса в отрасли ИТ. В ISO/IEC 27031 структура или общие рамки (точнее, совокупность методов и процессов)для любой организации – частной, государственной или неправительственной. В стандарте выявляются и уточняются все аспекты, связанные с обеспечением непрерывности бизнеса и повышением ИКТ-готовности как составляющей системы управления ИБ организации, в том числе критерии оценки деятельности, подробные вопросы разработки и внедрения. Внедрение стандарта дает организации возможность измерить и оценить непрерывность и безопасность своих ИКТ-процессов, а значит и собственную готовность справиться с аварийной ситуацией, действуя последовательно и организованно.

Для бизнес-процессов, которые описывает этот стандарт, был введен общий термин – Готовность ИКТ к обеспечению непрерывности деловой деятельности (IRBC). Если критерии IRBC соблюдаются должным образом, поддерживается управление непрерывностью бизнеса (BCM) “за счет обеспечения должной устойчивости ИКТ-сервисов и их способности восстанавливаться до заданного уровня в пределах временных рамок, требуемых и согласованных организацией».

Все эти системы стандартов охватывают широкий перечень процессов и операций, связанных с обеспечением безопасности, стабильности и отказоустойчивости информационных систем и управления ими. Однако по большей части эти стандарты не являются специфическими именно для Интернета. Будучи уникальным глобальным технологическим феноменом в сфере ИКТ, Интернет опирается на эти общие стандарты и рекомендации (и именно поэтому они рассматриваются в этой главе), но в то же время требует специфической стандартизации с поправкой на свои инфраструктурные особенности. Такая стандартизация действительно возникла и развивается на протяжений нескольких десятилетий, в том числе в части, связанной с обеспечением стабильности, безопасности и отказоустойчивости, выработке соответствующих требований и организацией бизнес-процессов.

Фундаментальная причина потребности в специфической отрасли стандартизации - наличие уникального комплекса инфраструктуры, который характерен исключительно для Интернета и не имеет аналогов среди любых других сегментов инфраструктуры ИКТ или компьютерных сетей. Речь идет о системе УИИ, которая и составляет объект настоящего исследования. В этом разделе система УИИ рассматривается в рамках второго, узкого понимания технической инфраструктуры Интернета, с акцентом на вопросы, бизнес-процессы и процедуры стандартизации, связанные с обеспечением ее стабильности, безопасности и отказоустойчивости (СБО).

Чтобы исходить из общепринятого и технически корректного понимания системы УИИ, мы заимствуем необходимое определение из Устава ICANN (Статья 1: Миссия и Ценности, раздел 1: Миссия), в соответствии с которым система УИИ состоит из трех наборов уникальных идентификаторов Интернета:

а. Доменные имена (которые формируют систему DNS),

[29] См.: http://www.iso27001security.com/html/27031.html (последнее посещение 1 марта 2016 г.).

б. Адреса интернет-протоколов (IP-адреса) и номера автономных систем (ASN).
гр.
в. Порты протоколов Интернета и параметры нумерации.

В части определений, связанных с составляющими системы УИИ, нужно отметить определенную двусмысленность в определении системы доменных имен DNS, которая заложена в Подтверждении обязательств (AOC) от 2009 г. между Корпорацией Интернета и Министерством торговли США. В тексте AOC система доменных имён и адресов Интернета (DNS) определяется как «доменные имена; адреса протокола IP и адреса автономных систем; порты протокола и номера параметров». Такое понимание DNS де-факто охватывает все три компонента УИИ Интернета. Мы будем считать это определение исключением и в дальнейшем будем определять на DNS как набор протоколов и глобально распределенную иерархическую базу данных, предназначенную для трансляции IPv4 и IPv6 адресов в удобочитаемый для пользователя формат доменных имен.

2. Для Автономных Систем (АС) в настоящем исследовании используется определение, выработанное в рамках IETF и изложенное в соответствующих RFC: Автономная система представляет собой совокупность IP адресов с единой политикой маршрутизации (реализуется с помощью сетевого оборудования – маршрутизаторов),.

3. В исследовании не вводится специальное определение для протоколов Интернета и их портов, так как эти понятия являются общеупотребительными и не требуют расшифровки.

Для целей этого раздела ограниченный круг заинтересованных сторон также рассматривается в качестве непосредственных бенефициаров стабильной, безопасной и отказоустойчивой работы системы УИИ. Поскольку обеспечение стабильности, безопасности и отказоустойчивости осуществляется на уровне глобальной инфраструктуры Интернета, в качестве бенефициаров таких бизнес-процессов рассматриваются организации и структуры, которые: а) напрямую зависимы от работы глобальной технической инфраструктуры; б) напрямую взаимодействуют со структурами, обеспечивающими стабильность, безопасность и отказоустойчивость системы УИИ.

Таким образом, список бенефициаров стабильной, безопасной и отказоустойчивой работы системы УИИ включает в себя:

- операторов страновых и общих доменов верхнего уровня (ccTLDs и gTLDs);
- Локальные регистратуры Интернета (LIRs, преимущественно интернет-провайдеры) и Национальные регистратуры Интернета (NIRs, существуют в некоторых государствах).
- Правительства (в некоторых случаях также участвуют в бизнес-процессах, связанных с обеспечением стабильности, безопасности и отказоустойчивости).

Система доменных имен (DNS)

Система доменных имен (DNS) представляет собой набор протоколов и глобальную иерархически распределенную базу данных, которая предназначена для обеспечения перевода удобочитаемых доменных имен в данные в других форматах, в том числе перевод доменных имен в IPv4 и IPv6 адресов. В то же время, как отмечает Общество Интернета (ISOC), сегодня DNS выполняет в Интернете гораздо более широкий спектр функций, чем изначально, и в настоящее время выступает в качестве своего рода «оператора справочной системы» как для интерфейсов человек-машина, так и для машинно-машинных взаимодействий. Помимо трансляции IP-адресов в имена, DNS используется для получения сведений о почтовых серверах, криптографических ключах, географических значениях широты и долготы, а также других разнообразных типов данных. Большинство возможностей, которые предоставляет пользователям Интернет, критически зависимы от безопасного, стабильного и отказоустойчивого функционирования DNS.

Хотя система доменных имен обладает свойствами многоуровневой архитектуры и инфраструктурной иерархии, применительно к вопросам обеспечения СБО системы УИИ особое значение имеет верхний, корневой уровень ее иерархии, который олицетворяет корневая зона DNS. Инциденты с доменами верхнего уровня могут затрагивать большое количество интернет-пользователей и организаций по всему миру (особенно в случаях с доменами верхнего уровня общего назначения, такими как .org, .com и т.д.), однако все же не несут угрозы для СБО глобального Интернета или даже всей системы доменных имен. А вот с инцидентами в корневой зоне DNS ситуация иная.

Корневая зона, представляя собой верхний уровень архитектуры DNS, имеет критическое значение для обеспечения СБО системы УИИ. В настоящем исследовании рассматриваются лишь те факторы, которые могут сказываться на СБО Интернета в целом, так что в поле анализа попадает только глобальный уровень инфраструктуры. Таким образом, из всей системы DNS рассматривается лишь уровень ее корневой зоны, в то время как деятельность регистраторов и регистратур доменов верхнего уровня не является объектом исследования. Здесь ключевым бизнес-процессом является управление корневой зоной DNS, которое включает в себя генерацию и рассылку файла корневой зоны DNS (изменений к этому файлу), содержащего информацию обо всех доменах верхнего уровня и отсылки к связанным с ними IP-адресам. Файл корневой зоны – один из важнейших элементов системы УИИ; он уникален сам по себе и определяет границы системы доменных имен. В системе DNS в единственный момент времени может существовать лишь один файл корневой зоны, двух или более таких файлов быть не может. Появление второго подобного файла в системе по сути означает создание параллельного корня DNS. Поэтому обеспечение триады «конфиденциальность-целостность-доступность» в отношении данных на уровне корневой зоны DNS особо важно для поддержания СБО системы УИИ. В настоящем исследовании этот бизнес-процесс рассмотрен подробнее в Разделе 3.3.

Процесс стандартизации предшественника корневого файла DNS, – онлайн-файла с официальным списком имен хостов (по сути, имён подключенных к сети серверов) и закрепленных за ними IP адресов, который администрировала NIC, – начался в 1973 г. с RFC 606. С того времени система имен претерпела сложную

эволюцию, основные этапы которой обобщены в RFC 799, 805, 819 830, 882, 1034, 1035. RFC 1034 и 1035 до их пор играют роль ключевых стандартов, на которые опирается функционирование DNS. Тем не менее, разработка и стандартизация DNS не завершилась на этих RFC и продолжилась в RFC, 1591 («Структура системы доменных имен и делегирование»), RFC 1886 («Расширения DNS для поддержки IPv6») и других RFC, в том числе посвященных расширениям безопасности DNSSEC, которые рассматриваются в Разделе 3.2.

В инфраструктурном плане корневая зона DNS включает в себя 13 авторитативных серверов доменных имен (корневые серверы), которые играют роль корня DNS; серверы озаглавлены латинскими буквами с A по M. Комплекс корневых серверов в действительности включает в себя далеко не 13 аппаратных устройств, а множество дублированных машин, причем каждая копия действует как единая система и хранит информацию, которая и составляет корневую зону системы доменных имен.

Каждый из корневых серверов представляет собой распределенный комплекс инфраструктуры, который проектируется таким образом, чтобы не иметь единой точки отказа. Обычно каждый корневой сервер устанавливается и работает по схеме H+2 (5 серверных машин находятся в рабочем состоянии, еще 2 – в оперативном резерве), что можно проследить на примере корневого сервера B.[30] Такое инженерное решение является частью стратегии избыточного резервирования критически важного компонента системы доменных имен.

В целом, система корневых серверов в той или иной степени отвечает требованию географической распределенности[31]. Количество корневых серверов с годами постоянно растет для того, чтобы возможности системы отвечали растущим потребностям глобального Интернета, а также для того, чтобы сделать систему более устойчивой. Изначально, в 1980-х гг. насчитывалось всего три корневых сервера, все в США. До 1987 г. серверов было четыре. Наконец, сегодня их количество достигло предела (13 серверов), преодолеть который не позволяет ограничение в 512 байт на размер ответа DNS типа «отсылка» (DNS referral response), установленное изначально при разработке системы доменных имен[32]. Преодолеть упомянутую проблему ограничения на количество корневых серверов позволяет распространение копий корневых серверов, так называемых «зеркал». Зеркало конкретного корневого сервера содержит ту же информацию, что и основной сервер, и обслуживает поступающие к нему запросы так же, как и сам сервер.

По состоянию на июль 2015 г., на территории РФ были расположены 7 «зеркал» корневых серверов DNS, 3 из них в Москве; управление работой 7 «зеркал» осуществляют 5 операторов. Таким образом, обеспечивается надежность и резервирование системы корневых серверов и снижения риска критических сбоев в работе DNS вследствие целенаправленной атаки или любой другой угрозы. Хотя этот архитектурный дизайн формировался как ответ на естественный процесс расширения Интернета и адаптации системы DNS к растущим

[30] См.: http://www.isi.edu/b-root/ (последний доступ 1 марта 2016 г.).
[31] См. подробнее на стр. 11.
[32] См.: RFC 1035б https://www.ietf.org/rfc/rfc1035.txt (последнее посещение 1 марта 2016 г.).

потребностям и нагрузкам, он также отвечает требованиям СБО в отношении системы корневых серверов как одного из ключевых компонентов системы УИИ.

Развертывание глобальной системы зеркал корневых серверов DNS стало возможно благодаря применению технологи anycast, которая за последнее десятилетие стала критически важна для обеспечения СБО системы доменных имен. Ранняя стандартизация и обобщенное описание этой технологии отражены в RFC 3258[33].

Внедрение anycast на уровне корня DNS началось в 2003 г., когда было развернуто первое «зеркало» корневого сервера F, оператор которого (ISF) начал использовать эту технологию. После того как в ходе «тестирования» была доказана эффективность технологии и не было выявлено никаких негативных эффектов для СБО системы УИИ, развертывание «зеркал» корневых серверов стало общепринятой практикой среди операторов корневых серверов. Благодаря технологии anycast появилась возможность резервирования и обеспечения глобальной географической распределенности системы корневых серверов. В результате сегодня в мире насчитывается более 460 корневых серверов и их зеркал.

Основные технические решения, нацеленные на обеспечение СБО DNS, разработаны и применены к системе корневых серверов DNS включают DNSSEC, который подробно описан в разделе 3.2.

Ключевым бизнес-процессом, связанным с системой авторитетных корневых серверов DNS, является администрирование корневой зоны DNS; в силу важности этого процесса для обеспечения СБО системы УИИ он также рассматривается в разделе 3.2.

Адреса Интернет-протокола (IP)

Система распределения адресов Интернет-протокола (IP-адресов) является основным компонентом УИИ Интернета и в сумме с номерами Автономных Систем (АС) образует систему Ресурсов Нумерации Интернета. Как указано в RFC 770 от января 1980 г., IP-адрес представляет собой «числовой ярлык, присваиваемый каждому устройству (например, компьютеру, принтеру), участвующему в компьютерной сети, которая использует для коммуникации Интернет-протокол»[34]. Двумя ключевыми функциями IP являются: определение интерфейса хоста или сети и обращение к ее местонахождению. В совокупности с номерами АС, системой доменных имен и глобальной системой маршрутизации ресурсы IP-адресов образуют систему УИИ, что и описывается в разделе RFC 791: «Имя указывает, что мы ищем. Адрес указывает место, где находится искомый объект. Маршрут показывает, как к нему попасть».[35]

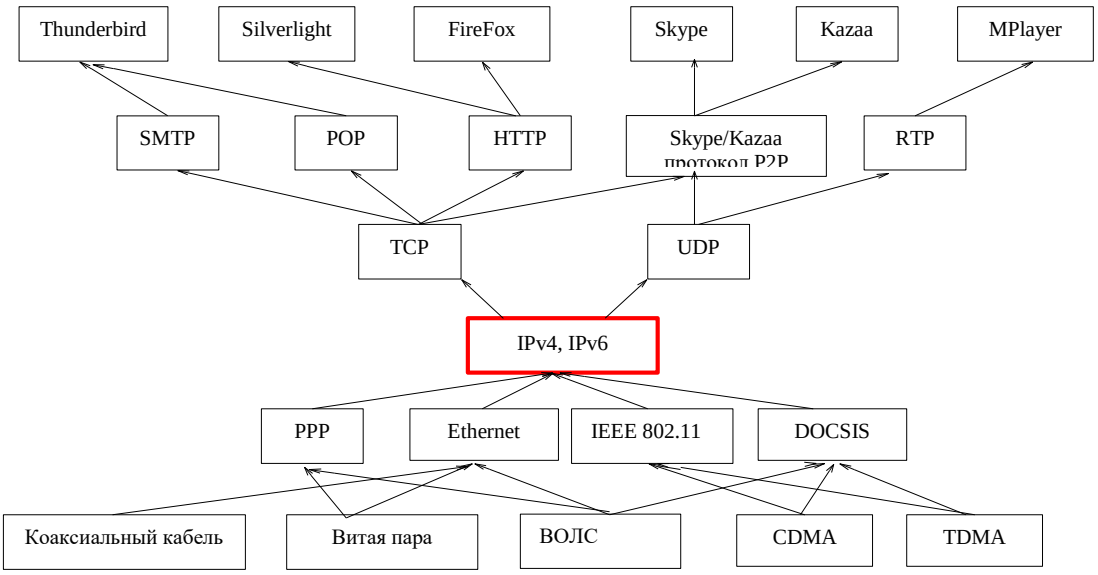
[33] RFC 3258. Distributing Authoritative Name Servers via Shared Unicast Addresses. См.: Рабочая группа по проектированию Интернет (IETF), https://www.ietf.org/rfc/rfc3258.txt (последнее посещение 1 марта 2016 г.).
[34] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc760 (последнее посещение 1 марта 2016 г.).
[35] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc791 (последнее посещение 1 марта 2016 г.).

Уникальность адресов Интернет-протокола (IP-адресов) – фундаментальное технологическое условие, за счет которого обеспечивается коммуникация и обмен трафиком между сетями в Интернете. Уникальность IP-адреса обеспечивает возможность того, что отправленные пакеты данных достигнут адресата, где бы тот не находился. Однако при этом сам Интернет-протокол – протокол без установки соединения, и вследствие этого при его использовании не обеспечивается гарантированное соединение и доставка дейтаграмм. Функцию установки соединения и гарантированной доставки данных выполняет Протокол управления передачей (TCP). Вместе с Интернет-протоколом TCP образует набор протоколов TCP/IP. И все же уникальность IP-адреса является ключевым условием, позволяющим системе маршрутизации построить рабочий маршрут к любому доступному ресурсу в Интернете. Если условие уникальности IP-адреса так или иначе нарушается, в системе маршрутизации может произойти коллизия, которая приведет к нарушению доступа к некоторым или ко всем таким узлам сети. Вот почему обеспечение и поддержание уникальности IP-адресов является критически важной задачей для всех заинтересованных сторон, вовлеченных в процесс функционирования системы УИИ. По этой причине существующий диапазон IP-адресов организован в глобальный пул IPv4 и IPv6 адресов, управление которым осуществляется в рамках иерархической модели распределения и присвоения IP-адресов с самого верхнего уровня (IANA) – Региональным регистратурам Интернет (РРИ), далее Локальным регистратурам и, в конце концов, конечным пользователям.

Сам Интернет-протокол не может быть необратимо поврежден или испорчен. Интернет-протокол не предполагает установления соединения между отправителем и получателем, равно как и не отслеживает маршрут пакета – его главная и единственная функция состоит в том, чтобы обработать пакет и отправить его к следующему узлу в Интернете; при этом нет никакой необходимости хранить данные об адресе его назначении и прочих параметрах. Эти свойства определяют феноменальную «живучесть» и устойчивость Интернета. Единственное условие, которое необходимо выполнять и поддерживать, – уникальность всех IP-адресов, анонсируемых и используемых в Интернете.

Основополагающую роль Интернет-протокола для функционирования системы УИИ и глобального Интернета в целом иллюстрирует схема EvoArch, разработанная в рамках исследования, проведенного в Колледже компьютерных наук при Технологическом институте Джорджии. *Схема песочных часов* отражает уникальность Интернет-протокола в многоуровневой модели протоколов, используемых для коммуникаций в Интернете. IP соответствует узкой горловине песочных часов, являясь ядром архитектуры Интернета в отсутствие каких-либо параллельных или альтернативных решений на том же уровне. В отличие от более высоких или низших уровней, на каждом из которых сосуществует множество протоколов и архитектурных решений, Интернет-протокол остается единственным в своем роде и незаменимым (хотя и претерпевает доработку до IPv6). Поэтому он не просто имеет критическое значение для Интернета – строго говоря, он и есть та технология, которая делает Интернет тем, чем он является – глобальной сетью сетей.

Схема 1. *Архитектурная модель Интернета в виде песочных часов (проект EvoArch)*



Источник: The Evolution of Layered Protocol Stacks Leads to an Hourglass-Shaped Architecture (extended version). Saamer Akhshabi, Constantine Dovrolis, College of Computing, Georgia Institute of Technology, http://www.cc.gatech.edu/~dovrolis/Papers/evoarch-extended.pdf (последнее посещение 1 марта 2016 г.).

Авторы RFC 760 изначально спроектировали IP-адреса виде 32-битных чисел; эта версия протокола известна как IPv4 и до сих пор широко используется во всем мире. Однако в последнее десятилетие все более активно ведется процесс внедрения следующей версии Интернет-протокола, IPv6. В конце 1980-х гг. техническому сообществу стало очевидно, что стремительное развитие и расширение Интернета не оставляют никаких шансов на то, что адресное пространство IPv4, ограниченное 4,295 млрд. уникальных адресов, смогло бы покрыть растущие потребности пользователей Интернета и ИТ-отрасли.

В качестве радикального технологического решения проблемы исчерпания адресного пространства IPv4 в 1995 г. была разработана и описана в RFC 1883 новая версия (спецификация) Интернет-протокола – IPv6, использующая адреса длиной 128 бит.[36] За счет увеличения длины адреса с 32 до 128 бит (или до 16 октетов), IPv6 формирует глобальное адресное пространство максимальным объемом до 2^{128}, или (с учетом возможных ограничений на практическое использование конечными пользователями) около 3.403×10^{38} адресов, что абсолютно покрывает все потребности интернет-пользователей даже при сценарии, когда бум Интернета Вещей создаст спрос на сотни триллионов уникальных адресов. Несмотря на довольно раннюю разработку и спецификацию IPv6 внедрение этой версии Интернет-протокола и обеспечение ее полной совместимости с предыдущей версией, IPv4, остается серьезной проблемой по сей день.

[36] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc2460 (последнее посещение 1 марта 2016 г.).

С точки зрения политик и бизнес-процессов, распределение ресурсов нумерации Интернета обеспечивается двумя основными акторами - ICANN (в основном в лице IANA) и Региональными регистратурами Интернет (РРИ). IANA в рамках своих функций распределяет крупные блоки ресурсов нумерации Интернета (IP-адресов и номеров АС) пяти Региональным регистратурам Интернета (РРИ): AFRINIC, APNIC, ARIN, LACNIC и RIPE NCC. РРИ, в свою очередь, распределяют меньшие блоки (стеки) ресурсов из полученного ими диапазона между организациями (такими как интернет-провайдеры) в рамках своих географических регионов. Политики и технические требования в отношении провайдеров, получающих стеки IP адресов, разрабатываются и осуществляются РРИ, поэтому в отличие от поддержания DNS и развития глобального пространства доменных имен, роль ICANN в распределении ресурсов нумерации Интернета не является ведущей. Именно РРИ являются ключевыми акторами, принимающими решения в сфере распределения и контроля использования ресурсов нумерации, которые имеют критическое значение для обеспечения СБО системы УИИ.

Подробная информация о РРИ и их политиках в сфере распределения Ресурсов Нумерации Интернета приводится в Разделе 3.2.

Что касается угроз СБО системы УИИ, ресурсы нумерации, включая собственно IP-адреса, сами по себе не имеют каких-либо критических уязвимостей. Однако система междоменной маршрутизации, основанная на Протоколе граничного шлюза 4-й версии (BGP-4) и использующая эти Ресурсы Нумерации, подвергается растущему числу масштабных инцидентов, которые влияют на работу глобальных интернет-сервисов. И все же, поскольку междоменная маршрутизация не входит в систему УИИ, ее слабые стороны и стратегии их нейтрализации лишь кратко рассматриваются в Разделе 3.4.

Автономные Системы (АС) и номера Автономных Систем (номера АС)

Автономные Системы (АС) и номера Автономных Систем (номера АС) вместе с адресами IP составляют Ресурсы Нумерации Интернета и, таким образом, являются частью системы УИИ.

Сама концепция Автономных Систем зародилась в инженерном сообществе в качестве идеи некоей «надстройки» над уровнем IP-адресов, которая бы позволяла агрегировать все их множество в ограниченную и управляемую совокупность более общих, но все же уникальных объектов Интернета. Необходимость в таком агрегировании обусловлена техническими ограничениями системы маршрутизации, связанной с невозможностью хранения на маршрутизаторах полной маршрутной таблицы для всего Интернета. Сегодня в этой системе используется Протокол граничного шлюза 4-й версии (BGP-4) для построения путей маршрутизации между Автономными Системами, которых насчитывается порядка 65 тыс. Количество доступных маршрутов передачи трафика прямо или опосредованно зависит от общего количества АС, и это важно для расчета путей маршрутизации, который производится на сетевом оборудовании, использующем BGP. Число доступных маршрутов в Интернете и их комбинации определяют размер так называемых таблиц маршрутизации, которые рассчитывают маршрутизаторы. Таким образом, в отсутствие

«агрегирования» междоменной маршрутизации до уровня АС, маршрутизация бы осуществлялась путем отправки пакетов данных напрямую между узлами сети с разными адресами IP. Даже применительно к Интернет-протоколу 4-й версии, глобальное адресное пространство которого ограничено 5,25 млрд. уникальных адресов, такой способ повлек бы колоссальный рост размера таблиц маршрутизации и ресурсоемкости процесса построения путей маршрутизации. В случае же с IPv6, глобальное адресное пространство которого составляет 2^{128} адресов, глобальная маршрутизация в Интернете стала бы невозможна из-за ограничений вычислительных мощностей сетевого оборудования, используемого для маршрутизации. Таким образом, АС по своей сути являются лишь необходимым средством упрощения процесса маршрутизации в сети Интернет.

В RFC 1930 Автономная Система (АС) определяется как группа из одного или нескольких префиксов IP (блоков IP адресов), находящихся в распоряжении у одного или нескольких сетевых операторов, которые имеют единую и четко определенную политику маршрутизации.[37] Процесс стандартизации АС стартовал чуть раньше с RFC 1771, опубликованном в марте 1995 г.[38]. Потребность в обновлении ранних RFC и определения АС возникла по мере развития инфраструктуры Интернета и связанных с ней изменений в политиках маршрутизации интернет-провайдеров.

Изначально, как было сформулировано в RFC 1771, понятие АС означало группу из одного или нескольких префиксов IP, работающих у одного сетевого оператора (интернет-провайдера или крупной организации, имеющей независимые множественные подключения к внешним сетям), которые имеют единую и четко определенную политику маршрутизации. Однако, это определение вскоре стало расходиться с практикой по мере того как различные организации получили возможность использовать Протокол граничного шлюза (BGP), предоставляя свои внутренние номера АС интернет-провайдерам, которые обеспечивали для них доступ в Интернет. Эти изменения обусловили нынешнее понимание АС и развитие процесса их стандартизации: даже если интернет-провайдер поддерживает множество АС, первостепенным критерием уникальной сущности, представленной и идентифицируемой в Интернете, является единая политика маршрутизации, которую осуществляет такой провайдер. Отсюда, официально зарегистрированный уникальный номер АС присваивается соответствующему интернет-провайдеру или иной организации, которая предоставляет доступ в Интернет. Таким образом, АС выполняют функцию еще одной разновидности Уникальных Идентификаторов Интернета для сетей, подключенных к Интернету.

Дальнейшая стандартизация АС и номеров АС после RFC 1930 была отражена в RFC 4271 (в котором рассматривался протокол BGP) и RFC 4893[39]. В последнем был введен новый формат номеров АС – 32-битные целые числа взамен использовавшихся ранее 16-битных. Это позволило увеличить общее доступное

[37] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc1930 (последнее посещение 1 марта 2016 г.).
[38] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc1771 (последнее посещение 1 марта 2016 г.).
[39] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc4893 (последнее посещение 1 марта 2016 г.).

количество уникальных номеров АС с 65,536 до 4,294,967,295 и предотвратить проблему их потенциально возможного исчерпания. Относительно недавно в RFC 6793[40] были сформулированы дальнейшие предложения по обновлению формата номеров АС – в частности, было предложено изменить присваиваемые АС номера с двухоктетного на четырехоктетный формат, чтобы подготовиться к возможному в будущем исчерпанию двухоктетных номеров. Такой шаг служит примером подхода, основанного на принципе раннего предупреждения проблем, поскольку текущее количество АС в глобальной системе маршрутизации по состоянию на 16 апреля 2015 г. составляло всего 50260.[41]

Регулирование АС и политик присвоения номеров АС осуществляется сходным путем с распределением IP-адресов. Администрация адресного пространства Интернет (IANA) распределяет блоки по 1024 номера АС между пятью РРИ, которые в свою очередь присваивают отдельные номера АС интернет-провайдерам и соответствующим другим организациям. Формальной базой для таких политик служит Политика распределения блоков номеров Автономных Систем между Региональными Регистратурами Интернет – часть Глобальных политик, согласованных между ICANN и Организацией поддержки адресов (ASO). Последний раз эта политика обновлялась в 2010 г.[42]

Сами процедуры распределения номеров АС никогда не вызывали серьезной критики со стороны технического сообщества, а стандарты и бизнес-процессы, связанные с номерами АС, не рассматривались в качестве уязвимых и способных стать причиной серьезных инцидентов, оказывающих влияние на СБО системы УИИ.

Номера портов и параметров протоколов Интернета

Номера портов и параметров протоколов, которые используются для коммуникации в Интернете, представляют собой заданные характеристики, составляющие третий и последний из рассматриваемых компонентов системы УИИ.

Из всех трех составляющих системы УИИ номера портов и параметров протоколов в наименьшей степени связаны с физической инфраструктурой. Согласованное использование номеров портов множеством сетевых операторов не требует наличия ресурсоемкой глобальной системы серверов, в отличие от, например, DNS. По сути, как параметры протоколов, так и номера портов Интернета являются открытой базой данных, которая закреплена за ответственной организацией, но ведется открыто и доступна каждому сетевому оператору в Интернете.

В силу своей открытой и реплицируемой сущности, номера портов сами по себе не подвержены каким-либо атакам или злонамеренным действиям, которые

[40] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc6793 (последнее посещение 1 марта 2016 г.).
[41] См.: CIDR REPORT for 16 Apr 15, http://www.cidr-report.org/as2.0/ (последнее посещение 1 марта 2016 г.).
[42] См.: https://www.icann.org/resources/pages/global-policy-asn-blocks-2010-09-21-en (последнее посещение 1 марта 2016 г.).

могли бы нарушить их работу в глобальном масштабе или нанести серьезный ущерб функционированию глобального Интернета. Использование номеров портов злоумышленниками имеет место при определенных видах атак, однако речь идет об инцидентах локального масштаба, которые можно успешно нейтрализовать силами самих сетевых операторов. Более того, изменение присваиваемых по умолчанию номеров портов иногда производится самими сетевыми операторами с целью предотвращения либо нейтрализации некоторых видов атак и других инцидентов. Например, анонсирование нового порта для входящего трафика HTTP вместо стандартного номера (Порт 80) иногда используется чтобы блокировать поток вредоносного трафика, сгенерированного в результате атаки типа Распределенный отказ в обслуживании (DDoS). Эксплуатация номеров портов злоумышленниками не представляет сколь-либо существенной угрозы СБО системы УИИ и потому не рассматривается в настоящем исследовании.

Параметры протоколов публикует и обновляет у себя на сайте IANA в виде Регистров [43] – открытых баз данных, которые дублируются на сайте Рабочей группы по проектированию Интернет. Совместный надзор за деятельностью IANA в качестве оператора Регистров параметров протоколов осуществляют Министерство торговли США и Совет по архитектуре Интернета (IAB)[44].

Номера портов протоколов также публикуются и поддерживаются IANA в форме Регистров (см., например: Регистр имен сервисов и номеров портов протоколов транспортного уровня[45]). Номера портов протоколов подразделяются на три категории: известные порты, зарегистрированные порты и динамически выделяемые и/или частные порты. К известным портам относятся порты с номерами от 0 до 1023; к зарегистрированным – от 1024 до 49151, а к динамически выделяемым/частным портам – от 49152 до 65535.

3.2. Ключевые участники стандартизации процесса обеспечения стабильности, безопасности и отказоустойчивости

Процесс стандартизации обеспечения СБО системы УИИ ведется при участии значительного числа организаций, форматов сотрудничества, рабочих площадок и процессов, которые в совокупности образуют глобальное техническое сообщество по управлению Интернетом. Основной рабочий процесс по стандартизации инфраструктуры Интернета, включая выработку стандартов СБО, исторически сложился в рамках формата Запроса комментариев (RFC) на площадке Рабочей группы по проектированию Интернета (IETF). Также участниками этого процесса являются: Общество Интернета (ISOC), Совет по архитектуре Интернета (IAB), Консорциум Всемирной Сети (W3C), Рабочая группа по проектированию Интернет (IETF), Рабочая группа по исследованию Интернет (IERG), а также Управляющая группа по проектированию Интернета (IESG), Региональные регистратуры Интернет , в том числе через Организацию ресурсов нумерации Интернет (NRO), а также многие другие рабочие площадки

[43] См.: http://www.iana.org/protocols (последнее посещение 1 марта 2016 г.).
[44] Подробнее см.: https://www.iana.org/about/presentations/cotton-internal-20101025.pdf (последнее посещение 1 марта 2016 г.).
[45] См.: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml (последнее посещение 1 марта 2016 г.).

технического сообщества. Кроме того, правительство США в лице Министерства торговли (а именно, Национальной администрации по телекоммуникациям и информации (NTIA)) также играет определенную роль в этом процессе, и в частности является участником контракта No.SA1301-12-CN-0035 от 1 октября 2012 г. (контракт на осуществление функций IANA), пока не завершен процесс передачи ответственного управления функциями IANA от NTIA глобальному сообществу заинтересованных сторон.[46] Наконец, некоторые субъекты частного сектора, такие как Verisign, также упоминаются в настоящем исследовании, поскольку выполняют определенные технические функции, связанные с обеспечением СБО системы УИИ, а их внутренние технические процедуры и стандарты могут требовать рассмотрения.

Правительства

Все правительства являются бенефициарами стабильной, безопасной и отказоустойчивой работы системы УИИ. Однако роль различных правительств как заинтересованных сторон в этой сфере неоднозначна: некоторые из них, такие как правительство США, исторически были вовлечены в осуществление и контроль критических бизнес-процессов. В юрисдикциях некоторых других государств находятся и ведут свою деятельность критически важные технические структуры и другие участники процесса обеспечения СБО глобальной инфраструктуры Интернета. В частности, в этом разделе рассматриваются государства, в чьих юрисдикциях находятся операторы корневых серверов DNS и Региональные регистратуры Интернет (РРИ). В большинстве случаев нахождение в рамках национальной юрисдикции для таких структур имеет лишь формальное значение и не влияет на повседневную техническую деятельность ни операторов корневых серверов, ни РРИ. Однако в некоторых случаях государственная юрисдикция может выступать мощным ресурсом правительств в их диалоге с вышеупомянутыми представителями глобального технического сообщества.

- *США*

Когда-то США создали Интернет, однако сегодня функции американского правительства, напрямую влияющие на обеспечение СБО системы УИИ, довольно ограничены и легко поддаются перечислению. Тем не менее, некоторые из них остаются критически важными для глобального Интернета.

Основной перечень таких полномочий правительства США включает в себя ответственное управление функциями Администрации адресного пространства Интернет (IANA), осуществляемое в рамках упомянутого контракта между ICANN и Министерством торговли США (в лице NTIA). Однако в настоящее время ожидается, что процесс передачи ответственного управления функциями IANA вскоре завершится.

Что также немаловажно, правительство США No. NCR 92-18742 остается участником договора (Соглашение о сотрудничестве No. NCR 92-18742) с

[46] См.: http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf (последнее посещение 1 марта 2016 г.).

компанией Verisign (ранее была известна как NSI), включая ряд поправок и обновлений к этому документу (всего 32 поправки). Несмотря на то, что предметом договора прежде всего являются функции Verisign в качестве регистратуры доменов верхнего уровня общего назначения .NET, .COM и .ORG, в Поправке 11 от 7 октября 1998 г. упоминается еще одна функция, которую Verisign в силу исторически сложившихся обстоятельств исполняет с начала 1990-х гг.[47] Речь идет о технической поддержке корневой зоны DNS, что в частности включает в себя два вида деятельности, которые являются частью более широкого процесса управления корневой зоной DNS (в котором также непосредственно участвуют IANA и NTIA). Функции NSI/Verisign в качестве технического менеджера корневой зоны включают: 1) генерирование файла корневой зоны на первичном авторитативном сервере и 2) рассылка сгенерированного файла корневой зоны на остальные авторитативные серверы корневой зоны. Эти критические функции NSI/Verisign более подробно рассматриваются в разделе 3.3.

За рамками ответственного управления функциями IANA, прямое участие правительства США в стандартизации и бизнес-процессах в сфере обеспечения СБО системы УИИ невелико. Вместе с тем, некоторые государственные организации в США остаются операторами корневых серверов DNS. Так, НАСА (в лице Исследовательского центра Эймса) является оператором корневого сервера E, Министерство обороны США (в лице Центра сетевой информации) управляет корневым сервером G; Исследовательская лаборатория Армии США – корневым сервером H. Кроме того, не следует забывать, что в целом 9 операторов авторитативных корневых серверов DNS из 13 зарегистрированы в американской юрисдикции.

Далее, одна из РРИ – ARIN, зарегистрирована и имеет штаб-квартиру в г. Шантильи, штат Вирджиния, и таким образом также ведет деятельность в юрисдикции США. Это находит отражение в корпоративных документах ARIN: согласно Уставу Регистратуры, ее главным органом управления является Попечительский совет, чьи полномочия “подпадают под все соответствующие ограничения, указанные в Уставе и соответствуют положениям Закона о неакционерных обществах штата Вирджиния в их нынешней формулировке или с учетом возможных будущих поправок».[48] Факты реального влияния американской юрисдикции на постоянные бизнес-процессы ARIN до сих пор не были выявлены. Однако национальная юрисдикция все имеет большое значение для понимания обязательств и правового статуса технических структур, таких как ARIN, которые участвуют в обеспечении и поддержании СБО системы УИИ.

- *Другие правительства*

Помимо США, список государств, осуществляющих юрисдикцию над РРИ включает *Нидерланды* (RIPE NCC); *Австралию* (APNIC), *Уругвай* (LacNIC) и *Маврикий* (AfriNIC). Как отмечается на странице вебсайте Организации ресурсов

[47] См.: http://www.ntia.doc.gov/files/ntia/publications/amend11_052206.pdf (последнее посещение 1 марта 2016 г.).
[48] См.: Bylaws of American Registry for Internet Numbers, Ltd. (Formed under the Virginia Nonstock Corporation Act). https://www.arin.net/about_us/corp_docs/bylaws.html (последнее посещение 1 марта 2016 г.).

нумерации (NRO) «Вопросы и ответы по подотчетности РРИ», техническая работа Регистратур должна вестись в соответствии с нормами законодательства того государства, на территории которого находится соответствующая Регистратура.[49] Конкретные разделы права, особо значимые для деятельности РРИ, включают законодательство о защите данных и корпоративное право. Важность последнего иллюстрирует приведенный выше пример ARIN. Кроме того, РРИ периодически сотрудничают с органами правопорядка, как в рамках «своих» национальных юрисдикций, так и с иностранными. Большинство Регистратур (за исключением AfriNIC) разработали правила и политики обработки запросов на предоставление информации от государственных органов правопорядка.

К примеру, RIPE NCC обобщила свои политики в специальном документе, выступающем в качестве руководства по взаимодействию с правительством Нидерландов по вопросам раскрытия информации.[50] В документе подчеркивается, что Регистратура не отказывается от сотрудничества с голландскими властями, но подчеркивается, что RIPE NCC не будет предоставлять органам правопорядка какую-либо конфиденциальную или приватную информацию в отсутствие судебного ордера или другого имеющего обязательную юридическую силу документа, выданного в соответствии с законодательством Нидерландов.

В плане обеспечения СБО важнее то, что в документе четко прописан отказ RIPE NCC добровольно исполнять запросы органов правопорядка на Специальные действия, такие как внесение изменений в какие-либо конкретные ресурсы нумерации Интернета. В документе перечислен ограниченный перечень обстоятельств и условий, при которых Регистратура будет вынуждена исполнить такой запрос от органов правопорядка:

«RIPE NCC будет удовлетворять такие запросы только в том случае, если орган правопорядка Нидерландов действует на основании соответствующего ордера, выданного органом судебной власти Нидерландов, либо на основании обязательного для исполнения приказа, изданного уполномоченным органом правопорядка или иным органом государственной власти Нидерландов, действующим в соответствии с нормами уголовного и административного права Нидерландов (в т.ч. Государственной Прокуратурой, Полицией, Налоговой службой и Службой расследований)». Особо подчеркивается, что в отношении правительств и органов правопорядка, представляющих другие юрисдикции, чем сама RIPE NCC (Нидерланды), доступные форматы взаимодействия ограничены процедурами, устанавливаемыми в рамках договоров о взаимной юридической помощи (MLAT), что означает невозможность принудительного исполнения требований и запросов, касающихся деятельности Регистратуры. Более того, даже в случае получения запроса, подкрепленного судебным или иным ордером, RIPE NCC оставляет за собой право не исполнять такой запрос в случае, если по итогам собственной правовой оценки сочтет его незаконным или не имеющим обязательной силы.

[49] См.: https://www.nro.net/about-the-nro/rir-accountability#241 (последнее посещение 1 марта 2016 г.).
[50] См.: Handling Requests for Information, Orders and Investigations from Law Enforcement Agencies. https://www.ripe.net/publications/docs/ripe-588 (последнее посещение 1 марта 2016 г.).

Такой подход обеспечивает определенные гарантии независимости деятельности РРИ от государственного вмешательства, особенно в отношении технических бизнес-процессов, связанных с обеспечением СБО системы УИИ. Вместе с тем, государство по определению обладает б*о*льшим объемом властного ресурса и правовых инструментов, чем любая организация в его юрисдикции, даже если у такой организации весьма хорошо проработаны политики взаимодействия. Поэтому роль государств, в чьей юрисдикции находятся РРИ, никогда не следует сбрасывать со счетов при оценке баланса интересов различных заинтересованных сторон в отношении СБО системы УИИ.

Также стоит отметить, что из числа РРИ RIPE NCC исторически имела самые развитые технические процедуры и политики, а также наиболее проработанные подходы к правовым вопросам и внутренним нормам. Другим Регистратурам, особенно LacNIC и AfriNIC, пока недостает комплексного и четкого подхода к взаимодействию с органами правопорядка, поскольку их практики и процедуры в этой области находятся лишь в стадии формирования. Что касается Запросов на специальные действия, на сегодняшний день RIPE NCC остается единственной Регистратурой, у которой есть подробно проработанная позиция, защищающая независимость бизнес-процессов по распределению Ресурсов Нумерации. Выработка подобных позиций, принципов и процедур важна, поскольку в регионах за пределами Европы у правительств может быть больше причин и утвердившихся практик вмешательства в работу организаций, находящихся в их юрисдикции. Однако на сегодняшний день не было зафиксировано случаев прямого государственного вмешательства в осуществление бизнес-процессов РРИ, которое могло бы сказаться на обеспечении СБО системы УИИ. На самом деле, задокументированных случае существенного государственного вмешательства в технические операции РРИ вообще не отмечалось.

Тем не менее, все существующие риски в этой области следует купировать на ранней стадии за счет укрепления и поддержки четко определяемых процедур, внутренних норм и общих принципов среди РРИ и других структур технического сообщества.

Два других государства, которые имеют особые интересы в качестве участников процесса обеспечения СБО системы УИИ – Швеция и Япония, на территории которых действуют операторы корневых серверов DNS. По сути, к списку можно добавить и Нидерланды, поскольку RIPE NCC помимо функций РРИ также является оператором корневого сервера K.

В Швеции управление корневым сервером I осуществляет некоммерческая, нейтральная и независимая техническая инфраструктурная организация Netnod Internet Exchange i Sverige (более известна как Netnod), которая также является оператором 5 точек обмена трафиком (IXPs) в Швеции и одной точки в Дании, а также предоставляет ряд других сервисов. В отличие от РРИ, операторы корневых серверов обычно не разрабатывают специальных политики и заявлений по работе с запросами от органов правопорядка. Вместе с тем, Netnod в числе других операторов корневых серверов развивает формализованные отношения с ICANN с 2009 г., когда оператор опубликовал письмо, подтверждающее

приверженность обеспечению безопасной и отказоустойчивой работы корневого сервера I.[51]

Управление корневым сервером M осуществляет Проект WIDE (аббр. от «Широко интегрированная распределенная среда»), который сегодня управляет опорной сетью в японском сегменте Интернета. Как и Netnod, Проект WIDE не публиковал никаких открытых политик в части исполнения запросов японского правительства, которые теоретически могли бы повлиять на функционирование сервера M. С другой стороны, в ходе исследования не удалось обнаружить какие-либо прецеденты, когда государственные структуры Японии пытались осуществить подобное вмешательство.

ICANN и IANA

Корпорация Интернета играет ключевую роль в обеспечении СБО системы УИИ, прежде всего, поскольку она отвечает за исполнение функций IANA и является участником договора на исполнение этих функций с NTIA. Как уже отмечалось ранее, в Уставе ICANN, включая изложенную в нем миссию, четко прописана ответственность Корпорации за обеспечение СБО системы УИИ[52]. Эта роль ICANN также закрепляется соглашениями между Корпорацией и правительством США (договор на исполнение функций IANA, Меморандум о намерениях от 2009 г. и проч.).

Вместе с тем, ICANN выступает не только в качестве оператора функций IANA – Корпорация также управляет одним из авторитативных корневых серверов системы доменных имен (корневой сервер L), устанавливает правила и политики делегирования и использования доменов верхнего уровня и, что особо важно для обеспечения СБО системы УИИ, формирует и обеспечивает работу множественных площадок и рабочих процессов, компетенция которых охватывает практически все ключевые вопросы обеспечения СБО. Так, вопросы СБО на площадке ICANN прорабатываются в рамках Консультативного комитета системы корневых серверов (RSSAC), формируемого из представителей операторов корневых серверов DNS.

Корпорация Интернета формирует и способствует развитию площадок взаимодействия между почти всеми существующими организациями и рабочими процессами глобального технического сообщества.[53] Сюда входит взаимодействие с IETF и IAB, РРИ (в рамках Организации поддержки адресов (ASO) и Организации ресурсов нумерации Интернет (NRO), Консорциумом Всемирной Сети (W3C) и Обществом Интернета (ISOC). Не забирая себе функции IETF по стандартизации системы УИИ, Корпорация Интернета играет роль ключевой площадки для обсуждения всех политики и вопросов, связанных с системой УИИ, в том числе вопросов обеспечения ее СБО.

[51] См.: http://www.netnod.se/sites/default/files/autonomica-signed-mri.pdf (последнее посещение 1 марта 2016 г.).
[52] См.: https://www.icann.org/resources/pages/governance/bylaws-en/#I (последнее посещение 1 марта 2016 г.).
[53] См.: https://www.icann.org/resources/unthemed-pages/ietf-icann-mou-2000-03-01-en (последнее посещение 1 марта 2016 г.).

Администрация адресного пространства Интернет (IANA) является техническим департаментом ICANN, который отвечает за осуществление определенных функций, связанных с DNS и СБО системы УИИ. Эти функции включают в себя:

- координация присвоения параметров технических протоколов, которые обеспечивают функционирование Интернета;
- управление файлом корневой зоны DNS и ряд других функций, связанных с системой корневых серверов DNS;
- собственно делегирование и распределение ресурсов нумерации Интернета (IP-адреса автономных систем);
- управление доменом верхнего уровня .int (зарезервирован для межправительственных организаций), а также доменом верхнего уровня .arpa и рядом других доменов, зарезервированных для специальных технических функций, связанных с поддержанием функциональности глобальной системы DNS.

Очевидно, что эти функции имеют критически важное значение для обеспечения СБО системы УИИ. Поскольку IANA до сих пор не имеет собственного юридического лица и остается инкорпорированной в структуру ICANN с 1999 г. по настоящий момент, над исполнением некоторых из ее функций осуществляет ответственное управление правительство США. Основой такого взаимодействия служит некоммерческий договор №.SA1301-12-CN-0035 от 1 октября 2012 г. (продлен до 30 сентября 2016 г.), известный как Договор об ответственном управлении исполнением функций IANA. В настоящее время ответственное управление функциями IANA находится в процессе передачи от правительства США глобальному сообществу заинтересованных сторон. Однако вне зависимости от структуры и статуса организации, которой планируется передать ответственное управление, процесс передачи не должен повлиять ни на сам круг функций IANA, ни на их техническое исполнение.

Рабочая группа по проектированию Интернет (IETF), Консорциум Всемирной Сети (W3C), Общество Интернета (ISOC)

Рабочая группа по проектированию Интернет (IETF) не имеет юридического лица и вообще не является организацией. Группу можно охарактеризовать как рабочий процесс, объединяющий представителей технического сообщества преимущественно на добровольной некоммерческой основе. При этом в течение многих лет IETF остается центральной площадкой работы по стандартизации протоколов и технических параметров DNS, распределения IP-адресов и решению других вопросов, связанных с обеспечением СБО системы УИИ.

Ключевым механизмом для работы IETF в сфере стандартизации является механизм Запроса комментариев (RFC); такие запросы публикуются онлайн и обычно содержат общее техническое описание предлагаемых систем стандартов. Хотя Запросы комментариев не имеют никакой юридической силы, они играют роль основополагающего механизма выработки консенсуса по вопросам стандартизации протоколов и параметров Интернета для технического сообщества, частного сектора и других заинтересованных сторон.

Вопросы обеспечения СБО также относятся к деятельности IETF поскольку почти каждому протоколу и стандарту Интернета присущи аспекты, связанные с обеспечением СБО, либо необходима проработка вопросов его собственных параметров и свойств в части безопасности. В структуре IETF, в той мере в которой она рассматриваться с формальной точки зрения, насчитывается более 120 Рабочих Групп, некоторые из которых занимаются непосредственно вопросами безопасности. Эти Рабочие группы, так же, как и IETF в целом, вносят вклад в дискуссии и практическую работу по стандартизации для обеспечения СБО, ведущиеся в рамках большинства структур технического сообщества, включая ICANN и IANA, Организацию ресурсов нумерации и Организацию поддержки адресов, РРИ, Совет по архитектуре Интернета и проч.

Что примечательно, IETF также определила процесс и цели разработки Стандартов Интернета в своем Запросе комментариев (RFC 2026): «Процесс выработки Стандарта Интернета является последовательным: предлагаемая спецификация проходит период разработки и несколько этапов рассмотрения и внесения поправок участниками интернет-сообщества, основывающимися на своем опыте, утверждается в качестве Стандарта соответствующей структурой и затем публикуется. На практике, процесс является более сложным в силу (1) сложности разработки спецификаций высокого технического качества; (2) необходимости учитывать интересы всех сторон; (3) важности достижения широкого консенсуса в рамках сообщества; и (4) сложности оценки полезности той или иной отдельно взятой спецификации для интернет-сообщества»[54].

IETF играет роль непосредственного рабочего процесса по созданию и обсуждению Стандартов Интернета, но в его работу вносят вклад и другие структуры технического сообщества, которые также участвуют в деятельности по стандартизации. В их числе Общество Интернета (ISOC) и Консорциум Всемирной Сети (W3C). Тогда как W3C разрабатывает определенные стандарты, такие как Open Web Platform для разработки приложений (CSS, SVG, WOFF, the набор Semantic Web, XML и проч.), Общество Интернета само по себе не разрабатывает стандарты, но выступает в качестве поддерживающей структуры и «проводника» работы и дискуссий IETF, продвигая ее повестку дня в сфере стандартизации.

Организация ресурсов нумерации Интернет (NRO), Организация поддержки адресов (ASO) и Региональные Регистратуры Интернет (РРИ)

Региональные Регистратуры Интернет (РРИ) управляют распределением и регистрацией Ресурсов Нумерации Интернет, которые им выделяет IANA. Сегодня насчитывается пять РРИ, которые вместе образуют Систему Регистрации Ресурсов Нумерации Интернет, описанную Рабочей группой по проектированию Интернет в RFC 7020.[55]. В число РРИ входят: APNIC, LACNIC, RIPE NCC, ARIN и AfriNIC, зоны деятельности которых более или менее строго соответствуют границам географических регионов, и в совокупности охватывают весь мир, включая даже Антарктиду (в зоне ARIN). С юридической точки зрения РРИ представляют собой некоммерческие неинкорпорированные ассоциации,

[54] См.: https://datatracker.ietf.org/doc/rfc2026 (последнее посещение 1 марта 2016 г.).
[55] https://tools.ietf.org/html/rfc7020 (последнее посещение 1 марта 2016 г.).

осуществляющие свою деятельность и объединяющие членов из определенных регионов. Вместе с тем, критерии членства в РРИ могут и не предполагать ограничений по географическому признаку (например, в случае с APNIC и RIPE NCC).

РРИ играют ключевую роль в распределении Ресурсов Нумерации Интернет, включая IP-адреса и номера Автономных Систем. Крупные блоки IP-адресов (начиная с 2011 г. речь идет об адресах 6-й версии, IPv6) и блоки номеров АС выделяет каждой из Регистратур IANA в рамках своих функций. Процесс выделения IP-адресов и номеров АС и соответствующие решения основываются на технических требованиях к РРИ, отчетам Регистратур перед ICANN и, в случае с недавно созданными РРИ, на оценке их соответствия техническим и иным установленным требованиям.

После получения Ресурсов Нумерации от IANA, Регистратуры в целом свободно могут распределять их между интернет-провайдерами и другими организациями в соответствии с политиками и процедурами, которые они сами устанавливают. Этот момент принципиально важен, так как ни Корпорация Интернета, ни Национальная администрация по телекоммуникациям и информации США (NTIA), ни государство, в чьей юрисдикции находится Регистратура, не имеют права контролировать политики РРИ по распределению Ресурсов Нумерации. Политики РРИ обобщаются в регулярно обновляемых Сравнительных обзорах политик РРИ. При этом начиная с первого издания этого документа, формулировка цели системы РРИ не изменилась: «Вся деятельность по распределению и присвоению ресурсов Интернета должна осуществляться в соответствии с целями Системы Регистрации Ресурсов Нумерации Интернета: агрегирование, сохранение и регистрация».[56] В Обзорах политик также приводится всеобъемлющий сравнительный перечень технических политик РРИ в отношении распределения Ресурсов Нумерации, технических требований и иных требований соответствия для получателей таких ресурсов и т.д. Для того, чтобы согласовывать, артикулировать и гармонизировать эти технические политики, равно как и другие вопросы, РРИ нуждаются в механизме взаимодействия. По вопросам, связанным с IP-адресами, таким механизмом изначально выступала Организация поддержки адресов (ASO), которая была основана в 1999 г. и аффилирована с Корпорацией Интернета.

Несколькими годами позже был запущен еще один механизм, со временем по большей части заместивший ASO в качестве интерфейса взаимодействия и разработки политик РРИ. Таким механизмом стала Организация ресурсов нумерации Интернет (NRO), не инкорпорированная организация, объединяющая 5 РРИ. NRO была учреждена 24 октября 2003 г., когда 4 существовавших на тот момент РРИ (без AfriNIC, которая была основана и присоединилась к NRO в 2005 г.) заключили Меморандум о взаимопонимании для того, чтобы осуществлять совместную деятельность, включая совместные технические проекты, координацию взаимодействия и политик. Согласно Меморандуму о взаимопонимании между ICANN и Организацией поддержки адресов от 2004 г. (который по сути был соглашением между ICANN и NRO), Организация ресурсов

[56] См.: https://www.nro.net/rir-comparative-policy-overview/rir-comparative-policy-overview-2015-01#1-1 (последнее посещение 1 марта 2016 г.).

нумерации Интернет взяла на себя роль, обязанности и функции ASO[57]. Сегодня РРИ взаимодействуют между собой, а также с ICANN и структурами технического сообщества преимущественно в рамках площадки NRO.

В процедурах, которым следуют РРИ при распределении Ресурсов Нумерации, в качестве ключевых контрагентов выступают Локальные Регистратуры Интернет (ЛРИ) и иногда, для некоторых национальных юрисдикций, Национальные Регистратуры Интернет (НРИ). В то время как функцию ЛРИ в большинстве случаев выполняют интернет-провайдеры, обслуживающие собственные АС (и таким образом соответствующие критериям получателя номера АС), в роли НРИ могут выступать более специфические организации. Обычно НРИ – это член Региональной Регистратуры Интернет, который отвечает за распределение Ресурсов Нумерации в рамках какого-либо государства или экономики. На сегодняшний день, НРИ отсутствуют в регионе ответственности RIPE NCC, однако определенное количество НРИ присутствует в регионах APNIC (в том числе китайская CNNIC, японская JPNIC, тайваньская TWNIC, Индийская регистратура имен и адресов Интернета т.д.), а также LACNIC (Центр сетевой информации Мексики (NIC Mexico), Центр сетевой информации Бразилии (NIC Brazil), Центр сетевой информации Чили (NIC Chile)).

Локальные (ЛРИ) и Национальные (НРИ) Регистратуры Интернет являются бенефициарами обеспечения СБО системы Ресурсов Нумерации Интернета; эти организации осуществляют дальнейшее распределение диапазонов IP-адресов между интернет-провайдерами, а также присваивают им номера АС. Цепочка распределения IP-адресов ведет от IANA к РРИ, затем к Локальным Регистратурам и далее к провайдерами последней мили, которые присваивают конкретные IP-адреса узлам сети, ассоциированным с устройствами конечных пользователей в Интернете. Что касается номеров АС, цепочка их распределения гораздо короче, так как она заканчивается, когда ЛРИ присваивают номера АС менее крупным интернет-провайдерам.

Межправительственные организации: Международный союз электросвязи

Международный союз электросвязи (МСЭ), специализированное агентство ООН по ИКТ, также частично участвует в стандартизации ИКТ-сектора, в том числе в связи с вопросами обеспечения СБО. Однако, в отношении системы УИИ МСЭ скорее представляет собой довольно любопытный случай латентного регуляторного потенциала, что вполне можно рассматривать и в позитивном ключе.

МСЭ внес существенный вклад в стандартизацию и продвижение базовой эталонной модели взаимодействия открытых систем (модель OSI). Модель также известна как модель ISO-OSI, поскольку ее разработку и стандартизацию изначально осуществляла Международная организация по стандартизации (ISO) в рамках проекта «Взаимодействие открытых систем» с присвоенным идентификатором ISO/IEC 7498-1. Стандарт Базовой эталонной модели взаимодействия открытых систем от 1983 г. был опубликован в 1984 г. самой ISO

[57] См.: https://aso.icann.org/about-the-aso/aso-memorandum-of-understanding (последнее посещение 1 марта 2016 г.).

(ISO 7498), а также, под кодом «Стандарт X.200», Международным консультативным комитетом по телеграфии и телефонии (CCTTI), который позднее был преобразован в Сектор стандартизации электросвязи МСЭ (МСЭ-Т).

Дальнейшее улучшение и развитие стандартизации модели ISO-OSI преимущественно проводилось на площадке МСЭ, хотя этот стандарт также до сих пор остается стандартом ISO.

Работа над моделью ISO-OSI в дальнейшем велась в рамках развития серии стандартов X.200, а также последующих серий стандартов.[58] Позднее, в рамках МСЭ была разработана отдельная серия стандартов (X.800), посвященная безопасности архитектуры Взаимодействия открытых систем. Первая рекомендация в рамках серии X.800 включала в себя набор механизмов обеспечения безопасности и сервисов для модели OSI, в том числе:[59]

- базовые сервисы безопасности (аутентификация равноправного объекта и аутентификация источника данных, конфиденциальность данных, контроль доступа и т.д.);
- специальные механизмы безопасности (симметричное или асимметричное шифрование (криптография), цифровая подпись и проч.);
- универсальные механизмы безопасности (доверительное функционирование, метки системы безопасности; обнаружений событий, нарушающих безопасность и журнал контроля системы безопасности, и т.д.).

Рекомендации также обеспечили видение того, как применять перечисленные механизмы и сервисы безопасности на разных уровнях модели OSI от физического уровня до уровня приложения. Более того, в документе была сформулирована базовая модель целей, средств и ресурсов управления безопасностью в рамках модели OSI. Позднее эта модель была существенно уточнена и развита в последующих рекомендациях в рамках серии X.800.[60]

Однако серии рекомендаций МСЭ не стали ни обязательными для ИКТ-отрасли, ни подлинно универсальными по масштабу своего внедрения. Исторически сложилось так, что МСЭ не попал в число зачинателей процесса создания и развития Интернета и системы УИИ – эту роль выполнило правительство США и техническое сообщество, оформившееся вокруг рабочего процесса IETF и других технических структур. В результате, в ходе попыток применить X.200, X.800 и другие серии стандартов МСЭ к Интернету и его глобальной инфраструктуре выяснилось, что эти документы скорее выступают средствами

[58] См.: X.200 (11/1998) Open Systems Interconnection (OSI) – Model and notation, service definition. International Telecommunication Union. http://www.itu.int/rec/T-REC-X.200-199407-I/en (последнее посещение 1 марта 2016 г.).
[59] См.: X.800 (03/1991) Security Architecture for the Open Systems Interconnection for CCITT Applications. International Telecommunication Union. http://www.itu.int/rec/T-REC-X.800-199103-I/en (последнее посещение 1 марта 2016 г.).
[60] See the X.800 series recommendations from X.802 to X.843 (Information technology - Security techniques - Specification of TTP services to support the application of digital signatures) and later. The X.800 recommendation series are available here: http://www.itu.int/rec/T-REC-X/en (последнее посещение 1 марта 2016 г.).

кодификации и обобщения уже существующих практик менеджмента и обеспечения безопасности, чем проводниками процесса обновления стандартов.

Более того, фундаментальная 7-и уровневая концепция технической архитектуры модели OSI проиграла глобальную конкуренцию с набором протоколов TCP/IP и теми принципами коммуникации, которые последний воплощал в рамках более простой и более вариативной в применении 4-х уровневой модели. К 1990-м гг., когда стандартизация OSI продолжалась в рамках МСЭ, основанный на TCP/IP глобальный Интернет перевёл некоторые архитектурные принципы модели OSI в сферу теоретических обсуждений. Таким образом, трек стандартизации модели OSI в рамках МСЭ в целом не стал процессом создания технических стандартов, поэтому некоторые рекомендаций из поздних серий стандартов X.…лишь отражали магистральные тенденции, развитие которых протекало преимущественно вне рамок регуляторной деятельности МСЭ. Тем не менее, к концу 1990-х гг. эти рекомендации по большей части были адаптированы к актуальным техническим трендам в развитии Интернета.

Сегодня МСЭ в качестве координатора Направления деятельности С5. Укрепление доверия и безопасности при использовании ИКТ ВВУИО участвует в стандартизации кибербезопасности в рамках Глобальной программы кибербезопасности (ГПК) и работы сектора МСЭ-Т, включая Исследовательскую группу МСЭ-Т №17 «Безопасность». Эта работа включает в принятие ряда резолюций Всемирной Ассамблеи по стандартизации электросвязи (WTSA) по стандартизации в сфере кибербезопасности. Однако эта полезная деятельность имеет мало отношения к обеспечению в конкретной плоскости СБО системы УИИ, несмотря на достаточно распространенное мнение, согласно которому МСЭ должен играть роль центрального органа по вопросам стандартизации глобальной инфраструктуры Интернета.

Частично сохраняющаяся разобщенность процесса стандартизации информационной инфраструктуры в рамках МСЭ с работой IETF в той же сфере до сих пор выглядит значительным пробелом, нарушающим целостность политик по обеспечению СБО системы УИИ. В некотором смысле попытка преодолеть этот барьер была сделана на Всемирной конференции по международной электросвязи 2012 г., когда ее участники озвучили ряд инициатив по расширению Положений о международной электросвязи (ITRs), аналога Устава для МСЭ. В Положения предлагалось наконец включить вопросы, связанные с Интернетом, включая вопросы стандартизации инфраструктуры Интернета, связанные с безопасностью.

Несмотря на то, что споры вокруг этих инициатив в Дубае привели к срыву консенсусного решения и изъятию большей части этих инициатив из проекта обновленных Положений, вопрос гармонизации различных треков и рабочих процессов в сфере стандартизации остается на повестке дня. К сожалению, поиск решений этого вопроса осложняется политизацией и противопоставлением МСЭ как источника глобальной международно-правовой легитимности ООН для норм и технических стандартов, Рабочей группе по проектированию Интернет (IETF) и техническому сообществу, которые не обладают международной легитимностью, но демонстрируют эффективную работу в сфере стандартизации

с вовлечением всех заинтересованных сторон. Эта проблема также является предметом обсуждения в Разделе 3.4.

3.3. Стандарты, бизнес-процессы и вызовы в сфере обеспечения стабильности, безопасности и отказоустойчивости

Угрозы СБО системы доменных имен DNS

В целом, в этом разделе используется модель угроз СБО системы УИИ, ранее сформулированная в подразделе 2.3 (угрозы конфиденциальности, доступности и целостности информационной системы). Однако для того, чтобы предметно рассмотреть определенные изъяны в стандартах и процессах, связанных с обеспечением СБО (особенно в отношении DNS), также используются выводы доклада Общества Интернета «К повышению безопасности, стабильности и отказоустойчивости системы доменных имен DNS», который содержит базовую классификацию атак типа «отказ в обслуживании» (DoS), угроз повреждения данных и угроз раскрытия информации.[61]

Бизнес-процесс управления корневой зоной DNS: необходима ли б*о*льшая открытость?

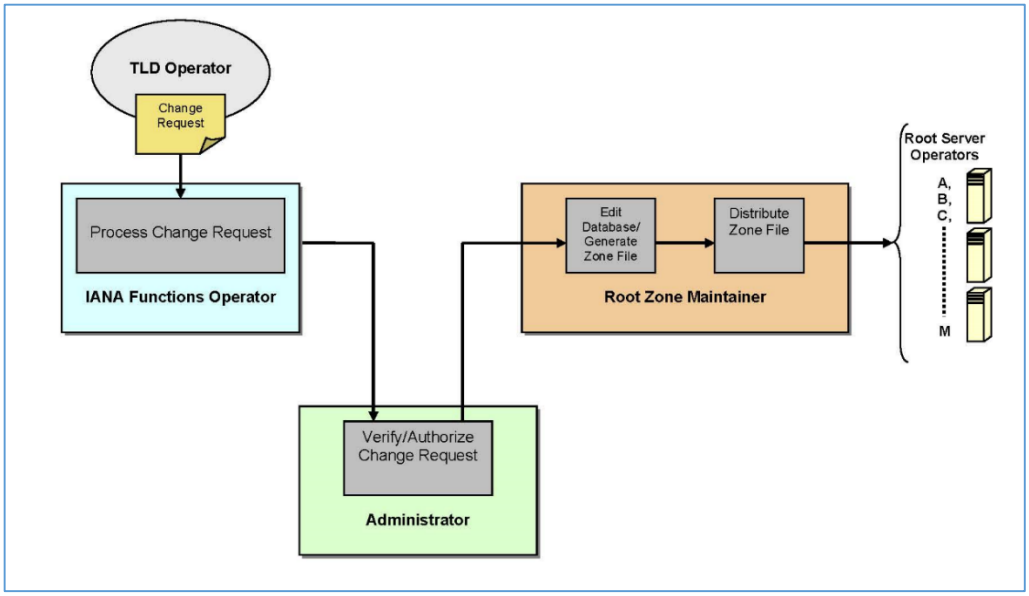
Управление корневой зоной DNS – критически важный процесс для обеспечения СБО системы УИИ, в котором на данный момент участвуют несколько сторон, в том числе:

- Оператор функций Администрации адресного пространства Интернет (IANA), в настоящее время представлен Корпорацией Интернета (ICANN). Оператор получает, рассматривает и обрабатывает запросы на внесение изменений в файл корневой зоны DNS, выполняет технические проверки, уведомляет операторов о выполнении запроса, а также вносит изменения в корневую базу данных WHOIS.
- Администратор корневой зоны, в настоящее время (до завершения передачи ответственного управления функциями IANA) представлен Национальной администрацией по телекоммуникациям и информации США (NTIA). Администратор осуществляет проверку процессов, процедур и политик, которым следует оператор функций IANA, уполномочивает технического менеджера вносить изменения в файл корневой зоны по запросу операторов доменов верхнего уровня, уполномочивает оператора функций IANA вносить изменения в базу данных WHOIS.
- Технический менеджер корневой зоны, в настоящее время представлен компанией Verisign. Технический менеджер корневой зоны вносит изменения в файл корневой зоны, генерируя обновленную версию файла, а также осуществляет рассылку файла по операторам авторитативных корневых серверов DNS.

[61] http://www.internetsociety.org/towards-improving-dns-security-stability-and-resiliency-0 (последнее посещение 1 марта 2016 г.).

Обзор процесса управления корневой зоной DNS и его участников представлен на Схеме 2.

Схема 2. *Процесс управления авторитативной корневой зоной по состоянию на 1 марта 2016 г.*



Источник: Бизнес-процесс управления авторитативной корневой зоны (в настоящее время). Сайт Национальной администрации по телекоммуникациям и информации (NTIA) США, http://www.ntia.doc.gov/legacy/DNS/CurrentProcessFlow.pdf (последнее посещение 1 марта 2016 г.).

Роль NTIA в этом бизнес-процессе достаточно ограничена и в определенной степени формальна. Тем не менее, NTIA действительно проверяет, соответствует ли запрос на внесение изменений в файл корневой зоны, подготовленный и направленный оператором, определенным требованиям, включая требования к безопасности.[62] В частности, Администратор учитывает, как ICANN соблюдает процесс уведомления о внесении изменений, принимая во внимание следующие критерии:

- Был ли запрос направлен безопасным способом?
- Включает ли запрос стандартный набор информации (то есть необходимое описание запрашиваемых изменений)?
- Одобрила ли сама ICANN запрашиваемые у Администратора изменения?
- Имел ли место запрос на утверждение изменений?

За последние годы не появилось никакой информации о серьезных инцидентах безопасности, связанных с бизнес-процессом по генерированию и рассылке файла корневой зоны DNS. Также, насколько можно судить по открытым источникам, NTIA ни разу не использовала свое право заблокировать запрос на внесение изменений в файл корневой зоны, направленный ей ICANN. Тем не

[6262] Более подробно см.: http://www.ntia.doc.gov/files/ntia/publications/ntias_role_root_zone_management_12162014.pdf (последнее посещение 1 марта 2016 г.).

менее, в рамках процесса передачи ответственного управления функциями IANA, NTIA либо должна уступить свою роль в этом бизнес-процессе некоей новой структуре, которая будет представлять глобальное сообщество заинтересованных сторон, либо сегодняшняя роль NTIA как администратора будет исключена из соответствующих бизнес-процессов.

Хотя передача ответственного управления функциями IANA не является предметом анализа в этой главе, одним из критически важных требований к деятельности в корневой зоне DNS является полная прозрачность бизнес-процессов. Однако тот уровень прозрачности и открытости, который удалось эффективно обеспечить в рамках бизнес-процесса обновления ключа для подписания ключей (KSK) корневой зоны DNSSEC, пока не достигнут в отношении двух других операций, входящих в бизнес-процесс управления авторитативной корневой зоной DNS. Речь идет о: 1) редактировании базы данных корневой зоны (КЗ) и генерировании файла КЗ; 2) рассылке файла КЗ операторам корневых серверов DNS. Поскольку обе эти операции выполняет технический менеджер КЗ – Verisign – подробности бизнес-процесса и технические параметры этих операций по большей части остаются недоступны для общественности.

Функции Verisign в отношении бизнес-процесса управления КЗ DNS были определены в отдельном договоре корпорации с правительством США (в лице NTIA) – Соглашении о сотрудничестве № NCR 92-18742.[63] Соглашение изначально было подписано 1 января 1993 г., а его участниками стали американский Национальный научный фонд (NSF, позже передавший свои функции в рамках контракта NTIA) и компания Network Solutions, Incorporated (NSI, позже была приобретена Verisign в 2000 г., которой таким образом перешли контрактные обязательства и статус участника Соглашения о сотрудничестве). С момента подписания Соглашения по настоящее время его текст был дополнен 32 поправками, которые отражали постепенное сужение функций NSI/Verisign, связанных с глобальной системой доменных имен. Стоит отметить, что до того, как управление доменными именами пришло к своему сегодняшнему состоянию и глобальное регулирование доменов верхнего уровня стала осуществлять ICANN, NSI как раз в рамках Соглашения о сотрудничестве № NCR 92-18742 обладал монопольным правом на регистрацию имен в доменах верхнего уровня .org, .net and .com. Однако все имевшие место поправки практически не затронули статус NSI/Verisign в качестве технического менеджера корневой зоны DNS.

Таким образом, с 1993 по 2001 гг. оформился бизнес-процесс управления корневой зоной DNS, включая операции, за которые отвечает Verisign. В течение этого периода файл корневой зоны DNS генерировался на корневом сервере A, оператором которого был и остается Verisign.

Для этого критического бизнес-процесса в определенной степени не была обеспечена должная подотчетность перед техническим сообществом. Verisign выполнял свои функции и в качестве оператора корневого сервера A в рамках американской юрисдикции, и в качестве технического менеджера корневой зоны

[63]Тексты Соглашения о сотрудничестве и всех прилагающихся к нему поправок см.: http://www.ntia.doc.gov/page/VeriSign-cooperative-agreement (последнее посещение 1 марта 2016 г.).

в рамках Соглашения о сотрудничестве с NTIA, оставаясь подотчетным лишь правительству США. Учреждение Корпорации Интернета в 1998 г. по большому счету не меняло ситуацию, так как до 2001 г. ICANN и NSI/Verisign не подписывали никаких соглашений и не выстраивали иных механизмов формализованного взаимодействия, которые бы затрагивали функции оператора корневого сервера A или технического менеджера корневой зоны DNS.[64]

В 2001 г. бизнес-процесс управления корневой зоной претерпел существенные изменения, включая обновления в части функций технического менеджера. Согласно Исследованию масштабирования корневой зоны ("Scaling the Root") от 7 сентября 2009 г., выполненному Исследовательской группой масштабирования корневой зоны, начиная с 1996 г. и заканчивая внедрением соответствующих изменений на уровне всех вторичных серверов DNS в 2001 г., произошел процесс перераспределения функций корневого мастер-сервера DNS от корневого сервера A к отдельному мастер-серверу распространения. Этот сервер также известен как «скрытый мастер-сервер распространения», поскольку он является авторитативным для корневой зоны DNS, и запись имени сервера (Name Server Record) по нему отсутствует. Мастер-серверы распространения в DNS обычно скрыты, так что в этом смысле обновление процесса управления корневой зоной не представляло собой уникальный случай.

Таким образом, с ноября 2001 г. 13 корневых серверов, включая бывший мастер-сервер A, стали вторичными авторитативными серверами. Все они теперь имеют равный в техническом смысле статус, поскольку все их операторы получают рассылку файла корневой зоны со скрытого первичного авторитативного сервера. На этом же скрытом мастер-сервере теперь и генерируется файл корневой зоны, который затем рассылается для 13 корневых серверов. Этот процесс осуществляется два раза в сутки, каждые 12 часов вне зависимости от того, были ли получены и обработаны какие-либо запросы на внесение изменений в содержание файла корневой зоны от операторов доменов верхнего уровня, или нет.

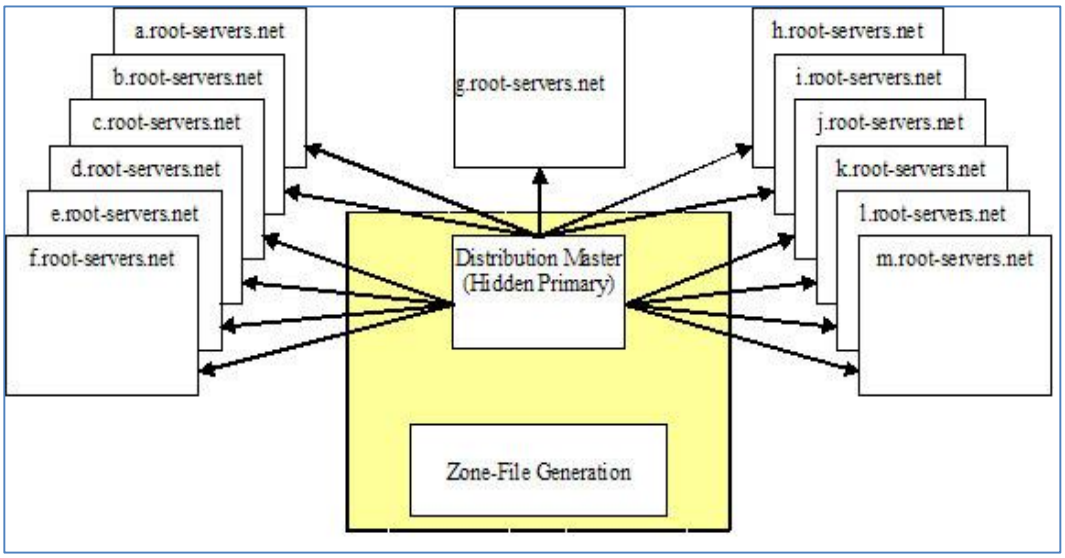
Функционирование скрытого мастер-сервера должно полностью подпадать под дополненное поправками Соглашение о сотрудничестве между Verisign и Министерством торговли США. Однако текст Соглашения не содержит прямых упоминаний к скрытому мастер-серверу, а также не поясняет необходимость его установки вместо бывшего первичного сервера A.

Это обновление бизнес-процесса и технической архитектуры управления корневой зоной DNS было направлено на поддержание высокого уровня СБО системы DNS и, насколько можно судить по открытой информации, ни разу не

[64] Это не означает, что ICANN и NSI/VeriSign вообще не устанавливали между собой формальных отношений. Начиная с 1999 г. была подписана серия соглашений касательно функций NSI/VeriSign в качестве регистратуры доменной зоны верхнего уровня общего назначения .NET, .COM и .ORG. Первым 10 ноября 1999 г. было подписано Соглашение о регистратуре между ICANN и NSI, текст соглашения см. здесь: http://archive.icann.org/en/nsi/nsi-registry-agreement-04nov99.htm (последнее посещение 1 марта 2016 г.). Позже был подготовлен и подписан ряд дальнейших соглашений, каждое из которых касалось функций регистратуры одного из трех доменов верхнего уровня общего назначения (.COM, .NET и .ORG).

повлекло за собой какие-либо инциденты, влияющие на обеспечение СБО системы УИИ.

Схема 3. *Архитектура корневой зоны DNS по состоянию на сегодняшний день*



Источник: K-Root Name Server Operations. Andrei Robachevsky, CTO, RIPE NCC. RIPE NCC Roundtable Meeting, March 2005, https://www.ripe.net/participate/meetings/roundtable/march-2005/presentations/the-root-name-server-system-operation-of-the-k-root-server, (последнее посещение 1 марта 2016 г.).

Один из таких вопросов – прозрачность и подотчетность бизнес-процесса, выполняемого Verisign в качестве технического менеджера корневой зоны. До сих пор, в части исполнения этих функций компания остается подотчетна лишь правительству США, тогда как подробности работы скрытого мастер-сервера остаются по большей части недоступны для заинтересованных сторон.

Также примечательно, что функции Verisign не в качестве технического менеджера корневой зоны не включаются в повестку дня в рамках Консультативного комитета системы корневых серверов (RSSAC). Установление формальных отношений между ICANN и операторами корневых серверов началось с Соглашения о взаимных обязательствах между ICANN и Консорциумом Интернет-систем (ISC), подписанного в декабре 2007 г.[65] В развитие этого взаимодействия недавно был опубликован новый документ RSSAC от 4 декабря 2015 г. – Ожидания в части обслуживания корневых серверов.[66]

В документе приводится подробная структуры для координации и улучшения работы операторов корневых серверов, включая положения о точном и своевременном обновлении корневой зоны, внедрении и обмене лучшими

[65] См.: http://archive.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf (последнее посещение 1 марта 2016 г.).
[66] См.: RSSAC001 Version 1. Service Expectations of Root Servers. An Advisory from the ICANN Root Server System Advisory Committee (RSSAC), 4 December 2015. ICANN Website, https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf (последнее посещение 1 марта 2016 г.).

практиками, публикации операторами актуальных для текущей деятельности данных о своей инфраструктуре, а также публикации документов, которые подтверждают следование оператором принципом постоянной доступности его сервиса, в том числе за счет надлежащего планирования обслуживания, и уведомлении о текущих событиях. Эти положения также адресованы Verisign как участнику RSSAC и сообщества операторов корневых серверов DNS (как оператору корневого сервера A). Тем не менее, в документе не приводится никаких положений, которые касались бы Verisign конкретно в качестве технического менеджера корневой зоны DNS и оператора скрытого мастер-сервера.

До последнего времени не было ясности в вопросе о том, подпадает ли функционирование скрытого мастер-сервера под какие-либо возможные будущие соглашения между Verisign и Корпорацией Интернета после завершения процесса передачи ответственного управления функциями IANA в середине 2016 г. Некоторой определенности по этому вопросу сообществу удалось достичь с опубликованием итогового Предложения по передаче ответственного управления функциями Администрации адресного пространства Интернет (IANA), которое в марте 2016 г. было направлено на рассмотрение NTIA Координационной группой по передаче координирующей роли в осуществлении функций IANA (ICG).

Во-первых, в Предложении прописано, что после завершения процесса передачи ответственного управления функциями IANA, «соглашение в той или иной форме» между оператором функций IANA и техническим менеджером корневой зоны «будет необходимо, когда NTIA выйдет из процесса управления корневой зоной DNS».[67] Во-вторых, в документе Координационная группа (ICG) отмечает, что «Полная и окончательная передача полномочий потребует пересмотра взаимоотношений между нынешним оператором функций IANA (ICANN), нынешним техническим менеджером корневой зоны DNS (Verisign) и нынешним Администратором корневой зоны (NTIA)». ICG также подчеркивает, что до завершения процесса передачи ответственного управления функциями IANA между ICANN и Verisign должно быть заключено письменное соглашение без участия NTIA, которое «должно быть открыто для публичного рассмотрения до своего вступления в силу».[68]

Принятие и реализация таких предложений может стать важным шагом в направлении повышения доверия к техническому менеджеру КЗ и в целом процессу управления КЗ DNS. До сих пор, отсутствие открытой информации о скрытом мастер-сервере Verisign и технических соображениях, и задачах, по которым он был установлен, а также неопределенность его будущего статуса в смысле прозрачности и подотчетности глобальному сообществу

[67] Предложения по передаче ответственного управления функциями Администрации адресного пространства Интернет (IANA) от Национальной администрации по телекоммуникациям и информации США (NTIA) глобальному сообществу заинтересованных сторон. Координационная группа по передаче координирующей роли в осуществлении функций IANA (ICG). Март 2016, стр. 6, &X017, https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf (последнее посещение 1 марта 2016 г.).
[68] Там же, стр. 7-8.

заинтересованных сторон провоцировала споры и критику, особенно со стороны отдельных правительств.

Один из поводов для беспокойства, которое неоднократно озвучивался представителями ряда правительств, включая Россию, Китай, Индию и Бразилию, основан на концентрации критических бизнес-процессов в руках Verisign, который является частной американской корпорацией и в плане открытости и глобализованности сильно уступает ICANN (при том что и последняя, с точки зрения ряда правительств, в этом смысле далеко не совершенна). В отличие от ICANN, Verisign, будучи акционерной коммерческой компанией, не обеспечивает площадки для открытых консультаций и не создает механизмы вовлечения всех заинтересованных сторон, на которых во многом основана модель управления на доверии. Недостаток открытой информации о работе скрытого мастер-сервера Verisign в сочетании с недостаточной прозрачностью функций технического менеджера корневой зоны иногда способствует распространению некорректной идеи о существовании Красной кнопки или Рубильника Интернета, с которой(-ым) отождествляется скрытый мастер-сервер. В случае с некоторыми правительствами эта концепция усугубляется недоверием к независимости Verisign от политически мотивированного вмешательства правительства США в его технические операции. При этом в качестве гипотетических механизмов такого вмешательства иногда рассматривается давление на Verisign при помощи указов правительства США или ордеров американских судов.

Один из подобных максимально неблагоприятных сценариев рассматривает д-р Вольфганг Кляйнвахтер в своем исследовании.[69]

В смоделированном сценарии правительство США в лице NTIA приказывает Verisign удалить записи о страновом домене верхнего уровня .FR из сгенерированного файла корневой зоны, таким образом «наказывая» Францию по выдуманному политическому поводу. Д-р Кляйнвахтер рассматривает в рамках своего сценария распространенные опасения, согласно которым его воплощение приведет к полной потере коммуникации в Интернете между пользователями, зарегистрированными в зоне .FR, и пользователями во всех остальных доменах.

[69] См.: Wolfgang Kleinwächter. De-Mystification Of The Internet Root: Do We Need Governmental Oversight? http://www.wgig.org/docs/book/Wolfgang_Kleinw%C3%A4chter%20.pdf (последнее посещение 1 марта 2016 г.).

Однако в исследовании доказывается техническая несостоятельность такого развития событий. Ключевая ее причина в том, что остаются еще 13 вторичных корневых серверов DNS, и их операторы могут просто проигнорировать изменения в файле корневой зоны, разосланном со скрытого мастер-сервера. Операторы вторичных корневых серверов могут не размещать новую версию файла на «зеркалах» своих серверов. Согласно д-ру Кляйнвахтеру, даже если операторы 10 корневых серверов, расположенных на территории США, будут вынуждены принять обновления файла, операторы трех оставшихся зарубежных корневых серверов (I, K M) все равно смогут обрабатывать запросы к ресурсам в зоне .FR, используя глобально распределенную систему «зеркал» своих серверов. Вместе с тем, негативные последствия такого сценария могут включать нарушение глобального авторитативного корня DNS. Конечным итогом этого будет нанесение существенного ущерба СБО всей глобальной DNS, а не Франции или ее интернет-пользователям.

Технический анализ показывает, что гипотетически возможные попытки манипулировать функциями Verisign в политических целях по большому счету оказались бы контрпродуктивны. Однако этот факт не всегда достаточно широко признается и осознается даже в среде технических экспертов, не говоря о дипломатах. Кроме того, на фоне закрытости бизнес-процесса эксплуатации скрытого корневого мастер-сервера дефицит доверия к бизнес-процессу управления корневой зоной DNS может создать условия для дальнейшей политизации дискуссий об управлении глобальной инфраструктурой Интернета и сместить фокус внимания с действительно важных вопросов, связанных с обеспечением СБО системы доменных имен.

Второй вопрос, связанный с бизнес-процессом Verisign – в какой степени функционирование скрытого первичного мастер-сервера отвечает критериям и требованиям в части обеспечения СБО. Работа скрытого мастера, пожалуй, относится к числу наиболее критических звеньев процесса управления корневой зоной, и является наиболее централизованным из них. Неизвестно о наличии глобально распределенных «зеркал» скрытого мастер-сервера, а избыточное резервирование ресурсов на основе эникаст вряд ли используется в его работе.

С одной стороны, скрытый мастер-сервер и не нуждается в подобном избыточном резервировании для исполнения своих задач: он не разрешает запросы к DNS, а используется лишь для генерирования и рассылки файла корневой зоны дважды в сутки. С другой стороны, из-за недостатка доступной информации невозможно сделать вывод о том, отвечает ли его работа каким-либо конкретным параметрам, стандартам и процедурам в части обеспечения СБО системы DNS.

В частности, можно обозначить следующие вопросы к функциям мастер-сервера под управлением Verisign:

- Какое программное и аппаратное обеспечение используется для генерирования файла КЗ?

- Как Verisign обеспечивает безопасность файла КЗ при его рассылке со скрытого мастер-сервера по вторичным авторитативным корневым серверам?
- Проводилась ли стандартизация в части обеспечения СБО для функций скрытого мастер-сервера и рассылки файла КЗ? Участвовали ли IETF или иные структуры технического сообщества в разработке таких стандартов?

- Проводится ли какой-либо внешний аудит работы скрытого мастер-сервера и кто его выполняет?

Один из немногих известных фактов – при рассылке файла КЗ для обеспечения конфиденциальности, целостности и доступности данных, а также предотвращения инцидентов безопасности используется протокол Подписи транзакции (Transaction SIGnature или TSIG). TSIG представляет собой протокол сетевого уровня, используемый по большей части в DNS и стандартизированный в RFC 2845.[70] В протоколе Подписи транзакции общие секретные ключи и однонаправленное хэширование используются для криптографически защищенной аутентификации каждой конечной точки соединения. В системе корневых серверов DNS секретный ключ TSIG генерируется трижды в год в рамках неформальных встреч представителей операторов корневых серверов, которые проходят на полях встреч Рабочей группы по проектированию Интернет.[71]

Достаточно ли использования TSIG для устранения риска подделки файла КЗ при его рассылке со скрытого мастер-сервера? Достаточно ли сам скрытый мастер-сервер защищен и обеспечен резервными ресурсами для того, чтобы выдержать серьезный инцидент безопасности, включая инцидент, вызванный умышленными действиями инсайдера? Учитывая, что скрытый мастер-сервер представляет собой высший имеющийся уровень иерархии DNS, ответы на эти вопросы напрямую связаны с обеспечением СБО системы DNS.

Как известно, функционирование системы УИИ сегодня основано на модели доверия, которая не предполагает юридически обязывающих международных гарантий для заинтересованных сторон, включая даже правительства. В целом эта система работает очень хорошо – несмотря на недостаток открытой информации о скрытом авторитативном корневом мастер-сервере, не было зафиксировано инцидентов, которые бы серьезно нарушали работу системы, и в том числе сказывались бы на доступности услуг для конечных пользователей. Однако фундаментальным условием для модели доверия остается тот факт, что доверия участников и заинтересованных сторон в Интернете основывается на открытости и прозрачности стандартов, процедур и архитектурных решений.

В свете сказанного, принятие и практическое воплощение положений, изложенных в итоговом Предложении ICG в отношении Verisign как технического менеджера корневой зоны DNS, имеют большое значение. Разработка и принятие прозрачного (и открытого для публичных комментариев)

[70] http://tools.ietf.org/html/rfc2845.
[71] See: Andrei Robachevsky. The Internet from the Inside Out. Ecosystem of the Global Network. Moscow: MSK-IX, 2015. – pp. 108-109 (in Russian).

соглашения между ICANN как оператором функций IANA и Verisign как техническим менеджером корневой зоны с четко прописанными и прозрачными техническими политиками и процедурами отчетности перед сообществом может стать существенным шагом к тому, чтобы вопрос доверия сообщества к бизнес-процессу управления корневой зоной DNS был наконец снят с повестки дня.

Стандартизация и бизнес-процесс расширений безопасности системы доменных имен (DNSSEC)

Расширения безопасности системы доменных имен (DNSSEC) остаются одним из ключевых технологических механизмов, которые обеспечивают и укрепляют СБО одной из трех рассматриваемых в настоящем исследовании составляющих систем УИИ. Помогая противодействовать различным атакам, которые подробно рассматриваются далее, DNSSEC вносит существенный вклад в обеспечение СБО системы доменных имен.

DNSSEC играет заметную роль в предотвращении и защите от атак и других вызовов безопасности DNS, такие как атаки типа искажения данных. В частности, расширения безопасности DNS могут использоваться для защиты данных при их передаче и хранении, таким образом сокращая риск отравления кэша и атак посредника (man-in-the-middle, MITM).

Идея расширений безопасности DNS (DNSSEC) была впервые описана в Запросе комментариев 2065 в январе 1997 г.[72] В документе была определена основа концепции новых расширений безопасности в протокол DNS. В частности, такие расширения должны были:

- предоставлять сервисы DNS резолверам и приложениям, которые следуют политикам безопасности, используя криптографические цифровые подписи, которые включаются в защищенные зоны DNS в качестве записей ресурсов (RRs).
- обеспечить возможность хранения аутентифицированных открытых ключей в DNS, что могло бы способствовать развитию общего сервиса распределения открытых ключей, а также укреплению безопасности DNS.
- обеспечить возможность опциональной аутентификации транзакций по протоколу DNS.

В документе также приводился обширный перечень технический соображений в отношении ключей подтверждения и их параметров, способов генерации, сроков действия и т.д. Позднее дизайн и техническая концепция DNSSEC были более подробны сформулированы и расширены в своих различных аспектах в рамках ряда RFC, включая RFC 2931, 3008, 3110, 3130, 3225, 3226 и некоторые другие Запросы комментариев, которые не всегда касались только вопросов DNSSEC.

Однако окончательно DNSSEC были стандартизированы позже с публикацией Рабочей группой по проектированию Интернет Запроса комментариев 4033 «Безопасность DNS: Внедрение и требования» в 2005 г.[73] Согласно документу, за

[72] См.: https://www.ietf.org/rfc/rfc2065.txt (последнее посещение 1 марта 2016 г.).
[73] См.: http://www.ietf.org/rfc/rfc4033.txt (последнее посещение 1 марта 2016 г.).

счет расширений безопасности DNS решаются задачи по аутентификации источника и обеспечению целостности сервисов для данных серверов доменных имен. В развитие RFC 4033 были опубликована единая серия из нескольких Запросов комментариев, которые включают в себя RFC 4034 «Записи ресурсов для расширений безопасности DNS"[74] и RFC 4035 "Модификации протокола для расширений безопасности DNS".[75]

Несмотря на ключевую роль в обеспечении безопасности DNS, расширения безопасности DNS никогда не разрабатывались в качестве универсального решения всех вызовов DNS и не стали таковым. В серии документов, посвященных DNSSEC, включая RFC 4033, был отмечен ряд проблем, которые отражают пределы возможностей использования DNSSEC и их вклада в обеспечение безопасности системы доменных имен. Так, Расширения безопасности не обеспечивают защиту от атак типа «распределенный отказ в обслуживании» (DDoS) на инфраструктуру доменных имен, и более того, иногда сами используются для организации некоторых видов атак.

На сегодня, одним из главных вопросов, связанных с DNSSEC, остается их полномасштабное внедрение на всех уровнях глобальной инфраструктуры DNS. Расширения безопасности разрабатывались таким образом, что для их полноценной работы требуется обеспечить полную цепочку валидации. Например, безопасный резолвер не может подтверждать запросы DNS, исходящие из неподписанной зоны, поскольку для этого необходимо чтобы все зоны на пути от исходной доверенной точки до зоны, содержащей ответы, были подписаны, а все серверы и резолверы, участвующие в разрешении запроса, являлись безопасными.

Внедрение DNSSEC представляет собой длительный процесс, который на сегодня постепенно продвигается, но все еще далек от завершения на уровне страновых доменных зон. Однако процедура подписания корневой зоны уже завершена. Она стартовала 1 декабря 2009 г., когда корневая зона была подписана в режиме внутреннего использования расширений безопасности, доступного для Verisign и ICANN, и завершилась 15 июля 2010 г., когда ICANN после проведения двух церемоний создания ключей, подписывающих ключи (KSK), опубликовала якорь доверия корневой зоны, а операторы корневых серверов начали обслуживать корневую зону с использованием действительных ключей.[76] 21 октября 2010 г. Команда разработки DNSSEC для корневой зоны опубликовала Заявление о практических методиках для операторов ключей, подписывающих ключи (KSK) в корневой зоне.[77] В Заявлении приводится обширное и комплексное техническое руководство для IANA как оператора корневой зоны и Verisign в отношении их специальных функций по техническому менеджменту файла корневой зоны.

Домен верхнего уровня .ORG был подписан ключами DNSSEC в июне 2010 г., за ним последовали домены .NET и .EDU в 2010 и 2011 гг. Страновые домены верхнего уровня получили возможность размещать ключи DNSSEC, начиная с

[74] См.: https://tools.ietf.org/html/rfc4034 (последнее посещение 1 марта 2016 г.).
[75] См.: https://www.ietf.org/rfc/rfc4035.txt (последнее посещение 1 марта 2016 г.).
[76] См.: http://www.root-dnssec.org (последнее посещение 1 марта 2016 г.).
[77] См.: https://www.iana.org/dnssec/icann-dps.txt (последнее посещение 1 марта 2016 г.).

мая 2010 г. Последующее развитие стандартизации Расширений безопасности DNS протекало в рамках Запросов комментариев, включая RFC[78], RFC 5702[79] и RFC 6944[80].

Одно примечательное обновление стандартов DNSSEC было отражено в RFC 5933, опубликованном в июне 2010 г.[81] В документе прописаны технические стандарты использования стандарта систем криптографической защиты информации (СКЗИ) ГОСТ (в том числе для алгоритмов цифровых подписей Р 34.10-2001 and ГОСТ 34.11-94.) для генерации цифровых подписей и функции хэширования для трех типов записей ресурсов в DNSSEC: DNSKEY, RRSIG и DS. Этот прецедент можно рассматривать в качестве положительного примера создания стимулов для внедрения DNSSEC в сегментах системы доменных имен, которые предоставляют сервисы DNS пользователям в тех национальных юрисдикциях, где применяются специфические технические стандарты и правовые нормы в области криптографии и защиты данных.

Еще один аспект, который требует проработки, состоит в том, что внедрение DNSSEC само по себе невольно способствовало распространению определенного типа инцидентов, затрагивающих безопасность DNS. Такие инциденты известны как «просмотр зон» (Zone Walking). Несмотря на то, что такие атаки не создают критической угрозы СБО самой системы DNS, они могут представлять угрозу безопасности пользователей сервисов DNS. Основной механизм борьбы с инцидентами просмотра зон описан в RFC 5155 «Безопасность DNS (Расширения безопасности DNS): Хэшированное аутентифицированное отрицание существования» и состоит во введении нового типа записи ресурсов (RR), специально разработанной для предотвращения инцидентов просмотра зон. Речь идет о записи ресурсов NSEC3, которая обеспечивает аутентифицированное отрицание существования для наборов записей ресурсов DNS.[82] Согласно RFC 5155, для защиты от просмотра зон, имена владельцев ресурсов, записываемые с использованием NSEC3, представляют собой криптографические хэши имен оригинальных владельцев, добавляемые перед именем зоны в виде единой записи. Несмотря на то, что использование записи ресурсов NSEC3 не ведет к полному устранению инцидентов просмотра зон, оно позволяет существенно сократить их число.

Внедрение Расширений безопасности DNS на уровне корневой зоны стало значимым шагом по обеспечению СБО системы доменных имен. Что особо важно, оно стало примером активного внедрения международных стандартов информационной безопасности и управления информационными технологиями. Для корневой зоны DNS требовалось обеспечить сквозной жизненный цикл безопасности, описанный в стандарте ISO 27001. В 2009 г. Национальная администрация по телекоммуникациям и информации (NTIA) США признавала и подчеркивала, что «для любой политики безопасности в части внедрения DNSSEC должно обеспечиваться соответствие имеющимся стандартам безопасности». В качестве таких стандартов в том числе упоминались ISO

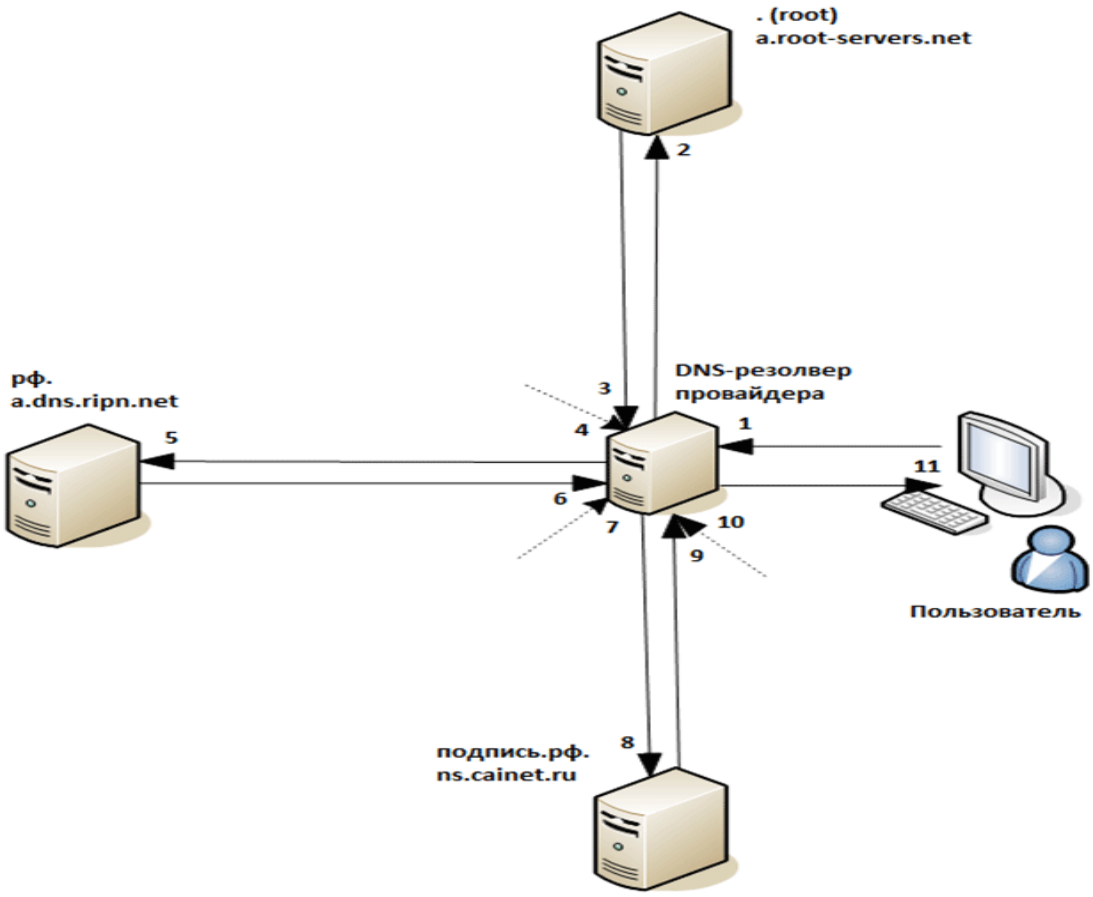
[78] См.: https://tools.ietf.org/html/rfc4398 (последнее посещение 1 марта 2016 г.).
[79] См.: https://tools.ietf.org/html/rfc5702 (последнее посещение 1 марта 2016 г.).
[80] См.: https://tools.ietf.org/html/rfc6944 (последнее посещение 1 марта 2016 г.).
[81] См.: https://tools.ietf.org/html/rfc5933 (последнее посещение 1 марта 2016 г.).
[82] См.: https://tools.ietf.org/html/rfc5155#section-3 (последнее посещение 1 марта 2016 г.).

27002:2005 (ранее ISO 17799:2005) и стандарт Национального института стандартов и технологий США (NIST) SP 800-53.[83] Также NTIA в своем документе отмечала, что отсылки к публикациям NIST (Специальные публикации (SP) и Федеральных стандартов обработки информации (FIPS) «не рассматриваются в качестве обязательных в рамках требований будущих проверок, но выступают в качестве необязывающего руководства и рекомендаций для разработки эффективной политики ИТ-безопасности» для внедрения DNSSEC в корневой зоне.[84] Таким образом, внедрение DNSSEC в корневой зоне можно рассматривать как довольно убедительный и позитивный пример бизнес-процесса, связанного с обеспечением СБО системы УИИ и соответствующего широко принятым стандартам информационной безопасности и ИТ-менеджмента. Единственную оговорку стоит сделать в связи с тем, что по большей части такие стандарты все же являются американскими, а не в прямом смысле слова международными.

Показательный пример внедрения и стандартизации DNSSEC в отношении вопросов, связанных с обеспечением СБО, можно выделить, если обратиться к документам по стандартизации бизнес-процесса подписания корневой зоны ключами, подписывающими ключи (как части процесса внедрения DNSSEC). В документе под названием «Руководство по организации церемоний подписания корневой зоны ключами, подписывающими ключи (KSK) DNSSEC», приводится точное и подробное описание соответствующей церемонии. Последняя включает регулярные встречи и особые технические процедуры, которые выполняют специальные участники – криптоофицеры, в чьи обязанности входит хранение и использование компонентов ключа, подписывающего ключи для корневой зоны DNS.[85] В технической части документа не только содержится подробное описание процедур и перечня установленных требований безопасности для всего процесса, но также отмечается необходимость внешнего аудита церемонии. Такой подход может служить ориентиром для остальных критических-бизнес процессов, от которых зависит обеспечение СБО системы УИИ – включая, например, все этапы процесса управления корневой зоной DNS.

Схема 4. *Алгоритм работы системы DNSSEC от уровня корневого сервера A до конечного пользователя*

[83] См.: Testing and Implementation Requirements for the Initial Deployment of DNSSEC in the Authoritative Root Zone.
http://www.ntia.doc.gov/files/ntia/publications/dnssec_requirements_102909.pdf (последнее посещение 1 марта 2016 г.).
[84] Там же.
[85] См.: http://www.root-dnssec.org/wp-content/uploads/2010/05/draft-icann-dnssec-ceremonies-01.txt (последнее посещение 1 марта 2016 г.).



Источник: Как это работает. Внедрение DNSSEC в информационные системы. Координационный центр национальных доменов .RU/.РФ, http://cctld.ru/ru/domains/dnssec/how/ (последнее посещение 1 марта 2016 г.).

Предотвращение атак на инфраструктуру DNS

Поскольку расширения DNSSEC не обеспечивают защиту от атак типа «отказ в обслуживании» (DoS) на систему DNS (включая целенаправленные распределенные DDoS-атаки, предпринимаемые злоумышленниками), ключевой стратегией по отражению таких атак остается избыточное резервирование ресурсов, за счет которого оператор, являющийся целью атаки, обеспечивает себе доступ к большему объему ресурсов, чем может вывести из строя атакующий.

Операторы DNS, учитывая критическую важность сервиса, который они поддерживают, весьма тщательно проектируют свою инфраструктуры и сервисы, укрепляя защиту систем от атак и используя масштабные технологии репликации и дублирования ресурсов, чтобы обеспечить устойчивость и выживаемость сервисов в случае DDoS-атаки.

Вопросам защиты от DDoS-атак не посвящены какие-либо специальные Запросы комментариев IETF, поэтому требования и критерии надлежащей защиты серверов DNS и другой инфраструктуры доменных имен разрабатываются и устанавливаются владельцами такой инфраструктуры на различных уровнях иерархии DNS (операторы корневых серверов – операторы доменов верхнего уровня – регистраторы и конечные пользователи). Стандартизация защиты от

DDoS-атак может быть выделена в качестве приоритетного направления дальнейшей работы технического сообщества и других заинтересованных сторон в области обеспечения СБО системы УИИ.

Конкретные рекомендации по противодействию DDoS-атакам, использующим инфраструктуру DNS, были разработаны Консультативным комитетом по безопасности и стабильности (SSAC) ICANN. Так, в Рекомендациях относительно DDoS-атак, использующих инфраструктуру DNS (SAC065), утвержденных Правлением ICANN 17 ноября 2014 г., приводится ряд рекомендаций, в том числе охватывающих специальные технические вопросы и меры:[86]

- Для Корпорации Интернета: содействовать деятельности в масштабах всего сообщества по сокращению количества открытых DNS-клиентов (резолверов, англ. resolver)[87], наличие которых создает возможности для сетевого спуфинга. Такая деятельность должна включать в себя разработку механизмов измерения проделанной работы и результатов.
- Для операторов серверов DNS: внедрить операционные процессы, которые позволяли бы удостовериться, что их программное обеспечение для DNS регулярно обновляется, а также наладить коммуникацию с вендорами такого ПО, чтобы регулярно получать информацию об обновлениях и инцидентах.

В том числе:

  - Для операторов авторитативных серверов DNS: поддержать работу по расследованию случаев ограничения скорости ответа авторитативных серверов DNS.
  - Для операторов резолверов DNS: принять незамедлительные меры по обеспечению безопасности открытых резолверов DNS.

- Для всех сетевых операторов: принять незамедлительные меры по пресечению спуфинга сетевых адресов.
- Для производителей и настройщиков сетевого абонентского оборудования, включая домашнее сетевое оборудование: принять незамедлительные меры по обеспечению безопасности таких устройств и удостовериться, что они своевременно обновляются при появлении нового ПО, предназначенного для закрытия уязвимостей безопасности; также – агрессивно замещать имеющуюся базу не подлежащих обновлениям ПО устройств за счет новых, обновляемых устройств.

В то время как приведенные рекомендации нацелены на то, чтобы закрыть пробелы в безопасности, за счет которых возможны масштабные DDoS-атаки на инфраструктуру DNS, ключевым вопросом остается способность ICANN, SSAC и других участников эффективно доносить свои рекомендации до их адресатов, для того чтобы те следовали им на практике. Эта задача может оказаться

[86] См.: https://www.icann.org/resources/board-material/resolutions-2014-11-17-en (последнее посещение 1 марта 2016 г.).
[87] Резолвер DNS

непростой и потребовать работы с прицелом на долгосрочный горизонт, поскольку внедрение таких рекомендаций в повседневную техническую деятельность может быть сопряжено с высокими издержками для производителей сетевого оборудования и сообщества сетевых операторов.

Обновление и стандартизация базы данных WHOIS

Как отмечается в документах ICANN, протокол WHOIS использовался интернет-операторами для установления лиц и организаций, ответственных за функционирование сетевых ресурсов в Интернете. Разработка и стандартизация протокола началась в 1982 г. с RFCs 812[88]и 954[89]. В последнем Запросе комментариев была изложена первая официальная спецификация протокола NICNAME/WHOIS. Развитие стандартизации WHOIS проходило параллельно с эволюцией и расширением самого сервиса. Накопившиеся за два десятилетия существенные обновления и нерешенные вопросы были обобщены в RFC 3912[90], который по сей день остается основой стандарта и технической спецификации WHOIS. Дальнейшее развитие технических параметров WHOIS осуществлялось силами технического сообщества. Однако с конца 1990-х гг. изменения, внесенные в сам протокол, оказались минимальны, что вылилось в растущий зазор между техническим дизайном и функциональностью WHOIS и, с другой стороны, развитием глобального Интернета и расширением использования WHOIS за рамки тех функций, которые предполагались в его исходной спецификации.

На сегодняшний день в отношении протокола WHOIS можно отметить ряд требующих решения вопросов:

- Недостаточная интернационализация (спецификация WHOIS была определена только для кодировки ASCII).
- Отсутствие модели данных (спецификация протокола WHOIS в RFC 3912 не определяет форматы запросов или кодирования, а также не предлагает структуру ответов и сообщений об ошибках).
- Отсутствие дифференцированного сервиса (отсутствие механизмов аутентификации).

Хотя сервис WHOIS не представляет критической важности для глобальной DNS, недостатки в работе его протокола в некоторой степени сказываться на безопасности, так как затрагивают конечных пользователей и других клиентов, а также саму DNS (например, использование WHOIS для генерации трафика ответов при организации DDoS-атаки на инфраструктуру DNS). Замечания и наблюдения по вопросу обновления WHOIS ранее уже были изложены в комментариях Консультативного комитета по безопасности и стабильности (SSAC) Корпорации Интернета, в том числе SAC051 «Доклад SSAC по терминологии и структуре базы данных доменных имен WHOIS».[91] Обобщая предыдущие комментарии, авторы SAC051 рекомендуют сообществу ICANN

[88] См.: https://tools.ietf.org/html/rfc812 (последнее посещение 1 марта 2016 г.).
[89] См.: https://tools.ietf.org/html/rfc954 (последнее посещение 1 марта 2016 г.).
[90] См.: https://tools.ietf.org/html/rfc3912 (последнее посещение 1 марта 2016 г.).
[91] См.: https://www.icann.org/en/system/files/files/sac-051-en.pdf (последнее посещение 1 марта 2016 г.).

оценить и принять замещающий протокол, который мог бы поддерживать запросы и отображать данные по интернационализированным регистрациям доменных ресурсов. Параллельно, Рабочая группа по проектированию Интернет запустила проект по разработке и стандартизации Протокола доступа к данным о регистрациях (RDAP) для доменных регистраторов на основе архитектурного стиля «Передача состояния представления» (RESTful). Предполагается, что проект сможет свести на нет большинство недостатков оригинального протокола WHOIS. Дискуссии по обновлению WHOIS ведутся на площадке ICANN, в том числе на полях недавних конференции Корпорации в 2013-2014 гг.; вопрос остается на повестке дня дальнейших обсуждений и работы по стандартизации.

3.4. Будущие стандарты и подходы к развитию процесса обеспечения стабильности, безопасности и отказоустойчивости

На основе сделанного в настоящей главе обзора можно обобщить некоторые наблюдения и ключевые вопросы, которые представляются актуальными для будущего развития дискуссии по обеспечению СБО системы УИИ.

1. Саму концепцию СБО целесообразно расширить в смысле ее применения к другим элементам и уровням глобальной инфраструктуры Интернета. Актуальность этой идеи подтверждает пример с глобальной системой маршрутизации, коротко описанный в подразделе 3.1. В силу недостаточно активной технической дискуссии и работы по стандартизации аспектов, связанных с обеспечением СБО, Протокол граничного шлюза до сих пор не обеспечен адекватной защитой от уязвимостей, создающих угрозу нарушения маршрутизации в глобальном масштабе. За счет интеграции технических политик и процессов стандартизации аспектов BGP, связанных с безопасностью, в концепцию обеспечения СБО системы УИИ можно обеспечить синергию усилий технического сообщества и всех заинтересованных участников этого процесса.

Однако такая интеграция потребует универсализации самого понятия СБО и расширения его за рамки DNS и в целом системы УИИ. Наряду с BGP и процессами глобальной маршрутизации существует множество уровней и сегментов инфраструктуры, критически важных для работы Интернета и противодействия полному спектру вызовов, связанных с обеспечением СБО. Речь идет в том числе об интернет-провайдерах, особенно провайдерах Tier 1, которые управляют опорной сетевой инфраструктурой, точках обмена трафиком (IXPs) и подключенной к Интернету критической информационной инфраструктуре (КИИ) (например, промышленные «умные» сети Smart Grid). Более того, даже частные компании и интернет-бизнесы, предоставляющие сервисы уровня приложения (например, поисковые системы) могут рассматриваться в рамках расширенной концепции обеспечения СБО, поскольку они имеют глобальную пользовательскую аудиторию, а предоставляемая их сервисами информация ежедневно используется клиентами для принятия решений.

В качестве далеко идущей долгосрочной цели, которую могло бы поставить и отрабатывать техническое сообщество, правительства и другие заинтересованные стороны, может выступать разработка Всеобъемлющей

Углубленной концепции обеспечения СБО технической инфраструктуры Интернета (не ограниченной системой УИИ).

2. Техническому сообществу не следует игнорировать нетехнические, в том числе политические вызовы обеспечению СБО системы УИИ; эффективная работа с такими вызовами требует согласованных мер. Среди правительств по всему миру нарастает уклон в сторону т.н. концепции цифрового суверенитета. Все большее число государств разрабатывают и принимают политики и законы, которые расширяют их суверенитет и правовые полномочия в отношении информационных систем и компьютерных сетей. Эта магистральная тенденция основывается на очевидном и по большому счету закономерной мотивации, такой как интересы национальной безопасности и быстро растущее влияние Интернета на национальные экономики.

Однако для того, чтобы определить разумные границы, которые предотвратили бы процесс фрагментации Интернета как следствие политик национальных государств, необходим системный, активный и комплексный диалог между политическими акторами и техническим сообществом. Несмотря на то, что Корпорация Интернета, IETF и другие структуры технического сообщества действительно претерпели глобализацию в плане географического представительства и спектра мнений своих представителей, от многих правительств их до сих пор отделяет барьер, обусловленный различными взглядами и недостаточно системной коммуникацией.

Глобальное техническое сообщество – и конкретно IETF – имеет шанс продвинуться в выполнении своей миссии в случае запуска стратегической программы консультаций с национальными правительствами по вопросам обеспечения СБО в рамках своей деятельности. Для этого нужен проактивный подход, поскольку для многих лиц, принимающих решения в развивающихся странах, деятельность и сами форматы IETF и Совета по архитектуре Интернета до сих пор остаются малоизвестны. Такая цель частично пересекается с задачами программы Глобального взаимодействия с заинтересованными сторонами ICANN, однако для ее достижения программа Корпорации Интернета должна дополняться вкладом от IETF, Совета по архитектуре Интернета, Общества Интернета и РРИ.

3. Для процесса стандартизации в области обеспечения СБО системы УИИ востребованы шаги по его гармонизации и универсализации. Речь идет об усилении роли и легитимности технических стандартов обеспечения СБО системы УИИ, разрабатываемых глобальным техническим сообществом. Для продвижения в этом направлении можно поставить первоочередную цель – укрепление правового статуса Запросов комментариев (RFCs) и самого рабочего процесса IETF. Хотя такая постановка задачи не связана ни с технической деятельностью, ни с выполнением бизнес-процессов, ее достижение может существенно способствовать соблюдению и принятию стандартов и технических политик в области обеспечения СБО, которые разрабатывает техническое сообщество, государствами, которые предпочитают поддерживать подход к обеспечению СБО информационных систем и УИИ в рамках межправительственных форматов.

В этом плане, одна из возможных идей для обсуждения – запуск программы сотрудничества между МСЭ и IETF с целью обеспечить взаимное признание их стандартов. Безусловно, в части обеспечения СБО системы УИИ ключевая цель может состоять в том, чтобы МСЭ признал и инкорпорировал в собственные серии стандартов Запросы комментариев IETF, связанные с обеспечением СБО. Такой шаг обеспечил бы мощную поддержку для IETF в смысле международно-правовой легитимности его работы по стандартизации, а также для бизнес-процессов, основанных на следовании RFC, в том числе в части обеспечения СБО.

Однако такая идея выходит за рамки технических вопросов и требует отдельного исследования правового характера, которое не укладывается в предмет этого раздела.

Раздел 4. Правовые аспекты безопасности, стабильности и отказоустойчивости глобальной инфраструктуры Интернета

Интернет призван служить всему миру. Вместе с тем его координация осуществляется по модели привлечения всех заинтересованных участников, развитие которой на начальных этапах в значительной степени было обусловлено техническим, научным и бизнес сообществами. Чем больше он используется в повседневной жизни, тем шире становится круг вопросов, связанных с управлением Интернетом и управлением в Интернете. В этот круг входят следующие вопросы (но не ограничивается ими): контроль за информацией, вопросы суверенитета в Интернете, кибершпионаж, защита критической инфраструктуры Интернета, кибервойны и другие. В этом разделе мы рассмотрим острые проблемы, связанные с управлением и контролем за инфраструктурой Интернета и спорные юридические вопросы, в особенности. Сначала мы рассмотрим текущую структуру управления, а затем перейдем к рассмотрению вопросов, которые могут возникнуть по мере изменения структуры управления.

4.1. Риски для инфраструктуры Интернета

Одним из ключевых вопросов, с которыми мы сталкиваемся сегодня, может быть сформулирован так - может ли случится технический сбой, который приведет к нарушению работы Интернета? Мы рассмотрим управление Интернетом в контексте его правовых форматов и проанализируем риски, возникающие перед Интернетом. Мы также рассмотрим каким образом будет развиваться управление и нормативно-правовая база, как в следствии правовых вопросов могут происходить сбои в работе Интернета, и как нормативно-правовая база может повлиять на технические проблемы.

Политические риски

Корпорация Интернета играет определяющую роль в работе Интернета, связанной с координацией системы доменных имен. Администрация адресного пространства Интернет (IANA) является департаментом ICANN, который отвечает за координацию ключевых элементов, поддерживающих безотказную работу Интернета. В частности, IANA выделяет и поддерживает уникальные коды и системы нумерации, которые используются в технических стандартах (протоколах), определяющих работу Интернета.[92] Исполнение функций IANA сейчас находится в процессе трансформации, который принято называть Передача координирующей роли Национального управления по телекоммуникациям и информации США (NTIA) в осуществлении функций IANA.[93]

Может ли система DNS использоваться в качестве рычага давления во время международных конфликтов? Возможность ошибки в обновлении файла корневой зоны, преднамеренное удаление кода определенной страны домена верхнего уровня (ccTLD) или определенного домена верхнего уровня общего

[92] См.: http://www.iana.org/about (последнее посещение 1 марта 2016 г.).
[93] См.: www.icann.org/stewardship (последнее посещение 1 марта 2016 г.).

назначения (gTLD) из корневой зоны во время международного конфликта остается причиной для беспокойства некоторых стран, которые выступают против сохранения исторической роли США в отношениях с Корпорацией Интернета. Текущий процесс обновления файла корневой зоны включает в себя всех заинтересованных участников. Процесс обновления файла корневой зоны предполагает контролирующую роль Министерства торговли США. Обеспокоенность некоторых правительств связана с тем, что США имеют необоснованный контроль за процессом управления и обновления файла корневой зоны. Что изменится когда процесс передачи координирующей роли NTIA в осуществлении функций IANA завершится как запланировано?[94]

Предложение в ходе Всемирной конференции по международной электросвязи в Дубае в декабре 2012 г., одобренное Россией, Китаем, Саудовской Аравией, Алжиром и Суданом, гласило: «Государства-члены имеют суверенное право разрабатывать и осуществлять государственную политику, включая международную политику, в вопросах управления Интернетом». Это предложение также содержало призыв к государствам-членам взять на себя большую часть функций ICANN, которые включают в себя распределение номеров, имен и адресов в Интернете. Документ не был рассмотрен на конференции, поэтому формальное голосование по этому документу не было проведено. Но это была не первая и не последняя попытка ввести такую формулировку на межправительственных встречах. К окончанию конференции делегация США подчеркнула, что «политика в сфере Интернета может определяться гражданами, сообществами и обществом в целом, а не странами-участницами».[95]

Технические риски

Корневые серверы являются частью критической инфраструктуры Интернета, и нарушения в их работе могут повлиять на работу Интернета. В прошлом предпринимались попытки осуществления распределенных атак типа «отказ в обслуживании» против корневых серверов, но безуспешно. Для минимизации риска таких атак в архитектуру инфраструктуры DNS встроены механизмы поддержания отказоустойчивости. Различные механизмы поддержания отказоустойчивости включают в себя локальное кэширование, резервные сервера, балансировку нагрузки и географическую распределенность серверов. Кроме того, интернет-провайдеры могут размещать файл корневой зоны на своих собственных серверах и перенаправлять трафик в пределах своих сетей к своим серверам вместо направления запросов напрямую одному из корневых серверов. Атака против популярного домена верхнего уровня (например, .com) может нарушить работу существенной части Интернета. Также необходимо помнить, что домены верхнего уровня зачастую управляются разными организациями, которые находятся в разных юрисдикциях. Тем не менее, это не мешает правоохранительным органам раскрывать уголовные дела с участием доменных имен физических лиц по всему миру.

[94] См.: http://icann.org/stewardship/ (последнее посещение 1 марта 2016 г.).
[95] См.: http://www.state.gov/r/pa/prs/ps/2012/12/202037.htm (последнее посещение 1 марта 2016 г.).

Существует мнение, что отсутствие однородности является еще одной угрозой стабильности DNS. Учитывая тот факт, что DNS является единой однородной и распределенной базой данных, ее гомогенность действительно может являться источником угроз. Против физических серверов также могут быть предприняты атаки нулевого дня, поскольку число серверов исчисляется сотнями и они хорошо известны. Но эта проблема уже частично разрешена техническим сообществом, которое разработало ряд решений, которые включают в себя создание зеркальных копий корневых серверов, а также разработку и внедрение набора расширений DNS DNSSEC[96]. Встроенные механизмы защиты включают в себя резервное копирование файла корневой зоны на каждом корневом сервере и обеспечение связности с другими серверами для получения обновлений. Любые изменения в файле корневой зоны проходят через тщательно спланированный процесс, предполагающий несколько уровней авторизации и проверки (включая ручную проверку). Для обеспечения достоверности и целостности данных DNS цепочка доверия начинается с корневых серверов и спускается вниз по иерархии разрешения доменов через цепочку серверов. Сигнатура зоны верхнего уровня проверяется с помощью открытого ключа на каждом уровне разрешения.

Риски передачи координирующей роли NTIA в осуществлении функций IANA

Контракт между Администрацией адресного пространства Интернет и Национальным управлением по телекоммуникациям и информации США истекает в сентябре 2016 г.

Некоторые страны пытались в течение многих лет перевести процессы управления Интернетом в компетенцию международных правительственных организаций таких, как Международный союз электросвязи (ITU). Все заинтересованные участники выражают свои сомнения в отношении такого развития событий. Одной из проблем при таком сценарии выступает скорость принятия решений. Тогда как для экосистемы Интернета существует необходимость в оперативном принятии решений, такие международные организации очень медленно принимают решения на основе консенсуса. Большая бюрократическая организация, которая осуществляет контроль за Интернетом, может свести на нет весь процесс управления и разрешения споров. И если существует голосование по определенным вопросам, то остаются вопросы относительно права вето — кто им может пользоваться, какие будут последствия его несоблюдения и т.д.

Управление конфликтами, связанными с фундаментальными принципами Интернета

Фундаментальным руководящим принципом Интернета является сетевая нейтральность, которая предполагает равный доступ к Интернету для всех пользователей без осуществления дискриминации. Этот принцип выступил движущей силой для предоставления доступа к Интернету миллиардам пользователей и создания стимулов для развития инноваций, которые трансформировали Интернет в новый мир. К угрозам для сетевой нейтральности

[96] См.: https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en (последнее посещение 1 марта 2016 г.).

можно отнести привилегированный доступ и ограничение доступа к сети Интернет. Принцип сетевого нейтралитета теперь находится под угрозой. Коммерческие компании запрашивают от телекоммуникационных компаний привилегированный доступ для своих данных, т. е. просят создавать быстрые и медленные каналы передачи данных с разными финансовыми условиями. Например, провайдеры услуг потокового видео могут запросить от компаний привилегированный доступ к своим услугам. 15 мая 2014 г. председатель Федеральной комиссии по связи США (FCC) предложил новые правила, которые предполагали, что «интернет-провайдеры могут разделять свой поток на уровни, предлагая приоритетный режим для крупных корпораций, которые будут платить более высокую плату». В ответ более, чем 200 тыс. человек высказались за отказ от предложенного правила. 26 февраля 2015 г. Федеральная комиссия по связи США (FCC) выступила с новыми правилами открытого Интернета для защиты сетевой нейтральности, которая относится к фиксированным и мобильным услугам передачи данных. Эти правила включают в себя следующие положения:

- интернет-провайдеры не могут блокировать доступ к правомерным материалами, приложениям, услугам и безвредным устройствам;
- интернет-провайдеры не могут повреждать или ухудшать правомерный интернет-трафик к материалам, приложениям, услугам и безвредным устройствам;
- интернет-провайдеры не вправе отдавать предпочтения никакому правомерному интернет-трафику за какую-либо оплату.

Эти правила запрещают провайдерам Интернет-услуг создавать быстрые и медленные каналы передачи данных, а также запрещают провайдерам Интернет-услуг предоставлять приоритетный доступ для аффилированных организаций. В то же время, обсуждение вопросов сетевой нейтральности продолжается в других странах таких, как Чили, Индия, Бразилия, Канада и Нидерланды.

Цензура в Интернете

Одной из ключевых проблем, связанной с утратой США контроля за процессом управления Интернетом, является цензура в Интернете. Между национальными государствами уже назрел конфликт в отношении их суверенных прав на осуществление цензуры информации в Интернете. Существует несколько способов осуществления цензуры в Интернете: (1) создание нормативно-правовой базы для накладывания ограничений на провайдеров Интернет-услуг, которые позволят государству наблюдать за источниками и блокировать веб-сайты; (2) контроль за поведением частных лиц, которые публикуют и получают доступ к неправомерной информации; (3) проведение активной фильтрации данных и ограничения доступа к данным и поиску в Интернете с помощью технических средств[97,98].

Китаю успешно удалось создать программу цензуры, с помощью которой он способен фильтровать слова из поисковых результатов и ограничивать доступ к сайтам на уровне маршрутизаторов восьми Интернет-шлюзов, центров

[97] См.: http://www.fas.org/sgp/crs/row/R42601.pdf (последнее посещение 1 марта 2016 г.).
[98] См.: https://www.fas.org/sgp/crs/misc/R42351.pdf (последнее посещение 1 марта 2016 г.).

обработки данных телекоммуникационных компаний, и Интернет-порталов. Китай также осуществляет регулирование и мониторинг за деятельностью провайдеров интернет-услуг, интернет-кафе и внутренних систем университетов; регистрации вебсайтов и блогов, а также отслеживание диссидентской активности. Автоматическая фильтрация выполняется для материалов, затрагивающим следующие темы: демократия, права человека, Фалуньгун. Автоматическая фильтрация также применяется для социальных медиа, отнесенных к политически чувствительным, файлообменные сайты. Все это дополняется наблюдением за сетевой активностью в ручном режиме с привлечением массивной армии аналитиков. Ряд законов, которые могут применяться для показательных наказаний, а также технические средства для обнаружения неправомерной активности, стимулирует граждан соблюдать существующие правила.

Некоторые страны Ближнего Востока используют схожие методы осуществления цензуры в Интернете. Например, ограничивают скорость Интернета, чтобы предотвратить распространение фотографий и видео, а также блокирование веб-сайтов, размещающих материалы, которые считаются враждебными по мнению политических или религиозных лидеров. Египет пошел еще дальше и отключил Интернет в период политической нестабильности, а египетские блогеры были обнаружены и арестованы или подвержены жестокости полиции. Иран, Саудовская Аравия и Сирия также предпринимали попытки осуществлять цензуру в Интернете в разное время по целому ряду причин таких, как политическая нестабильность, распространение порнографии, а также религиозная критика.

Некоторые заинтересованные участники опасаются, что сокращение роли США в процессе управления Интернетом может привести к тому, что авторитарные правительства могут оказать воздействие на свободы в Интернете. Учитывая тот факт, что некоторые из ключевых мировых держав уже осуществляют цензуру в Интернете, не исключено, что в модели управления без контроля США большинство государств будет склоняться к цензуре и осуществлению суверенного контроля за материалами в Интернете. Этот страх зачастую ошибочно связывают с процессом передачи координирующей роли NTIA в осуществлении функций IANA, который может создать базу для осуществления цензуры. Но это не так, поскольку ICANN не занимается материалами или какими-либо другими вопросами, связанными с веб-сайтами. К тому же, модель с привлечением всех заинтересованных участников будет нуждаться в необходимости предоставления гарантий того, что основные положения и принципы Интернета не будут нарушены при передаче полномочий от правительства США ко всем заинтересованным участникам.

4.2. Законы и соглашения, регулирующие поведение в киберпространстве

В связи с глобальной природой Интернета, возникает необходимость в международном регулировании международных конфликтов в Интернете. В условиях отсутствия глобального режима регулирования Интернета, лица, совершающие преступления, могут использовать Интернет в качестве безопасного места для осуществления киберпреступлений и террористической деятельности. Гармонизация законодательств всех стран мира является сложной

задачей, которая при этом становится все более и более важной на уровне национальных и региональных законодательных актов, носящих временный характер. В то время, как анонимность является основополагающим принципом Интернета, совершенствование судами своих технических возможностей и законный доступ к информации интернет-провайдеров упрощает процесс идентификации пользователей. Однако отсутствие закрепленных договорами международно-признанных норм публичного права усложняет процесс правоприменения. Необходимо принятие норм международного частного права для регулирования не только преступной и террористической деятельности, но и других аспектов, таких как нарушения обязательств по договорам и правонарушения. Очертания норм международного частного права можно увидеть в национальных законодательствах, а нормы права определяют надлежащую юрисдикцию при ведении судебного процесса.

Региональные и многосторонние межгосударственные соглашения

Эстония

Эстония действует в соответствии с нормами права для разрешения проблем, влияющих на деятельность международных организаций, занимающихся проблемами непрерывного развитием и эффективного применения норм международного права - в частности, ООН и Совета Европы. Верховенство закона определяет стремление к мирному и взаимовыгодному сотрудничеству между государствами, поддерживая баланс интересов и гарантию стабильности глобального общества. Одной из целей к которым стремится Эстония является стабильное развитие стран, составляющий регион Балтийского моря: Швеции, Финляндии, Германии, Латвии, Литвы и Польши. Достижение этой цели будет успехом на пути к диалогу по политическим проблемам и вопросам безопасности между Скандинавскими странами и государствами Прибалтики. Чтобы достичь потенциального процветания региона, Эстония принимает активное участие в реализации Стратегии ЕС для региона Балтийского моря, которая является первой всеобъемлющей стратегией ЕС, направленной на развитие макрорегиона. Задача заключается в обеспечении более сбалансированного развития региона Балтийского моря путем мобилизации всех подходящих источников финансирования и применения соответствующих политических практик Европейского союза, а также координации действий, предписанных Европейским союзом, странами и регионами ЕС, панбалтийскими организациями, финансовыми институтами и негосударственными организациями.

Внимание Эстонии привлекло развитие демократии и рост благосостояния в России. Это привело к развитию российско-эстонских отношений параллельно усилиям Европейского Союза и НАТО, направленным на установление взаимовыгодных отношений с Россией. Подобное нацеленное на сотрудничество взаимодействие, основанное на демократический ценностях более долговечно, устойчиво и продуктивно в долгосрочной перспективе. В идеале, Эстония стремится к открытому диалогу с Россией по всем возникающим вопросам, пытаясь найти возможности практического сотрудничества в порядке, установленном ЕС и НАТО.

США

Потребность в ресурсах, конкурирующие императивы стран-членов и необходимость реформ в ряде политических и административных областей - вот некоторые из вызовов, стоящих перед ООН и другими многосторонними институтами. Если смотреть дальше, то отсутствует согласие по вопросу, как менять функционирующую в настоящее время систему. США, как страна, пользующаяся авторитетом в сфере проведения стратегической политики, заняты выработкой устойчивых решений во всех сферах внешней политики, привлекая к этому дипломатические и иные необходимые ресурсы. США используют концепции, основанные на послевоенной правовой системе регулирующей поставки товаров первой необходимости для строительства справедливого и мирного мира, где каждый имел бы возможность полностью раскрыть свой потенциал. Эта послевоенная правовая система восходит к Уставу ООН, а также многосторонним соглашениям, регулирующим займы правительствам другим стран для ведения войны, соблюдения прав человека, поддержания режима нераспространения и многие другие вопросы глобальной значимости. Для того, чтобы усовершенствовать и модернизировать свои подходы к решению подобных задач, США работают совместно с ООН и другими многосторонними институтами, а также их странами-членами, чтобы гарантировать защиту, стабильность и поддержку будущим поколениям.

США также борются с преступной деятельностью при помощи направленных экономических санкций и мер принуждения, которые приводят к издержкам для тех, кто своей военной агрессией, неспровоцированным насилием или иными незаконными действиями ставит под угрозу международные правила и нормы. При том, что США, если надо, могут действовать и в одиночку; когда надо, они будут стремиться к принятию многосторонних санкций, включая санкции ООН. Вводимые США санкции продолжают разрабатываться под выполнение отдельных целей, работающих также на минимизацию непредвиденных последствий для глобальной экономики и гражданского населения. Также эти санкции работают на сдерживание серьезных угроз с целью поддержания стабильности и порядка на региональном уровне. Целью этих санкций является также поддержание долгосрочной конструктивной повестки во всех регионах с упором на обновление альянсов в формате дружественных отношений, вложение инвестиций в партнерство с молодыми демократиями, разделяющими интересы с США, а также на дальнейшую поддержку развития функционирующих региональных институтов, которые будут работать на закрепление устоявшихся норм международного права.

Россия

В вопросе развития механизмов двухстороннего и многостороннего сотрудничества, внешняя политика России делает упор на развитие отношений с членами Содружества Независимых Государств (СНГ), беря за основу углубление регионального взаимодействия между членами организации, построенного на общей истории и потенциале к интеграции в различных сферах. Дружественные отношения России со странами СНГ строятся на принципах равенства, взаимной выгоды, уважения и учета взаимных интересов, а также развитии интеграционных процессов.

Россия рассматривает Организацию по безопасности и сотрудничеству в Европе (ОБСЕ) в качестве важнейшего инструмента выстраивания справедливой и неделимой системы общеевропейской безопасности. Россия хочет усилить роль и поднять авторитет ОБСЕ путем выработки устава организации и концентрации на действительно неотложных проблемах - особенно на тех, которые связаны с транснациональными вызовами и угрозами безопасности.

Российская Федерация рассчитывает выстроить отношения с США в различных областях, развивать взаимовыгодное сотрудничество, а также укреплять двусторонние связи, делая акцент на ответственности обоих государств в сфере глобальной стратегической стабильности и международной безопасности.

Россия также стремится к открытому диалогу с региональными организациями Юго-Восточной Азии и АСЕАН.

Дружественные отношения с Китаем и Индией являются одним из приоритетов развития внешней политики России. Это подразумевает выстраивание всеобъемлющего, равного и доверительного партнерства, а также стратегического сотрудничества с Китаем на основе идентичности фундаментальных подходов к решению ключевых глобальных проблем, которая является ключевым элементом региональной и глобальной стабильности. Россия стремится отвечать на новые угрозы и вызовы и находить решения срочных региональных и международных проблем в сотрудничестве с Советом Безопасности ООН, Большой Двадцаткой, БРИКС, Саммитом Стран Восточной Азии, ШОС и другими многосторонними форматами.

Россия стала ключевым сторонником продвижения проекта правил поведения в Интернете по линии Шанхайской Организации Сотрудничества (больше про ШОС читайте ниже) и на других уровнях, включая ООН.

Индия

Индия ведет работу с несколькими государствами с целью выстраивания с ними отношений и стимулирования глобального и регионального экономического роста. Вместе с США Индия способствует достижению мира, процветания и стабильности в Азиатско-Тихоокеанском регионе и регионе Индийского океана. Продвижение создания все более взаимосвязанной инфраструктуры, а также идей экономического развития позволило связать регионы Южной, Юго-Восточной и Средней Азии, что стимулировало развитие процессов передачи электроэнергии, а также контактов между людьми из различных стран. Предложения избегать к угрозам и применению силы для разрешения территориальных споров будут соответствовать принципам, заложенным международным правом, в том числе и нормам, принятым ООН. Совместные усилия Индии и США также направлены на борьбу с терроризмом, пиратством и распространением оружия в рамках региона или за его пределы. Их целью также является повышение значимости Саммита Стран Восточной Азии, а также продвижение регионального диалога по ключевым политическим аспектам и проблемам безопасности путем развития сотрудничества. Индия стремится достичь поставленных задач в течение следующих пяти лет путем развития регионального диалога, приложения усилий к совершенствованию трехсторонних консультаций с третьими странами

региона, а также углубления региональной интеграции, повышения значимости региональных форумов, поиска новых многосторонних форматов и сфер, которые можно использовать для достижения глобального процветания.

Открывая Британско-индийский стратегический диалог, Индия и Великобритания договорились вместе работать над вопросами, представляющими общий интерес в сфере киберпространства. Индия и Великобритания разделяют ключевые принципы свободы, прозрачности, свободы слова и верховенства закона в киберпространстве. В 2012 г. Индия и Великобритания провели первый организованный диалог по сотрудничеству в киберпространстве, который теперь проводится раз в полгода для достижения целей, поставленных странами. В ходе диалога стороны обсуждают следующие вопросы: развитие международного сотрудничества с целью снижения угроз международной безопасности, исходящих из киберпространства; укрепление двухстороннего сотрудничества для борьбы с киберпреступностью; сотрудничество по совершенствованию навыков персонала и наращиванию потенциала для борьбы с киберугрозами и использование ИКТ в целях экономического развитие; создание глобальной, многосторонней демократической системы управления киберпространством, подразумевающую участие всех заинтересованных в этом сторон.

ШОС

Шанхайская Организация Сотрудничества (ШОС) была образована в 2001 г. после подписания «Декларации о создании Шанхайской Организации Сотрудничества» Китаем, Россией, Казахстаном, Кыргызстаном и Узбекистаном. Главными целями ШОС являются: укрепление взаимного доверия и дружественных отношений между странами-участниками; развитие сотрудничества в политической, торговой, экономической, социальной, научно-технической и культурной сферах; приложение совместных усилий для установления и обеспечения мира, безопасности и стабильности в регионе, а также движение навстречу новому демократическому, справедливому и рациональному международному экономическому порядку. Внутренняя политика ШОС основана на принципах взаимного доверия, равноправия, совещательности, уважения к разнообразным культурам, а также развития всех участников организации. Внешняя политика организации базируется на принципах неприсоединения, не направленности против какой-либо третьей стороны и прозрачности.

Высшим органом принятия решений в ШОС является Совет Глав Государств (СГГ). СГГ собирается раз в год для принятия различных решений и выработки инструкций по важнейшим аспектам деятельности ШОС. Совет глав правительств (СГП) также собирается раз в год для обсуждения стратегий многостороннего сотрудничества и приоритетных направлений деятельности организации с целью обеспечения лучшего исполнения решений по вопросам экономической политики и принятия бюджета организации на год. Также проводятся встречи на уровне спикеров парламентов, секретарей советов безопасности, министров иностранных дел, министров обороны, экономики и т.д. Взаимодействие по вопросам основополагающих принципов ШОС обсуждается в рамках совета национальных координаторов стран ШОС.

В 2011 г. четверо членов ШОС передали на рассмотрение Генеральной Ассамблеи ООН проект правил поведения в области обеспечения международной информационной безопасности. Целью проекта было добиться международного признания общих вызовов в сфере информационной безопасности, для противодействия которым необходимо развитие международного сотрудничества и взаимного уважения. Проект получил неоднозначный консенсус в проблеме регулирования и его влияния на права человека. Соглашение между правительствами государств-членов Шанхайской Организации Сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности - договор, заключенный странами ШОС. Известный также как Екатеринбургская декларация, он был подписан в 2009 г. и призывал к созданию более справедливой и рациональной системы межправительственных отношений и делал упор на сотрудничестве. В сентябре 2014 г. на саммите в Душанбе страны-члены ШОС подтвердили свою позицию по вопросам информационной безопасности, а также приняли в состав организации два новых члена: Индию и Пакистан.

НАТО

Организация Североатлантического Договора впервые ввела проблему кибербезопасности в свою политическую повестку на Пражском саммите 2002 г. и с тех пор многократно возвращалась к ней. Более внимательно относиться к проблемам кибербезопасности НАТО заставили кибератаки на Эстонию в 2007 году, которые вывели из строя ключевые веб-сайты эстонских организаций и отключения интернета у широкой общественности. В 2008 г. НАТО подготовила свою первую программу кибероборонь. НАТО включила проблему кибероборонь в свою Стратегическую Концепцию на Лиссабонском саммите в 2010 году, на котором была принята декларация, обновленная в Политике НАТО в области кибербезопасности в 2011 г. Наряду с этим в 2012 г. был принят План действий. Углубленная политика кибероборонь была принята на саммите 2014 г. в Уэльсе. Этот документ подтвердил, что крупная кибератака на одного из членов альянса будет подпадать под пятую статью Вашингтонского договора. Пятая статья Вашингтонского договора является основополагающим принципом НАТО, согласно которому, если один из членов НАТО подвергается вооруженному нападению, то все остальные члены альянса рассматривают подобный акт как нападение на всех членов НАТО, что повлечет за собой действия, направленные на защиту атакованного союзника в том случае, если они будут сочтены необходимыми. Политика кибероборонь также совершенствует механизмы обмена информацией и взаимопомощи, а также продолжает развивать сотрудничество в киберпространстве.

Вопросами кибероборонь в НАТО занимается множество органов. Если речь заходит об ответных действиях на кибератаку в рамках коллективной обороны, то такие действия требуют консенсусного решения Североатлантического Совета, состоящего из представителей всех стран-членов альянса и возглавляемого генеральным секретарем альянса. Вместе с Североатлантическим Советом вопросами кибероборонь занимается также Комитет по кибероборонь, который также дает консультации членам альянса и осуществляет всеобъемлющее руководство внутренней кибероборонь НАТО. Существует

также Управляющий совет по кибероборонe который действует под эгидой Отдела по ключевым вызовам безопасности штаб-квартиры НАТО. Данный орган состоит изо всех существенных игроков, заинтересованных в обеспечении кибербезопасности НАТО, включая Стратегическое командование НАТО по операциям и Командование НАТО по трансформации. Управляющий Совет по кибероборонe обладает полномочиями подписания меморандумов о взаимопонимании между членами альянса в целях содействия обмену информацией, координирования помощи, осуществления стратегического планирования выработки решений, касающихся исполнительных директив по вопросам сетей, принадлежащих альянсу.

В 2012 г. в соответствии с целями, заложенными декларацией, принятой в ходе Лиссабонского саммита, в результате слияния двух агентств НАТО, занимавшихся командованием, контролем, коммуникациями, разведкой и наблюдением, и деятельностью в киберпространстве, было создано Агентство НАТО по коммуникациям и информации. В рамках Агентства НАТО по коммуникациям и информации создан Координационный центр НАТО по реагированию на компьютерные инциденты, отвечающий за централизованную техническую защиту объектов цифровой инфраструктуры НАТО. Также в структуру НАТО входит Объединенный центр передовых практик в области кибероборонbы (CCD COE), который является аккредитованным научно-практическим центром, занимающимся обучением кадров, консультированием, исследованиями и дальнейшим развитием сферы кибербезопасности.

ОБСЕ

Организация по безопасности и сотрудничеству в Европе занимается широким набором вопросов безопасности и иных проблем, включая права человека, демократизацию и противодействие терроризму. ОБСЕ занимается теми аспектами кибербезопасности, которые связаны с противодействием терроризму и киберпреступности. На советах министров в 2004 и 2006 годах на межгосударственном уровне были приняты решения, направленные на углубление международного сотрудничества для противодействия использованию социальных сетей в террористических целях. Начиная с 2008 г. последующие декларация Парламентской Ассамблеи призывали государства принимать меры и сотрудничать в целях противодействия киберпреступности и укрепления кибербезопасности. Последняя декларация Парламентской Ассамблеи восходит к Монакской Декларации и Резолюции 2012 года. Резолюция призывала создать и организовать в рамках ОБСЕ систему распространения взглядов и методических рекомендаций касательно мер выстраивания доверия и безопасности, особенно в сфере кибербезопасности и кибертерроризма. Ранее ОБСЕ приняла меры по выстраиванию доверия по вопросам киберпространства, которые должны укрепить межгосударственное сотрудничество, повысить прозрачность, предсказуемость и стабильность наряду с минимизацией рисков недопонимания, эскалации и конфликтов, которые могут возникнуть в результате использования ИКТ. Меры по выстраиванию доверия были одобрены в ходе заседания совета министров в декабре 2013 года, где также обсуждался обмен информацией по киберугрозам, велись консультации с целью снижения рисков возникновения напряженности, осуществлялся обмен мнениями по поводу использования ОБСЕ в качестве платформы для диалога.

Внутриполитические аспекты (включая методические рекомендации)

Эстония

Безопасность Эстонии зависит от внутренней обстановки и от международной обстановки. Наиболее серьезные угрозы для Эстонии сочетают в себе воздействие внешних и внутренних факторов. События, ставящие под угрозу единство НАТО и солидарность ее стран-членов, несут в себе угрозу, как для безопасности Эстонии, так и для всего трансатлантического региона. Внешние факторы могу представлять собой применение силы в отношении Эстонии, угрозы безопасности страны в результате нанесения ущерба ее международной репутации, создание внутренней нестабильности, военное давление или принуждение Эстонии или ее союзников к принятию таких решений, которые поставят под сомнение независимость и суверенный статус страны. Еще одна угроза исходит от деятельности секретных служб иностранных государств, направленной против Эстонии. Однако членство Эстонии в НАТО и Европейском союзе, а также наличие близких двусторонних отношений с союзниками, позволяют Эстонии противостоять любому возможному внешнему давлению.

В связи с тем, что экономика Эстонии глубоко интегрирована в мировую экономику, любые глобальные события будут влиять на Эстонию. Это само по себе вызывает опасения касательно возможных изменений в существующей структуре энергопоставок между ЕС и Россией, которые могут повлиять на успешно функционирующую экономику Эстонии. Любой кризис в экономическом и финансовом секторе может создать благоприятные условия для ненужной социальной напряженности и распространения организованной преступности. Также важна защита информационно-коммуникационных систем, поскольку от них зависит работа ключевых государственных служб. Так как большинство информационно-коммуникационных систем взаимосвязаны, то временное вывод из строя критических систем, скорее всего, приведет к недоступности услуг критически важных для общества служб. Неверная ответная реакция или недостаточная защита инфраструктуры может усилить эффект от угроз аварий и кибератак. Эстония выработала политику внутренней безопасности, направленной на создание такого общества, где бы людям было гарантировано проживание в безопасной среде и которое было бы способно справиться с любыми угрозами. Для этого Эстония прибегает, когда нужно, к технологическим новшествам, а также к привлечению гражданских ассоциаций. Кроме того, вступление в Шенгенскую зону повысило важность сотрудничества между Эстонией и Европейским Союзом.

Борьба с киберпреступностью включает в себя противодействие другим факторам, таким как терроризм и международная организованная преступность, а также обеспечение функционирования информационно-коммуникационных систем и финансовой безопасности. В связи с тем, что существует зависимость между критическими информационно-коммуникационными системами и информационными технологиями, Эстония в настоящее время развивает сотрудничество между различными агентствами как на национальном, так и на

международном уровне. Эстония также намерена осуществлять дальнейшие шаги на законодательном уровне и повышать осведомленность общества.

США

Национальная и экономическая безопасность Соединенных Штатов зависит от надежности функционирования критической инфраструктуры. Для выполнения данной задачи президент США Барак Обама издал Президентский Указ, призывающий к развитию независимой системы кибербезопасности, призванную стать приоритетным, гибким и недорогим вариантом устранения рисков для процессов, информации и систем, напрямую вовлеченных в функционирование критической инфраструктуры. Президентский Указ определяет критическую инфраструктуру как «физические и виртуальные системы и мощности, настолько важные для Соединенных Штатов, что вывод из строя или уничтожение таких систем и мощностей подорвет безопасность, национальную экономическую безопасность, безопасность национальной системы здравоохранения или несколько указанных факторов в любом сочетании». На фоне растущего давления со стороны внешних и внутренних угроз, организации вовлеченные в функционирование критических инфраструктур, должны быть постоянно в состоянии распознать и оценить любые риски кибербезопасности, а также суметь справиться с ними. Имеющие доступ к критической инфраструктуре организации подразделяются на общественных и частных собственников, а также на компании-операторы и иные группы, играющие значимую роль в обеспечении безопасности национальной критической инфраструктуры, выполняющие функции поддержания функционирования информационных технологий и промышленных систем управления (ICS). Важной особенностью упомянутого президентского указа является то, что он содержит в себе методологию защиты приватности и гражданских свобод, поскольку два эти принципа играют важнейшую роль при выстраивании общественного доверия. Эта методология составлена таким образом, чтобы предоставленное руководство по снижению рисков, связанных с приватностью, соответствовало подходу организаций к управлению рисками кибербезопасности. Интегрирование безопасности личных данных и кибербезопасности может быть выгодным для организаций, поскольку оно повышает уверенность клиентов, предоставляя более стандартизированный метод обмена информацией и упрощая осуществление операций в рамках различных правовых режимов.

Система обеспечения работы критической инфраструктуры функционирует, основываясь на уже существующих стандартах, рекомендациях и практиках, которые стимулируют провайдеров критической инфраструктуры добиваться устойчивости ее функционирования, особенно используя при этом практики, которые были разработаны, введены и усовершенствованы мировой индустрией. Инструменты и методы, используемые для развития этой системы нацелены на то, чтобы результаты ее функционирования имели международную значимость, позволили бы признать глобальную природу рисков кибербезопасности и сочетались бы с технологическим прогрессом и требованиями бизнеса. Данная система предлагает организациям общий механизм для оценки их положения в системе кибербезопасности, потенциальных рисков и других факторов.

Данная система закладывает основанный на оценке рисков подход к управлению рисками кибербезопасности, который состоит из трех частей: ядро системы, уровни реализации системы и рамки системы. Ядро системы представляет собой сочетание деятельности в сфере кибербезопасности, желаемых результатов и соответствующих примечаний, свойственных для секторов критической инфраструктуры. Ядро системы состоит из пяти постоянных функций: распознавание, защита, выявление, реагирование и восстановление. Уровни реализации системы предоставляют организациям возможность взглянуть на риски кибербезопасности и процессы, используемые для управления этими кибер-рисками. В соответствии с названием, уровни реализации системы определенным образом ранжируют практики организаций, подразделяя их на: частичные (Уровень 1), в условиях осведомленности о риске (Уровень 2), повторяющиеся (Уровень 3) и адаптивные (Уровень 4). Эти уровни демонстрируют прогресс практик от относительно неформальных и носящих реактивный характер ответных мер к гораздо более гибким формам в условиях осведомленности о риске. В рамках системы рассматриваются результаты, вытекающие из нужд бизнеса, которые организация выбирает из категорий и подкатегорий системы. Эта схема может быть использована для выявления возможностей улучшения ситуации в сфере кибербезопасности путем сравнении схемы «нынешнего» и «будущего» кейса. Эта система является адаптивной и способной обеспечивать гибкие решения, основанные на анализе рисков. Такие решения могут быть использованы во множестве процессов управления рисками в тех или иных сферах и отраслях.

В 2015 г. Барак Обама принял президентский указ, направленный на противодействие криминальной деятельности в киберпространстве, представляющей угрозу национальной безопасности. Президентский указ уполномочивает министра финансов США после проведения консультаций с генеральным прокурором и государственным секретарем накладывать санкции на индивидов и организации, замешанные или участвующие в преступной деятельности в киберпространстве, допускающей возможность возникновения серьезной угрозы национальной безопасности, внешней политике, экономическому благосостоянию или финансовой стабильности США. Президентский указ был принят в связи с участившимися случаями совершения серьезных преступлений в киберпространстве, многие из которых были совершены лицами, находящимися за пределами штатов, что представляет серьезную угрозу для США.

Президентский Указ расписывает действия, которые необходимо предпринимать в ответ на нанесение различного ущерба включая: нанесение ущерба или дискредитирование служб обеспечения, имеющих отношение к сектору критической инфраструктуры, незаконное присвоение средств или экономических ресурсов; разглашение торговой тайны, личных данных и финансовой информации для получения конкурентного преимущества; намеренное получение или использование торговой тайны, присвоенной посредством деятельности в киберпространстве.

Президентский указ мог, в конечно счете, привести в началу необходимого межгосударственного диалога по созданию норм поведения в киберпространстве и противодействию киберпреступности. Президентский указ поднимает вопрос о

том, как страна должна развивать инструменты, позволяющие ей принять соответствующие ответные меры, и предлагает новый метод противодействия растущей угрозе со стороны наиболее опасных акторов незаконной деятельности в киберпространстве. У документа также есть потенциал сдерживания других акторов от участия в подобной деятельности.

Наряду с Президентским указом, США располагают также иными инструментами противодействия киберпреступности, такими как дипломатическое вмешательство, торговая политика и правоприменительные механизмы. Другие методы включают в себя совершенствование защиты правительственных систем, обмен информацией с частным сектором, а также создание Интегрированного Центра по Разведке Киберугроз, который должен будет осуществлять интегрированный анализ зарубежный киберугроз для федерального правительства и помогать осуществлять меры, необходимые для обеспечения кибербезопасности и защиты сетей.

Россия

Целью российской политики является создание стабильной и устойчивой системы международных отношений, основанной на международном праве и принципах равенства, а также на взаимном уважении и невмешательстве во внутренние дела других государств. В рамках данного подхода Россия считает обеспечение и защиту информационной сферы важной задачей для обеспечения своих национальных интересов, которые включают в себя укрепление демократии, создание социального государства, уделяющего особое значение верховенству закона, а также достижению и поддержанию социальной гармонии. Исходя из этих интересов, Россия формирует свою внешнюю политику, которая носит стратегический и направленный на внутреннюю политику характер для достижения цели обеспечения информационной безопасности. Эта политика берет за основу четыре составляющих национальных интересов России. Первый компонент включает в себя соблюдение конституционных прав и свобод человека и гражданина на получение и использование информации, на сохранение и укрепление моральных ценностей, представленных в обществе, традиций патриотизма, а также культурного и научного потенциала страны. Второй компонент предоставляет информационную поддержку государственной политике Российской Федерации, предоставляя российской и мировой общественности достоверную информацию о государственной политике Российской Федерации и делая доступной российскую позицию на открытых правительственных источниках. Третий компонент касается продвижения современных информационных технологий, содействующих развитию национальной информационной индустрии, удовлетворяющих запросы внутреннего рынка и обеспечивающих надежность хранения и эффективность использования данных национальных информационных ресурсов. Четвертый компонент включает в себя защиту информационных источников от несанкционированного доступа, а также надежность информационно-коммуникационных систем, независимо от их нынешнего статуса.

Индия

Индия стремится создать надежное и устойчивое к угрозам киберпространство для своих граждан, бизнеса и правительства, создать ресурсы для предотвращения и реагирования на киберугрозы и минимизировать ущерб от инцидентов в киберпространстве. Индия ставит перед собой задачи создать надежную систему выработки политики безопасности, укрепить нормативно-правовую базу для обеспечения безопасности киберпространства, усовершенствовать защиту и устойчивость национальной критической инфраструктуры за счет функционирования круглосуточного Национального Центра Защиты Критической Информационной Инфраструктуры, усовершенствовать механизм обеспечения неприкосновенности ИКТ продуктов и услуг, создать культуру кибербезопасности и приватности, стимулируя ответственное поведение пользователей, а также многие другие задачи. Для создания надежной системы кибербезопасности Индия стимулирует все организации разрабатывать свою политику информационной безопасности, назначать Центральное национальное агентство с четко ограниченными функциями и ответственностью для координации всех аспектов, связанных с кибербезопасностью в стране, а также предотвращать единичные и повторные инциденты в киберпространстве, поощряя развитие технологий, следование правилам кибербезопасности и проактивные действия.

Индия также ставит своей целью продвижение мирового опыта в сфере кибербезопасности, а также приверженности укреплению кибербезопасности; встраивание мирового опыта в формальные процессы оценки и управления рисками; стимулирование развитие программного обеспечения с опорой на мировой опыт; а также согласование системы оценивания для периодического контроля соблюдения стандартов передового опыта и рекомендаций в сфере кибербезопасности. Для того чтобы создать механизм раннего оповещения, управления уязвимостью и реагирования на угрозы безопасности, Индия намерена создать на национальном уровне системы, процессы и структуры наряду с круглосуточной Национальной Командой Реагирования на Компьютерные Происшествия, которая выполняет функцию узлового агентства для кризисного управления в сфере кибербезопасности.

Также Индия поощряет использование инфраструктуры открытых ключей в правительстве для осуществления коммуникаций и транзакций. Для обеспечения всех аспектов развития, направленных на выполнение краткосрочных, среднесрочных и долгосрочных задач, также осуществляются научно-исследовательские программы. Данные программы будут включать в себя все аспекты, включая развитие надежных систем, тестирование процедур, развертывание и дальнейшее их поддержание на протяжении всего жизненного цикла. Научно-исследовательские программы будут осуществляться совместно с промышленным и научным сообществом и будет направлено на развитие передовых технологий и практико-ориентированных исследований, а также на создание инновационных центров в областях, стратегически значимых для безопасности киберпространства.

Нерешенные правовые вопросы

Необходимо выйти за рамки рассмотрения вопросов на базовом уровне и искать такие возможности улучшения нынешней ситуации, которые были бы

согласованы всеми заинтересованными сторонами и выгодны для глобальной экономики. Регулирование киберпространства это не одиночное плавание, в которое можно пускаться, не учитывая интересы других. Нужно достичь взаимного согласия в части предпринимаемых действий, наладить надлежащий уровень коммуникации и сотрудничества. В случае сохранения разногласий или просто отсутствия необходимого уровня коммуникации ситуация зайдет в тупик. Прогресс достижим, когда формируется партнерство, а не когда идеи и намерения удерживаются в тайне. Киберпространство сегодня остается зоной неизвестности, однако можно достичь много за счет формирования лучших практик и планов разрешения правовых вопросов, создания международного альянса и активной работы с вызовами XXI века.

4.3 Содействие подотчетности в корпоративном управлении Корпорации Интернета в рамках корпоративного права Калифорнии

С точки зрения организационной структуры Корпорация Интернета по распределению имен и адресов является некоммерческой корпорацией, учрежденной в соответствии с законами штата Калифорния, США. Поэтому при рассмотрении подходов ICANN к международному управлению критически важно также учитывать обязательства и ограничения, которые накладывает законодательство Калифорнии на функционирование Корпорации Интернета.

Корпоративное право Калифорнии устанавливает разрешенные рамки и структуру некоммерческой организации, а также устанавливает определенные права и полномочия для частных лиц и групп, которые принимают участие в корпоративном управлении.

В рамках процесса по передаче координирующей роли NTIA в осуществлении функций IANA Конгресс США принял резолюцию[99], которая предполагает расширение степени ответственности во внутренней структуре управления Корпорации Интернета и призывает ее разработать новые принципы подотчетности для защиты глобальной сети Интернет.

На протяжении многих лет Корпорацию Интернета критиковали за недостаточную подотчетность. Некоторые считают, что необходимо содействовать обеспечению стабильности и отказоустойчивости ICANN изнутри путем внедрения нового механизма сдержек и противовесов в текущую структуру принятия решений.

Текущая структура корпоративного управления Корпорации Интернета

В этом разделе рассматривается структура корпоративного управления ICANN по состоянию на конец 2015 г. Предполагается, что структура Корпорации Интернета может измениться в ближайшие месяцы или годы, и могут потребоваться корректировки в текущем анализе. Тем не менее, обсуждаемые в этом разделе принципы корпоративного права Калифорнии, скорее всего, останутся актуальными и должны рассматриваться в рамках процесса реструктуризации.

---

99 См.: United States 114th Congress, Senate Congressional Resolution 71 (February 5, 2015).

Текущая корпоративная структура ICANN включает двадцать одного члена Правления. Шестнадцать членов Правления имеют право голоса, а пять оставшихся членов выступают координаторами без права голоса. Восемь членов Правления выбираются независимым Комитетом по назначениям, каждая из трех вспомогательных организаций Корпорации Интернета выбирает по два члена Правления, и оставшиеся члены Правления с правом голоса утверждаются представителями Сообщества ICANN At-Large, также как и Президент или генеральный директор Корпорации.

После того, как члены Правления назначены, внутренняя корпоративная структура ICANN ограничивает сообщество в его возможности призвать к ответственности Правления. На данном этапе, единственным правовым механизмом, доступным для сообщества, призвать Правление действовать в соответствии с заявленными целями организации является уведомление генерального прокурора Калифорнии. Если генеральный прокурор Калифорнии соглашается с тем, что Правление не действовало в соответствии с интересами организации, он может возбудить судебное разбирательство.

Критики текущей корпоративной структуры сформулировали следующие цели, которые должны быть достигнуты в связи с передачей ответственного управления функциями IANA:

- создать механизмы для осуществления сдержек и противовесов для решений Правления;
- создать механизмы выбора директоров, которые будут действовать в соответствии с заявленными целями организации, и замены директоров, которые не соблюдают интересы организации;
- укрепить и расширить меры по обеспечению прозрачности и подотчетности для обеспечения доступа сообщества к документам и записям ICANN.

Понимание общественной миссии Корпорации Интернета

Целью данного раздела является рассмотрение двух ключевых источников права — некоммерческое корпоративное право Калифорнии и договорное право Калифорнии, - для оценки возможных вариантов реорганизации корпоративной структуры ICANN, отвечающей обозначенным ранее целям. Этот анализ не является исчерпывающим, и не учитывает все возможные варианты. Он также не затрагивает все вопросы, которые могут возникнуть при принятии рассмотренных вариантов. Дополнительные поправки могут потребоваться в случае изменений в приоритезации целей и внесения изменений в корпоративную структуру ICANN.

Законодательство Калифорнии предъявляет к некоммерческим организациям требования изложить свои благотворительные цели в учредительном договоре организации. Согласно закону, активы некоммерческой организации должны передаваться в благотворительный фонд и могут использоваться и тратиться в рамках достижения благотворительной некоммерческой цели. Действия

Правления и его членов должны, в свою очередь, проводиться в соответствии с благотворительной целью.

Учредительный договор Корпорации Интернета излагает свои «благотворительные и общественные цели» как сокращение управленческого бремени и привлечение интереса мировой общественности к вопросам обеспечения стабильности работы Интернета. Деятельность ICANN «ведется в интересах всего интернет-сообщества, все действия отвечают соответствующим принципам международного законодательства и применимым международным конвенциям и местным законам и, в соответствующих рамках и согласно настоящему Учредительному договору и Уставу, путем открытых и прозрачных процессов, обеспечивающих конкуренцию и открытый доступ на относящиеся к Интернету рынки».

Реорганизация корпоративной структуры Корпорации Интернета в целях обеспечения стабильности и устойчивости Правления

В соответствии с некоммерческим корпоративным правом Калифорнии, Правление отвечает за ведение дел корпорации в целях содействия благотворительной цели корпорации. Члены Правления обязаны направлять финансы и ресурсы на эту благотворительную цель, а также благоразумно действовать на основе информации и с разумной осторожностью.

Эти обязательства в равной степени относятся к Правлению ICANN в рамках существующей структуры управления. Но, как было упомянуто выше, существует опасение, что даже с учетом этих попечительских обязанностей сообществу не хватает механизмов для обеспечения достаточного уровня подотчетности. Но корпоративное право Калифорнии предусматривает несколько возможных вариантов увеличения степени подотчетности в рамках некоммерческих корпораций.

Участники и делегаты

Некоммерческие корпорации, в соответствии с законодательством штата Калифорния, могут назначать членов или делегатов, которые могут стать частью корпоративной структуры управления с предоставлением им прав и полномочий для сдерживания неквалифицированного принятий решений Правлением. Права и полномочия незначительно различаются между этим двумя формами. Полномочия, предоставляемые делегатам, в большей степени ограничены, чем полномочия членов. Некоммерческая корпорация может включать как обе формы, так и какую-либо одну из них. Текущая корпоративная структура ICANN не имеет ни членов, ни делегатов, и любая реструктуризация потребует изменений в уставных документах корпорации.

Согласно корпоративному праву Калифорнии, члены имеют широкие права, включая право голоса по поправкам к Учредительному договору и Уставу[100], право на проведение специальных встреч[101], право на получение уведомлений о

100 Закон Cal. Corp. Code § 5812.
101 Cal. Corp. Code § 5510.

членских встречах[102], право просматривать списки членов и бухгалтерские книги и записи для любой надлежащей цели[103], а также право выбирать и отстранять руководителей Правления[104].

Законодательство Калифорнии разрешает некоммерческим корпорациям также передавать дополнительные полномочия членам в своих учредительных договорах и уставах. Эти полномочия могут включать в себя право отозвать все Правление в чрезвычайных ситуациях, или право голосовать за поправки к уставу с предписанием, устанавливающим пороговое значение для голосования.

К другим возможным полномочиям, которые отвечают целям ICANN и которые могут быть предоставлены в соответствии с законодательством штата Калифорния, можно отнести право вето на решение Правления и блокирование его вступления в силу, а также полномочия предлагать новые инициативы в качестве альтернативного решения неприятного решения Правления. Устав может разделять членов в классы членов, каждый из которых имеет различные полномочия и права.

Возможно, разумным подходом к преобразованию Корпорация Интернета в организацию членов было бы предоставление статуса члена существующим поддерживающим организациям и экспертным комиссиям.[105] Получив статус корпоративного члена, сообщество ICANN получит право, в соответствии с законодательством штата Калифорния, выбирать и отзывать членов Правления, а также совершать другие правовые действия, доступные для членов в рамках документов по корпоративному управлению ICANN.

Наконец, члены имеют возможность возбудить дело в отношении корпорации для обеспечения соблюдения прав корпорации.[106] В контексте ICANN это право может быть представлено как Catch-22. В то время, как это является сильным механизмом содействия подотчетности, такое право создает риски истощения ресурсов для ведения процесса.

В соответствии с некоммерческим корпоративным правом Калифорнии, в дополнение или в качестве альтернативы для членов, корпорация может назначать делегатов. Делегаты, в основном, являются порождением контракта и не располагают стандартными правами в рамках корпоративного права Калифорнии. Делегаты, как правило, способны выбирать и сменять их членов Правления. Примечательно, что в отличие от членов, делегаты не имеют возможности возбудить дело против некоммерческой корпорации и добиваться выполнения ее благотворительной цели. В уставе могут быть явно указаны, какие права и обязанности предоставлены делегатам.

---

102 Cal. Corp. Code § 5511.

103 Cal. Corp. Code §§ 6330, 6333, 6335-38.

104 Cal. Corp. Code § 5222.

105 В соответствии с законодательством Калифорнии, члены должны быть юридическим лицом (см. Cal. Corp. Code §§ 5313, 17001(ae). Текущие заинтересованные участники не являются юридическими лицами, и, вероятно, должны быть преобразованы в некоммерческие ассоциации или корпорации.

106 Cal. Corp. Code § 5710.

Бюджеты и стратегические планы

В соответствии с корпоративным правом Калифорнии, затруднительно создать механизмы, с помощью которых сообщество может переопределить бюджеты и стратегические планы, утвержденные Правлением. Тем не менее, корпорация может внести изменения в свой устав, которые позволят организациям-членам утверждать бюджет и стратегические планы перед окончательным утверждением Правлением. Правление может устанавливать в своих постановлениях необходимые пороговые значения для одобрения от каждого класса.

Отзыв членов Правления

Калифорнийское право позволяет частному или юридическому лицу, которое выбирает члена Правления некоммерческой организации, отозвать этого человека с должности. Если в корпоративной структуре представлены классы членов, то, как правило, члены не имеют права отзывать членов Правления за пределами их класса. В случае с Корпорации Интернета, это будет препятствием для совершения тщательной проверки или отзыва всего Правления при чрезвычайных обстоятельствах.

Тем не менее, этот барьер не является непреодолимым. В соответствии с законодательством Калифорнии, классы и члены могут достигать контрактных договоренностей друг с другом, связывая их с голосами сообщества для отзыва членов Правления. В этих контрактах может быть указано, какой тип большинства сообщества потребуется для отзыва члена Правления. При таких контрактных договоренностях, члены или классы обязаны по контракту отозвать члена Правления, если сообщество так проголосует.

Недостатки реорганизации Корпорации Интернета

Члены и делегаты не имеют попечительских обязанностей перед корпорацией и не имеют никакой личной ответственности за действия корпорации или ее Правления. Соответственно, по мере того, как предоставленные членам и делегатам полномочия начнут пересекаться с полномочиями и влиянием членов Правления директоров, которые имеют попечительские обязанности, корпорация может стать более восприимчивой к краткосрочным интересам голосующих в ущерб долгосрочному стратегическому планированию. К тому же, предоставление широких полномочий по блокированию окончательного утверждения бюджета или стратегического плана может привести к патовой ситуации. Вероятно, тогда Правлению потребуется принять комплекс мер, которые позволят Корпорации Интернета продолжить свою операционную работу в ситуации, когда переговоры о бюджете зайдут в тупик.

Меньшее по численности Правление может быть более эффективным для принятия решений в корпорации. Предоставление сообществу широких полномочий по отмене решений Правления с большой вероятностью может привести к подрыву ежедневных операций ICANN. Таким образом, для поддержания эффективности процесса принятия решений любое дополнительное расширение полномочий сообщества должно быть тщательно сбалансировано.

Добавление членов в учредительные документы и устав корпорации наряду с условиями членства, правами, полномочиями и классами членства может стать сложной задачей. Управление Корпорацией Интернета в формате, который учитывает все эти права, также потребует значительных ресурсов. Более того, после того как структура членства создана ее уже сложно изменить. Соответственно, до запуска процесса реорганизации, ICANN и ее заинтересованным участникам следует тщательно оценить возможные управленческие риски, которые существуют сейчас и могут возникнуть в будущем, а также проанализировать, могут ли новые меры по обеспечению подотчетности минимизировать существующие риски без чрезмерного давления на управление Корпорацией Интернета.

Заключение

Существует несколько вариантов реорганизации структуры Корпорации Интернета для достижения необходимой степени подотчетности и повышения СБО технических функций Корпорации Интернета в соответствии с законодательством штата Калифорния. Хотя приведенные выше методы не являются исчерпывающими, они, тем не менее, перспективны для ICANN. Особое внимание должно быть уделено механизмам обеспечения подотчетности, и ответу на вопрос, позволят ли предложенные механизмы решить существующие системные проблемы без создания чрезмерной нагрузки на процесс принятия решений в долгосрочной перспективе.

Резюме исследования

По итогам проведенного исследования можно сделать ряд базовых фундаментальных наблюдений, описывающих ситуацию в области обеспечения СБО системы УИИ по состоянию на начало 2016 г. Стоит подчеркнуть, что эти наблюдения не содержат оценок технических и иных политик в сфере обеспечения СБО и не носят характера целевых рекомендаций для тех или иных отдельных заинтересованных сторон.

1. Задачи обеспечения СБО системы УИИ с точки зрения применяемых политик и стандартов, обеспечиваемых ресурсов и поддерживаемого управления бизнес-процессами в целом решаются в режиме, приближенном к оптимальному и не нуждаются в срочном кардинальном пересмотре или реформировании. Риски критических инцидентов в отношении системы УИИ как глобальной инфраструктуры Интернета остаются достаточно низкими. Действующая система в целом готова к появлению новых рисков и обладает достаточным запасом гибкости, прочности и адаптации как в технологическом, так и институциональном плане. Вместе с тем, по отдельным направлениям требуется дальнейшие развитие стандартизации и укрепление СБО существующей инфраструктуры и бизнес-процессов.

2. Из числа составляющих системы УИИ наибольшие риски в плане обеспечения СБО существуют в отношении глобальной системы доменных имен DNS, что объясняется высокой инфраструктурной сложностью этой системы и высокой нагрузкой на нее в силу ее использования, в том числе большим количеством операторов и конечных пользователей. Инфраструктурная сложность и иерархичность DNS создает возможности для реализации в отношении нее различных видов угроз, включая целенаправленные сетевые атаки (в т.ч. DDoS). При этом именно для DNS сегодня реализуются наиболее серьезные меры и политики обеспечения СБО, включая стратегии избыточного ресурсного резервирования и стандартизации безопасности (расширения DNSSEC). В обозримой перспективе приоритет DNS как объекта политик обеспечения СБО системы УИИ по всей вероятности будет сохраняться.

3. Техническое управление системой УИИ на сегодняшний день осуществляется достаточно преемственно и стабильно и сопровождается постоянным развитием стандартизации, в том числе в части обеспечения СБО. В то же время институциональная экосистема управления уникальными идентификаторами подвержена реорганизации и трансформациям, которые затрагивают ее организационную схему, подотчетность, а также роль правительств и национальных юрисдикций. Эти процессы, в том числе процесс передачи ответственного управления функциями Администрации адресного пространства Интернет (IANA), в определенной степени включаются в глобальный международно-политический контекст и оказываются подвержены политизации. Однако в практическом ключе основным принципом и приоритетом этих процессов с точки зрения обеспечения СБО системы УИИ представляется поддержание и сохранение той модели технической деятельности, которая сложилась на данный момент, несмотря на реструктуризацию и изменение схемы подотчетности ее организационных составляющих.