# Инфраструктура Интернета в контексте регулирования жизненно важных услуг и критических информационных инфраструктур: обзор международного и российского опыта

*Олег Демидов, Алёна Махукова*

## Оглавление

## Резюме исследования

Исследование охватывает регионально распределенную выборку из семи государств (Аргентина, Германия, КНР, РФ, США, Швеция, Япония), одной надгосударственной структуры (ЕС) и одной международной организации (ОЭСР). Объектом анализа служат нормативные, нормативно-методические, рекомендательные и прочие документы государственных регуляторов, а также, где применимо, документы, разработанные представителями ИТ-отрасли. Задача исследования – на основе приведенной выборки представить и описать срез существующих подходов и практик, которые определяют место и статус инфраструктуры и сервисов Интернета в контексте регулирования, защиты, обеспечения безопасности стабильности и отказоустойчивости (БСО) критических информационных инфраструктур (КИИ), защиты ключевых систем информационной инфраструктуры (КСИИ), а также обеспечения безопасности информационных инфраструктур/систем (ИС) критических важных объектов (КВО).

Особое значение в рамках исследования имеют два вопроса:

1) Выделяется ли Интернет и его инфраструктура в качестве отдельного, самостоятельного сектора КИИ в регуляторной практике рассматриваемых государств и МО? Необходимо уточнить, что под инфраструктурой Интернета в рамках задач исследования понимаются прежде всего следующие составляющие:

- Инфраструктурные элементы глобальной системы уникальных идентификаторов Интернета (система УИИ), прежде всего инфраструктура DNS:
    - инфраструктурные элементы глобальной системы DNS: авторитативные корневые серверы DNS и их «зеркала»;
    - авторитативные серверы DNS, поддерживающие страновые и общие домены верхнего уровня;
    - нижестоящая по уровню иерархии DNS по отношению к авторитативным корневым серверам инфраструктура DNS-резолверов;
- Сетевая инфраструктура ключевых интернет-провайдеров: магистральные волоконно-оптические сети, интерконнекты, инфраструктура энергоснабжения и проч., сетевое оборудование маршрутизации и проч.
- Инфраструктура, обеспечивающая связность и взаимодействие сетей различных операторов: точки обмена трафиком (IXPs), стыки инфраструктуры различных провайдеров (интерконнекты) и проч.

2) Какие критерии, признаки и параметры определения критичности для объектов информационной инфраструктуры используются в международной практике?

Основные выводы исследования:

1. На сегодняшний день в международной практике отсутствует единый подход к регулированию КИИ, и, в то же время, единое понимание того, как соотносятся с КИИ сервисы и инфраструктура Интернета. Также не существует универсальной методологии, таксономии и системы критериев, применяемой для категорирования и классификации КИИ, а также сервисов и инфраструктуры Интернета в контексте КИИ. Рассмотренные регуляторные практики можно условно сгруппировать в несколько подходов:

1) Объектом регулирования является ИТ-инфраструктура КВО, которая с точки зрения категорирования и таксономии является производной по отношению к КВО. В этом случае информационно-телекоммуникационные сервисы и сети, включая Интернет, не выделяются в отдельную категорию/сектор КВО и рассматриваются как ИТ-инфраструктура КВО. Однако при этом в отдельный сектор могут выделяться правительственные сети передачи данных, сети и системы связи специального и двойного назначения. Основой системы критериев и категорирования в рамках такого подхода выступает влияние штатной устойчивой работы ИТ-систем КВО на обеспечение национальной безопасности, функционирование экономики и работу жизненно важных социальных сервисов.

Регулирование и обеспечение безопасности /защита инфраструктуры Интернета как самостоятельной категории КВО не предусматривается. Примеры такого подхода представляют США, Япония.

2) Разновидностью описанного выше подхода можно назвать практику, когда КИИ выделяется как отдельная категория объектов регулирования, однако по системе критериев и таксономии также является производной по отношению к КВО. В отдельных случаях понятие КИИ привязывается к АСУ ПТП КВО, а также системам, обеспечивающим передачу данных и штатное функционирование АСУ ПТП КВО. В рамках такого подхода инфраструктура сетей передачи данных, включая Интернет, может включаться в состав КИИ, но только в привязке к обеспечению функционирования КВО, на которых эксплуатируются АСУ ПТП. Таким образом, такие инфраструктуры как система УИИ Интернета и ее отдельные компоненты, точки обмена трафиком, магистральная инфраструктура интернет-провайдеров не выступают в качестве отдельной категории КВО, хотя на них могут распространяться требования, связанные с обеспечением передачи данных и обеспечения функционирования АСУ ПТП и других ИТ-систем КВО. Примером такого подхода на сегодняшний день является РФ, однако появившиеся в последние месяцы проекты законодательных документов и документов стратегического планирования в РФ демонстрируют возможное изменение подхода.
3) Регулирование КИИ полностью, либо по отдельным вопросам и актам развивается отдельно и параллельно с регулированием КВО. Инфраструктура и сервисы Интернета и сектора телекоммуникаций (включая интернет-сектор) выделяется в самостоятельную категорию регулирования и описывается отдельной линейкой параметров и критериев важности. Объектами, которые подпадают под установление требований по различным аспектам защиты, могут выступать и инфраструктуры сетевых операторов (сети и оборудование магистральных провайдеров, точки обмена трафиком, авторитативные серверы и сети резолверов DNS, поддерживающие национальные домены верхнего уровня). При этом по сравнению с регулированием КВО меняется подход, целеполагание и терминология в части требований и иных норм: на первый план выходят требования к обеспечению БСО сервисов и систем, а также обеспечению сетевой безопасности. Кроме того, в случае ЕС принципиально меняется основа системы параметров и критериев: вместо обеспечения национальной безопасности в узком понимании этого термина приоритетом становится обеспечение непрерывности бизнеса и гарантированное предоставление гражданам соответствующих сервисов, т.е. безопасность важных для

граждан, общества, бизнеса и государства сервисов и процессов. Соответственно, меняется и понятийный аппарат в части самих регулируемых объектов: КИИ и понятие критичности в целом заменяется понятием «жизненно важных услуг» (essential services), «критически важных услуг» (kritischen Dienstleistungen) и «жизненно важных общественных функций» (Vital Societal Functions) (см. ЕС, Германию и Швецию).

4) Гибридный подход между подходами демонстрирует КНР, который развивает регулирование КИИ в целом в привязке к КВО, однако выделяет в отдельную категорию КИИ сети и системы с большим числом пользователей и прямо устанавливает требования к сетевым операторам, в том числе в части обработки и хранения персональных данных.

Если рассматривать развитие представленных подходов в динамике, можно выделить следующие общие закономерности:

- В большинстве стран наблюдается тенденция к развитию регуляторного подхода за рамки обеспечения безопасности ИТ-систем КВО в сторону идентификации КИИ как относительно самостоятельной категории объектов регулирования.
- Понимание КИИ постепенно выходит за рамки ИТ-систем, которые обеспечивают надлежащее функционирование производственных и технологических процессов.
- Вместе с тем, до сих пор примеры относительно непротиворечивой и систематической интеграции элементов инфраструктуры Интернета в концепцию регулирования КИИ крайне ограничены, для большинства государств это вопрос на будущую перспективу.
- Пример ЕС показывает, что интеграция инфраструктуры и сервисов Интернета в данный регуляторный контекст неизбежно требует изменения самого подхода к целеполаганию такого регулирования и переориентации с обеспечения узко понимаемой национальной безопасности в смысле защиты конституционного строя и борьбы с терроризмом на вопросы обеспечения непрерывности бизнес-процессов и гарантированного предоставления жизненно важных услуг, включая услуги сервисов DNS. Вместе с тем, такая переориентация не отменяет роста объема требований и регуляторных предписаний в отношении операторов жизненно важных услуг, а также несет риск создания избыточной бюрократической и финансовой нагрузки на такие субъекты, включая средний и малый бизнес.
- Фундаментальной тенденций становится не только переориентация на непрерывность бизнес-процессов предоставления критически/жизненно важных услуг и интересы их потребителей, но и селективный подход к определению конкретного перечня операторов таких услуг. В этом плане передовые практики мирового уровня демонстрирует Германия, где в основу регулирования положена система количественных пороговых значений для определения операторов критически важных услуг. Такие пороговые значения привязаны к числу пользователей услуг, которое может достигать критической доли от населения Германии – или нет. В результате, вся регуляторная парадигма оказывается привязана не столько к обеспечению «общего блага» (например, защита национальной безопасности или общественная стабильность), сколько к обеспечению потребностей граждан как потребителей конкретных услуг.

- Отдельного упоминания заслуживает подход Швеции, где государство, выступая как субъект, заинтересованный в повышении уровня защиты инфраструктуры объектов, предоставляющих жизненно важные для общества услуги, включая Интернет и отрасль телекоммуникаций, не только устанавливает требования для операторов таких объектов, но и само активно участвует в развитии инфраструктуры и стимулирует операторов, в том числе финансово и материально, повышать защиту и устойчивость функционирования их объектов.

Как уже отмечалось выше, в РФ появились признаки наметившейся модернизации подхода к регулированию КИИ. В рамках модернизации российского подхода в обозначенной области с учетом международного опыта могут быть актуальным следующие рекомендации:

- Изменение подхода к защите/обеспечению ИБ КВО/КИИ целесообразно осуществлять в направлении комплексного рассмотрения, основанного на общих принципах и охватывающего все сектора и отрасли инфраструктуры и жизненно важных услуг.
- Внимательного анализа на предмет применимости в российского нормотворческой практике заслуживает тенденция перехода от регулирования объектов инфраструктуры как таковых к регулированию жизненно важных услуг, в том числе в отрасли телекоммуникаций и Интернет-секторе. Важной частью такого регуляторного подхода является ориентация на потребителей жизненно важных услуг и интеграция в законодательство национальных и международных стандартов управления рисками и обеспечения непрерывности бизнес-процессов.
- Важнейшим условием эффективности для стратегии защиты КИИ и жизненно важных услуг ИТ-сектора является развитие системы государственно-частного взаимодействия и закрепление за операторами соответствующих объектов и услуг роли и возможностей по самостоятельному формированию отраслевых стандартов, практик и политики в сфере ИБ и обеспечения непрерывности бизнеса. Такой подход в сочетании с внедрением системы обязательных требований может обеспечивать необходимую гибкость и адаптивность при меняющейся картине угроз БСО критически важных объектов и услуг. Важным компонентом такого подхода также является стимулирование развития системы CSIRT для обеспечения оперативного реагирования на инциденты безопасности в ИТ системах КИИ/КВО в промышленности и сфере услуг.
- С учетом ключевой роли сектора ИТ и телекоммуникаций в экономическом развитии РФ, востребовано может быть использование опыта стран (в основном, государства ЕС, включая ФРГ), которые разрабатывают методологию определения количественных показателей для выявления круга операторов жизненно/критически важных услуг на основе количества граждан/пользователей, которые находятся в зависимости от услуг того или иного оператора. Число пользователей, которые охватывают такие услуги, как правило, коррелирует с размером и показателями провайдера таких услуг как экономической единицы. Таким образом, за счет отсечения операторов услуг, не подпадающих под критерии КВУ по количественным показателям, из-под регулирования выводится большая часть малых операторов, для которых предоставление отчетности и выполнение повышенных требований по защите своих объектов может стать серьезным финансовым бременем.

- Важнейшим инструментом в обеспечении ИБ является национальная система CSIRT, в первую очередь для защиты непрерывности бизнеса при наличии координации со стороны специально созданного для этого субъекта, которого обычно называют координационным центром CSIRT. Созданный в России GOV-CERT (как следствие положений Указа №31) ограничен в своих функциях защитой государственных информационных систем и ограниченного круга КВО. Вместе с тем, международный опыт, включая опыт Японии, КНР, США, ЕС и отдельных стран ЕС, показывает тенденцию к развитию широкой системы национальных отраслевых CSIRT и CERT, выстроенной на основе учета секторальной специфики и государственно-частного взаимодействия. Так, китайский CERT-CN имеет статус неправительственной организации; японская экосистема реагирования на киберинциденты, включая JCERT/cc и NIRT, также опирается на взаимодействие частных телекоммуникационных операторов. Основой системы реагирования на трансграничные инциденты, в том числе на объектах операторов ЖВУ, в ЕС служит сеть национальных CSIRT, обеспечивающая оперативное реагирование и предупреждение в границах всего Союза. В России эта тенденция также частично находит отражение с учетом появления в 2015 г. FinCERT, тесно взаимодействующего с операторами банковского сектора. Однако для комплексной защиты жизненно важных объектов Интернет-отрасли и сектора телекоммуникаций может быть востребована профильная структура, такая как, например, CII-CSIRT или Telecom-CSIRT. Основные задачи такой структуры могут решаться за счет взаимодействия и обмена информацией между частными операторами при координации соответствующих госорганов.

## Организация экономического сотрудничества и развития (ОЭСР)

Впервые в документах Организации экономического сотрудничества и развития (ОЭСР) упоминание о критичности информационных систем для общества и бизнеса (здравоохранения, энергетики, транспортной и коммуникационной систем) появилось в Директивах по безопасности информационных систем и сетей, которые совет ОЭСР принял в 1992 г.[1] В следующей версии Директив[2] в 2002 г. Совет ОЭСР отмечал, что «критические инфраструктуры, такие, как энергетика, транспорт, финансы, опираются на Интернет, и Интернет Интернет играет значительную роль в методах ведения бизнеса, предоставлении гражданам и предприятиям госуслуг и коммуникациях и обмене информацией между гражданами».

Основным документом ОЭСР, описывающим политики в отношении КИИ, в настоящее время являются «Рекомендации Совета ОЭСР по защите критических информационных инфраструктур», опубликованные в 2008 г.[3] В документе дается следующее определение КИИ: соединенные между собой информационные системы и сети, сбой работы или разрушение которых окажется серьезное влияние на здоровье, безопасность, экономическое благополучие граждан или эффективную работу правительства или экономики. Для определения национальных КИИ проводится оценка рисков. Как правило, они включают в себя какие-либо из нижеследующих инфраструктур:

- Информационные компоненты, поддерживающие работу критических инфраструктур;
- Информационные инфраструктуры, на которые опирается работа важнейших компонентов предприятий или государственных органов;
- Важнейшие для национальной экономики информационные инфраструктуры.

Директива подразумевает, что страны-члены ОЭСР предпримут на государственном уровне следующие меры для защиты КИИ:

1) Определение четких целей политики на высшем уровне;
2) Определение ответственных за реализацию этой политики государственных органов и других организаций;
3) Консультации с частными владельцами и операторами КИИ для установления сотрудничества и достижения целей политики;
4) Обеспечение прозрачности в вопросе передачи госорганам и государственным агентствам ответственности за исполнение целей;
5) Систематический пересмотр политик, правовой базы и саморегулирования в отношении КИИ – в том числе, в отношении трансграничных угроз;
6) Предпринимать шаги для повышения уровня безопасности компонентов информационных систем и сетей, из которых состоит КИИ.

[1] OECD Guidelines for the Security of Information Systems, 1992 http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.
[2] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. The 2002 Security Guidelines (http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm)
[3] OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures (https://www.oecd.org/sti/40825404.pdf)

Продвижением и развитием последней и предыдущих директив должен заниматься Комитет по информационной, компьютерной и коммуникационной политике (Committee for Information, Computer and Communication Policy), который в 2014 г. был переименован в Комитет по цифровой экономике.[4]

В 2015 г. были опубликованы рекомендации ОЭСР «Управление рисками в цифровой безопасности для экономического и социального процветания» и сопровождающий документ к ним[5]. Эти рекомендации призывают страны, входящие в организацию, принять национальные стратегии по управлению рисками в цифровой безопасности. В стратегиях должна быть четко артикулирована (1) цель использовать возможности открытой цифровой среды для экономического и социального процветания; (2) цель обеспечить предоставление основных услуг и работу критических инфраструктур, защитить отдельных лиц от угроз цифровой безопасности с учетом необходимости сохранения национальной и международной безопасности и соблюдения прав человека. Эти же рекомендации называют цифровую среду и, в частности, Интернет, *жизненно важными* для экономической и социальной жизни стран ОЭСР, обеспечивающими рост, инновации, социальное благополучие и представительность.

В документах ОЭСР не приводится какое-либо общее рекомендованное для всех стран определение КИ. При этом в нескольких директивах по управлению рисками приводятся рекомендации для операторов КИ. Например, в опубликованных в 2014 г. Рекомендациях Совета ОЭСР по управлению критическими рисками[6] предлагается стимулировать операторов КИ:

1) разрабатывать стандарты и учебные материалы для управления рисками;
2) обеспечивать функционирование КИ, информационных систем и сетей после непредвиденных внешних воздействий;
3) требовать от должностных лиц, находящихся на объектах КИ, разрабатывать планы по продолжению работы в случае чрезвычайной ситуации.

Исследование, в 2008 г. опубликованное секретариатом ОЭСР, показало, что почти во всех странах организации определение «критической» относится к инфраструктуре, являющейся важнейшей основой социального и экономического благополучия, общественной безопасности и функционирования государства.[7] В таблице ниже приведены примеры определений КИ и КИИ из текущих стратегий кибербезопасности и других документов стран ОЭСР. Многие страны, входящие в организацию, тем не менее, не создали соответствующих структур и не дали подобных определений, несмотря на рекомендации Совета ОЭСР. Некоторые государства находятся в процессе выработки таких норм. Совет ОЭСР не дает критериев определения критичности, а государства-члены нередко оставляют эту работу компаниям-операторам КИ.

---

[4] Resolution of the Council [C(2008)209], Committee for Information, Computer and Communications Policy (ICCP), On-Line Guide to OECD Intergovernmental Activity, http://webnet.oecd.org/OECDGROUPS/Bodies/ShowBodyView.aspx?BodyID=1837&BodyPID=7425&Lang=en&Book=False.

[5] Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document. © OECD 2015 (http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[6] Recommendation of the Council on the Governance of Critical Risks. Adopted on 6 May 2014. Meeting of the OECD Council at Ministerial Level (http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf.

[7] Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security. Investment Division, Directorate for Financial and Enterprise Affairs, OECD, May 2008 (https://www.oecd.org/investment/investment-policy/40700392.pdf).

**Таблица. Определение КИ и КИИ в некоторых странах ОЭСР**

| | КИ | КИИ | Документы |
|---|---|---|---|
| **Австралия** | Технические объекты, системы снабжения, информационные технологии и коммуникационные сети, которые, в случае нарушения работы или разрушения, или находящегося вне доступа на протяжении продолжительного периода времени, значительно повлияли бы на социально-экономическое благополучие нации или на способность Австралии оборонять свои границы и обеспечивать национальную безопасность | ИКТ-компонент КИ | КИ: Critical Infrastructure Resilience Strategy, 2010 (http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy.pdf)<br><br>КИИ: Critical Information Infrastructure Risk Management, VICTORIAN GOVERNMENT CIO COUNCIL, 2012 (http://www.enterprisesolutions.vic.gov.au//wp-content/uploads/2014/07/SEC-STD-02-Critical-Information-Infrastructure-Risk-Management1.pdf) |
| **Австрия** | Инфраструктуры или их части, представляющие критическую важность для обеспечения важных социальных функций. Остановка их работы или их разрушение имеет серьезные последствия на здоровье, безопасность, экономическое и социальное благополучие населения или функционирование государственных институтов | Информационные составляющие КИ | Austrian Cyber Security Strategy, Federal Chancellery of the Republic of Austria, Vienna (2013) (http://www.bmi.gv.at/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdf) |

| | | | |
|---|---|---|---|
| **Германия** | Объекты, системы или их составляющие, которые:<br>1. относятся к секторам энергетики, ИТ и телекоммуникаций, транспорта, здравоохранения, водоснабжения, питания, финансирования и страхования и<br>2. имеют высокую значимость для общественной жизнедеятельности, поскольку отказ либо нарушение их функционирования создаст угрозы общественной безопасности или приведет к снижению уровня ее обеспечения. | **Нет определения** | Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz - ITSG k.a.Abk.), http://www.buzer.de/gesetz/11682/a193756.htm. |
| **США** | Системы и оборудование, которые жизненно важны для США и повреждение или разрушение которых повлекло бы уменьшение безопасности, национальной экономической безопасности, национального общественного здравоохранения или безопасности, или на любую комбинацию данных сфер. | **Нет определения** | An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. <<NOTE: Oct. 26, 2001 - [H.R. 3162]>> (https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm) |
| **Финляндия** | Структуры и функции, обеспечивающие информационную систему жизненно важных функций общества. Инфраструктура состоит из физической и электронной частей. | Структуры и функции, обеспечивающие информационную систему жизненно важных функций общества, которая хранит, передает и получает или как-то иначе обрабатывает данные | Finland´s Cyber security Strategy. Government Resolution 24.1.2013 (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf) |

| | | | |
|---|---|---|---|
| **Франция** | Жизненно важные объекты инфраструктуры - учреждение или структура, работу которых в случае их недоступности или уничтожения из-за злонамеренного действия, будет трудно заменить, а ущерб таким инфраструктурам повлияет также на военный или экономический потенциал, национальную безопасность или выживание нации, или серьезно повлияет на здоровье или жизнь населения. | **Нет определения** | L'instruction générale interministérielle n° 6600/SGDSN/PSE/PSN du 7 janvier 2014 (http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf) |
| **Чехия** | Инфраструктура или система элементов инфраструктуры, разрушение которых приведе к значительным последствиям для системы государственной безопасности, повлияет на обеспечение основных жизненных потребностей населения, здоровье граждан и экономики в целом | Критически важные компоненты информационной инфраструктуры или ИК-элементы системы критической инфраструктуры | КИ: Act No. 240/2000 Coll. on Crisis Management (the Crisis Act), as amended by Act No. 320/2002 Coll. and Act No. 430/2010 Coll. (http://www.hzscr.cz/hasicien/file/crisis-management-act-n-240-2000-coll-pdf.aspx)<br><br>КИИ: Act No. 181 of 23 July 2014 On Cyber Security and Change of Related Acts (Act on Cyber Security) (http://www.govcert.cz/download/nodeid-1143/) |
| **Эстония** | **Нет определения** | Информационные и коммуникационные системы, обслуживание, надежность и безопасность которых имеют большое значение для обеспечения надлежащего функционирования государства. КИ - часть КИИ | КИИ: Critical Information Infrastructure Protection Estonia (https://www.ria.ee/CIIP/) |

| | | | |
|---|---|---|---|
| **Южная Корея** | **Нет определения** | Главы центральных административных органов могут обозначить как критические информационные инфраструктуры, находящиеся под их юрисдикцией, принимая во внимание следующие факторы:<br>1) важность для государства и общества осуществляемых органом функций (duties);<br>2) зависимость исполнения функций органа от ИКИ;<br>3) взаимозависимость с другими информационными и коммуникационными инфраструктурами;<br>4) сферы, в которых информационные инциденты могут принести ущерб национальной безопасности, экономике и обществу, и размер этого ущерба;<br>5) вероятность информационных инцидентов и простота (easiness) восстановления после инцидента | КИИ: Act on Promotion of Information and Communications Network Utilization and Information Protection, amended jun. 13, 2008 (http://elaw.klri.re.kr/kor_service/converter.do?hseq=7288&type=PDF) |

| | | | |
|---|---|---|---|
| **Япония** | Бизнесы и структуры, предоставляющие сервисы, заменить которые в случае прекращения или ухудшения их работы было бы крайне трудно, и прекращение (ухудшение) работы которых значительно повлияло бы на социальную жизнь населения и деловую активность | Основа общественной жизни и экономической активности, осуществляется через бизнесы, предоставляющие услуги такой важности, что заменить их было бы крайне сложно. | КИ: The Second Action Plan on Information Security Measures for Critical Infrastructures. February 3, 2009. The Information Security Policy Council (http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf)<br><br>КИИ: The Basic Policy of Critical Information Infrastructure Protection (3rd Edition May 25, 2015 (http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf) |

## Аргентина

За последние два года Аргентине в отношении телекоммуникационной отрасли и конкретно интернета было принято несколько новых законов и приказов, значительно изменивших регулирование этой отрасли в стране. Основным законодательством, регулирующим интернет-отрасль в Аргентине, являются Закон 27.078 «Argentina Digital» («Цифровая Аргентина»), вступивший в силу в 2015 г., и Приказ 677/2015 Федерального органа по информационным технологиям и коммуникациям. Телеком-отрасль в целом регулируется также Приказом 764/2000 Национальной коммуникационной комиссии. Последний приказ сделал конкурентным рынок телекоммуникаций в стране, оставив регуляторный режим только в отношении ставки интерконнекта, лицензирования, справедливого распределения и универсальных обязанностей по предоставлению услуг.

По закону «Argentina Digital» был создан новый контролирующий отрасль орган - Федеральный орган по информационным технологиям и коммуникациям - и новый консультативный орган - Федеральный совет по телекоммуникациям. Перед этими органами стоит задача обеспечить «электронную социальную интеграцию». Согласно «Argentina Digital», все ИК-сервисы являются «сервисами в общественных интересах», и задача закона – построить конкурентную среду и установить равный доступ к существующей инфраструктуре в независимости от ее первоначального создателя.

Кроме упомянутых выше, регуляторами интернет- и телеком-отраслей являются Министерство федерального планирования, государственных инвестиций и услуг, Министерство коммуникаций, Министерство модернизации, Национальная комиссия по коммуникациям .

Одним из основных интернет- и телеком-провайдеров в Аргентине является государственная компания ARSAT. В 2010 г. правительство объявило о запуске пятилетнего плана Argentina Conectada («Аргентина соединенная»), направленного на вовлечение граждан в использование цифровых технологий. По этому плану ARSAT должна была построить 12 тыс. км волоконно-оптических линий связи (ВОЛС), на что правительство выделило ей сумму, эквивалентную 1 млрд долларов США.

В 2015 г. президент Аргентины объявил о новом, плане по развитию интернет-инфраструктуры – «Федеральном плане по интернету», по которому к 2018 г. к интернету должны быть подключены дополнительные 1,1 тыс. небольших населенных пунктов (по сравнению с 2015 г.), причем обозначенные государственные учреждения: школы, больницы, местные органы управления, отделения полиции – должны предоставлять граждан бесплатный доступ в Интернет.

В Аргентине действует Национальная программа по защите критических информационных инфраструктур и кибербезопасности. В рамках этой программы должна быть выработана и принята нормативная база, которая позволила бы определять и защищать стратегические и критические государственные инфраструктуры. Среди других целей программы: укрепление кибербезопасности в государственном секторе, создание общих стратегий защиты информации и критических инфраструктур, налаживание связей между

обществом, бизнесом, академической средой с целью принятия рамочных директив для увеличения общего уровня информационной защиты, а также влияние на международные процессы в сфере кибербезопасности и защиты критической инфраструктуры. Все обозначенные цели подразумевают одновременное участие и государственных органов, и частных компаний. Однако поскольку участие бизнеса в этих процессах не было закреплено как обязательное, реализация планов идет довольно медленно. По состоянию на 2016 г. документ, в котором было бы закреплено определение КИ или КИИ, так и не был принят.

Несмотря на это, профильные ведомства предпринимают меры для усиления кибербезопасности КИ. С 2011 г. ежегодно проводятся киберучения ENRIC (El Ejercicio Nacional de Respuesta a Incidentes Cibernéticos), а на базе Национального института государственного администрирования созданы курсы повышения квалификации для специалистов, обеспечивающих кибербезопасность на государственных объектах. В Аргентине действует государственный CERT – ICIC CERT.

С момента законодательной дерегуляции ИКТ-отрасли в Аргентине (закреплена в Национальном регламенте взаимоподключения, прилагающемся к Приказу 764/2000) было введено понятие «важнейших технических средств» (Facilidades Esenciales)[8]. Таковыми являются элементы сетей или функции, поддерживаемые и предоставляемые преимущественно или исключительно единственным провайдером или малым числом провайдеров и замещение которых невозможно из-за технических или экономических факторов. В приказе и Регламенте под «важнейшими» чаще всего подразумеваются важнейшие для бизнеса или отрасли объекты. Однако в преамбуле Приказа четко обозначена необходимость обеспечения всего населения доступом к важнейшим телекоммуникационным сервисам «в независимости от экономических условий, местоположения и физических ограничений».

Конкретно в этом приказе под важнейшими объектами в телекоммуникациях подразумеваются отдельные технические характеристики, объекты или услуги сети/оператора: локальный доступ, абонентская «последняя миля», порты, размещение выделенных серверов, локальный трафик и др. На услуги, связанные с важнейшими объектами, цены регулируются этим же приказом.

Понятие «важнейших средств в ИКТ» вводит закон 27.078 “Argentina Digital”. К таким средствам в нем отнесены:

1) Радиоэлектронный спектр
2) Спутниковые ресурсы
3) Фундаментальные планы (планы нумерации, систем оповещения, переносов номеров и др.)
4) Доступ и взаимоподключение.

В первой редакции «Argentina Digital» вводилось понятие «важнейшего и стратегического ИКТ-сервиса» - такой сервис должен был бы обладать

[8] См. Национальный регламент взаимоподключения сетей Reglamento Nacional de Interconexion (RNI), Annexo II, Decreto 764/2000, Desregulación de los servicios. Apruébanse los Reglamentos de Licencias para Servicios de Telecomunicaciones, Nacional de Interconexión, General del Servicio Universal y Sobre Administración, Gestión y Control de Espectro Radioeléctrico. Deróganse diversas normas. Vigencia, http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64222/norma.htm.

свойствами всеобщности, неизменности, однородности, непрерывности и регулярности, однако после внесения в закон поправок в 2015 г. это понятие из закона исчезло. Хотя у правительства Аргентины на протяжении последних лет есть четкое понимание Интернета как «жизненно важной услуги» и важнейшего сервиса (это следует и из масштабного государственного строительства ВОЛС, и из программ развития Интернета, и из законодательства о телекоммуникациях), а также есть осознание рисков, связанных со столько масштабной информатизацией, конкретные меры по противодействию информационным угрозам пока предпринимаются редко. Существование законодательства, нацеленного анализ возможностей защиты критических инфраструктур, в том числе КИИ, в ближайшие годы, вероятно, приведет к активным действиям в этом направлении.

## Германия

Один из примечательных примеров подхода к категорированию и разработке системы параметров и критериев для КИИ, в том числе в отношении инфраструктуры ИТ-сектора и Интернет-отрасли дает недавнее законодательство Германии. В 2009 г. был принят Акт о повышении безопасности информационных технологий Федерации (BSIG)[9], который закреплял роль центрального федерального регулятора по ИБ за Федеральным управлением по информационной безопасности (BSI), подотчетным МВД. Закон определял круг задач и профильных направлений деятельности Управления, включая обеспечение безопасности онлайн-коммуникаций, сертификацию продуктов ИБ и аккредитацию лабораторий по тестированию решений в области ИБ, регулирование криптографической защиты данных, противодействие компрометации систем и утечкам данных, и проч. В том числе к кругу задач регулятора было отнесено обеспечение безопасности КИИ. Согласно закону, Управление несет ответственность за выстраивание структуры коммуникаций для раннего выявления и реагирования на кризисные ситуации и инциденты в отношении КИИ во взаимодействии с частным сектором. Закон не содержал определения и системы категорирования КИИ, а также не описывал подробно функции регулятора в этой области.

Ситуация изменилась 17 июля 2015 г., когда после годичного обсуждения был принят Акт об информационной безопасности (ITSG)[10], который вносит поправки в ряд законов, включая Акт о телекоммуникациях от 2004 г., Акт об энергетической промышленности от 2005 г., Акт о телекоммуникационных медиа от 2007 г. и ряд других НПА, включая вышеупомянутый BSIG (в части информационной безопасности КИ). В поправках КИ определяются как объекты, системы или их составляющие, которые:

1. относятся к секторам энергетики, ИТ и телекоммуникаций, транспорта, здравоохранения, водоснабжения, питания, финансирования и страхования и
2. имеют высокую значимость для общественной жизнедеятельности, поскольку отказ либо нарушение их функционирования создаст угрозы общественной безопасности или приведет к снижению уровня ее обеспечения.

Операторам КИ предписывается не позднее двух лет с момента вступления закона в силу разработать и внедрить на своих объектах систему организационных и технических мер для повышения уровня их ИБ и защиты от возможных инцидентов, включая обеспечение целостности, доступности, аутентичности и конфиденциальности данных в критических компонентах ИТ-систем КИ. Подчеркивается, что внедряемые меры должны быть пропорциональны по отношению к потенциальным последствиям сбоя в соответствующем компоненте инфраструктуры. Операторы КИ и их ассоциации могут самостоятельно разрабатывать и внедрять отраслевые стандарты промышленной безопасности для своих объектов, в том числе с целью выполнения требований закона. BSI выносит

[9] Act on the Federal Office for Information Security (BSI Act – BSIG). https://www.gesetze-im-internet.de/englisch_bsig/englisch_bsig.html.
[10] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz - ITSG k.a.Abk.) http://www.buzer.de/gesetz/11682/a193756.htm.

заключение о соответствии предлагаемых операторами стандартов целям закона на основе консультаций с Федеральным управлением по защите гражданского населения и реагированию на катастрофы и МВД. По истечении двух лет, отведенных операторам КИ на выполнение требований закона, соответствие этим требованиям устанавливается с помощью аудита, проверок безопасности и процесса сертификации. Операторы КИ отчитываются перед BSI о проведенном аудите, пройденной сертификации и их результатах, включая выявленные недостатки в системе обеспечения ИБ; при этом регулятор вправе затребовать дополнительную информацию и результатах проверок и, после консультаций с другими профильными госорганами, выдать предписание об устранении выявленных уязвимостей.

Однако отдельным пунктом поправок оговаривается, что вышеперечисленные нормы не применяются к четырем категориям субъектов:

- операторам КИ, которые управляют телекоммуникационными сетями общего пользования либо предоставляют телекоммуникационные сервисы общего доступа;
- операторам магистральных электросетей высокого напряжения и электростанций, подпадающих под нормы отраслевого регулирования в рамках Закона об энергетике 2005 г.;
- владельцам разрешений на медицинское применение препаратов;
- иным операторам КИ, которые уже подпадают под требования отраслевого регулирования в части обеспечения безопасности, сопоставимые с требованиями ITSG.

Вместе с тем, законопроектом были установлены отдельные нормы и требования по обеспечению ИБ для операторов объектов сектора электроэнергетики. Так, в рамках поправок к Акту об энергетической промышленности от 2005 г. операторам КИ, чья инфраструктура подключена к магистральным сетям передачи электроэнергии, в течение двух лет с момента вступления закона в силу предписывается разработать и внедрить меры по защите телекоммуникационных систем и систем обработки данных, необходимых для осуществления производственных процессов.

Помимо требований к операторам различных объектов и сервисов, прежде всего КИ, закон уточняет и расширяет полномочия BSI по обеспечению ИБ, которые включают в себя:

- сбор информации об угрозах ИБ систем и сервисов, необходимой для выявления и предотвращения угроз, эксплуатации уязвимостей перед вредоносным ПО;
- оценка потенциального воздействия выявленных угроз и уязвимостей на КИ и их функционирование;
- проводить регулярный мониторинг и анализ состояния защищенности объектов КИ и существующих угроз;
- информирование и взаимодействие с операторами КИ и другими профильными регуляторами по вопросам противодействия выявленным угрозам и закрытия уязвимостей системам объектов КИ.

Для осуществления оперативного обмена информацией и иного взаимодействия с BSI операторы КИ, подпадающие под нормы закона, в течение шести месяцев определяют контактных лиц для коммуникаций с Управлением.

Кроме того, закон закрепляет за BSI роль ключевого регулятора федерального уровня по вопросам ИБ, что включает в себя задачу по разработке минимальных государственных стандартов безопасности для защиты ИТ-систем. МВД, проводя консультации с Советом по ИТ, может устанавливать такие стандарты в качестве административных правил для всех федеральных органов ФРГ. В свою очередь, BSI может предоставлять по запросу других госорганов консультации по внедрению таких стандартов и обеспечению соответствия им.

Немалая часть положений ISTG вносит поправки в Акт о телекоммуникациях (TKG) от 22 июня 2004 г. Закон обязывает операторов телекоммуникационных сервисов и сетей общего доступа незамедлительно информировать Федеральное сетевое агентство ФРГ (Bundesnetzagentur) об инцидентах или сбоях в предоставлении услуг в случаях, когда такие сбои и инциденты ведут или могут повлечь серьезные нарушения безопасности. Норма охватывает сбои и инциденты, которые могут привести к ограничению или отказу в предоставлении телекоммуникационных услуг, либо неавторизованному доступу к данным пользователей телекоммуникационных сервисов. Если причина инцидента связана с ИТ, Федеральное сетевое агентство в свою очередь сообщает об инциденте BSI. Кроме того, телекоммуникационные провайдеры обязаны уведомлять своих пользователей об ИТ-инцидентах, источником которых служат пользовательские системы, а также предоставлять пользователям информацию о том, как можно устранить причину таких инцидентов.

В соответствии с поправками к Акту о телекоммуникационных медиа от 26 февраля 2007 г. (TMA), провайдеры таких медиа, независимо от того, подпадают ли их объекты под понятие КИ, обязаны применять передовые технические меры (например, шифрование данных), достижимые технически и оправданные с коммерческой точки зрения, для предотвращения неавторизованного доступа к техническим системам, обеспечивающим их услуги, а также защищать такие системы от утечки данных и других инцидентов ИБ, включая исходящие извне компьютерные и сетевые атаки.

В ITSG не приводится методология категорирования КИ, а также критериев и параметров для их определения, однако в общих чертах расписывается алгоритм их выработки. Такую задачу решает МВД по итогам консультаций с широким кругом профильных федеральных органов[11], структурами частного сектора, операторами и научным сообществом. Процедура определения категорий и перечня КИ должна опираться на уровень охвата населения и организаций соответствующими критически важными услугами, секторальную проработку и определение того, какие именно компоненты и составляющие инфраструктурных комплексов следует включать в число КИ.

Эта задача была решена в рамках распоряжения BSI об определении КИ в соответствии с (обновленным) Актом о повышении безопасности ИТ Федерации

[11] Федеральное министерство экономики и энергетики, Федеральное министерство юстиции и защиты потребителей, Федеральное министерство финансов, Федеральное министерство труда и социальных вопросов, Федеральное министерство продовольствия и сельского хозяйства, Министерство здравоохранения, Федеральное министерство транспорта и цифровой инфраструктуры, Минобороны и Федеральное министерство окружающей среды, охраны природы, строительства и безопасности ядерных реакторов.

(BSIG), которое было опубликовано 22 апреля 2016 г. (BSI-KritisV)[12]. В документе существенно уточняется и дополняется терминология, используемая в ITSG – в т.ч. закрепляется понятие и вводится определение «критически важной услуги» (КВУ) (Kritische Dienstleistung); к числу КВУ относятся услуги, предоставляемые населению [в рамках обозначенных в распоряжении секторов], отказ или нарушение в предоставлении которых создаст угрозы общественной безопасности или приведет к снижению уровня ее обеспечения. Такое определение максимально преемственно по отношению к введенному в ITSG определению КИ.

Под оператором в BSI-KritisV подразумевается физическое или юридическое лицо, которое с учетом правовых, экономических и фактических обстоятельств оказывает решающее влияние на структуру и функционирование объекта. В свою очередь, под объектами понимаются:

1. Функционирующие заводы или иные стационарные сооружения, которые необходимы для предоставления КВУ.
2. Оборудование, техническая аппаратура и другие портативные устройства, которые необходимы для предоставления КВУ.

Нужно подчеркнуть, что такой понятийный аппарат делает немецкий подход соответствующим подходу, оформленному в Директиве ЕС от 6 июля 2016 г.: ключевым, центральным объектом регулирования становятся именно услуги (КВУ/ОЖВУ), а необходимая для их предоставления структура выносится в производную по отношению к ним логическую и терминологическую категорию. Такая близость отражает осознанное решение немецкого регулятора: ITSG и распоряжение BSI разрабатывались и принимались параллельно с доработкой Директивы ЕС и дебатами вокруг нее, в которых активно участвовали и немецкие представители.

Наконец, в распоряжении BSI формулируется определение порогового значения (Schwellenwert), используемое в документе для выстраивания секторальной таксономии КВУ (показатель, характеризующий роль того или иного объекта инфраструктуры или его составляющих как существенную в предоставлении критически важной услуги (по смыслу Статьи 1, части 1, абзаца 10 BSIG 2009 г. с учетом изменений, внесенных ITSG 2015 г.)).

С учетом данного понятийного аппарата в распоряжении приводится подробная секторальная таксономия КВУ, которая включает:

a) посекторальное категорирование объектов (с четырехступенчатой детализацией по отраслям-категориям-подкатегориям-конкретным видам услуг и объектов);
b) определяющие критерии критической важности услуг в рамках принятой таксономии;
c) принятые для соответствующих критериев пороговые значения.

Выделяются следующие секторы и объекты:

1. Энергетический сектор (к КВУ причисляются отрасли энергоснабжения, газоснабжения, снабжение жидким топливом, а также централизованного теплоснабжения).

[12] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), https://www.gesetze-im-internet.de/bundesrecht/bsi-kritisv/gesamt.pdf.

2. Сектор водоснабжения (к КВУ причисляются системы общественного снабжения питьевой водой, а также системы очистки сточных вод).
3. Продовольственный сектор (к КВУ причисляется общественное снабжение продовольствием, включая производство и обработку продуктов питания, а также торговлю продовольствием).
4. Сектор ИТ и телекоммуникаций (к КВУ причисляется голосовая связь и передача данных, включая локализованный доступ к голосовой связи и передаче данных, передачу данных, обмен трафиком и управление DNS; хранение и обработка данных, включая предоставление инфраструктуры для размещения и хранения данных, дата-хостинг, управление удостоверяющими центрами и выдача цифровых сертификатов).

Перечень секторов и отраслей КВУ, приведенный в документ BSI, не является окончательным и теоретически может быть дополнен в будущем. Но даже в нынешнем виде он содержит одну из самых подробных и проработанных систем критериев и параметров для определения критической важности. При этом сектор ИТ и телекоммуникаций с точки зрения параметров стоит несколько особняком: во всех других секторах основой для пороговых значений критериев служит так называемое «правило 500 тыс.»: для присвоения услуге статуса КВУ необходимо, чтобы ей пользовались не менее 500 тыс. человек. В свою очередь, это значение используется в качестве базы для расчета непосредственных пороговых значений, связанных с производственными показателями по тем или иным видам КВУ. К примеру, если согласно статистике, 500 тыс. граждан ФРГ в среднем потребляют на свои нужды 355 млн литров жидкого топлива в год, то КВУ отрасли снабжения жидким топливом присваивается именно такое пороговое значение. По оценкам немецкого экспертного сообщества и СМИ, новое регулирование охватывает более 700 объектов, используемых для предоставления КВУ.

Эта формула в большинстве случаев может применяться и в секторе ИТ и телекоммуникаций, с расчетом конечной базы клиентов/абонентов, напрямую охваченных той или иной услугой. Так, для определения порогового значения количества DNS-запросов (2,5 млн) на 500 тыс. (пользователей) умножается количество IP-терминалов, которое в среднем использует каждый пользователь для создания DNS-запроса (пять). Итоговая формула: 5x500 тыс. = 2,5 млн. Для других видов КВУ используется «коэффициент порогового значения» на основе правила 500 тыс.: умножающим коэффициентом служит доля 500 тыс. человек от округленного общего населения Германии (80 млн) – 0,625%. В результате, например, чтобы определить пороговое значение для количества доменов, поддерживаемых авторитативным сервером, общее количество доменов, которые обслуживают немецкие регистраторы и регистратуры (40 млн) умножается на 0,625%, результат – 250 тыс. доменов. Аналогично рассчитывается формула для порогового значения количества АС, напрямую подключенных к IXP:

$$300 \approx \frac{500\,000}{80\,000\,000} \times 50\,000$$

Для некоторых видов КВУ «правило 500 тыс.» малоприменимо из-за того, что затруднительно связать предоставляемую услугу с количеством охваченных ей напрямую пользователей (например, услуги удостоверяющих центров по выпуску цифровых сертификатов). Тем не менее, фундаментальный принцип подхода BSI к категорированию КВУ остается неизменным: *ни один конкретный класс/вид объектов, обеспечивающих предоставление тех или иных услуг, не причисляется*

*к КВУ по умолчанию* – все определяют точные пороговые значения, которые отражают значение конкретного объекта для пользователей/населения ФРГ.

Значение такого подхода как прецедента тем больше, что немецкие регуляторы рассматривают его не как эндемичную национальную практику, а готовую модель внедрения на национальном уровне положений Директивы ЕС о повышении уровня защищенности сетей и информационных систем от 6 июля 2016 г. ФРГ, таким образом, дает пилотный подход к реализации Директивы ЕС, который может рассматриваться в качестве образца и другими государствами Евросоюза.

Из интересных особенностей BSI-Kritis в части сектора ИТ и телекоммуникаций стоит также отметить попытку адаптировать предложенные регуляторные нормы и к распределенным инфраструктурам. В документ для множественных установок и объектов, находятся в тесном производственным взаимодействии и не превышают пороговых критериальных значений по отдельности, но превышают их в совокупности, то к КВУ причисляется все множество соответствующих инфраструктур, независимо от взаимной территориальной удаленности. Под эту норму попадают объекты и установки, которые:

- расположены в пределах одного инфраструктурного комплекса (т.е. имеется в виду все же локальная территориальная удаленность – *прим. авт.*):
- связаны друг с другом через общие производственные мощности;
- эксплуатируются в сходных целях и по схожей технологии:
- находятся под единой системой контроля и управления.

Нужно подчеркнуть, что столь проработанная система количественных оценок критериев и параметров КВУ не случайно появилась в Германии одной из первых в мире, опережая даже сам ЕС. Германский национальный сегмент Интернета относится к числу крупнейших в Европе (71 млн пользователей) и весьма развит с инфраструктурной точки зрения. Немецкий ccTLD .DE лишь недавно уступил китайскому .CN первое место по числу регистраций среди страновых доменов (16 млн). Точка обмена трафиком DE-CIX, созданная во Франкфурте-на-Майне, имеет инфраструктуру в 11 локациях в Европе, Азии и Северной Америке и является крупнейшей мировой IXP с пиковым значением пропуска трафика 5 Тб/сек[13]. В условиях наличия чрезвычайно развитой инфраструктуры ИТ-сектора и сектора телекоммуникаций ее непродуманное регулирование может серьезно сказаться на развитии германской экономики в целом. Поэтому выбор подхода, основанного на весьма избирательном и тщательно просчитанном применении регулирования КВУ выглядит логичным для BSI и других регуляторов.

Количество пользователей, которые охватывает та или иная КВУ, в большинстве случаев коррелирует с размером и показателями провайдера таких услуг как экономической единицы. Таким образом, за счет отсечения операторов услуг, не подпадающих под критерии КВУ по количественным показателям, из-под регулирования выводится большая часть малых операторов, для которых предоставление отчетности и выполнение повышенных требований по защите своих объектов может стать серьезным финансовым бременем.

[13]DE-CIX Frankfurt Statistics. DE-CIX, https://www.de-cix.net/about/statistics/.

*Таблица категорирования и критериев КВУ в секторе ИТ и телекоммуникаций в соответствии с BSI-Kritis*

| №. | Категория КВУ | Измеряемый критерий критической важности | Пороговое значение |
|---|---|---|---|
| **1.** | **Голосовая связь и передача данных** | | |
| 1.1 | Доступ | | |
| 1.1.1 | Сети локального доступа, обеспечивающие общедоступные услуги телефонной связи и сетям передачи данных. | Число клиентов сети локального доступа | 100 000 чел. |
| 1.2. | Передача голосового сигнала и данных | | |
| 1.2.1 | Передающие сети, поддерживающие общедоступные услуги телефонной связи и передачи данных, а также услуги доступа к Интернету (не включается пункт 1.1.1) | Количество пользователей соответствующей услуги | 100 000 чел. |
| 1.3 | Обмен трафика | | |
| 1.3.1 | Точки обмена трафиком (IXP) для общедоступных услуг телефонной связи, сервисов передачи данных и услуг доступа к Интернету | Среднегодовое количество подключенных АС (автономных систем) | 300 АС |
| 1.4. | Управление DNS | | |
| 1.4.1 | DNS-резолверы, используемые для поддержки общедоступных услуг телефонной связи, сервисов передачи данных и услуг доступа к Интернету. | Количество DNS-запросов (среднегодовое) | 2 500 000 запросов |
| 1.4.2 | Авторитативные доменные серверы DNS, используемые для поддержки общедоступных услуг телефонной связи, сервисов передачи данных и услуг доступа к Интернету. | Количество доменов, для которых сервер является авторитативным или на который делегирована доменная зона | 250 000 доменов |
| **2.** | **Хранение и обработка данных** | | |
| 2.1 | Инфраструктурные площадки для хранения данных | | |
| 2.1.1 | Дата-центры | Законтрактованная мощность в МВт<br>(по состоянию на 30 июня календарного года) | 5 МВт |
| 2.2. | Предоставление мощностей для размещения и хранения данных | | |

| №. | Категория КВУ | Измеряемый критерий критической важности | Пороговое значение |
|---|---|---|---|
| 2.2.1 | Серверные парки | Количество находящихся в эксплуатации серверов (среднегодовое) | 25 000 серверов |
| 2.2.2 | Сети доставки контента (CDN) | Объем передаваемых данных (терабайт в год) | 75 000 ТБ |
| 2.3. | Выпуск цифровых сертификатов | | |
| 2.3.1 | Удостоверяющие центры | Количество выпущенных квалифицированных цифровых сертификатов | 500 000 сертификатов |
| | | Количество сертификатов для аутентификации общедоступного сервера (серверные сертификаты, например, для веб-серверов, серверов электронной почты, облачных сертификатов (включая сертификаты TLS/SSL). | 10 000 сертификатов |

## КНР

Регулирование критической инфраструктуры сектора ИТ в КНР на уровне общегосударственного законодательства активно развивается в данный момент.

До недавнего времени вопросы защиты КИИ не были адресно проработаны в китайском законодательстве, равно как и соответствующее понятие, несмотря на наличие в КНР достаточно развитой системы обеспечения сетевой и информационной безопасности, а также разветвленной структуры государственных регуляторов в области ИТ.

- Общие вопросы информационной безопасности и кибербезопасности курирует Министерство промышленности и информатизации КНР, предметами ведения которого также являются регулирование и развитие в стране почтовой связи, Интернета, беспроводной связи, теле- и радиовещания, производства электронных и информационных товаров, индустрии программного обеспечения и развитие информационного общества.
- Вопросы борьбы с противоправным контентом и пресечения иной противозаконной деятельности в китайском сегменте Интернета находятся в ведении профильных структур Министерства Общественной Безопасности КНР, включая Департамент интернет-безопасности и защиты.
- Центральная руководящая группа (ЦРГ) по безопасности в Интернете и информатизации при ЦК КПК и подотчетная ей Центральная руководящая группа по вопросам киберпространства (последняя создана в 2014 г. и также известна как Администрация по вопросам киберпространства КНР) осуществляют разработку и реализацию стратегии регулирования контента в китайском сегменте Сети и противодействия угрозам безопасности в Интернете. Формальным главой ЦРГ по безопасности и информатизации является генеральный секретарь ЦК КПК Си Цзиньпин. В сферу компетенции ЦРГ при ЦП КПК в числе прочего входит и разработка политик по защите критической инфраструктуры КНР в ИТ-секторе.
- Практическую деятельность по защите информационных систем и ресурсов КНР осуществляет Техническая группа реагирования на чрезвычайные ситуации национальной компьютерной сети Китая/Координационный центр (CNCERT/CC), исполняющая функцию национального CERT. CNCERT/CC создан в форме некоммерческой организации при участии Министерства промышленности и информатизации в сентябре 2002 г. и является центральной структурой по реагированию на инциденты сетевой и компьютерной безопасности в КНР, в том числе в отношении критически важных объектов.

В число функций CNCERT/CC, напрямую затрагивающих вопросы защиты критической инфраструктуры входит[14]:

  - Укрепление общенациональных позиций в сфере обеспечения кибербезопасности и обеспечение кибербезопасности критической инфраструктуры КНР;

[14] National Computer Network Emergency Response Technical Team/Coordination Center of China
1. Brief Introduction, http://www.cert.org.cn/publish/english/index.html.

- Выявление рисков, уязвимостей и проактивное выявление инцидентов безопасности на объектах критической инфраструктуры.
- Приоритетное реагирование и управление инцидентами которые могут повлиять на безопасное функционирование Интернета, затронуть большое количество интернет-пользователей, или ключевые структуры государственного аппарата и критическую инфраструктуру, повлечь заявления пользователей о существенном ущербе, и иными инцидентами.

Несмотря на центральную роль CNCERT/CC в реагировании на инциденты компьютерной безопасности в отношении объектов КИИ, Техническая группа сама по себе не является источником нормотворческой инициативы по данным вопросам. Нужно также отметить, что в доступных документах CNCERT/CC не встречается китайский аналог термина «критическая информационная инфраструктура», хотя речь идет об информационных системах и компьютерных сетях критических объектов. Круг инцидентов, на которые реагирует Техническая группа, в подавляющем большинстве относится к сфере сетевой безопасности и интернет-безопасности (распространение вредоносного ПО, дефейс вебсайтов, внедрение и эксплуатация недекларируемого функционала ПО, фишинг, эксплуатация уязвимостей, уничтожение информации, DDoS-атаки, перехват маршрутизации трафика, неавторизованный доступ к ресурсам, распространение спама, инциденты кибербезопасности смешанного профиля и проч.).

Поиск по открытым документам CNCERT/CC и ресурсам вышеперечисленных государственных органов не дал результатов в части какой-либо рабочей, не закрепленной на законодательном уровне модели классификации/категорирования КИ ИТ-сектора либо КИИ. Таким образом подтверждается незавершенный характер процесса законодательного и концептуального оформления подхода к регулированию данных вопросов в КНР. Вместе с тем, за последние годы в этой сфере прослеживается значительный прогресс, который может завершиться принятием комплексного законодательства по вопросам защиты КИИ уже до конца 2016 г.

Одним из недавних существенных шагов в сторону проработки регуляторной концепции КИИ стала публикация «Голубой книги» «Защита китайской КИИ». Доклад опубликовал Центр исследований права информационной безопасности Университета Сиань Цзяотун, одного из 9 ведущих китайских университетов, в 2012 г.[15] Несмотря на то, что документ не имел официального статуса, в состав рабочей группы по его подготовке входили представители главного управления охраны общественного порядка Министерства общественной безопасности (МОБ) КНР, первого и третьего исследовательских институтов при МОБ КНР, КПК, а также представители частного сектора (Microsoft, Intel, Qihoo и Huawei).

В исследовании была представлена одна из первых в КНР попыток категорирования КИИ; в частности, были выделены следующие приоритетные категории КИИ:

- Информационные системы государственных органов;

[15] China's Critical Cyber Infrastructure Protection, http://ewipolicy.tumblr.com/post/64666359685/chinas-critical-cyber-infrastructure-protection.

- Информационные системы КПК (отдельным пунктом);
- Основные секторы народного хозяйства и экономики (финансы, банковская отрасль, система налогообложения, таможня, аудиторское дело, промышленное производство и коммерция, соцобеспечение и энергетика, коммуникации, транспорт и система национальной обороны);
- Образовательные учреждения и государственные исследовательские институты;
- Системы общественных коммуникаций, в том числе радио и телевидение.

В докладе также отмечалась потенциальная роль для защиты КИИ стандартов в сфере криптографии, аутентификации, инфраструктуры публичных ключей (PKI), включая 18 стандартов, разработанных и принятых в 2010 г. китайским Техническим комитетом по стандартизации в области информационной безопасности.

27 июня 2016 г. Постоянный комитет Всекитайского собрания народных представителей КНР опубликовал вторую, переработанную редакцию проекта Закона КНР о кибербезопасности, в которую включен ряд положений, определений и требований к операторам критической информационной инфраструктуры (наиболее близкий по смыслу перевод используемого в тексте законопроекта термина).

Новая редакция законопроекта претерпела существенные изменения в части КИИ по сравнению с предыдущей, исходной версией. Первая версия законопроекта была опубликована и открыта для комментариев в рамках 15-м заседания Постоянного комитета 12-го Всекитайского собрания народных представителей КНР в июне 2014 г. Прием комментариев по тексту законопроекта был открыт до 5 августа 2015 г. Вопросам КИИ в тексте документа была посвящена отдельная глава – Секция 2 Раздела 3. Безопасность при эксплуатации критической информационной инфраструктуры.

Раздел по КИИ в первой редакции законопроекта охватывал следующие вопросы[16]:

- Формирование базового перечня секторов КИИ;
- Определение круга ОГВ, ответственных за обеспечение защищенности КИИ в процессе ее эксплуатации;
- Определение обязанностей и ответственности операторов КИИ в части обеспечения защищенности такой инфраструктуры, а также устойчивости ее функционирования и непрерывности бизнес-процессов.
- Выстраивание базовой системы мер по взаимодействию государственных регуляторов с операторами КИИ, включая организацию и проведение проверок и тестов защищенности и устойчивого функционирования объектов, а также их аудита.
- Прочие вопросы, включая вопросы локализации хранения операторами данных пользователей сервисов, которые, согласно законопроекту, относились к числу критически важных.

[16] См. оригинал проекта документа: 网络安全法（草案）全文 浏览字号： 大 中 小 来源： 中国人大网 2015年7月6日, http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm. Также см. неофициальный перевод документа на англйиский: Cybersecurity Law (Draft) by China Law Translate On July 6, 2015, http://chinalawtranslate.com/cybersecuritydraft/?lang=en .

Нужно подчеркнуть, что в исходной версии законопроекта не приводилось четкого определения КИИ. В Статье 25 соответствующая инфраструктура определялась через посекторальное перечисление, включая в том числе:

- основные информационные сети, за счет которых предоставляются такие сервисы как доставка общественной корреспонденции и теле- и радиовещание;
- важные информационные системы для ключевых отраслей промышленности таких как энергетика, транспорт, охрана вод и водопользование; система финансов, а также коммунальное услуги такие как снабжение электричеством, водоснабжение и газификация, здравоохранение и санитарно-гигиеническая служба, а также социальное обеспечение;
- оборонные сети и сети органов государственного управления начиная с уровня уличных комитетов (цзедао баньшичу) и выше;
- сети и системы, находящиеся в собственности, либо управляемые провайдерами сетевых услуг с большим количеством клиентов.

Следует отметить, что в приведенной классификации в качестве отдельного сектора КИИ не выделяется как таковая инфраструктура Интернета (инфраструктурные элементы системы УИИ, точки обмена трафиком и проч.), несмотря на то, что в круг КИИ попадают «системы и сети» крупных сетевых операторов.

Помимо понятия КИИ, законопроект также оперировал термином «критическое сетевое оборудование», которое должно отвечать обязательным требованиям по соответствию национальным и отраслевым стандартам, а также проходить безопасную сертификацию и оценку соответствия требованиям по безопасности до продажи. Точное определение и перечень критического сетевого оборудования в законопроекте не приводился, однако уточнялось, что подразделения государственных органов КНР, отвечающие за сетевую информацию, совместно с профильными департаментами Госсовета, должны составить и опубликовать перечень такого оборудования и «специализированной продукции для обеспечения сетевой безопасности». На данный момент такой перечень не опубликован в открытом доступе, поскольку сам законопроект еще не был принят.

Первичная редакция законопроекта закрепляла ответственность за выработку мер обеспечения защиты КИИ за Госсоветом КНР. В частности, за отдельными департаментами Госсовета (например, курирующими вопросы радио- и телевещания, энергетики, транспорта и проч.) Статьей 26 устанавливалась ответственность по руководству и надзору за обеспечением эксплуатационной безопасности соответствующих объектов КИИ.

К числу ключевых требований, которые должны соблюдаться при строительстве эксплуатации объектов КИИ, законопроект относил в том числе обеспечение стабильности бизнес-процессов и устойчивости функционирования. При этом в тексте самого законопроекта не было сделано отсылок к существующим международным стандартам и рекомендациям в части непрерывности бизнеса и отказоустойчивости, будь то стандарты ISO или рекомендации ОЭСР.

Вместе с тем, законопроект вводил собственную систему требований для операторов объектов КИИ. Причем для операторов КИИ такая система

требований и обязательной мер являлась дополнением к более общему многоуровневому подходу по обеспечению сетевой безопасности. Такой подход распространялся законопроектом на всех сетевых операторов, был одним из центральных концептуальных нововведений законопроекта и предполагал формирование следующих пяти уровней:

1. Выработка сетевыми операторами внутренних процедур управления безопасностью и правил деятельности;
2. Принятие технических мер по противодействию угрозам вредоносного ПО, сетевых атак и вторжений, а также иных инцидентов, угрожающих сетевой безопасности.
3. Принятие технических мер по записи и отслеживанию статуса сетевых операций, а также мониторингу и записи инцидентов сетевой безопасности.
4. Принятие мер по классификации данных, а также резервированию и шифрованию важных данных.
5. Иные установленные законом или административными документами обязательства.

В дополнение к этому перечню требований, для операторов КИИ также устанавливались дополнительные обязательства в части обеспечения защищенности эксплуатируемых систем. Перечень таких требований включал в себя:

(1) Создание профильных подразделений безопасности и назначение лиц, ответственных за ее управление безопасностью, а также проведение проверок служебной истории таких лиц и иного персонала, отвечающего за безопасность критически важных процессов.
(2) Организацию и проведение регулярных мероприятий по повышению уровня образования в сфере сетевой безопасности, технических тренингов и оценки навыков для сотрудников объектов КИИ.
(3) Резервирование важных систем и баз данных на случай катастроф.
(4) Составление планов кризисного реагирования на инциденты сетевой безопасности и периодическое проведение учений по соответствующему сценарию.
(5) Иные установленные законом или административными документами обязательства.

Несмотря на то, что документ не содержал системы критериев для отнесения сетевой инфраструктуры к категории КИИ, в качестве неявного, но приоритетного признака критической важности в нем фигурирует значение инфраструктуры и сервисов для обеспечения национальной безопасности КНР. В качестве примера стоит отметить Статью 30 законопроекта, в которой для операторов КИИ, приобретающих сетевые продукты и услуги, способные оказать влияние на национальную безопасность, устанавливается обязательная проверка безопасности. Составление плана и схемы проверок возлагается на Госсовет, а их проведение – на его профильные департаменты и подразделения госорганов КНР, ответственных за обеспечение сетевой безопасности. Также операторы КИИ при приобретении сетевых сервисов и услуг обязаны заключать с поставщиками соглашение о безопасности и конфиденциальности.

Невыполнение требования об обязательной проверке безопасности продуктов,

которые приобретают операторы КИИ, согласно законопроекту должно повлечь прекращение использования таких продуктов на объектах КИИ, а также штраф оператору в размере от 1 до 10 эквивалентов закупочной стоимости такой продукции, плюс непосредственные взыскания с ответственных лиц.

Любопытной и достаточно противоречивой особенностью законопроекта стало также введение обязательства операторов КИИ хранить персональные данные граждан КНР и «другие важные данные», накопленные и обработанные в ходе их деятельности, на территории материкового Китая. Особые случаи, когда хранение персональных данных за пределами материковой территории КНР «действительно необходимо», подлежат дополнительному рассмотрению государственными регуляторами.

Помимо проверок безопасности, проводимых государственными органами, операторам КИИ также предписывается как минимум раз в год проводить проверку и оценку рисков сетевой безопасности на своих объектах самостоятельно, либо при помощи уполномоченных организаций. Отчеты о проведении и результатах проверки и оценки выявленных рисков направляются профильному государственному органу.

Наконец, помимо перечисленных мер и требований по обеспечению защиты КИИ, в законопроекте перечислены следующие меры, которые могут принимать профильные государственные структуры во взаимодействии с операторами таких объектов:

1. Осуществлять внеплановые выборочные проверки и тестирование рисков безопасности КИИ. По результатам таких проверок госорганами могут предлагаться меры по улучшению ситуации, и при необходимости назначаться специалисты или специализированные организации для проведения тестирования и оценки рисков безопасности.
2. Периодически организовать проведение операторами КИИ срочных учений по обеспечению сетевой безопасности для повышения навыков и уровня координации при реагировании на инциденты сетевой безопасности на критически важны объектах.
3. Способствовать обмену информацией по сетевой безопасности среди профильных подразделений госорганов, операторов КИИ, специализированных учреждений в сфере сетевой безопасности и исследовательских структур.
4. Оказывать техническую поддержку и содействие по вопросам кризисного управления сетевой безопасностью, восстановлением после инцидентов и проч.

Нужно отметить, что помимо непосредственного реагирования на инциденты и восстановления после них в документе отдельно освещаются вопросы раннего предупреждения и мониторинга рисков и инцидентов сетевой безопасности, в том числе на объектах КИИ. Так, в число задач профильных регуляторов и иных государственных органов включается создание систем мониторинга, раннего предупреждения и оперативного информирования по событиям сетевой безопасности «для отдельных отраслей промышленности и сфер хозяйства». Аналогичная задача в рамках секторального подхода ставится и в части выработки планов кризисного реагирования и проведений регулярных учений по сетевой безопасности.

Наконец, в рамках законопроекта уже на этапе первой его редакции были достаточно подробно прописана ответственность операторов КИИ за соблюдение вводимых норм. Преимущественно речь идет о системе штрафов и иных административно-денежных санкций. Так, в документе отмечается, что в случае неисполнения операторами КИИ требований по обеспечению сетевой безопасности профильные регуляторы выносят операторам замечания и предупреждения. Если оператор игнорирует такие меры или в случае, когда несоблюдение им установленных требований ведет к нарушению сетевой безопасности, меры ответственности могут включать штрафы. При этом для операторов КИИ разброс суммы штрафов (от 100 тыс. до 1 млн юаней) в 10 раз больше, чем для обычных сетевых операторов. Помимо юридических лиц, взысканию (в размере от 10 до 100 тыс. юаней) также могут подвергаться напрямую ответственные на нарушение установленных требований представители менеджмента операторов КИИ.

Более жесткие меры ответственности устанавливаются за невыполнение требований по хранению персональных данных граждан КНР «и иных важных данных» на территории КНР операторами объектов КИИ. Помимо предупреждений и штрафов, невыполнение нормы может повлечь «временное прекращение деятельности, запрет ведения бизнеса до устранения выявленных нарушений, закрытие вебсайтов, отзыв разрешений на ведение того или иного вида деятельности, или отзыв предпринимательской лицензии».

Такие меры достаточно часто упоминаются в тексте законопроекта применительно к сетевым операторам в целом, и не являются чем-то исключительным в уже имеющей место в КНР практике регулирования отрасли сетевых операторов. Однако нужно отметить их нетипичный характер именно в разрезе КИИ, с учетом того, что ранее в документе отмечается важность обеспечения непрерывности бизнес-процессов КИИ и следования международным отраслевым стандартам в этой области. Дополнительных пояснений в этой части не содержала ни исходная, ни вторая, переработанная редакция законопроекта.

Представленная в 2014 г. версия законопроекта не была принята сразу, и прошла через долгий период сбора комментариев и доработки, который, по всей видимости, завершился лишь к июню 2016 г. В результате вторая редакция законопроекта имеет ряд отличий от первоначальной версии, в том числе в части КИИ, несмотря на то, что большая часть определений, требований и иных предлагаемых нормативных нововведений осталась прежней.

Ключевые отличия второй редакции законопроекта в части КИИ[17]:

- Во-первых, из определения КИИ в статье документа исчезло перечисление отраслей промышленности и сфер народного хозяйства, объекты, сети и информационные системы которых относятся к КИИ. Согласно

[17] См. оригинал второй версии законопроекта: 网络安全法（草案二次审议稿）全文

浏览字号： 大 中 小 来源： 中国人大网 2016年05月04日, The Natonal Paople's Congress of the People's Republic of China, http://www.npc.gov.cn/npc/flcazqyj/2016-07/05/content_1993343.htm
Также см. неофициальный перевод документа на английский: Cybersecurity Law (Draft) (Second Reading Draft) by China Law Translate On July 4, 2016, http://chinalawtranslate.com/cybersecurity2/?lang=en#_Toc455489576.

обновленной формулировке, государство на основе многоуровневой системы защиты обеспечивает ключевые меры по безопасности КИИ, «уничтожение которой, либо потеря функциональности, либо утечка данных из которой могут серьезно угрожать национальной безопасности, народному благосостоянию и качеству жизни граждан, либо общественным интересам».

- Вместе с тем, формирование окончательного перечня КИИ по-прежнему отнесено к прерогативам Госсовета. По всей видимости, формирование перечня/реестра КИИ КНР будет осуществляться в рамках отдельного направления работы, возможно, в рамках соответствующего подзаконного акта. Таким образом, в целях исследования по-прежнему имеет смысл ориентироваться на открытый базовый перечень отраслей и сфер хозяйства, приведенный в первой редакции законопроекта. При этом и в первой, и во второй редакции законопроекта отдельно отмечается, что обеспечение безопасности и защита военных сетей относятся к сфере ответственности Центральной военной комиссии КНР и, таким образом, не охватываются данным законопроектом полностью.
- В законопроекте появился призыв к сетевым операторам, чьи объекты не относятся к КИИ, на добровольной основе взаимодействовать с операторами КИИ по вопросам обеспечения сетевой безопасности. Такой призыв в духе саморегулирования не находит дальнейшего развития в тексте обновленного законопроекта.
- Добавлено ограничение на распространение информации, собранной профильными государственными органами в ходе деятельности по защите КИИ. Такая информация может использоваться непосредственно для обеспечения сетевой безопасности, использование в иных целях запрещается.

Таким образом, на сегодняшний день законопроект предлагает достаточно комплексный подход к защите КИИ КНР, при этом его принятие в редакции, близкой к июньской, может произойти уже до конца 2016 г. Обобщая практику регулирования и обеспечения безопасности КИИ в Китае с учетом рассмотренного законопроекта, можно сделать ряд базовых выводов:

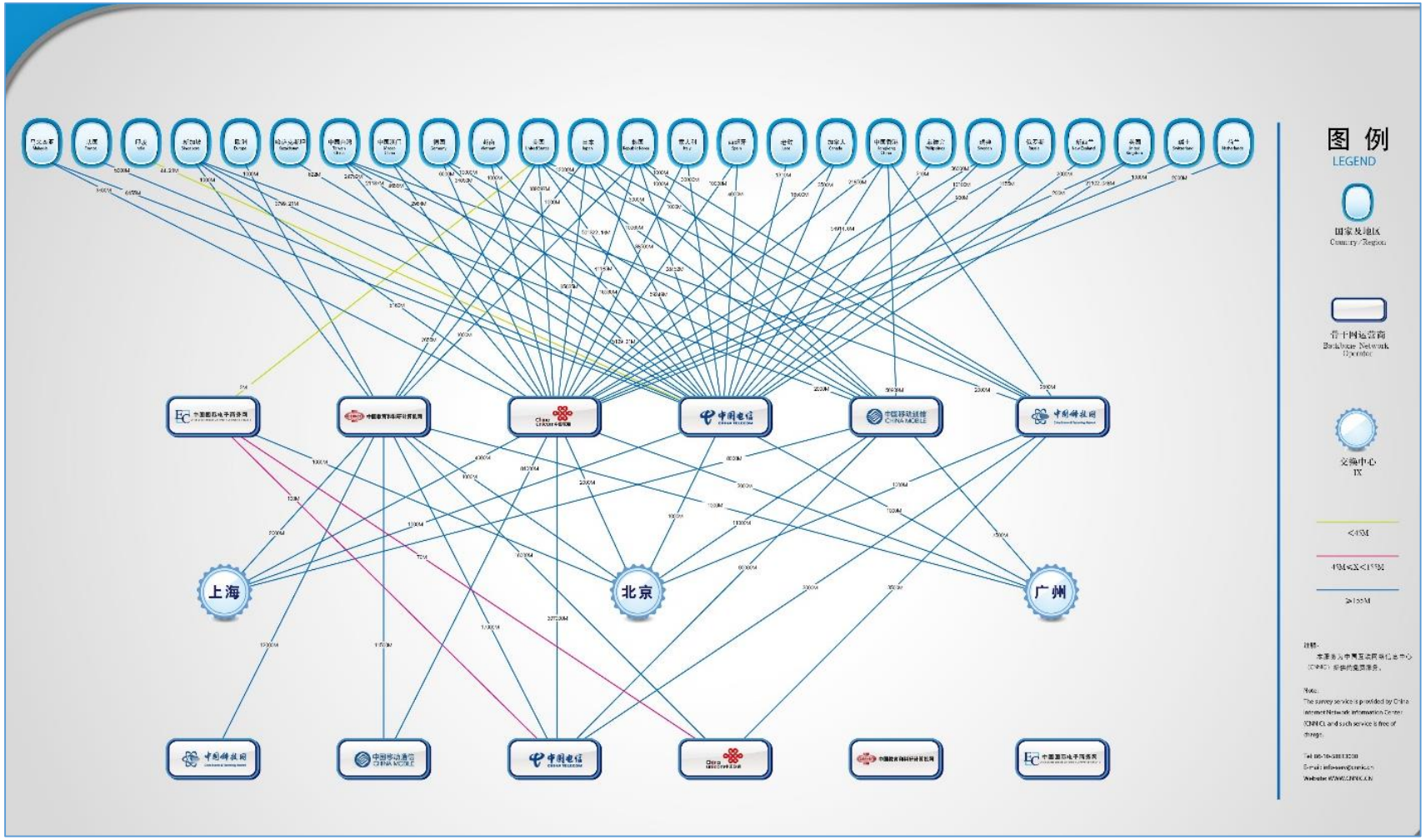
1. Китайские регуляторы не сводят КИИ к АСУ ТП и иным системам управления технологическими процессами на КВО. В сферу регулирования попадают непосредственно системы передачи данных и компьютерные сети, в том числе функционирующие на основе Интернета. Несмотря на то, что круг операторов КИИ на сегодняшний день прямо не обозначен ни в законопроекте по КИИ, ни в иных доступных документах, предлагаемые формулировки распространяются в том числе на операторов сервисов, обрабатывающих персональные данные пользователей и «большие данные». С большой долей вероятности в число операторов КИИ КНР будут включены крупнейшие национальные операторы связи и инфраструктурные провайдеры (China Mobile, China Netcom, China Telecom и проч.).
2. Вместе с тем, развивающаяся в КНР регуляторная модель, не предполагает непосредственного выделения инфраструктуры Интернета в качестве отдельного сектора КИИ. Несмотря на то, что рассмотренные подходы к категорированию КИИ пока не закреплены законодательно и являются неокончательными, их общая черта – отсутствие в перечне секторов КИИ сектора инфраструктуры Интернета. При этом подразумевается, что

базовые инфраструктурные сервисы глобальной сети (точки обмена трафиком, инфраструктура DNS и система ресурсов нумерации Интернета) выполняют роль инфраструктурной основы для отраслей и объектов, которые попадают под разрабатываемые регуляторные нормы.

3. Разработка окончательной модели категорирования и системы критериев КИИ остается открытой задачей для КНР. Однако на данный момент можно говорить о кристаллизации базового, основополагающего критерия для признания объекта информационной инфраструктуры критически важным: это серьезная угроза национальной безопасности, народному благосостоянию и качеству жизни граждан, либо общественным интересам в случае разрушения, нарушения функциональности объекта либо похищения из него данных. Такой критерий крайне широк и носит неопределенный характер, однако в целом может быть достаточно четко отграничен, например, от подхода ЕС, где первостепенное значение имеет необходимость и доступность сервисов для граждан, а также непрерывность бизнеса. В китайском случае приоритет все же уделяется обеспечению национальной и общественной безопасности.
4. Формирующийся в КНР подход достаточно сам по себе достаточно опосредованно учитывает международный опыт, международные стандарты в области БСО и особенно непрерывности бизнеса. Вместе с тем, он не создает никаких препятствий к тому, чтобы операторы КИИ внедряли и использовали такие стандарты, что в Китае уже является общей практикой (например, крупные телеком-операторы, такие как China Telecom, ведут свою деятельность в соответствии с ISO27001, ITIL и прочими международными стандартами).
5. На данный момент отсутствие окончательно принятого законодательства и особенно подзаконных актов, которые закрепляли систему критериев КИИ и, возможно, реестр ее операторов, не позволяют сделать окончательный вывод о том, попадают ли в круг операторов КИИ организации, обеспечивающие функционирование китайского сегмента инфраструктуры глобальной сети – например, китайского сегмента DNS и системы распределения ресурсов нумерации между китайскими интернет-провайдерами. В настоящий момент ключевую роль в выполнении этих функций играет Китайский сетевой информационный центр (CNNIC). НПО, созданная в 1997 г., является администратором национального домена .CN и интернационализированного ДВУ .中国, и распределяет между китайскими интернет-провайдерами пулы IP-адресов и номера АС, которые получает от Региональной регистратуры Интернета APNIC. Основная задача организации формулируется как обеспечение функционирования, администрирование и организация сервисов национальных критических сетевых ресурсов[18]. Исходя из общей логики законопроекта о кибербезопасности КНР, CNNIC сам по себе не относится к какому-либо из секторов КИИ, однако отвечает за работу сервисов, критически важных для остальных секторов. Вероятно, включение/невключение CNNIC в число операторов КИИ после принятия законопроекта послужит иллюстрацией того, как сами китайские регуляторы понимают сформулированный ими подход.

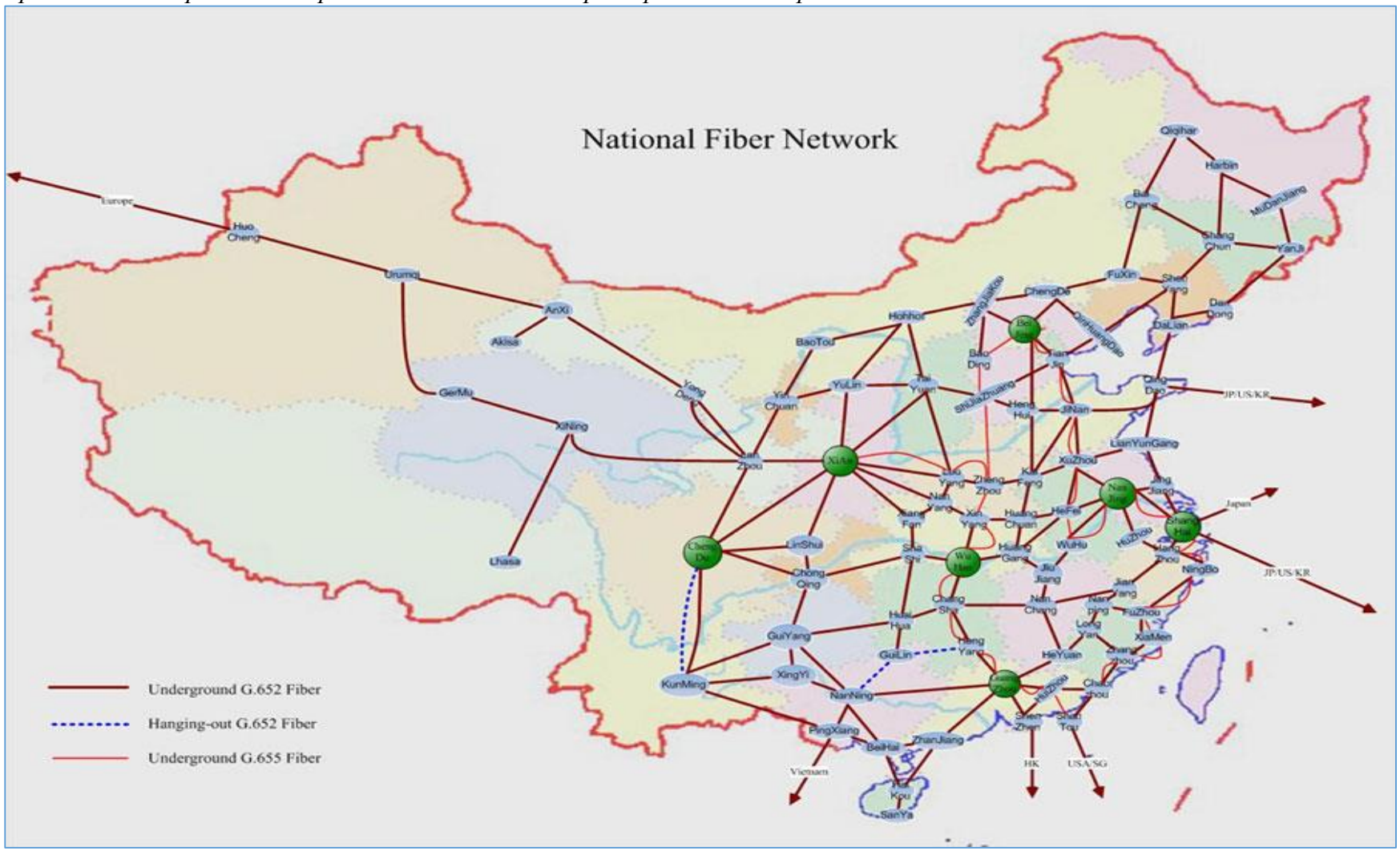
[18] ccTLD in the Frontier of the IG Ecosystem - Mo Dong, .cn | Presentation [EN], https://meetings.icann.org/en/dublin54/schedule/wed-ccnso-members/presentation-cctld-ig-ecosystem-21oct15-en.pdf.

*Карта подключений китайских операторов магистральных сетей и точек обмена трафиком к зарубежным сегментам Интернета*




Источник: Internet Connection Map of China. CNNIC website, https://www1.cnnic.cn/IDR/GlobalInternetNews/201209/P020120904346790476519.jpg (последнее посещение 15.07.2016).

*Приложение: Карта магистральных ВОЛС КНР с трансграничными переходами*




Источник: 2013 Annual Report. China Internet Network Information Center, https://www.cnnic.net.cn/gywm/zzkw/cnnicndbg/201401/U020140314621129945634.pdf.

## Российская Федерация

Российская регуляторная и нормативная практика в рассматриваемой области находится в процессе формирования, который до сих пор не завершен, прежде всего, по причине отсутствия законодательства федерального уровня, которое бы комплексно охватывало вопросы КИИ, включая обеспечение ее БСО. С 2006 г. по 2013 г. предпринималось три попытки разработать и принять закон по защите/обеспечению безопасности КИИ, но ни один из разработанных проектов документа так и не был принят.

Разработка и дискуссия вокруг этих законопроектов шли параллельно с формированием и принятием системы доктринальных и нормативно-методических ведомственных документов. Участие в этой деятельности принимали различные государственные органы, включая:

- Президента РФ;
- Федеральную комиссию по техническому и экспортному контролю РФ;
- Федеральную службу безопасности РФ;
- Совет безопасности РФ;
- Министерство связи и массовых коммуникаций РФ;
- Министерство энергетики РФ;
- Министерство экономического развития РФ;
- Прочие ведомства и министерства по отдельным документам либо в рамках обсуждения документов, подготовленных другими регуляторами.

Следует отметить, что на сегодняшний момент в рамках деятельности различных государственных регуляторов в РФ существуют серии документов, охватывающие несколько достаточно близких, но не идентичных понятий:

1. Ключевые (критически важные) системы информационной инфраструктуры (КСИИ) (нормативно-методические документы ФСТЭК).
2. Критически важные объекты (КВО) (нормативно-методические документы ФСТЭК, документы Совета безопасности, нормативно-методические документы МЧС РФ, ряд федеральных законов РФ, в том числе федеральный закон «О безопасности объектов топливно-энергетического комплекса» № 256-ФЗ от 21.07.2011). Как таковые, КВО представляют собой отдельную от КИИ категорию, как и в регуляторной практике большинства государств мира. Однако в ряд документов различных ведомств, включая Совет безопасности РФ, используются понятия, содержательно близкие к КИИ понятия, основанные на термине КВО (например, «функционирующие в составе КВО информационно-телекоммуникационные системы, защищаемые от деструктивных воздействий»).
3. Критическая информационная инфраструктура (КИИ) – законопроект 2013 г. «О безопасности критической информационной инфраструктуры Российской Федерации»).

Четкое закрепление соотношения этих понятий между собой и закрепление единого определения на уровне федерального законодательства служат одним из доводов в пользу необходимости принятия соответствующего ФЗ. Однако именно различные взгляды тех или иных регуляторов на подходы и понятийную, а также распределение полномочий и ответственности в этой сфере (ФСТЭК/ФСБ) являются одной из причин, по которой работа над принятием комплексного ФЗ до сих пор не завершена. Далее по тексту в случаях, когда речь не идет об отсылке к

тексту какого-либо конкретного документа, будет использоваться КИИ как общий термин.

По причине того, что не принято комплексное законодательство федерального уровня, нельзя говорить и о наличии законодательно закрепленной единой классификации объектов КИИ. Однако деятельность по разработке системы категорирования и критериев отнесения к таким объектам ведется с середины 2000-х гг. на площадке ФСТЭК и Совета Безопасности (СБ) РФ.

8 ноябре 2005 г. СБ РФ принял секретный документ «Система признаков КВО и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий». Несмотря на закрытый статус документа и давность разработки, сформулированные в нем 20 критериев до сих пор остаются основой системы классификации объектов КИИ в РФ.

С интервалом в два года ФСТЭК разработала и приняла серию нормативно-методических документов, в которой был сформулирован подход и методологическая база по обеспечению информационной безопасности КСИИ, а также категорированию таких объектов и созданию их перечня. В 2007 г. были приняты четыре документа:

- Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007).

Указанные документы имеют статус для служебного пользования, однако они доступны, в частности, операторам объектов, подпадающих под регулирование ФСТЭК. Значение этих документов для обеспечения безопасности КИИ/КСИИ РФ заключается в:

А) выработке ряда базовых определений, которые используются и в более поздних нормативных актах и иных документах. В частности, в документах ФСТЭК даются следующие определения КВО и КСИИ:

- КВО - объект, оказывающий существенное влияние на национальную безопасность РФ, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени.

- КСИИ - информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления

таким объектом (процессом), или официальное информирование граждан и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

Согласно пояснению ФСТЭК, понятие КСИИ обобщает в себе множество различных классов информационных, автоматизированных систем и информационно- телекоммуникационных сетей (системы предупреждения и ликвидации чрезвычайных ситуаций, географические и навигационные системы, системы управления водоснабжением, энергоснабжением, транспортом и другие системы и сети).

Таким образом, понятие КСИИ является принципиально более широким, чем АСУ ТП, вокруг которых строится понятийное и содержательное наполнение ряда документов СБ РФ, а также, частично, законопроекта по КИИ, разработанного ФСБ РФ в 2013 г. Важно подчеркнуть, что КСИИ также не совсем равнозначны информационным системам КВО, так как помимо них включают в себя системы, обеспечивающие официальное информирование граждан РФ.

Б) формировании системы категорирования КСИИ. До настоящего момента изложенная в документах ФСТЭК секторальная классификация остается единственной и основной для объектов КСИИ/КИИ в РФ. В документах регулятора были выделены следующие системы, в состав которых входят КСИИ:

- системы органов государственной власти;
- системы органов управления правоохранительных структур;
- системы финансово-кредитной и банковской деятельности;
- системы предупреждения и ликвидации чрезвычайных ситуаций;
- географические и навигационные систем;
- сети связи общего пользования на участках, без резервных видов связи;
- системы специального назначения;
- спутниковые системы для обеспечения органов управления и в специальных целях;
- системы управления добычей и транспортировкой нефти, нефтепродуктов и газа;
- программно-технические комплексов центров управления ВСС;
- систем управления водоснабжением и энергоснабжением;
- системы управления транспортом (наземным, воздушным, морским);
- системы управления потенциально опасными объектами.

Следует отметить следующие особенности определений и классификации КСИИ из документов ФСТЭК, в том числе по сравнению с международной практикой регулирования КИИ:

1. Определения КВО и КСИИ, включающие перечисления их базовых свойств, не включают влияние таких систем и объектов на обеспечение непрерывности бизнеса; однако отмечается их существенное влияние на национальную экономику и жизнедеятельность населения.
2. Перечень систем, в состав которых входят КСИИ, не включает в себя системы, составляющие инфраструктуру Интернета, несмотря на то, что в нем упоминаются программно-технические комплексы центров управления

взаимоувязанной сетью связи (ВСС) РФ и сети связи общего пользования на участках.

3. В отличие от регуляторной практики в отношении КИИ во многих странах мира (см. ЕС, США, Аргентина, Япония), выделенные ФСТЭК категории систем, в состав которых входят КСИИ, преимущественно относится к государственной инфраструктуре.

В развитие принятых документов в 2009 г. ФСТЭК приказом от 4 марта 2009 г. утвердила Положение о реестре КСИИ[19], придавшее официальный статус государственному реестру, который служба к тому времени вела уже более года. По данным открытых источников, еще до утверждения Положения в реестр было включено более 1200 КСИИ[20]. Именно ФСТЭК выступила разработчиком первых двух версий проекта федерального закона, который был призван комплексно охватить вопросы регулирования КИИ/КСИИ. В 2006 г. был разработан проект ФЗ «Об особенностях обеспечения информационной безопасности КВО информационной и телекоммуникационной инфраструктуры». В название законопроекта было вынесено понятие «КВО информационной и телекоммуникационной инфраструктуры», которое в тексте определялось как «объект информационной и телекоммуникационной инфраструктуры, прекращение или нарушение функционирования которого приводит к негативным последствиям, идентичным тем, что в 2007 г. были включены в упомянутое выше определение КВО.

При этом собственно под объектом информационной и телекоммуникационной инфраструктуры в законопроекте понималась «совокупность зданий, строений, сооружений, технических средств и установленных в них объектов информатизации, телекоммуникации и связи, объединенных единым технологическим процессом и функционирующих ради достижения определенной цели, а также иные здания, строения, сооружения, устройства и оборудование, обеспечивающие их функционирование». Стоит отметить, что такое широкое определение теоретически могло распространяться и на инфраструктурные элементы Интернета – например, инфраструктуру точек обмена трафиком (IXPs), системы DNS и распределения ресурсов нумерации Интернета, а также непосредственно на инфраструктуру интернет-провайдеров. Однако сам по себе Интернет, как и обеспечивающие его работу сервисы и инфраструктуре, в тексте законопроекта не упоминался и, по всей видимости, не рассматривался в качестве объекта регулирования. В силу того, что закон не был принят, указанные понятия и определения не получили дальнейшего распространения в российской нормотворческой практике.

В законопроекте также использовалось понятие КСИИ, однако в отличие от более поздней версии, получившей развитие в нормотворчестве ФСТЭК, здесь КСИИ четко определялись как системы, входящие в состав КВО.

---

[19] Информационное сообщение по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 25 июля 2014 г. № 240/22/2748, Федеральная служба по техническому и экспортному контролю, http://fstec.ru/component/attachments/download/715.

[20] Критические системы информационной инфраструктуры. Бизнес без опасности, персональный блог Алексея Лукацкого, Blogspot.ru, 13.07.08, http://lukatsky.blogspot.ru/2008/07/blog-post_12.html.

В плане регуляторного охвата законопроект носил достаточно комплексный характер и был нацелен на решение следующих задач:

- Формирование комплексной понятийной базы в части КСИИ, КВО и критически важных сегментов информационной и телекоммуникационной инфраструктуры, а также определения угроз информационной безопасности таких объектов, систем и сегментов.
- Оценка уязвимости объектов информационно-телекоммуникационной инфраструктуры и объектов информатизации от актов незаконного вмешательства и деструктивных информационных воздействий. В частности, предлагалась разработки общей модели реализации угроз информационной безопасности для КВО информационно-телекоммуникационной инфраструктуры, а также разработка частных моделей реализации угроз для каждой категории таких объектов и отдельных объектов.
- Категорирование КВО информационно-телекоммуникационной инфраструктуры и объектов информатизации. Базовым критерием по-прежнему было наступление негативных последствий, возникающих вследствие прекращения или нарушения функционирования таких объектов. В законопроекте приводился перечень критически важных сегментов информационной и телекоммуникационной инфраструктуры, сходный с перечнем систем, в состав которых входят КСИИ, утвержденным в 2007 г.. Из существенных отличий можно отметить наличие в перечне 2006 г. сегментов управления автоматизированными системами управления войсками и оружием, а также ГИС «Выборы».
- Разработка требований и реализации мер по обеспечению информационной безопасности КВО информационной и телекоммуникационной инфраструктуры.

В пояснительной записке к законопроекту отмечалось, что одним из ключевых факторов, делающих закон необходимым, является рост террористической угрозы в отношении объектов информационной и телекоммуникационной инфраструктуры. Кроме того, отмечалась возможная роль закона как средства ликвидации правового пробела в отношении обеспечения конфиденциальности «технологической информации» (оперативно-диспетчерская, телеметрическая информация, команды телеуправления и телемеханики, а также статистическая, аналитическая и иная оперативная информация, на основе которой принимаются управленческие решения), не подпадающей под нормы 149-ФЗ «Об информации, информационных технологиях и о защите информации». Вскоре после внесения в Государственную Думу РФ в 2006 г. законопроект был отозван.

Еще одна попытка разработать законодательство, регулирующее вопросы обеспечения информационной безопасности КВО, была предпринята ФСТЭК в 2012 г., когда Службой был разработан проект поправок в ФЗ-149 «Об информации, информационных технологиях и о защите информации». Проектом предлагалось дополнить текст 149-ФЗ статьей 16.2 (Защита информации в информационных системах КВО), которая:

- Вводила ряд требований по обеспечению информационной безопасности для операторов и заказчиков информационных систем КВО, включая предотвращение неправомерного доступа к информации или удаления информации, обеспечивающей управление и контроль над технологическими процессами; недопущение воздействия на технологические средства обработки информации, способного нарушить функционирование таких систем;

- Среди вводимых законопроектом требований к операторам и заказчикам ИС КВО стоит выделить требование обеспечить реагирование на инциденты ИБ и возможность оперативного восстановления ИС КВО после инцидентов. Такие формулировки отражают приближение нормотворческого подхода российского регулятора к международным стандартам и практикам по реагированию на инциденты ИБ/кибербезопасности и обеспечению (БСО) объектов КИИ.

Кроме того, авторы законопроекта предложили ввести систему классификации ИС КВО заказчиками таких системах на основе а) уже утвержденных категорий КВО; б) степени влияния информационных систем на функционирование самих КВО. ФСТЭК в тексте законопроекта предлагала закрепить за собой полномочия по установлению требований к защите информации в ИС КВО. При этом заказчикам таких систем предоставлялась возможность самостоятельно определять дополнительные требования к защите информации с учетом особенностей технологических процессов, управление и контроль над которыми они обеспечивают.

Продвижение законопроекта остановилось после предоставления Министерством экономического развития отрицательного отзыва на него, преимущественно посвященного вопросам экономической целесообразности предлагаемых ФСТЭК мер по защите информации в ИС КВО. Так, Министерством были представлены данные расчетов затрат на обеспечение защиты информации в ИС КВО в зависимости от особенностей информационных систем и уровней ущерба по отраслям промышленности (см. Таблицу 1), а также статистика инцидентов ИБ по различным отраслям и категориям КВО.

| Отрасль | Оценочная средняя стоимость информационной системы КВО (млн.руб.) | Ориентировочная стоимость построения системы защиты информации (млн.руб.) | Средний уровень ущерба (млн.руб.) |
|---|---|---|---|
| Автомобильная промышленность | 30 | 2.5 | 100 |
| *Химическая промышленность* | *50* | *3.5* | *1* |
| Радиоэлектронная промышленность | 50 | 3.5 | 5 |
| Пищевая промышленность | 5 | 0.5 | 10 |
| *Металлообработка* | *30* | *2.5* | *0.1* |
| *Общее машиностроение* | *30* | *2.5* | *0.5* |
| Нефтегазовая отрасль | 100 | 7 | 200 |
| Энергетика | 100 | 7 | 300 |
| Транспорт | 50 | 3.5 | 300 |
| Водоснабжение и канализация | 20 | 1.6 | 5 |

Источник: Заключение об оценке регулирующего воздействия на проект федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», Министерство экономического развития РФ, 17 августа 2012 г.

Регулятор сделал вывод о том, что применение предлагаемых ФСТЭК требований в химической промышленности, металлообрабатывающей промышленности, общем машиностроении нецелесообразно, так как затраты на их выполнение

многократно превышают средний размер ущерба от инцидентов информационной безопасности. Также в своем заключении МЭР отметил, что приоритет в обеспечении безопасности ИС КВО должны иметь отрасли автомобилестроения, нефтегазовой промышленности, энергетики и транспорта.

В отношении топливно-энергетического комплекса заключение Министерства еще раз высвечивает тенденцию, до сих пор характерную для российского подхода к защите КИИ / информационных систем КВО. В отсутствие единого федерального законодательства, охватывающего все сферы промышленности и экономики, отдельные отраслевые регуляторы развивают собственные системы требований и ведомственных норм, а также продвигают законодательство по вопросам собственных отраслевых компетенций. В заключении по законопроекту ФСТЭК МЭР ссылается на то, что для объектов ТЭК уже был принят закон, охватывающий в том числе вопросы информационной безопасности - 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» от 21.07.2011. Статья 11 закона обязывает операторов объектов ТЭК создавать системы защиты информации и информационно-телекоммуникационных сетей от угроз информационной безопасности, включая неправомерный доступ, уничтожение, модифицирование, блокирования информации и иных неправомерные действия[21]. Технические и организационные меры, которые должен предпринять оператор для выполнения этих требований, рассматриваются в том числе как часть комплекса мер по обеспечению антитеррористической защищенности объектов ТЭК, включая КВО этого сектора.

Однако этим закон в части защиты ИС объектов ТЭК и ограничивается: не предусматривается мер по обеспечению БСО таких систем, реагированию на компьютерные инциденты, резервированию критических ИС и содержащихся в них данных, созданию профильных организационных структур и назначению ответственных лиц по вопросам ИБ, и проч. Кроме того, не производится дифференциация и категорирование информационной инфраструктуры объектов ТЭК: в частности, затруднительно понять, как из текста закона, так и из практики его применения, рассматривают ли регуляторы, в том числе Минэнерго и ФСТЭК, сетевую безопасность как составляющую ИБ КВО ТЭК. Нечеткость положений закона служит почвой для обсуждения возможности принятия конкретизирующих поправок, которое началось вскоре после принятия НПА и с различной периодичностью ведется до сих пор.

Еще одна характерная тенденция последних лет, которую зафиксировало заключение МЭР – перераспределение роли в обеспечении защиты КИИ от ФСТЭК в пользу ФСБ. В своем заключении МЭР отмечает, что координатором деятельности ФОИВ в сфере защиты КИИ является ФСБ РФ, ссылаясь принятые СБ РФ в феврале 2012 г. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами КВО инфраструктуры РФ[22].

---

[21] См.: Федеральный закон от 21 июля 2011 г. N 256-ФЗ "О безопасности объектов топливно-энергетического комплекса". Российская газета - Федеральный выпуск №5537 (161), 26 июля 2011 г. https://rg.ru/2011/07/26/tek-dok.html.

[22] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803). Совет Безопасности Российской Федерации, http://www.scrf.gov.ru/documents/6/113.html.

В документе используется устоявшееся понятие КВО РФ, однако в нем же впервые в российской практике возник термин КИИ РФ, определяемый как совокупность АСУ КВО и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий.

Это определение КИИ на данный момент близко к консенсусному в российской практике, с учетом его уточненной и доработанной версии, представленной в законопроекте ФСБ в 2013 г. Важно то, что такое понимание КИИ жестко привязано к специфическому сегменту информационных систем – АСУ (ТП); при этом информационно-телекоммуникационные сети (в том числе потенциально и Интернет) в рамках определения оказываются вторичны, поскольку рассматриваются в качестве элементов КИИ не сами по себе, а как средство, обеспечивающее взаимодействие АСУ. Таким образом, в терминах КИИ не может рассматриваться сама по себе инфраструктура, обеспечивающая функционирование Интернета (системы серверов доменных имен, реестры и инфраструктура РРИ, точки обмена трафиком и сети магистральных провайдеров), так как эти инфраструктурные системы сами по себе не включают АСУ ТП или иными процессами. Это косвенно подтверждается и определением АСУ КВО, приведенным в документе СБ РФ, которое в целом соответствует международной практике в отношении АСУ ТП (ICS). Речь идет об инфраструктуре, используемой для оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса – в данном случае на КВО. Вместе с тем, в документе в качестве факторов, влияющих на обеспечение ИБ АСУ КВО и КИИ, отмечается глобализация информационно-телекоммуникационных сетей и размытыми границ их национальных сегментов. Кроме того, в число основных задач в области безопасности АСУ КВО включается «обеспечение устойчивого функционирования национального сегмента единой мировой информационно-телекоммуникационной сети», т.е. Интернета, в условиях роста трансграничных атак.

Основы государственной политики… стали российским доктринальным документом, в котором угрозы АСУ КВО определяются в терминах компьютерной и сетевой безопасности (компьютерный инцидент, компьютерная атака). При этом инцидент рассматривается как нарушение штатного режима функционирования элемента КИИ. В части противодействия компьютерным атакам и инцидентам на объектах КИИ в документе СБ были анонсированы следующие задачи:

- Создание сил обнаружения и предупреждения компьютерных атак на базе ФСБ РФ, функции которых включают обнаружение и предупреждение компьютерных атак на КИИ РФ, мониторинг уровня ее защищенности и ликвидацию последствий компьютерных инцидентов.
- Силы ликвидации последствий компьютерных инцидентов в КИИ, также в статусе уполномоченных подразделений ФСБ РФ, принимающие участие в восстановлении штатного режима функционирования элементов КИИ после компьютерных инцидентов.
- Создание централизованной, иерархической, территориально распределенной государственной системы обнаружения и предупреждения

компьютерных атак на КИИ и оценки уровня реальной защищенности ее элементов.

Кроме того, в Основах государственной политики…разграничиваются полномочия ФСБ и ФСТЭК РФ в сфере защиты КИИ, причем приоритетная роль отводится ФСБ РФ. Реализация отдельных задач, сформулированных в документе СБ РФ, началась параллельно с его разработкой и принятием. В июле 2012 г. ФСБ объявила о создании Центра реагирования на компьютерные инциденты в информационных системах органов государственной власти РФ (GOV-CERT.RU), в задачи которого входит реагирование на:

- DDoS-атаки против ИТС органов государственной власти РФ;
- вовлечение объектов ИТС в бот-сети и распространение вредоносного ПО;
- попытки несанкционированного доступа к объектам ИТС органов государственной власти РФ.

При этом GOV-CERT не специализируется конкретно на реагировании на инциденты в КИИ РФ.

Задаче внедрения положений документа СБ РФ на практическом уровне в части защиты ПТП АСУ ПТП отвечает приказ ФСТЭК «Об утверждении требований к обеспечению защиты информации в АСУ ПТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14 марта 2014 г.[23] Приказ устанавливает подробную систему требований к операторам и разработчикам АСУ ПТП указанных в нем объектов, включая КВО. В документе в число мер, которые принимаются в рамках оценки необходимости защиты информации в АСУ ПТП, включено определение оператором критически важной информации (информация, нарушение доступности, целостности или конфиденциальности (C.I.A.) которой может привести к нарушению штатного режима функционирования АСУ).

Требования к защите информации в АСУ, согласно приказу, устанавливаются в соответствии классом защищенности АСУ, который оценивается оператором объекта на основе методологии, изложенной в приказе. Класс защищенности АСУ (по нарастающей от первого к третьему) определяется на основе уровня критичности информации в АСУ (три уровня от низкого к высокому). Оператор определяет такой уровень, оценивая степень возможного ущерба от нарушения целостности, доступности и конфиденциальности информации в АСУ ПТП. Например, высокому уровню критичности информации соответствует ситуация, когда нарушение ее C.I.A. может повлечь ЧС федерального или межрегионального характера, или иные существенные последствия в социальной, политической, экономической, военной или иных областях деятельности. Нужно отметить, что приказ при определении требований к защите АСУ предписывает учитывать не только российские ГОСТы, но и адаптированную версию ISO 27001 (ГОСТ Р ИСО/МЭК 27001).

[23] Федеральная служба по техническому и экспортному контролю. Приказ от 14 марта 2014 г. N 31. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. ФСТЭК России. http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31.

На более высоком уровне следующим шагом по решению задач, сформулированных в документе СБ РФ стало подписание Указа Президента РФ №31с от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ». Ответственность за создание системы ГосСОПКА Указ возлагает на ФСБ РФ, а в число основных задач системы включается осуществление контроля степени защищенности КИИ РФ от компьютерных атак. Для решения этой и других задач, определенных Указом, ФСБ[24]:

- ведет работы по созданию системы ГосСОПКА;
- разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети госорганов, а также, по согласованию – иных операторов;
- определяет порядок обмена информацией о компьютерных атаках между ФОИВ;
- организует и проводит мероприятия по оценке степени защищенности КИИ РФ от компьютерных атак;
- разрабатывает методические рекомендации по организации защиты КИИ.

Согласно Концепции ГосСОПКА, утвержденной 12 декабря 2014 г., в состав системы входит созданный на базе ФСБ РФ Национальный координационный центр по компьютерным инцидентам. В задачи Центра входит организация обмена информацией о компьютерных инцидентах с юридическими лицами-операторами объектов КИИ и операторами связи, обеспечивающими взаимодействие объектов КИИ, а также международное сотрудничество по противодействию компьютерным инцидентам. Такая структура частично воспроизводит функции CERT\CSIRT, но не ограничивается ими и представляет собой оригинальный формат деятельности.

В целом, Указ №31с закрепил сохраняющуюся на сегодня роль ФСБ РФ как ключевого регулятора в сфере защиты государственной информационной инфраструктуры РФ, в том числе государственной КИИ РФ. С этого момента, а точнее еще со второй половины 2012 г., ФСТЭК перестала выступать в качестве субъекта законодательной инициативы по вопросам комплексного регулирования защиты КИИ/ КСИИ РФ. Эту функцию также перехватила ФСБ, которая к апрелю 2013 г. разработала новый документ – законопроект «О безопасности КИИ РФ»[25], отражающий как ключевые моменты и задачи Основ государственной политики… 2012 г., так и Указа 31с в части создания и дальнейшего развития системы ГосСОПКА. Законопроект к настоящему моменту прошел несколько кругов доработки и сбора комментариев, однако до сих пор не был принят. В отличие от предыдущего законопроекта ФСТЭК, законопроект ФСБ сталкивается с несколько иными препятствиями: имея более комплексный и всеобъемлющий характер, чем его предшественник, разработанный ФСТЭК, инициатива ФСБ претендует на закрепление единого и непротиворечивого подхода к обеспечению безопасности КИИ. А это означает, что для принятия законопроекта желательно снять все накопившиеся за более чем 10 лет понятийные противоречия, устранить

[24] Указ Президента Российской Федерации от 15 января 2013 г. N 31с г. Москва «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Выписка), Российская Газета, 18 января 2013 г., https://rg.ru/2013/01/18/komp-ataki-site-dok.html.

[25] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации». Паспорт законопроекта. https://regulation.gov.ru/projects?type=ListView#npa=597.

имеющееся дублирование и лакуны между функциями различных регуляторов и подвести накопленную нормативную базу и регуляторную практику под относительно единый знаменатель, что объективно непросто.

Задачи, заявленные в законопроекте - заложить организационно- правовые основы обеспечения безопасности КИИ РФ в целях предотвращения компьютерных инцидентов, выстроить единую систему принципов и методов регулирования в этой сфере, а также определить и разграничить полномочия регуляторов и установить права, обязанности и ответственность операторов КИИ. Отдельно подчеркивается необходимость определить порядок субъектов КИИ с системой ГосСОПКА.

В плане терминологии законопроект опирается на Основы государственной политики… СБ РФ, приводя определения КВО, АСУ ТП КВО и КИИ. Законопроект дает, пожалуй, наиболее проработанное на сегодня определение КИИ: «совокупность АСУ производственными и технологическими процессами КВО и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка». Под безопасностью КИИ понимается состояние, когда компьютерные инциденты на объектах не ведут к наступлению существенных негативных последствий (потеря управления экономикой и/или обеспечения обороноспособности, безопасности и правопорядка, необратимому негативному изменению (разрушению) экономики либо существенному снижению безопасности жизнедеятельности населения.

Законопроект также определяет круг субъектов КИИ, в который включаются не только сами владельцы/операторы КИИ, но и «операторы связи и операторы государственных информационных систем (ГИС), обеспечивающие функционирование и взаимодействие объектов КИИ». Таким образом, к числу субъектов КИИ в рамках логики законопроекта могут быть отнесены и крупнейшие телекоммуникационные и интернет-провайдеры, сети которых используются в том числе для организации связи между территориально распределенными объектами КИИ (Ростелеком). Помимо субъектов КИИ, в законопроекте выделяются круг организаций, аккредитуемых ФСТЭК для оценки защищенности объектов КИИ.

В рамках систематизации и унификации подхода к защите КИИ в документе предлагается новая система категорирования таких объектов на основе следующих критериев:

- критерий экономической значимости;
- критерий экологической значимости;
- критерий значимости для обеспечения обороноспособности;
- критерий значимости для национальной безопасности;
- критерий социальной значимости;
- критерий важности в части реализации управленческой функции;
- критерий важности в части предоставления значительного объема информационных услуг.

Параллельно с критериями значимости также вводятся три класса опасности объектов КИИ:

1) объекты КИИ РФ высокой категории опасности;

2) объекты КИИ РФ средней категории опасности;
3) объекты КИИ РФ низкой категории опасности.

Отнесение объекта КИИ к тому или иному классу опасности в рамках законопроекта служит своего водоразделом между сферой ответственности и полномочиями ФСТЭК и ФСБ РФ. Взаимодействие с субъектами КИИ высокого класса опасности, в том числе по вопросам отнесения объектов к соответствующему классу опасности, предлагается закрепить за ФСБ, по объектам среднего и низкого класса опасности – за ФСТЭК. При этом ФСБ и ФСТЭК должны вести собственные отдельные реестры объектов КИИ соответствующих классов опасности. Аналогичным образом разводятся полномочия двух служб в части установления порядка оценки защищенности КИИ и требований для аккредитации организаций, выполняющих такую оценку.

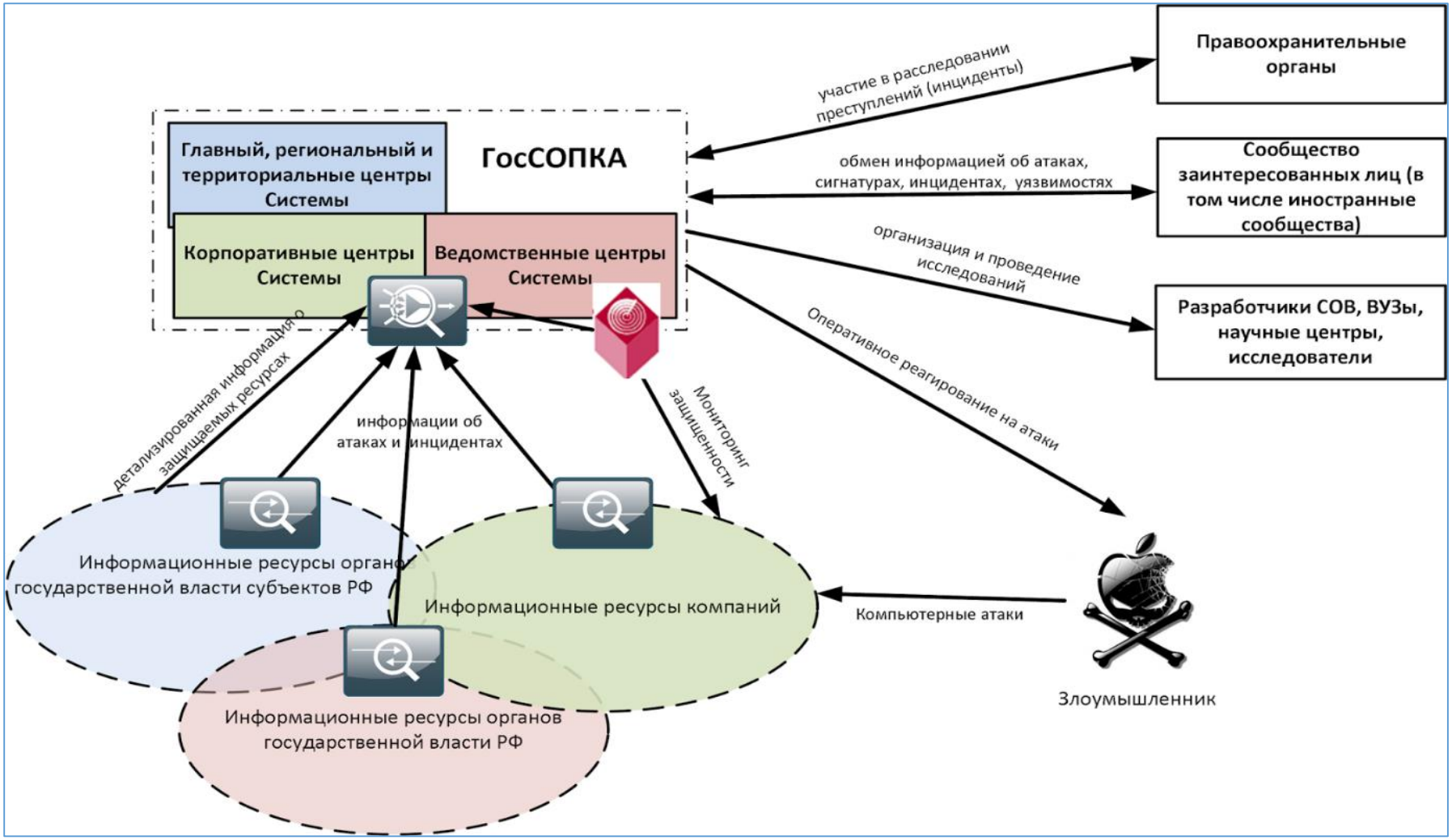
В самом законопроекте не приводится система количественных показателей и признаков, которую предполагается использовать для категорирования КИИ как в части критериев значимости, так и классов опасности. Из-за этого невозможно определить, какие отрасли и конкретные объекты подпадают под действие законопроекта. Разработать такие показатели должны ФСТЭК и ФСБ. Для сектора телекоммуникаций и интернет-отрасли актуален критерий важности объекта в части предоставления значительного объема информационных услуг - однако понятие информационных услуг в тексте также не конкретизировано.

Законопроект закрепляет роль системы ГосСОПКА в защите информационных ресурсов РФ, противодействии компьютерным атакам и инцидентам, и в том числе определяет режим взаимодействия системы с субъектами КИИ РФ. Последние обязаны передавать в систему информацию, перечень которой устанавливается ФСБ, а также принимать незамедлительные меры по ликвидации последствий компьютерных инцидентов на своих объектах. Кроме того, на субъектов КИИ РФ, в т.ч. на операторов связи и операторов ГИС, обеспечивающих функционирование КВО, распространяются следующие обязанности:

- обеспечивать защиту объектов КИИ;
- направлять сведения о выполнении мероприятий по итогам оценки защищенности и выполнять предписания ФСБ и ФСТЭК по устранению нарушений требований по безопасности объектов КИИ;
- незамедлительно информировать ФСБ РФ о компьютерных инцидентах на объектах РФ. РАЭК в своей Позиции по законопроекту от 23 августа 2013 г. отмечала некоторую расплывчатость этого требования в части сроков информирования[26].
- обеспечивать беспрепятственный доступ представителей ФСБ/ФСТЭК на объекты;
- содействовать госорганам выявлении, предупреждении и пресечении компьютерных инцидентов, а также в ликвидации их последствий, установлении причин и условий их совершения.
- обеспечивать выполнение технических условий, порядка установки и эксплуатации, а также сохранность технических средств, предназначенных для поиска признаков компьютерных атак в сообщениях электросвязи.

[26] Позиция РАЭК по законопроектам ФСБ России о безопасности критической информационной инфраструктуры, Российская ассоциация электронных коммуникаций, 22 Августа 2013, http://raec.ru/times/detail/2826/.

*Схема взаимодействия системы ГосСОПКА с внешними субъектами*




Источник: СОИБ. Анализ. ГосСОПКА. Сергей Борисов, 20 марта 2015 г. Блог SecurityLab.RU. http://www.securitylab.ru/blog/personal/sborisov/131813.php.

Таким образом, законопроект ФСБ, развивая положения, сформулированные в Основах государственной политики… СБ РФ, Указе 31с и других документах, должен завершить оформление российского подхода в области защиты КИИ по следующих позициям:

- Центральная роль среди госрегуляторов в защите КИИ переходит от ФСТЭК к ФСБ; деятельность по защите КИИ осуществляется в тесной связке с созданием общегосударственной системы ГосСОПКА, обеспечивающей противодействие компьютерным атакам и инцидентам на государственных информационных ресурсах РФ, включая объекты КИИ. Таким образом тематика защиты КИИ плотно включается в более общий контекст построения общегосударственного механизма борьбы с атаками и реагирования на инциденты ИБ.
- Вместе с перераспределением полномочий меняется и терминология и понимание сферы регулирования. КСИИ как основной термин уходит в прошлое, его заменяет АСУ (ТП) КВО и, в первую очередь, собственно КИИ. Понятие КИИ имеет четкую привязку к АСУ ПТП и КВО. Ключевая его черта – прописанный «вспомогательный» статус информационных и телекоммуникационных сетей, связывающих между собой АСУ ПТП КВО, но не образующих самостоятельного сектора КИИ.
- Смена терминологии сопровождается сменой подхода к категорированию – на смену достаточно неочевидной и «специальной» линейке секторов КСИИ, разработанной ФСТЭК порядка 10 лет назад, предлагается более стройная и гибкая система категоризации по критериям значимости и классам опасности. Базовая линейка критериев значимости теоретически позволяет распространять категорирование КИИ и на объекты гражданского коммерческого сектора. Однако пока не завершена проработка параметров, включая количественные, для новой системы категорирования, ее практическая полезность не может быть достоверное оценена.
- Оформляется комплексная система взаимодействия между госрегуляторами и операторами КИИ, в которой наконец устанавливается системный перечень требований, обязательств и процедур для последних. При этом помимо самих операторов КИИ под регуляторную сетку попадают и другие субъекты – в том числе операторы связи и операторы государственных информационных систем (ГИС), от которых зависит работа КИИ. Такой подход воспроизводит логику из самого определения КИИ – операторы связи не имеют в собственности КИИ, но от их деятельности и от управляемой ими инфраструктуры зависит работа таких объектов.
- По причине того, что госурегуляторы до сих пор определяют окончательные параметры системы требований к операторам КИИ, и в законодательстве четко не размечена сфера ответственности самих операторов, последние не проявляют большой активности – имеется в виду саморегулирование и развитие корпоративных практик и стандартов по вопросам защиты КИИ. Одна из немногих крупных компаний, очевидно попадающая в категорию как субъектов, так и операторов КИИ, и выработавшая собственные стандарты в части защиты своей информационной инфраструктуры – ПАО «Газпром». В 2009-2010 гг. корпорация приняла серию из четырех стандартов организации (СТО), которая в том числе охватывает требования к информационно-управляющим системам и АСУ ТП предприятия, разработку требований к объектам защиты информации, а также сами требования по технической защите информации. Субъекты российской интернет-отрасли, в том числе крупнейшие сетевые операторы, инфраструктурные и контент-провайдеры, точки обмена трафиков и ведущие интернет-сервисы (поисковый движок,

например) обычно не рассматривают себя в качестве операторов КИИ в том понимании, которое заложено в последнюю серию российских документов по защите АСУ ПТП КВО и КИИ.

Один из важных моментов состоит в том, что законопроект ФСБ РФ продолжает устойчивую черту российского подхода к защите ИС КВО / КСИИ / КИИ – в нем напрямую не рассматривается Интернет. Присущее ФСТЭК, ФСБ, отраслевым министерствам и СБ РФ видение проблематики защиты КИИ / КСИИ предполагает привязку к АСУ (ПТП) КВО и, в конечном счете, к самим ПТП КВО. Интернет, в т.ч. элементы системы DNS и системы ресурсов нумерации, инфраструктура магистральных сетей передачи данных, интерконнектов, точек доступа и IXP такой привязки не имеет. Ситуация не меняется, даже если формально многие инфраструктурные объекты Рунета соответствуют критериям социальной, экономической и иной значимости согласно законопроекту ФСБ.

Другая особенность подготовленного ФСБ законопроекта состоит в отсутствии приоритета международных механизмов и форматов взаимодействия по вопросам защиты КИИ. Международное сотрудничество не включено в список как основных направлений обеспечения безопасности КИИ РФ, так и принципов такой работы. В документе в общих чертах за ФОИВ РФ закрепляются задачи по участию в:

- международном сотрудничестве в области обеспечения безопасности КИИ РФ;
- работе международных организаций (МО), совещаний и конференций по вопросам обеспечения безопасности КИИ РФ;
- обмену информацией с иностранными государствами и МО о возможных угрозах безопасности и выявленных компьютерных инцидентах.

Однако конкретный круг российских госорганов, ответственных за решение этих задач, не очерчивается. Среди перечисляемых в законопроекте функций конкретно ФСБ и ФСТЭК указанные задачи отсутствуют – таким образом, ответственность за их выполнение в рамках законопроекта носит размытый характер. Не обозначены и внешние контрагенты такой деятельности: иностранные государства-партнеры, МО, форумы, конференции и иные рабочие механизмы, с которыми российские ФОИВ могли взаимодействовать по вопросам обеспечения безопасности КИИ.

Исключением является третья из перечисленных задач (международный обмен информацией), решение которой обеспечивает система ГосСОПКА. Но никакой конкретики по кругу субъектов и содержанию такого обмена не приводится, в том числе в части зарубежных и международных CSIRT, их ассоциаций, форумов и проч. Такой подход достаточно резко отличается от международных практик в сфере реагирования на инциденты на объектах КИИ (в том числе опыта ЕС и государств-членов ЕС, Японии, США и проч.).

Вместе с тем, законопроект ФСБ РФ отвечает некоторым принципам и практикам, выделенным в международных документах, включая Рекомендации Совета ОЭСР по защите КИИ от 2008 г., включая определение четких целей политики по обеспечению безопасности КИИ на высшем уровне и определение круга ответственных за ее реализацию регуляторов и иных структур, а также принятие мер по повышению уровня безопасности компонентов информационных систем и сетей, из которых состоят КИИ. Кроме того, подход к критериям и определению

КИИ, закрепляемый в законопроекте, укладывается в обозначенный в документе ОЭСР спектр подходов к определению и категорированию КИИ. Расхождения законопроекта с практиками и документами ОЭСР помимо вопросов международного сотрудничества и роли CSIRT/CERT касаются взаимодействия регуляторов с операторами, роли саморегулирования и вклада частного сектора в части реализации государственной политики по обеспечению безопасности КИИ.

В целом подход законопроекта не уникален и характерен для других нормативных и доктринальных документов по обеспечению безопасности КИИ/КСИИ РФ и защите АСУ ПТП КВО РФ, включая Основы государственной политики… СБ РФ от 2012 г. По этому же направлению пошла работа над обновлением Доктрины информационной безопасности, которая ведется с 2014 г. по настоящее время. В июне 2016 г. Совет Безопасности открыл для комментариев проект обновленной Доктрины, который представляет собой глубокую переработку оригинального документа 2000 г.[27] Проект Доктрины относит обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, включая КИИ и единую сеть электросвязи РФ, к числу национальных интересов РФ, а защиту КИИ – к стратегическим целям обеспечения информационной безопасности (ИБ) РФ. К основным угрозам и «негативным факторам» для ИБ РФ отнесено деструктивное воздействие на информационную инфраструктуру, включая КИИ РФ, «ведущих зарубежных государств» и террористических и экстремистских организаций. Отмечена тенденция к постоянному повышению сложности, масштабов и скоординированности компьютерных атак на КИИ РФ и растущей активности иностранных разведок. Интернет в проекте Доктрины упоминается вне контекста КИИ, в рамках стратегической цели по обеспечению национального управления российским сегментом Сети. В документе ставится проблема, связанная с «существующим распределением критических интернет-ресурсов» (КИР), которое «не позволяет реализовать справедливое совместное управление ими на принципах межгосударственного доверия». Определение и перечень КИР в проекте Доктрины не приводятся. Из международных направлений деятельности упор сделан на продвижение на международной арене российского подхода по вопросам формирования системы международной информационной безопасности (МИБ), обеспечения стратегической стабильности, предотвращения конфликтов в информационном пространстве и проч. При этом практически не отводится места механизмам международного сотрудничества, обмена практиками и опытом по защите КИИ в рамках существующих площадок и рабочих форматов. Предлагаемая версия Доктрины полностью уходит от освещения роли CSIRT в обеспечении ИБ РФ, в т.ч. в защите КИИ, а также международного взаимодействия в сфере реагирования и управления инцидентами. Наконец, в проекте документа собственники объектов КИИ включаются в число участников системы обеспечения ИБ РФ, но им не отводится какой-либо роли в части саморегулирования, в т.ч. в рамках частного сектора. Проект Доктрины не освещает роль ГЧП в обеспечении безопасности КИИ РФ и не дает отсылок к международным рекомендациям, стандартам и практикам в этой части.

Альтернативный регуляторный дискурс и деятельность, направленная на выработку подхода к регулированию инфраструктуры Интернета как отдельной отрасли в контексте КИИ начали прорабатываться в РФ начиная с 2012-2013 г. В

[27] Доктрина информационной безопасности Российской Федерации (проект). Совет Безопасности Российской Федерации. http://www.scrf.gov.ru/documents/6/135.html.

июле 2014 г. были по поручению президента РФ проведены первые масштабные киберучения Минкомсвязи РФ с участием ФСБ, ФСО, Минобороны, МВД, Ростелекома, КЦ .RU/.РФ, крупнейшей российской точки обмена трафиком (IXP) MSK-IX и других организаций. Тематикой учений стало обеспечение устойчивости национального сегмента сети Интернет в условиях целенаправленных воздействий. Цикл подготовки учений составил недели, в течение которых с участием представителей госструктур и ряда организаций телекоммуникационной отрасли РФ была сформирована модель угроз, которая во многом совпадала с моделью угроз устойчивому функционированию Интернета, разработанной ENISA с 2008 г.[28] Дальнейшая подготовительная работа к учениям велась в рамках межведомственной рабочей группы более узкого состава, в которую из числа внешних участников вошли представители КЦ .RU/.РФ, ТЦИ, MSK-IX и Ростелекома. Был согласован высокоуровневый сценарий учений и временные регламенты взаимодействия участников учений по различным видам угроз. Отработка регламентов взаимодействия велась в течение 5 дней между дежурными сменами привлеченных к учениям организаций под координацией Ситуационного центра Роскомнадзора (в части масштабных DDoS-атак), а также Центра реагирования на компьютерные инциденты ФСБ РФ (GOV-CERT.RU). Учения проводились на обособленной инфраструктуре, для того чтобы избежать возможного воздействия на работу сетей и инфраструктуры российского сегмента Интернета, предоставляющих сервисы населению, предприятиям и структурам государственного управления.

Непосредственно учения проводились в течение восьми часов 26 июля 2014 г, после частных учений с привлечением руководства задействованных организаций 25 июля. Инфраструктуру для проведения учений предоставили MSK-IX, ТЦИ и Ростелеком. В рамках учений были смоделированы и отработаны следующие сценарии угроз:

- Угрозы DNS: отказ авторитативных серверов DNS, обслуживающих российские национальные домены; подмена DNA-сервера (атака «cash poisoning»), подмена ресурсных записей (RRs) в российских зонах национальных доменов.
- Угрозы реестрам адресации: недоступность реестра адресации RIPE NCC, подмена записей о выделенных российским сетевым операторам ресурсах нумерации (IP-адресах и AC) в реестре RIPE NCC.
- Угрозы маршрутизации интернет-трафика: угрозы утечки маршрутов BGP (BGP leak), т.е. утечки префиксов IP-адресов и номеров AC.
- Угрозы отказа в обслуживании: угроза крупномасштабных DDoS-атак на критическое оборудование национального сетевого оператора, инфраструктуру IXP, российского сегмента DNS и проч.
- Угроза инфраструктуре международного обмена трафиком: отказ доступа / отказ трансграничных каналов обмена трафиком и отказ в обслуживании для российских сетевых операторов на международной точке обмена трафиком.

Выбор угроз для отработки осуществлялся на основе сочетания двух параметров: возможного воздействия инцидента на инфраструктуру и сервисы, а также риска развития такого инцидента. Таким образом, в итоговый сценарий учений были

[28] Обновленную методологию ENISA по выявлению и систематизацию угроз устойчивому функционированию инфраструктуры Интернета см. в материале: Threat Landscape and Good Practice Guide for Internet Infrastructure January 2015. ENISA, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure.

включены и те угрозы, риск реализации которых оценивался как низкий, однако потенциальный ущерб являлся неприемлемым (отказ трансграничных каналов или отказ в обслуживании на международной IXP). По данным экспертов, принимавших непосредственное участие в подготовке и проведении учений:

- Основные опасения, связанные с тем, что смоделированные и отработанные в ходе учений угрозы повлекут сетевую фрагментацию Рунета и его распад на отдельные слабо связанные между собой сети с последующей деградацией сервисов, не подтвердились. Российский сегмент Интернета оказался способен выдержать смоделированные угрозы без утраты связности.
- Была выявлена недостаточная координация действий между субъектами, ответственными за кризисное реагирование на подобные инциденты. Полное восстановление функционирования сервисов и сетей, на которых моделировались инциденты, заняло достаточно продолжительное время. В качестве возможной меры по улучшению ситуации была названа разработка сетевыми операторами регламентов действий в условиях кризисных ситуаций.
- Учения подтвердили необходимость создания в России собственных центров экспертизы по защите КИИ для поддержки экспертного сообщества и сообщества отраслевых специалистов и площадок для взаимодействия технического сообщества.
- Была отмечена важность проведения систематических исследований, наблюдений и мониторинга российского сегмента сети Интернет и «критических ресурсов Интернета».

Однако в интервью по итогам учений помощник президента РФ Игорь Щеголев подчеркнул, что управление глобальным интернетом до сих пор сконцентрировано в руках США. Видимо, имелась в виду роль Администрации адресного пространства интернета (IANA) в управлении верхним уровнем системы DNS (корневая зона DNS), а также распределении блоков ресурсов нумерации между РРИ и гипотетически обусловленная этим возможность внешних целенаправленных воздействий на инфраструктуру Рунета, санкционированных на государственном уровне.

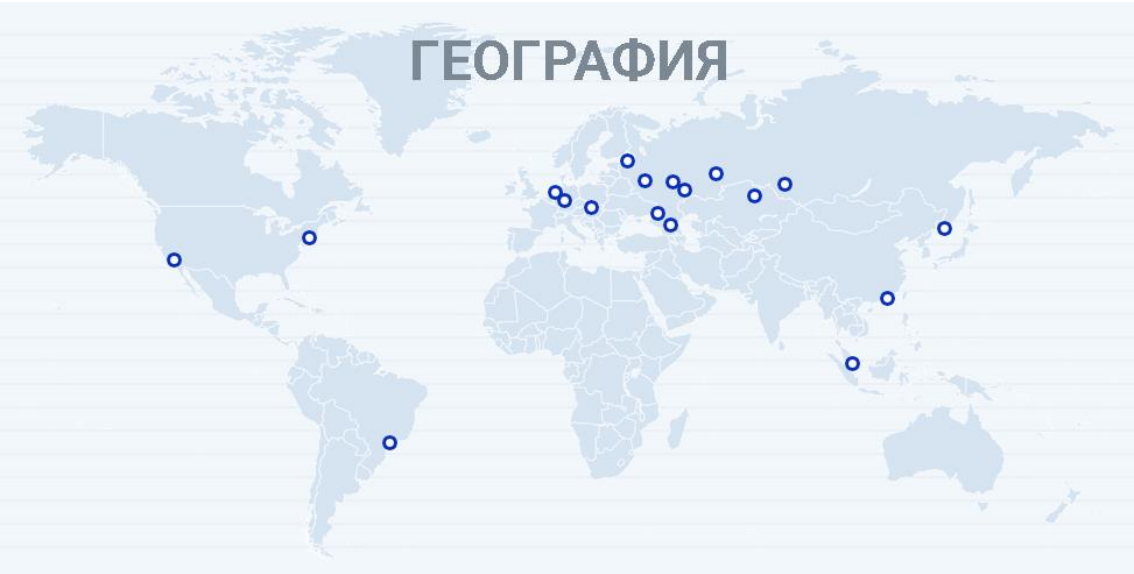
По итогам учений в августе 2014 г. был подготовлен доклад президенту РФ. Также киберучений обсуждались в закрытом формате на заседании Совета Безопасности РФ в сентябре 2014 г. В апреле 2015 г. главой Минкомсвязи РФ Н.А. Никифоровым подготовлен доклад для правительства РФ, посвященный вопросам обеспечения безопасности и устойчивости российского сегмента Интернета и отражающий итоги учений. В докладе отмечалась необходимость резервирования данных из системы корневых DNS-серверов и создания дублирующего реестра IP-адресов. Задача создания дублирующего реестра информации, необходимой для разрешения DNS-запросов к ресурсам в доменах .RU и .РФ отмечалась не только в докладе Минкомсвязи. Осенью 2014 г. о работе в этом направлении сообщали представители КЦ .RU/.РФ и Технического центра Интернет.

Наконец, в феврале 2016 г. стало известно о подготовке на площадке Минкомсвязи РФ новых законотворческих инициатив, преследующих целью повышение устойчивости и защищенности «критических элементов российской части сети Интернет» и вводящих определение этого понятия. Подробный анализ упомянутых инициатив не входит в задачи настоящего исследования, так как

формально проекты соответствующих документов в медийном поле не появлялись. Но следует обратить внимание на тот факт, что на сегодняшний день по ряду позиций инфраструктура Рунета относится к числу наиболее распределенных, высокосвязанных, устойчивых и защищенных среди всех условных национальных сегментов глобального Интернета. В том числе:

> Домен .RU с 5,3 млн доменных имен второго уровня является пятым по популярности страновым доменом в мире (ccTLD) и входит в топ-10 крупнейших доменов вообще; кириллический домен .РФ с порядка 900 тыс. доменных имен второго уровня является крупнейшим интернационализированным доменом верхнего уровня. При этом серьезных инцидентов, связанных с нарушением доступа к ресурсам в доменах .RU и .РФ, за всю историю существования этих страновых доменов зафиксировано не было. Инфраструктуру для поддержки системы авторитативной DNS для российских доменов .RU, .РФ, все еще действующего домена верхнего уровня для СССР - .SU, а также доменов верхнего уровня .ДЕТИ, .TATAR) предоставляет крупнейшая российская точка обмена трафиком MSK-IX на базе распределенного программно-аппаратного комплекса MSK-IX DNS Cloud, поддерживающего anycast. Сеть DNS Cloud распределена глобально, имеет 18 точек присутствия (PoPs), из которых 9 размещено в России, остальные в Европе, Азии, Северной и Южной Америке и непосредственно доступен для более чем со 100 сетевых операторов.
>
> При этом представители Технического Центра Интернет (ТЦИ – дочерняя структура АНО «Координационный центр национального домена сети интернет») уже осенью 2014 г. сообщали СМИ о том, что по собственным внутренним соображениям провели и завершили работу по формированию резервного реестра доменной информации, включая зоны .RU и .РФ.

*Карта №1: Карта узлов распределенной сети MSK-IX, обеспечивающей поддержку авторитативной DNS для российских страновых доменов*




Источник: MSK-IX. Авторитативный DNS. http://www.msk-ix.ru/dns/ (последнее посещение 15.07.2016).

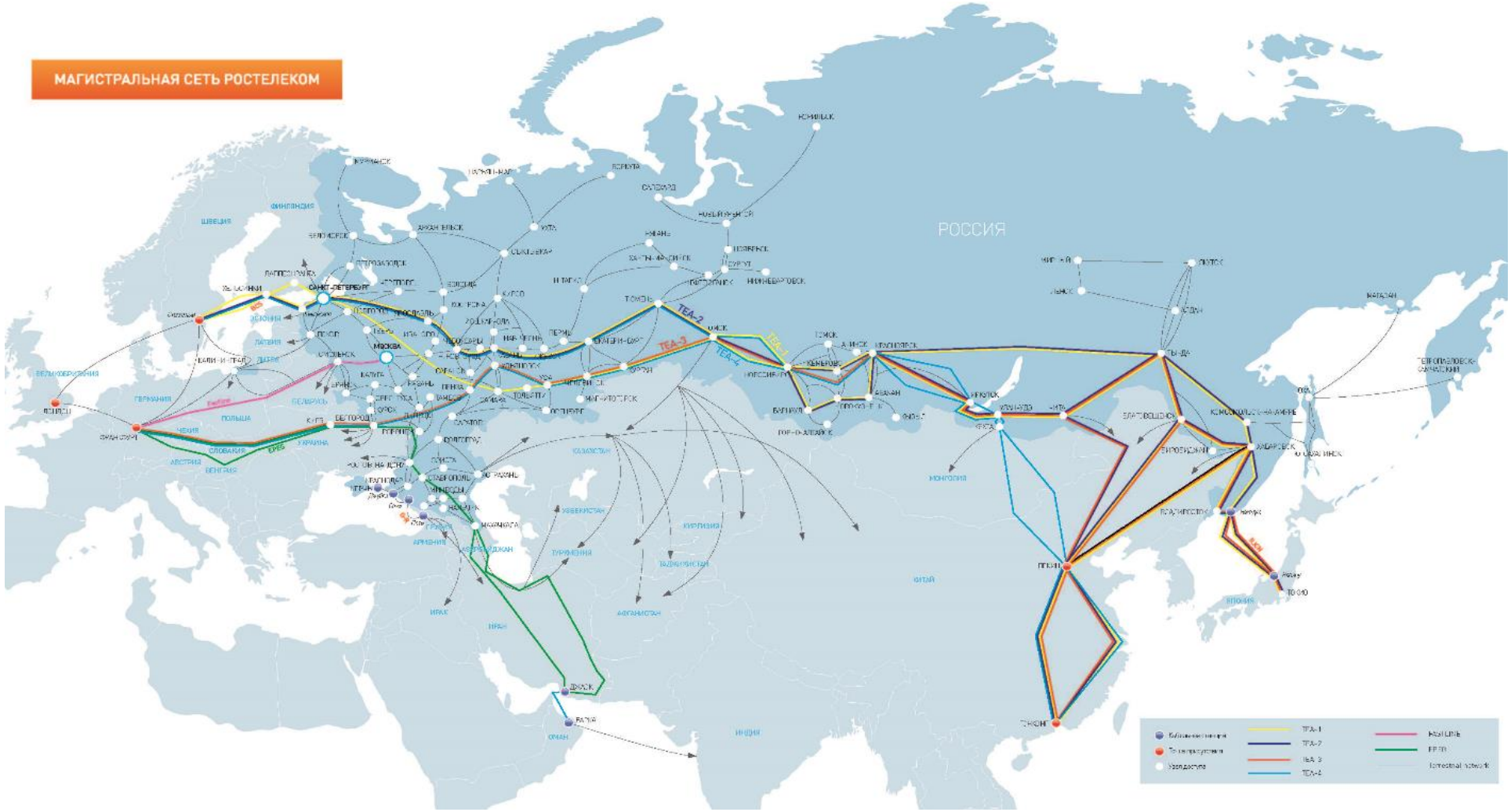
2) В плане топологии физических каналов (прежде всего магистральные ВОЛС) Рунет относится к числу диверсифицированных и устойчивых национальных сегментов Интернета с высоким уровнем связности. Такая оценка подтверждается исследованиями устойчивости национальных сегментов Интернета. Согласно исследованию компании Qrator Labs, специализирующейся на противодействии DDoS-атакам, Рунет занимает третье место в мире среди национальных сегментов Интернета. В основу оценки была положена методология определения потенциальной единой «точки отказа» в лице крупнейшего национального интернет-провайдера. Роль оператора в обеспечении связности национального сегмента Интернета оценивалась с помощью карты сетевых префиксов для Рунета, которая показывает, сколько других российских провайдеров осуществляют внешнюю маршрутизацию своего трафика с использованием префиксов номеров АС, делегированных такому оператору (т.е. через его АС). В российском сегменте Интернета крупнейшим оператором является Ростелеком, в распоряжении которого (с учетом региональных структур и подразделений) находится 98 АС. Масштабный сбой в работе сетевой инфраструктуры Ростелекома и полная потеря возможности передавать трафик через его АС привела бы к глобальной недоступности не более 5,5% сетей российского сегмента интернета. Более низкие показатели имеют лишь Великобритания (3,4 % сетей будут недоступны в случае отказа инфраструктуры Virgin Media) и США (5% сетей потеряют доступность без провайдера TATA).

3) На картину связности Рунета, отраженную в исследовании, накладывает отпечаток исторически сложившаяся практика высокой диверсификации используемых сетевыми операторами ресурсов нумерации именно на уровне АС. В настоящее время Россия лидирует по числу АС, используемых ее операторами – российским операторам были делегированы порядка 5600 номеров АС из 75000, делегированных по миру в целом (7,46%), при том что Рунет существенно уступает китайскому, индийскому и американскому сегменту по количеству пользователей. Отмеченное положение вещей является следствием высокой конкуренции на всех уровнях телекоммуникационного рынка в России. В результате каждый даже самый небольшой оператор связи имеет альтернативные варианты подключения своей сети к сетям более «серьезных» игроков, а также к сетям себе подобных, что порождает необходимость наличия собственного блока IP-адресов и соответствующей АС.

   Также для Рунета характерна практика непосредственного обмена трафиком между крупными операторами в разных точках и практический отказ от использования точек обмена трафиком в качестве посредника для связи между крупными операторами (прежде всего, имея в виду топ-5 российских сетевых операторов: Ростелеком, Мегафон, МТС, Вымпелком (Билайн) и Трансгелеком (ТТК)). При этом практически все ведущие операторы присутствуют на крупнейших международных точках обмена трафиком, включая LINX (Лондон), AMS-IX (Амстердам), DE-CIX (Франкфурт-на-Майне), Netnod (Стокгольм), ESPANIX (Мадрид), MIX (Милан), France-IX (Париж) и проч. В последние годы отмечается усиление присутствия крупнейших российских операторов на азиатских IXPs, включая Гонконг (HKIX) и Токио (Equinix). Примером служит

развитие магистральной сети ПАО «Ростелеком», в том числе с учетом модернизации MPLS IP-магистрали в 2012-2014 гг. Магистральная сеть Ростелекома сегодня имеет четыре зарубежные точки присутствия (PoPs) (Лондон, Стокгольм, Франкфурт-на-Майне, Гонконг) и порядка 20 трансграничных переходов (см. карту ниже).

*Карта MPLS-сети ПАО «Ростелеком» с зарубежными фрагментами и точками присутствия за рубежом*




Источник: Магистральная сеть ПАО «Ростелеком». Вебсайт ПАО «Ростелеком», http://www.rt.ru/data/doc/backbone_map.pdf.

Магистральная цифровая сеть связи (МЦСС) (и опирающаяся на нее сеть MPLS IP) ЗАО «Трансгелеком» (ТТК) имеет точки взаимодействия с сетями операторов Финляндии, государств Балтии, Польши, Белоруссии, Украины, Азербайджана, Казахстана, Монголии, Китая и Японии. На сети оператора имеется не менее 14 трансграничных переходов.

*Карта магистральной цифровой сети связи (МЦСС) ЗАО «Трансгелеком»*


Источник: Магистральная цифровая сеть связи ТТК. Вебсайт ТТК-Урал. https://www.uralttk.ru/net/ttk/.

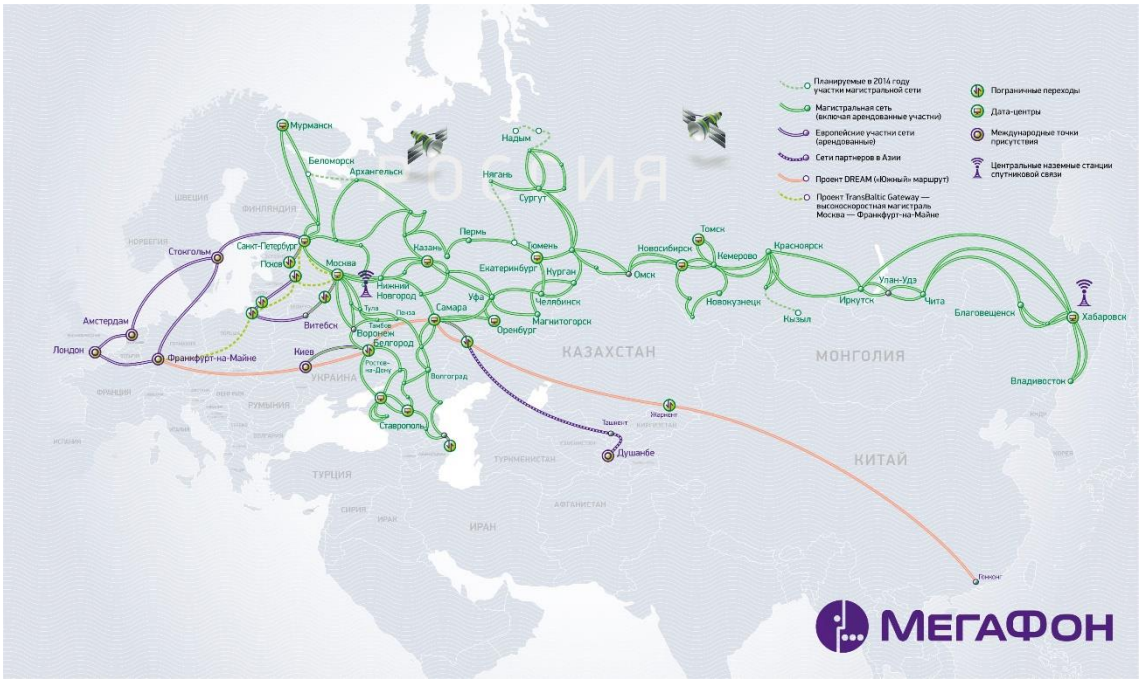
Магистральная сеть ПАО «МТС» имеет не менее пяти трансграничных переходов (четыре в европейской части РФ и один на Дальнем Востоке).

*Карта магистральной сети ПАО «МТС»*

Источник: Ольга Макарова. Уязвимость Интернета: мифы и реальность, Индекс Безопасности, № 4 (115), Том 21, стр. 75-98, http://pircenter.org/media/content/files/13/14513991300.pdf.

На магистральной сети ПАО «Мегафон» насчитывается девять трансграничных переходов (семь в европейской части страны, по одному в Закавказье и в ЦА); сеть оператора имеет доступ к шести PoPs в Стокгольме, Амстердаме, Лондоне, Франкфурте-на-Майне, Киеве и Душанбе.

*Карта магистральной сети ПАО «Мегафон»*



Источник: Карта магистральной сети. Вебсайт ПАО «Мегафон». http://moscow.megafon.ru/ai/html/4391/files/mgfon-MAP_RU_v45.jpg.

Сочетание прямого обмена трафиком между крупнейшими сетевыми операторами и активных присутствия таких операторов на ведущих международных точках обмена трафиком, обеспечивает условия для сбалансированной, с точки зрения устойчивости, архитектуры национального сегмента Интернета. С одной стороны, интенсивный прямой обмен трафиком между крупными операторами внутри страны по сравнению с архитектурой взаимодействия только через IXP позволяет увеличить количество маршрутов обмена трафиком и повысить устойчивость национального сегмента на уровне маршрутизации трафика в пределах РФ. С другой стороны, активное присутствие на международных IXP крупнейших операторов при наличии существенного количества трансграничных каналов обеспечивает более высокий уровень связности национального сегмента с глобальным Интернетом при сохранении высокой степени локализации пропуска национального интернет-трафика в пределах национального же сегмента. По оценкам представителей крупнейших российских операторов связи доля национального интернет-трафика, маршрутизируемого исключительно в пределах территории России, в настоящее время практически равна 100%. В связи с этим вызывает удивление оценка Микомсвязи в 75% по итогам 2015 г.[29].

[29] См.: целевой индикатор «Доля объема национального интернет-трафика, маршрутизируемого, пропускаемого и терминируемого в пределах территории Российской Федерации» в тексте документа: Проект Постановления Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской Федерации от 15

Устойчивость Рунета в смысле отсутствия «единой точки отказа» в лице критического национального оператора также обуславливается тем, что Ростелеком, будучи крупнейшим в стране сетевым оператором, тем не менее далеко не является монополистом по критерию совокупной длины магистральных ВОЛС. По состоянию на начало 2016 г. в управлении Ростелекома находилось порядка 520 тыс. км линий магистральных ВОЛС, что примерно соответствует суммарному показателю следующих четырех крупнейших операторов (Транстелеком, Мегафон, МТС, Билайн (Вымпелком)).

Кроме того, общая топология Рунета в плане физических каналов характеризуется наличием относительно большого числа трансграничных переходов. Точное число таких переходов назвать затруднительно в связи с несовершенством процедуры их учета государством. Формальным механизмом учета служит Реестр выданных и аннулированных разрешений на строительство, реконструкцию, проведение изыскательских работ для проектирования и ликвидацию сухопутных линий связи при пересечении государственной границы Российской Федерации и на приграничной территории, который ведет Роскомнадзор[30]. По состоянию на конец июля 2016 г. в первой части реестра насчитывалось 74 выданных разрешения на строительство линий связи при пересечении госграницы, в том числе:

- ОАО «Мобильные ТелеСистемы» – 11 разрешений;
- ЗАО «ТрансТелеком» – девять разрешений;
- ПАО «Ростелеком» – семь разрешений;
- ОАО «Северо-Западный Телеком» – пять разрешений;
- ПАО «Вымпел-Коммуникации» – два разрешения;
- ПАО «МегаФон» – семь разрешений (включая шесть разрешений, выданных ЗАО «Синтерра», которое было присоединено к ПАО МегаФон в 2011 году).

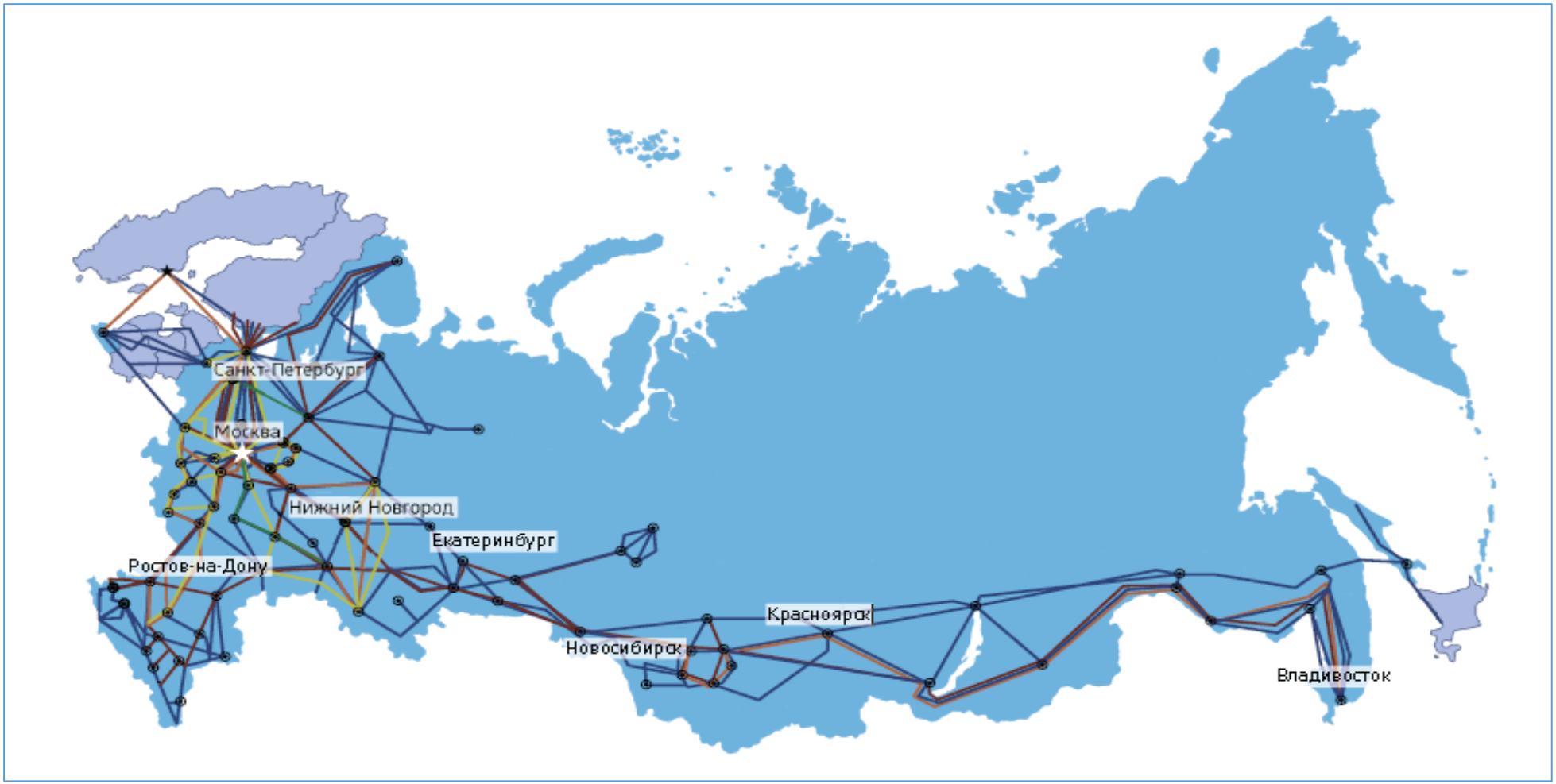
Однако число разрешений в реестре РКН не в полной мере характеризует количество трансграничных переходов операторов связи, так как при оформлении заявки на получение разрешения в ней единожды указывается какой-либо сетевой оператор, а впоследствии инфраструктура перехода может использоваться и другими организациями. Также реестр РКН охватывает лишь сухопутные трансграничные переходы и не распространяется на морские лини связи, стыкующиеся с сетями зарубежных операторов. В итоге реальное количество трансграничных переходов по оценкам отраслевых экспертов может достигать 150-200. В любом случае, речь идет о весьма значительном по мировым стандартам показателе. Диверсификация трансграничных переходов служит одним из существенных условий устойчивости национального сегмента Сети. Помимо использования собственных трансграничных переходов, российские операторы с 2010-х гг. все более активно арендуют каналы у существующих игроков до крупнейших телехаусов Европы.

---

апреля 2014 г. № 3132 (подготовлен Минкомсвязью России 28.12.2015), Гарант.ру, http://www.garant.ru/products/ipo/prime/doc/56557521/#ixzz4FrKaCMKF.

[30] Реестр выданных и аннулированных разрешений на строительство, реконструкцию, проведение изыскательских работ для проектирования и ликвидацию сухопутных линий связи при пересечении государственной границы Российской Федерации и на приграничной территории. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), http://rkn.gov.ru/communication/register/p191/.

*Карта №2. Основные магистральные ВОЛС и трансграничные переходы на территории РФ*




Источник: Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества / Олег Демидов. — М.: Альпина Паблишер, 2016. –196 с. – стр. 30.

С учетом приведенных выше данных, возникающий время от времени в обсуждениях на разных уровнях тезис о недостаточной устойчивости и защищенности инфраструктуры и сервисов российского сегмента Интернета должен требовать детальных обоснований.

Также в пояснениях и обоснованиях нуждаются сформулированные в упомянутом выше, официально не опубликованном пока проекте закона предложения по отнесению к «критическим элементам, имеющим существенное значения для обеспечения безопасности функционирования, устойчивости и целостности российской части сети Интернет» ряда объектов, не относящихся ни к инфраструктуре, ни к (жизненно важным) услугам. В частности, речь идет об АС, делегированных российским операторам связи. АС являются не физическими, а логическими объектами, используемыми для оптимизации сетевой междоменной маршрутизации, осуществляемой на основе протокола прикладного уровня BGPv4.

Изначально, как было сформулировано в RFC 1771[31], понятие АС означало группу из одного или нескольких префиксов IP, работающих у одного сетевого оператора (интернет-провайдера или иной крупной организации, имеющей независимые множественные подключения к внешним сетям), которые имеют единую и четко определенную политику маршрутизации. Такое определение стало расходиться с практикой по мере того как различные организации получили возможность использовать Протокол граничного шлюза (BGPv4), предоставляя свои внутренние номера АС интернет-провайдерам, которые обеспечивали для них доступ в Интернет. Эти изменения обусловили нынешний подход к определению и стандартизации АС: даже если сетевой оператор поддерживает множество АС, ключевым критерием уникальной сущности, представленной и идентифицируемой в Интернете, является единая политика маршрутизации, которую осуществляет такой оператор. Соответственно, в RFC 1930 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.[32]

По этой причине представляется некорректным введение категории регулируемых объектов «инфраструктура АС». Оборудование маршрутизации, установленное у сетевого оператора, может перенастраиваться, заменяться и обновляться без какой-либо связи с изменением его АС. С другой стороны, получение оператором новых номеров АС и префиксов IP-адресов, изменение им политики маршрутизации также могут происходить при сохранении прежней инфраструктуры сетевого оборудования. Кроме того, АС, по сути представляя собой назначенные политики использования оператором ресурсов нумерации, не могут укладываться в регуляторные концепции, основанные на идентификации территориально определяемых национальных сегментов Интернета. В качестве примера можно отметить, что многие крупнейшие российские сетевые операторы имеют зарубежные фрагменты магистральных сетей и точки присутствия; при этом для такой трансграничной инфраструктуры зачастую используются те же политики маршрутизации (и соответственно АС), что и для на сетях в пределах

[31] A Border Gateway Protocol 4 (BGP-4). Request for Comments: 1771. March 1995. IETF, https://tools.ietf.org/html/rfc1771.

[32] См.: Рабочая группа по проектированию Интернет (IETF), http://tools.ietf.org/html/rfc1930.

территории РФ. С учетом сказанного, некорректным и не применимым в рамках регулирования передачи данных через трансграничные каналы представляется понятие «АС, непосредственно взаимодействующей с АС иностранного государства».

Наконец, нужно подчеркнуть, что рассмотренные подходы зарубежных государств и МО не содержат примеров причисления АС и иных логических объектов к КИИ или критическим элементам национального сегмента Интернета. Существующая практика в максимально обобщенном виде может подразделяться на два подхода: 1) регулирование КИИ, т.е. инфраструктуры программно-аппаратных комплексов, обеспечивающих функционирование КВО, и каналов передачи данных между такими комплексами; 2) регулирование жизненно важных услуг (ЖВУ) – сервисов и служб, обеспечиваемых за счет той или иной инфраструктуры. Регулирование сетевых логических объектов не попадает ни в один из этих подходов и таким образом оказывается оторван от международных лучших практик. В определенной степени эти замечания применимы и к идее отнесения к критическим элементам непосредственно страновых доменов верхнего уровня (ccTLD). ЕС, Германия и ряд других государств включают в состав КИИ / операторов жизненно важных услуг инфраструктуру ccTLD – а именно, авторитативные серверы DNS верхнего уровня, а также сети DNS-резолверов, поддерживающие соответствующие страновые домены. Однако сами по себе доменные зоны ни в одной страновой/международной практике не причисляются к КИИ/ЖВУ.

Основная причина состоит в том, что попытка включить страновые домены как таковые в список ключевых элементов национальной инфраструктуры в определенной степени противоречит существующей международной практике управления DNS как глобальной иерархически распределенной на логическом и инфраструктурном уровне базой данных. Создание и делегирование страновых зон верхнего уровня в рамках устоявшейся процедуры осуществляется Корпорацией Интернета по присвоению имен и адресов (ICANN) (с техническим участием Verisign) путем генерации и рассылки операторам 13 корневых серверов DNS файла корневой зоны DNS (RZF) с обновляемым списком доменов верхнего уровня. Т.е. первичные записи, содержащие информацию о российских ccTLDs, создаются в юрисдикции США и рассылаются операторам корневых серверов DNS по всему миру (с учетом «зеркал», дублирующих авторитативные серверы), и поддерживаются ими вне российской юрисдикции. Именно на операторах корневых серверов DNS лежит задача по обеспечению БСО поддерживаемой ими инфраструктур и защите хранящихся в них данных. Таким образом, национальное регулирование страновых доменов верхнего уровня как ключевых элементов национального сегмента Сети представляется заведомо неэффективным, особенно в рамках регуляторного подхода, основанного на выделении территориально ограниченных национальных сегментов сети Интернет.

## Япония

В Японии регулирование Интернета в частности и всей телекоммуникационной отрасли в целом осуществляется преимущественно в рамках Закона о телекоммуникационном бизнесе[33], а профильным регулятором является Министерство внутренних дел и коммуникаций (МВДК)[34]. Кроме того, нормативные акты для отрасли разрабатывает антимонопольное ведомство - Комиссия по справедливой торговле Японии (КСТЯ)[35]. МВДК и КСТЯ в 2001 г. вместе выпустили Регулирование по развитию конкуренции в области телекоммуникационного бизнеса[36].

Под «критической инфраструктурой» в Японии понимаются бизнесы и структуры, предоставляющие сервисы, заменить которые в случае прекращения или ухудшения их работы было бы крайне трудно, и прекращение (ухудшение) работы которых значительно повлияло бы на социальную жизнь населения и деловую активность[37]. Сюда относятся:

- Передача данных;
- Финансы;
- Авиалинии;
- Железная дорога;
- Электроэнергетика;
- Газовая отрасль;
- Государственные и административные услуги;
- Медицинские услуги;
- Водоснабжение;
- Перевозки.

К операторам критических информационно-коммуникационных инфраструктур (КИИ) относятся основные телеком-операторы и основные телевещательные компании. Эти два типа инфраструктур регулируются по-разному, хотя и те, и другие относятся к критическим. Телекоммуникационные услуги – то есть, передача и получение кодов, звуков или изображений с помощью кабельной связи, радиоволн или других способов передачи данных путем электромагнитных волн – отличает защита конфиденциальности переданного через них контента.[38] Это приводит к тому, что телекоммуникационная отрасль регулируется довольно слабо, в то время как телевещание регулируется исходя из принципа общественного блага[39].

---

[33] Telecommunications Business Law (Law No. 86 of December 25, 1984). Ministry of Internal Affairs and Communications, Japan (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/2001TBL.pdf)
[34] Ministry of Internal Affairs and Communications (MIC), http://www.soumu.go.jp/.
[35] Japan Fair Trade Commission, www.jftc.go.jp.
[36] http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/010914_1.html
[37] The Second Action Plan on Information Security Measures for Critical Infrastructures. February 3, 2009. The Information Security Policy Council (http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf)
[38] Telecommunications Business Law (Law No. 86 of December 25, 1984). As amended last by: Law No. 125 of July 24, 2003 (Unofficial Translation). 2003, Ministry of Internal Affairs and Communications, Japan. Article 78 “Confidentiality, Etc.” (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/2001TBL.pdf)
[39] The Broadcast Act (Act No. 132 of 1950). As amended last by the Act for Partial Revision of the Broadcast Act and Other Related Acts (Act No. 65 of 2010) (Unofficial Translation http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_5.pdf)

Определение оператора телекоммуникационной инфраструктуры как оператора КИ влечет за собой требование следовать определенным стандартам. Например, сбой в работе телекоммуникационной системы не должен вызвать остановки в предоставлении услуг или значительного ухудшения качества их предоставления более чем на 2 часа или более чем для 30 тыс. пользователей.[40]

Агентство для продвижения информационных технологий (IPA)[41] в 2010 г. выпустило подробный справочник по оценке нефункциональных требований к информационным системам, в котором приводятся параметры для оценки критичности информационных систем в инфраструктурах.[42] Параметры разбиты на следующие основные категории: доступность, производительность и масштабируемость, функциональность и восстановление работоспособности, способность к перегруппировке, безопасность, среда установки системы и экологичность. Выделяется три модели систем:

1) не имеющие социальной значимости;
2) имеющие ограниченную социальную значимость;
3) имеющие ощутимую социальную значимость.

Последняя модель по определению является моделью для критических инфраструктур – то есть, таких, которые при ухудшении качества или отсутствии возможности обслуживания будут иметь серьезное влияние на жизни или социо-экономическую активность граждан страны.[43]

При выработке системы оценки нефункциональных требований IPA опиралось на международный стандарт ISO/IEC 9126 «Программирование. Качество продукта», однако между ними есть и различия: например, в японской системе оценки не учитываются такие факторы, как пригодность, точность, совместимость, понятность, привлекательность для пользователя, модифицируемость, стабильность, пригодность для тестирования, которые есть в стандарте ISO/IEC 9126.

IPA также опубликовало отдельную инструкцию по использованию системы оценки нефункциональных требований[44].

В Общей политике в отношении защиты критической информационной инфраструктуры, принятой правительством Японии в 2015 г., к КИИ относятся информационно-коммуникационная инфраструктура, электро-, водо- и газоснабжение, финансовая, авиационная, железнодорожная, логистическая инфраструктуры, медицинская и нефтяная отрасли, государственные услуги и

[40] The Second Action Plan on Information Security Measures for Critical Infrastructures. February 3, 2009. The Information Security Policy Council. Appendix 2 (http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf)
[41] IPA. Better Life with IT, https://www.ipa.go.jp/index-e.html.
[42]Non-Functional Requirements Grades Usage Guide [Description Manual]. Information-Technology Promotion Agency, Japan Software Engineering Center. April 2010 (https://www.ipa.go.jp/files/000027768.pdf).
[43] Non-Functional Requirements Grades Usage Guide [Description Manual]. Page 14.
[44] Non-Functional Requirements Grades Usage Guide [Usage Manual]. ]. Information-Technology Promotion Agency, Japan Software Engineering Center. April 2010 (https://www.ipa.go.jp/files/000027769.pdf).

обслуживание кредитных карт[45]. К информационно-коммуникационным службам, согласно этой политике, относятся службы кабельного телевидения, электросвязи и вещания.

Таким образом, интернет, относящийся к электросвязи, не обособляется как отдельная критическая инфраструктура или как критическая информационная инфраструктура. Информационные системы, системы управления объектами КИ называются КИИ.

В соответствии с Базовым актом по кибербезопасности, операторы КИИ обязаны не только приоритетно обеспечивать кибербезопасность своих объектов, но и сотрудничать с местными и национальными властями в этом вопросе. Такое же требование предъявляется к предприятиям, имеющим отношение к киберпространству (то есть, занимающиеся обслуживанием интернет-инфраструктуры и других информационных и телекоммуникационных сетей, а также занимающиеся кибербезопасностью).[46]

Национальные органы государственного управления, административные учреждения, специальные корпорации должны, кроме прочего, проводить учения и тренинги по кибербезопасности и обмениваться соответствующей информацией с другими органами, агентствами и предприятиями внутри государства, а также с зарубежными сторонами.[47]

В соответствии с Базовым актом по кибербезопасности, правительство Японии приняло и обновляет Стратегию кибербезопасности[48]. Этот документ определяет роль различных заинтересованных сторон в обеспечении информационной безопасности государства – в частности, безопасности критической информационной инфраструктуры. В Стратегии подчеркивается, что невозможно обеспечить кибербезопасность критических инфраструктур силами одного только правительства, и такая же мысль проходит через все планы действий по ИБ критических инфраструктур.[49] Защитой КИИ, согласно Стратегии кибербезопасности, должны заниматься операторы КИИ и профильные для этих операторов министерства. Сюда относятся секретариат правительства, Агентство финансовых услуг, МВДК, Министерство благосостояния и труда, Министерство экономики и промышленности (МЭП), Министерство земли и транспорта – эти министерства координируют отрасли, в которых есть те или иные критические инфраструктуры. Собственно информационной безопасностью занимаются МВДК, Национальное полицейское агентство, МЭП и Министерство обороны.

Операторы и министерства должны вырабатывать стандарты безопасности и эксплуатационного обслуживания, проводить учения. К примеру, МЭП

---

[45] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (Tentative Translation) May 19, 2014 Information Security Policy Council, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf.

[46] The Basic Act on Cybersecurity (Tentative translation). Act No. 104 of November 12, 2014. Articles 6, 7. (http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&x=0&y=0&co=01&ia=03&ky=%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3&page=1)

[47] The Basic Act on Cybersecurity. Article 13.

[48] Provisional Translation CYBERSECURITY STRATEGY September 4, 2015 Cabinet Decision The Government of Japan, http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

[49] The Second Action Plan on Information Security Measures for Critical Infrastructures (http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf)

предлагает тренинг по кибер-рискам, разработанный Научно-исследовательским институтом Мицубиси и нацеленный на обучение реагированию на реальные кибер-атаки, осуществленные с целью приостановки работы и/или причинения ущерба системам управления критическими инфраструктурами. МВДК совместно с банками проводит программу CYDER (Cyber Defence Exercise with Recurrence), целью которой является увеличение потенциала реагирования на происшествия в локальных сетях.[50] С 2006 г. проводятся совместные учения, организованные Национальным центром информационной безопасности (NISC) по программе CEPTOAR (Capability for Engineering of Protection, Technical. Operation, Analysis and Response)[51]. Для каждой группы КИ существует свой CEPTOAR. Основной целью CEPTOAR является организация обмена информацией, касающейся угроз информационной безопасности, между государственными и негосударственными органами, агентствами и операторами КИ.

Для телекоммуникационной отрасли такие функции выполняет T-CEPTOAR. Основанный в 2007 г., по состоянию на 2016 г. он объединяет 24 организации, среди которых операторы сетевой инфраструктуры, телекоммуникационные компании, мобильные и интернет-операторы.[52] Ежемесячно T-CEPTOAR проводит встречи для обмена информацией.
Система уведомления об инцидентах информационной безопасности на КИ в Японии включает в себя следующие организации:

1) Национальный центр реагирования на инциденты (National Incident Response Team, NIRT), являющийся частью Группы реагирования на компьютерные инциденты (CERT).[53] В состав NIRT входят 17 правительственных и неправительственных экспертов, которые анализируют инциденты, разрабатывают стратегии для разрешения экстренных ситуаций и для предотвращения повторения инцидентов, предоставляют другим государственным организациям помощь в решении вопросов, связанных с информационной безопасностью и др.
2) Координационный центр японской группы реагирования на компьютерные инциденты (JCERT/cc) – первый в Японии CSIRT.[54] В его состав входят поставщики интернет-услуг, решений и услуг для информационной безопасности, государственные агентства и отраслевые ассоциации. Центр координирует меры обеспечения информационной безопасности.
3) Кибер-отряд в Национальном полицейском агентстве[55] – специализируется в основном на борьбе с киберпреступностью, но также оповещает операторов КИИ о случаях нестандартного использования интернета в целях предотвращения террористических кибератак.
4) Министерство экономики и промышленности – взаимодействуя с JCERT/cc и IPA выпускает отчеты о компьютерных инцидентах, вирусных угрозах и причиненном ими ущербе.

[50] The Japanese Min of Internal Affairs and Communications conducted the first cyber exercise with four ministries and private companies including Hitachi. SHILED Security Research Center, Sep 26, 2013, http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-052-en.html.
[51] По сути, аналог ISAC в США.
[52] http://www.nisc.go.jp/conference/cs/ciip/dai05/pdf/05shiryou04.pdf
[53] http://www.nisc.go.jp/itso/shoukai/nirt/
[54] https://www.jpcert.or.jp/
[55] https://www.npa.go.jp/cyberpolice/english/action02_e.html

Помимо перечисленных выше институтов, образованных из представителей государственных ведомств и частных компаний, в Японии существует Стратегический штаб по кибербезопасности, создание которого предусмотрено в Базовом акте по кибербезопасности (поправки от 2014 г.)[56]. Штаб возглавляет главный секретарь Кабинета министров Японии, в состав штаба также входят министр иностранных дел, глава Национальной Комиссии общественной безопасности, министр внутренних дел и коммуникаций, министр экономики, министр обороны и другие министры, а также эксперты, которых в состав штаба может включить премьер-министр Японии. Среди задач штаба – разработка Стратегии кибербезопасности.

В мае 2015 г. штаб опубликовал обновленные Директивы для установления стандартов безопасности КИИ.[57] Эти директивы предлагают операторам КИ план действий для формирования и обновления стандартов безопасности в каждом секторе КИ.

В 2016 г. правительство Японии анонсировало создание Агентства для содействия развитию кибербезопасности промышленных объектов[58]. Агентство должно стать неправительственным органом, аффилированным с Министерством торговли и нацеленным на развитие кадрового потенциала и анализ инцидентов и угроз. На его базе будут проводиться киберучения при участии исследовательских организаций, университетов и зарубежных профильных ведомств.

Атаки на инфраструктуру интернета в Японии

Для борьбы с атаками типа «отравление трафика» на DNS-инфраструктуру Служба регистрации Японии (оператор домена верхнего уровня .JP) предприняла следующие действия:

- Взаимодействие с производителями программного обеспечения для DNS-серверов, требование от них более эффективных мер противодействия
- Взаимодействие с JCERT для обмена информацией и намерениями о дальнейших действиях
- Взаимодействие с основными интернет-провайдерами Японии для обмена информацией и требованием направить потребителям сообщений об инциденте
- Ежемесячное представление в регистратуры информации об уязвимых резолверах и требования о направлении сообщений об инцидентах
- Обмен практиками.[59]

[56] The Basic Act on Cybersecurity. Article 24
[57] Guidelines for the Establishment of Safety Standards of CIIP (4th Edition). Cybersecurity Strategic Headquarters, Government of JAPAN, May 25, 2015 (http://www.nisc.go.jp/eng/pdf/principles_ci_eng_v4.pdf)
[58] 'White hat hackers' top get official support in Japan. Standard Examiner, May 19, 2016 (http://www.standard.net/World/2016/05/19/White-hat-hackers-top-get-official-support-in-Japan)
[59] Actions against DNS security issues which .JP faced. Yoshiro YONEYA. APNIC 40 LT Session, 8th September 2015 (https://conference.apnic.net/data/40/jp-actions-apnic_1441335387.pdf)

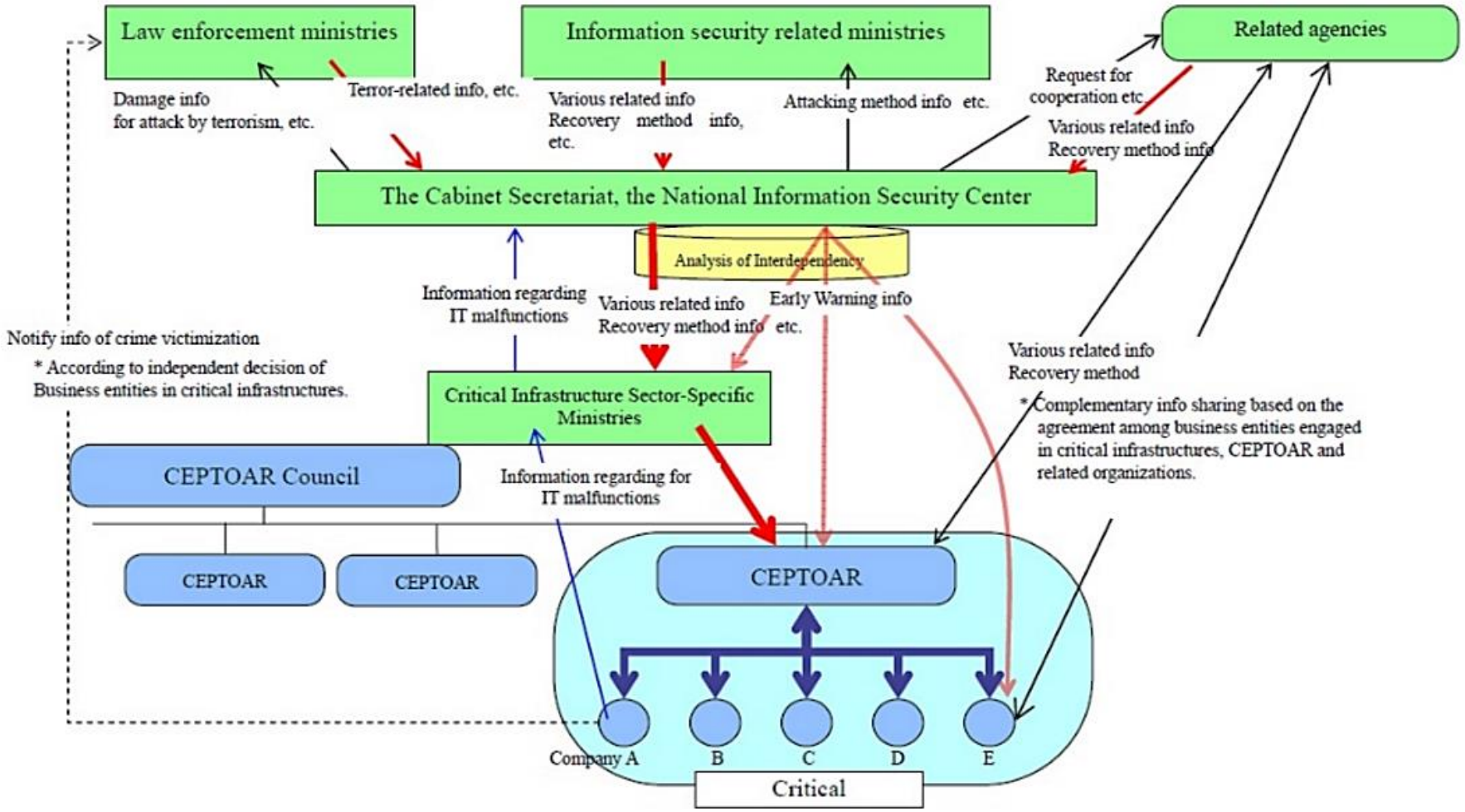
*Список организаций, входящих в T-CEPTOAR*

| | | |
|---|---|---|
| T-CEPTOAR representative | : | General Foundation data communication Japan Society Telecom Isaac Promotion Council Chairman Hisao Iizuka |
| T-CEPTOAR members | : | ※ alphabetical order<br>IDC Frontier Inc.<br>Internet Initiative Japan Inc.<br>NTT Communications Corporation<br>NTT Com Online Marketing Solutions Corporation<br>NTT DoCoMo, Inc.<br>NTT Learning Systems Corporation<br>KDDI CORPORATION<br>K-Opticom Corporation<br>Jupiter Telecommunications Co., Ltd.<br>Sonnet Corporation<br>SOFTBANK CORP.<br>Nippon Telegraph and Telephone West Corporation<br>NIFTY Corporation<br>Nippon general Foundation data communication Association Telecom Isaac Promotion Council<br>Nippon Telegraph and Telephone Corporation<br>Microsoft Japan Co., Ltd.<br>Japan Registry Services Co., Ltd.<br>Nippon Telegraph and Telephone East Corporation<br>Hitachi, Ltd.<br>BIGLOBE, Ltd.<br>Fujitsu Limited<br>Marubeni OKI Network Solutions Co., Ltd.<br>Corporation Co., Ltd. |
| T-CEPTOAR Steering Committee | : | T-CEPTOAR Steering Committee: General Foundation Haruki data communication Association Telecom Isaac Promotion Council Sato Japan (T-PoC) |

| | |
|---|---|
| NTT Communications Corporation | (Sub PoC: SG1) |
| Nippon Telegraph and Telephone West Corporation | (Sub PoC: SG2) |
| Internet Initiative Japan Inc. | (Sub PoC: SG3) |
| KDDI CORPORATION | (Sub PoC: SG4) |

Источник: T-CEPTOARとしての業務, Telecom-ISAC Japan, Telecom Information Sharing and Analysis Center Japan, https://www.telecom-isac.jp/public/t-ceptoar.html.

*Схема №3. Взаимодействие государственных и частных структур в Японии для обеспечения информационной безопасности объектов КИ*



## Европейский Союз

В ЕС подход к регулированию КИИ начал формироваться в рамках выработки общей стратегии регулирования критических инфраструктур (КИ). В июне 2004 г. Европейский Совет запросил Еврокомиссию подготовить такую стратегию, которая должна была прежде всего обеспечивать антитеррористическую безопасность критических объектов и европейских граждан. В рамках этой работы в октябре 2004 г. Еврокомиссия подготовила Коммуникацию «Защита КИ в борьбе с терроризмом (COM(2004) 702)[60]. Уже на этой предварительной стадии было отмечено, что одна из ключевых угроз, связанных с атаками на объекты КИ, связана с возможным каскадным эффектом, когда отказ в функционировании какой-либо одной инфраструктуры ведет к отказу в работе другой инфраструктуры из-за их синергетического взаимодействия. В первую очередь риск каскадных эффектов связывался с инцидентами в сфере энергоснабжения.

В Коммуникации также впервые предлагалось определение европейских КИ, которые включали в себя физические и ИТ-инфраструктуры, сети, сервисы и активы, нарушение функционирования или уничтожение которых оказало бы серьезное влияние на состояние здоровья, безопасность и экономическое благополучие граждан, либо эффективную работу правительств стран-членов ЕС. В документе были выделены следующие секторы КИ, включая сектор ИКТ:

- Энергодобывающие и энергораспределяющие установки и сети (объекты электроэнергетики, нефтегазовое производство, перегонные сооружения и инфраструктура хранения энергоносителей, системы транспортировки и распределения).
- Коммуникации и ИТ (в т.ч. телекоммуникации, системы массового вещания, программное и аппаратное обеспечение, а также сети, включая Интернет).
- Финансы (в т.ч. банковский сектор, страхование и инвестиции).
- Здравоохранение (госпитали, сооружения объектов здравоохранения и переливания крови, медицинские и фармацевтические лаборатории, службы поиска и спасения, а также службы скорой помощи).
- Продовольствие (инфраструктура пищевой безопасности, средства пищевого производства, оптовое распространение и пищевая промышленность).
- Водоснабжение (например, дамбы, водохранилища и водные резервуары, сети водоснабжения);
- Транспорт (включая порты и аэропорты, интермодальные транспортные стыки и узлы, сети железнодорожных и иных массовых перевозок, системы управления трафиком).
- Производство, хранение и транспортировка опасных веществ и изделий (химически, биологически, радиологически активные или ядерные материалы).
- Государственное управление (включая критические услуги и их инфраструктуру, государственные информационные сети, иные объекты и ключевые национальные культурные объекты и монументы).

[60] Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight Against Terrorism. Brussels, 20.10.2004. COM(2004) 702 final, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=en.

Несмотря на то, что классификация имела предварительный характер, в ее развитие в рамках Коммуникации была изложена система параметров и критериев, которые могли бы использоваться для категорирования объектов КИ. В качестве методологического инструмента первичной классификации КИ были предложены три фактора:

*Масштаб:* потеря элемента КИ оценивается по размеру географической области, которая будет затронута такой потерей или нарушением доступности КИ. Приводится градация по четырем уровням: международный, национальный, региональный/ территориальный и локальный.

*Степень воздействия:* Степень воздействия (в результате потери либо нарушения функциональности КИ):

- Отсутствует;
- Минимальная;
- Умеренная;
- Максимальная.

Также была сформулирована система критериев для установления степени воздействия:
(a) Воздействие на общество (численность затронутого населения, количество человеческих жертв, количество случаев ухудшения состояния здоровья, серьезных травм, эвакуаций).
(b) Воздействие на экономику (влияние на ВВП, величина экономического ущерба /или ухудшения качества продуктов и услуг).
(c) Воздействие на окружающую среду (влияние на общественные пространства и окружающие территории).
(d) Взаимозависимость с другими элементами КИ.
(e) Воздействие на политическую обстановку (уверенность в дееспособности структур государственного управления).

*Продолжительность:* Учитывается временной порог, при пересечении которого инцидент с КИ вызывает серьезные последствия по остальным критериям (немедленно, 24-48 часов, одна неделя, прочие случаи).

Несмотря на достаточно подробную и проработанную систему критериев параметров оценки инцидентов на КИ, Коммуникация предлагала ее лишь как возможный вариант для дальнейшего рассмотрения. Идентификация КИ была обозначена в Коммуникации как одна из ключевых задач на уровне ЕС и отдельных стран-членов ЕС. Списки КИ ЕС и стран-членов ЕС предлагалось составить до конца 2005 г. В части Интернета и ИТ-инфраструктуры документ не содержит подробного анализа, однако в нем отмечается, что КИ в целом становятся все более зависимы от общедоступных ИТ, включая Интернет и спутниковые системы навигации и связи. Таким образом, уже на первом этапе развития подхода ЕС обозначается дуализм места и статуса Интернета в контексте КИ: с одной стороны, Интернет и ИТ-коммуникации выделяются в отдельный сектор, с другой – подчеркивается зависимость от них всех остальных секторов.

Помимо идентификации и категорирования КИ, в Коммуникации приводится обзор существовавших на 2004 г. мер и политик управления рисками безопасности КИ по отдельным секторам – довольно разрозненных на тот момент. Для преодоления

фрагментарности имеющихся мер и выработки системного подхода к защите КИ на уровне ЕС в Коммуникации был анонсирован запуск Европейской программы по защите КИ (EPCIP). Нормативной основой программы должна была стать ежегодно издаваемая Еврокомиссией коммуникация по защите КИ и работе, проделанной в этой области. Реализация EPCIP должна была оцениваться по следующим ключевым направлениям:

- Идентификация и составление списков КИ государствами-членами ЕС.
- Бизнес-взаимодействие между собой разных секторов КИ, а также их взаимодействие с правительствами по обмену информацией и снижению риска серьезных инцидентов на КИ.
- Выработка Еврокомиссией общего подхода к обеспечению безопасности и защите КИ.

Для содействия обмена информацией в рамках реализации программы было предложено уже в 2005 г. сформировать Информационную сеть предупреждения для КИ (CIWIN), объединяющую специалистов по защите КИ из стран ЕС.

С целью обсуждения документа и реализации обозначенных в нем мер, включая прежде всего запуск EPCIP, Еврокомиссия (тогда еще Комиссия Европейских Сообществ) организовала два семинара ЕС по защите КИ в июне и сентябре 2005 г. По итогам семинаров были в том числе собраны и рассмотрены предложения от государств-членов ЕС по развитию общей политики в сфере защиты КИ. Для развития более широкой и предметной дискуссии Еврокомиссия в ноябре 2005 г. опубликовала «Зеленую книгу по EPCIP»[61], в которой были обобщены основные возможные варианты развития программы и обозначены ключевые вопросы для заинтересованных сторон.

Одним из заметных нововведений «Зеленой книги» стало вынесение на обсуждение вопроса о критериях разграничения КИ ЕС и КИ государств ЕС. Авторы документа предложили относить к КИ ЕС те объекты, нарушение функционирования которых оказывает влияние на два или более государства-члена Союза, таким образом учитывая свойство взаимозависимостей и каскадных эффектов.

В документе была представлен и уточненный проект секторальной категоризации КИ, непринципиально отличающийся от списка из Коммуникации 2004 г. (секторов стало 11). В рамках сектора ИКТ были выделены восемь критических сервисов/продуктов:

1. Защита информационных систем и сетей;
2. Промышленная автоматика и системы управления производственными и технологическими процессами (например, SCADA);
3. Интернет
4. Предоставление фиксированных телекоммуникационных услуг;
5. Предоставление мобильных телекоммуникационных услуг;
6. Радио-коммуникации и системы навигации;
7. Спутниковые коммуникации;
8. Эфирное вещание.

[61] Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final, Commission of the European Communities, http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.

Нужно подчеркнуть, что такая сегментация ИТ-сектора КИ по критическим сервисам стала окончательной в рамках подхода ЕС; однако тенденция выделять Интернет в качестве отдельного сервиса/подсектора КИ сохранилась и в дальнейшем.

Несмотря на то, что «Зеленая книга» не была нормативным документом, именно в приложениях к ней впервые появились важные терминологические нововведения, которые затем получили развитие в рамках развития подхода ЕС уже к регулированию КИИ. В документе впервые в практике ЕС было введено само понятие КИИ, которое определялось как системы ИКТ, которые являются КИ сами по себе, либо являются необходимыми для функционирования других КИ (включая телекоммуникации, компьютеры и ПО, Интернет, спутники и т.д.). Задач защиты КИИ исходя из такого определения включала в себя программы и деятельность владельцев инфраструктуры, операторов, производителей, пользователей и госрегуляторов, нацеленные на поддержание функционирования КИИ на уровне не ниже минимально приемлемого качества сервисов в случае сбоев, атак или иных инцидентов, а также на минимизацию времени восстановления систем и объема ущерба.

Авторы «Зеленой книги» подчеркивали, что в русле такого подхода защиту КИИ следует рассматривать как межсекторальную деятельность, не ограничивающуюся какими-либо отдельными секторами инфраструктуры. Для обеспечения системного подхода защита КИИ должна быть плотно увязана с защитой КИ.

Вторым важным терминологическим и концептуальным прецедентом стало упоминание в документе жизненно важных услуг (essential services), впервые в регуляторном контексте подхода ЕС к защите КИ и КИИ. Согласно тексту «Зеленой книги», понятие жизненно важных услуг, которое часто применяется к инфраструктуре коммунальных служб (водоснабжение, газоснабжение и энергоснабжение), может также включать в себя резервные системы энергопитания, системы контроля состояния окружающей среды или коммуникационные сети, нарушение функционирования которых создает риски для общественной безопасности, угрожает экономической безопасности, либо подрывает дееспособность структур и сервисов госуправления государства-члена ЕС. Несмотря на то, что понятие жизненно важных услуг не легло в основу последующих базовых документов ЕС по защите КИ в 2000-х гг., лежащая в его основе концепция вышла на первый план в регулировании КИИ ЕС в настоящее время, хотя и в видоизмененном варианте.

Наработки «Зеленой книги» заложили необходимую базу для разработки следующего доктринального документа по защите КИ ЕС. В декабре 2005 г. принять такой документ призвал Совет по правосудию и внутренним вопросам ЕС. 12 декабря 2006 г. Еврокомиссия приняла Коммуникацию по Европейской программе защиты КИ (COM(2006) 786 final)[62], которая и стала основной политики дальнейшего развития EPCIP. Одной из главных задач Коммуникации была разработка общей организационной и функциональной структуры, в рамках которой должна была реализовываться EP CIP. Для наполнения этой структуры предлагалось:

- Утвердить и приступить к реализации сформулированного в документе плана действий EP CIP в рамках трех рабочих потоков, сфокусированных на общей

[62] Communication from rhe Commission on a European Programme for Critical Infrastructure Protection, Brussels, 12.12.2006 COM(2006) 786 final, Commission of the European Communities, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN.

координации деятельности, проработке вопросов защиты КИ ЕС и, наконец, решении вопросов защиты национальных КИ государств-членов ЕС.

- Сформировать и запустить Информационную сеть для предупреждений об угрозах КИ (CIWIN). Такая сеть должна была содействовать государствам-членам ЕС и органам ЕС в обмене информацией об угрозах и уязвимостях КИ и необходимых мерах и лучших практиках по их минимизации, а также способствовать распространению данных исследований и иной информации среди всех заинтересованных сторон в ЕС. Однако на практике предложение Совету ЕС принять решение по созданию CIWIN лишь в октябре 2008 г. Портал сети стал активен с 2013 г. В настоящее время работу CIWIN координирует Генеральный директорат по миграции и внутренним вопросам ЕС (DG HOME). В качестве базового механизма обмена информацией сеть объединяет контактных лиц из каждого государства-члена ЕС, которые участвуют в ее деятельности[63].
- Сформировать группы экспертов по вопросам защиты КИ на уровне ЕС.
- Обеспечить разработку планов аварийных мероприятий регуляторами и операторами КИ ЕС и государств-членов ЕС, а также проработать направление международного взаимодействия по вопросам защиты КИ.
- Проработать вопросы финансирования EP CIP, в т.ч. в рамках Специальной программы ЕС по предотвращению, обеспечению готовности и управлению последствиями террористических актов и других рисков в сфере безопасности на 2007-2013 гг.

Приоритетной задачей в рамках Коммуникации и изложенного в ней Плана действий называлось определение и присвоение статуса КИ ЕС и государств членов ЕС, равно как и выработка окончательной модели категорирования. В первую очередь предлагалось сконцентрировать усилия на секторах транспорта и энергетики.

В самой коммуникации не предлагалось подробной методологии категорирования КИ, равно как параметров и критериев, за исключением минимального набора параметров, рекомендованного государствам-членам для разработки ими собственных подходов к определению и присвоению статуса КИ. Приведенный в Коммуникации набор был почти идентичен предложенному годом ранее в «Зеленой книге», за исключением набора параметров для оценки степени воздействия: параметр взаимовлияния заменили на параметр психологического воздействия инцидента на КИ.

Коммуникация 786 предложила достаточную базу для последующего принятия первой Директивы ЕС по защите КИ в 2008 г., однако при этом не содержала упоминания КИИ и жизненно важных услуг, а также не рассматривала отдельно вопросы защиты Интернета и сектора ИТ в разрезе КИ/КИИ. В апреле 2007 г. Еврокомиссия приняла заключение по программе EPCIP, в которых подтверждался принцип субсидиарности – государству-члены ЕС несли ответственность за защиту своих КИ.

Наконец, 8 декабря 2008 г. была принята первая Директива ЕС по определению и присвоению статуса европейских КИ и установлению потребности в улучшении их защиты. Цель Директивы была заявлена как выработка комплексного пошагового

[63] Подробнее см.: Critical Infrastructure Warning Information Network (CIWIN). http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm.

подхода к определению и присвоению статуса КИ ЕС, в качестве основных субъектов такой деятельности указывались государства-члены ЕС и операторы самих КИ. В Директиве закреплялось определение КИ ЕС, выработанное в предыдущих документах: «КИ, расположенные на территории государств-членов ЕС, уничтожение или нарушение функционирования которых окажет существенное влияние на два или более государства-члена ЕС. В этом определении и в Директиве в целом подчеркивается важность межсекторальной зависимости и каскадных эффектов при нарушении работы КИ, которые во многом и определяют трансграничные последствия таких инцидентов.

Для процедуры определения КИ ЕС в документе предлагался предварительный набор межсекторальных критериев:

(a) человеческие жертвы (оценка на основе потенциально возможного числа жертв и ранений);
(b) экономические последствия (оценка на основе размера экономического ущерба и ухудшения качества предоставляемых продуктов и услуг, включая потенциальное воздействие на окружающую среду);
(c) последствия для общества (оценка на основе влияния инцидента на общественное доверие, причинения физических страданий и нарушения повседневной жизни, включая потерю доступа к жизненно важным услугам).

В Директиве не содержалось точных параметров, которые позволяли бы оценивать инциденты на КИ на соответствие этим критериям, но отмечалось, что такие параметры будут применяться и рассматриваться государствами-членами ЕС отдельно для каждого сектора/объекта КИ. Определение и присвоение статуса КИ ЕС в документе было более подробно расписано как часть процедуры в рамках Планов безопасности для операторов (OSP) (разработать и регулярно обновлять такие планы предписывалось каждому государству-члену ЕС). Такая процедура включала в себя четыре шага для государств-членов ЕС: применение секторальных критериев для определения первичного круга КИ ЕС; применения данного в директиве определения КИ к выделенным в рамках предыдущей фазы потенциальным КИ ЕС на территории государств-членов; оценка КИ, определенных в предыдущих двух фазах, на предмет наличия трансграничных эффектов, присущих КИ ЕС; наконец, анализ полученного списка потенциальных КИ на предмет соответствия межотраслевым критериям, включая степень воздействия инцидента; наличие альтернатив инфраструктурам, обеспечивающим жизненно важные услуги, а также продолжительность нарушения функционирования и последующего восстановления системы.

При этом Директива охватывала лишь два сектора КИ – энергетику и транспорт как своего рода «пилотные» секторы для реализации программы EP CIP. Выбор был в том числе обусловлен тем, что именно в этих секторах (особенно энергетике) особенно выражены каскадные эффекты и межотраслевая взаимозависимость, которые служат определяющим фактором для причисления объекта к КИ ЕС. Закреплялась подотраслевая детализация указанных секторов (автотранспорт, ж/д транспорт, авиатранспорт, внутренний, морской и океанский водный транспорт для сектора транспорта; отрасль генерации и распределения электроэнергии, нефтяная и газовая промышленность для энергетики). При этом Директива не охватывала вопросы КИИ и вообще сектор ИКТ; однако отмечалось, что при дальнейшем ее обновлении и

реализации пошагового подхода к EP CIP приоритет должен быть уделен именно сектору ИКТ.

Таким образом, несмотря на то, что Директива законодательно зафиксировала подход к защите КИ, в части КИИ, инфраструктуры Интернета и сектора ИКТ, она не только не обеспечила дальнейшего развития европейского подхода, но и де-факто не использовала наработки, имевшиеся как минимум с 2005 г. и «Зеленой книги». После принятия директивы была сделана попытка включить в нее сектор ИКТ, однако итоговое голосование дало отрицательный результат. В качестве причины нежелания поддержать изменения в Директиву государства-члены указали существенные различия между ИКТ и другими секторами КИИ, в том числе в части трансграничных эффектов и межсекторальной взаимозависимости.

Попытка сдвинуть регуляторную ситуацию с мертвой точки в части ИТ и КИИ была предпринята в 2009 г., когда была принята Коммуникация Еврокомиссии «Защита Европы от крупномасштабных кибератак и сбоев инфраструктуры: усиление готовности, безопасности и устойчивости» (COM(2009) 149 final)[64]. В Коммуникации отмечался рост угроз для КИИ, исходящих от кибератак, природных катастроф и сбоев оборудования, а также подчеркивалась зависимость как критических секторов, так и экономики в целом от надежного функционирования инфраструктуры ИКТ-сектора. Основной целью признавалось предотвращение инцидентов, повышение уровня готовности и осведомленности и разработка срочного плана действий для повышения безопасности и устойчивости КИИ в ЕС. В Коммуникации выделялись четыре ключевые задачи:

- Содействие обмену информацией и внедрению лучших практик и отраслевых технических политик для укрепления общего понимания вопросов защиты КИИ.
- Обсуждение и проработка приоритетных общественно значимых политик, целей и мер по защите КИИ.
- Выработка базовых требований по обеспечению безопасности и устойчивости для КИИ в Европе.
- Выявление и содействие принятию базовых лучших практик в части обеспечения безопасности и устойчивости КИИ.

Примечательно, что Коммуникация ссылается на Директиву 2008 г. и программу EP CIP, но по сути задает новое, самостоятельное направление деятельности для структур ЕС, государств-членов и операторов инфраструктуры. В документе используется понятие и определение КИИ, сформулированное в «Зеленой книге» 2005 г., и подчеркивается роль КИИ в обеспечении жизненно важных услуг. Изложенный в Коммуникации подход лежит уже не в русле EP CIP, а укладывается в общую канву политики по обеспечению сетевой и информационной безопасности (NIS), которая к этому времени развивалась в ЕС под координацией Европейского агентства по сетевой и информационной безопасности (ENISA). ENISA было учреждено в марте 2004 г. решением Европарламента и Совета ЕС (Regulation (EC) No 460/2004).

[64] Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400}, Brussels, 30.3.2009 COM(2009) 149 final, Commission of the European Communities, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

Изначальный мандат определял роль агентства как общеевропейского (в рамках ЕС) центра экспертизы по вопросам NIS, обеспечивающего рекомендации и руководства, консультации, исследования и содействующего развитию обмена информацией и компетенций по вопросам сетевой и информационной безопасности между государствами-членами ЕС, операторами информационных сетей и систем, и другими заинтересованными сторонами. Вопросы повышения устойчивости и защищенности сетевой инфраструктуры изначально включались в спектр деятельности ENISA, однако первый мандат не выделял КИИ как отдельную сферу компетенций агентства. Решениями Европарламента и Совета ЕС от 24 сентября 2008 г. (Regulation (EC) No 1007/2008)[65], 8 июня 2011 г. (Regulation 580/2011)[66] и 21 мая 2013 г. (Regulation (EU) No 526/2013)[67] мандат ENISA был трижды продлен и обновлен, что способствовало закрепление за Агентством центральной роли в реализации планов и программ деятельности по защите КИИ, обозначенных в Коммуникации 2009 г. В упомянутых Решениях и в заключениях министерской конференции ЕС по защите КИИ, проведенной в Таллинне 27-28 апреля 2009 г., отмечалась общая целесообразность деятельности ENISA и необходимость ее усиления по следующим направлениям и форматам, а также для решения следующих задач:

- Усиление операционной поддержки агентства как структуры, обеспечивающей кооперативный подход государств-членов ЕС к вопросам сетевой безопасности, и тем самым предотвращающей риск фрагментации политики ЕС в этой области.
- Поддержка деятельности ENISA по развитию и совершенствованию средств раннего предупреждения и мер реагирования на инциденты NIS, развитию технических навыков и компетенций в сообществе профильных специалистов. Сюда же относится и ведущая роль агентства в развитии системы центров реагирования на компьютерные инциденты (CERTs/CSIRTs) в масштабах ЕС, обеспечение координации политик и обмена информацией, лучшими практиками и знаниями между такими структурами.
- Содействие в продвижении и укреплении агентством культуры информационной и сетевой безопасности по всему ЕС, в том числе среди субъектов частного сектора, операторов информационных инфраструктур и граждан, пользующихся сетевыми сервисами и продуктами.
- Отведение агентству центральной роли в формировании систему взаимодействия государственных структур ЕС с частным бизнесом ИТ-сектора по вопросам повышения сетевой безопасности и защиты информационных систем, а также выявления уязвимостей в ПО, формировании у частных организаций практик реагирования на инциденты и противодействия кибератакам.

[65] Regulations Regulation (Ec) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, Official Journal of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF.

[66] REGULATION (EU) No 580/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, Official Journal of the European Union, https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1.

[67] REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, Official Journal of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN.

- Необходимость развития и расширения практики проведения европейских киберучений по противодействию кибератакам, реагированию на инциденты и обеспечению устойчивости КИИ; такие учения должны способствовать росту координации действий между государствами-членами ЕС, охватывать как можно более широкий их круг и поднимать уровень компетенций и практической готовности операторов КИИ к раннему предупреждению, реагированию и преодолению последствий сетевых инцидентов.

В части взаимодействия государственных структур с частным бизнесом по вопросам NIS документы, продлившие и обновившие мандат ENISA, перекликаются и ссылаются в том числе на вышеупомянутую Коммуникацию 2009 г. В Коммуникации отмечалось, что государства-члены ЕС, за которыми закреплена основная роль в формировании и реализации политик по защите КИИ, нуждаются в системном участии частного сектора, к которому принадлежит большая часть операторов таких объектов. Однако частный рынок зачастую не обеспечивал своим субъектам достаточных стимулов для того, чтобы инвестировать в защиту КИИ и развивать собственные подходы и практики в этой сфере в той степени, в которой это предписывали национальные правительства.

Для решения задачи по стимулированию вовлечения частной отрасли в программу защиты КИИ (CIIP) Коммуникация предлагала сформировать и продвигать программу европейских ГЧП (PPPs), которая позволила бы развить механизмы таких партнерств за рамки национальных программ и обеспечить сближение национальных регуляторных норм и политик с операционными политиками операторов КИИ. Институциональную основу такой программы составило Европейское государственно-частное партнерство по устойчивости (European Public Private Partnership for Resilience, EP3R)[68], которое было учреждено в июне 2010 г. в рамках реализации программы CIIP из Коммуникации 2009 г. Механизм EP3R должен был способствовать решению задач по формированию ГЧП в масштабах всего в телекоммуникационном и ИТ-секторе, разработке операторами КИИ политик и планов действий по предупреждению, реагированию и восстановлению после кибератак, катастроф и сбоев сетевого оборудования, налаживанию регулярного обмена информацией между операторами и регуляторами по защите КИИ, проработке вопросов трансграничного влияния инцидентов на КИИ отрасли ИТ и телекоммуникаций. Координацию деятельности Партнерства осуществляют совместно Еврокомиссия и ENISA.

Вскоре после учреждения в рамках EP3R были три выделены тематические области и сформированы соответствующие Рабочие группы (РГ):

- РГ1: Ключевые активы, ресурсы и функции для обеспечения непрерываемой и безопасной электронной связи между странами.
- РГ2: Основные требования к безопасности и устойчивости электросвязи.
- РГ3: Требования и механизмы координации и кооперации для готовности и реагирования на крупномасштабные разрушения в секторе электронных коммуникаций.

[68] European Public Private Partnership for Resilience (EP3R), European Union Agency for Network and Information Security, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

Среди трех РГ к 2013 г. наибольших практических результатов удалось добиться группе №3, деятельность которой способствовала формированию общеевропейской сети CERT/CSIRT, а также развитию практики ежегодных общеевропейских киберучений CyberEurope, первые из которых прошли в ноябре 2010 г. В 2011 г. были проведены первые совместные киберучения с США - Cyber Atlantic 2011.

*Сводная карта европейских киберучений по состоянию на 2015 г.*


Источник: Европейский опыт проведения киберучений: методические рекомендации ENISA, Экспертный центр электронного государства, 28.09.15, http://d-russia.ru/evropejskij-opyt-provedeniya-kiberuchenij-metodicheskie-rekomendacii-enisa.html.

Однако по направлениям деятельности двух других РГ успех оказался менее очевиден. Так, по итогам работы РГ1 в направлении идентификации и составлении таксономии КИИ ЕС в 2012 г. был подготовлен проект неофициального отчета по критериям для ИКТ-сектора (ICT Criteria Non-Paper). В документе в контексте КИИ рассматривался широкий круг объектов и систем сетевой и телекоммуникационной инфраструктуры, который в т.ч. включал в себя элементы интернет-инфраструктуры:

- корневые авторитативные серверы DNS, поддерживающие национальные домены государств-членов ЕС;
- точки обмена трафиком IXP;
- магистральные трансграничные каналы передачи интернет-трафика.

Однако проект доклада встретил критику от представителей технического сообщества, которая в частности касалась чрезмерной широты представленного списка КИИ и отсутствия четкого политико-регуляторного контекста, в который мог бы укладываться такой список. В результате, проект так и остался в статусе Non-Paper.

В итоге, к 2013 г. сложилась ситуация, когда общеевропейская политика в области NIS активно развивалась, в т.ч. по направлению реагирования на инциденты, проведения тренингов и киберучений, обмена опытом и лучшими практиками; успешно решались задачи в области европейских и национальных программ электронной идентификации, защиты персональных данных, созданию безопасной программной среды для конечных пользователей и проч. Но при этом одна из несущих конструкций политики NIS – защита КИИ – оставалась до конца не проработанным и не урегулированным направлением, где так и не были введены систематизированные требования к операторам, разработана итоговая шкала критериев и параметров для самих объектов и связанных с ними инцидентов, отсутствовал единый утвержденный подход к категорированию и таксономии объектов КИИ, включая сектор телекоммуникаций и Интернет-отрасль.

В этих условиях Еврокомиссия запустила новый длительный виток регуляторной активности, промежуточные итоги которого определяют состояние европейского подхода к защите КИИ на данный момент. 7 февраля 2013 г. регулятор опубликовал Предложение по Директиве о мерах обеспечения повышенного уровня безопасности сетевых и информационных систем в ЕС (COM(2013) 48 final)[69]. Документ комплексно охватывает вопросы NIS, но отдельно выделяет тематику защиты КИИ и обеспечения жизненно важных услуг применительно к интернет-сектору. Под повышением уровня NIS в масштабе ЕС подразумевалось повышение безопасности Интернета, частных сетей и информационных систем, поддерживающих общественную жизнь и экономическую активность. Решать такую задачу предлагалось путем:

A. выработки требований к государствам ЕС по повышению готовности к инцидентам и усилению их взаимодействия друг с другом;
B. выработки норм и требований к операторам КИ в секторах энергетики и транспорта, «ключевым поставщикам услуг информационного общества» (платформы электронной коммерции, социальные сети и проч.), а также госорганам по принятию дополнительных мер в части управления рисками безопасности и информирования профильных национальных регуляторов о серьезных сетевых инцидентах.

В Предложении отмечались следующие моменты:

- Операторы КИ и провайдеры жизненно важных услуг не охвачены системой требований и обязательств в части управления рисками и обменом информацией с профильными регуляторами.
- Частному бизнесу не хватает стимулов для внедрения систематических практик управления рисками, которые включали оценку рисков в сфере NIS и принятие мер по их устранению.
- Существенная доля инцидентов остается незамеченной регуляторами, так как о них не докладывается, что препятствует выработке профильными госструктурами стратегий управления инцидентами и более эффективному их предупреждению.
- Существующая система регулирования в части информирования о серьезных инцидентах сетевой и информационной безопасности только компании

[69] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union {SWD(2013) 31 final} {SWD(2013) 32 final}, Brussels, 7.2.2013 COM(2013) 48 final 2013/0027 (COD), European Commission, https://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.

телекоммуникационного сектора, тогда как остальные критически важные секторы также зависят от ИКТ и должны охватываться регулированием в сфере сетевой безопасности.

В документе были обозначены секторы инфраструктуры и провайдеры услуг, «особо уязвимые к инцидентам сетевой безопасности, в силу высокой зависимости от надлежащего функционирования сетей и информационных систем»: банковский сектор, биржи, сектор генерации, передачи и распределения электроэнергии, транспорт, здравоохранение, интернет-сервисы и сервисы государственного управления.

Помимо выработки норм и требований, в рамках приоритетных задач будущей директивы предлагалось:

1) Обеспечить минимально достаточную ресурсную базу (capabilities) частным и государственным структурам для повышения NIS и противодействия угрозам, усиления взаимодействия в рамках общеевропейской координации деятельности CERT, а также содействовать разработке государствами-членами национальных стратегий и планов действий по обеспечению NIS.

2) Запустить взаимодействие профильных национальных госструктур стран ЕС в рамках сети, обеспечивающей надежную и эффективную координацию действий, включая обмен информацией, выявление угроз и инцидентов и скоординированное на общеевропейском уровне реагирование на них. Предполагалось, что в рамках такой сети государства-члены будут не только обмениваться информацией и экспертизой, но и оперативно согласовывать свои действия по реагированию на инциденты и отражению угроз сетевой и информационной безопасности на базе общеевропейского плана координации.

3) Внедрить культуру управления рисками NIS и информационного обмена между частными и государственными субъектами, прежде всего в отношении КИИ. Для этого, в частности, обязать компании определенных критических секторов проводить оценку актуальных для них рисков NIS и принимать соответствующие меры по них нейтрализации. Предлагалось обязать такие компании сообщать компетентным госорганам о любых сетевых инцидентах, которые серьезно угрожают безопасности их сетей и информационных систем и существенно сказываются на обеспечении непрерывности работы критических сервисов и поставке критических рыночных продуктов.

Обсуждение проекта Директивы и работа над согласованием ее итоговой версии в общей сложности заняли более трех лет и сопровождались ожесточенными дебатами – прежде всего, по поводу введения новых категорий субъектов частного сектора, подпадающих под расширенные требования по обеспечению безопасности. В итоге, Директива в своем окончательном варианте была принята Европарламентом и Советом ЕС 6 июля 2016 г. (2013/0027 (COD) LEX 1683)[70]. В рамках комплексного подхода к

[70] 2013/0027 (COD) LEX 1683 PE-CONS 26/16 TELECOM 122 DATAPROTECT 64 CYBER 71 MI 460 CSC 189 CODEC 904, DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION, Strasbourg, 6 July 2016, http://data.consilium.europa.eu/doc/document/PE-26-2016-INIT/en/pdf.

созданию общей нормативной основы для повышения сетевой и информационной безопасности в ЕС Директива предусматривает следующие группы мер и требований на трех уровнях – общеевропейском, национальном и уровне субъектов (операторов), предоставляющих сервисы, подпадающие под требования Директивы по NIS:

1. Укрепление потенциалов кибербезопасности на национальном уровне в государствах-членах ЕС.

Согласно Директиве, каждый член ЕС должен разработать и принять национальную стратегию защиты сетей и информационных систем. Такая стратегия должна включать стратегические цели, приоритеты и рамочные политики; определять круг мер по обеспечению готовности к инцидентам, реагированию и восстановлению; определять механизмы взаимодействия между государственным и частным сектором; содержать меры по повышению осведомленности, проведению тренинговой и образовательной деятельности; определять планы исследований и разработок в сфере NIS; включать план по оценке рисков и определять круг субъектов, вовлеченных в реализацию такой стратегии. Кроме того, каждое государство должно назначить профильное ведомство (или несколько ведомств) для мониторинга реализации положений Директивы на своем страновом уровне. Также государства назначают единое контактное лицо для обеспечения трансграничного сотрудничества с профильными ведомствами в других государствах-членах ЕС, а также в рамках механизмов уровня ЕС, устанавливаемых самой Директивой.

Во исполнение норм Директивы по взаимодействию CSIRTs государства-члены ЕС определяют одну или несколько групп реагирования на компьютерные инциденты, за которой закрепляются следующие функции:

- мониторинг инцидентов на национальном уровне;
- обеспечение раннего предупреждения и информирования об угрозах, объявления и распространения информации о рисках и инцидентах сетевой и информационной безопасности среди заинтересованных сторон;
- реагирование на инциденты;
- проведение динамического анализа рисков и инцидентов и поддержание ситуационной готовности;
- участие в сети национальных CSIRT в рамках общеевропейского механизма взаимодействия.

2. Укрепление сотрудничества на уровне ЕС.

Директива учреждает Группу по взаимодействию, в задачи которой входит поддержка и содействие стратегического сотрудничества и обмена информацией между странами ЕС, а также укреплению доверия в сфере информационной и сетевой безопасности. В состав Группы войдут представители государств-членов ЕС, Еврокомиссии и ENISA; функцию секретариата будет выполнять Еврокомиссия, которая также отвечает за проработку процедурных аспектов комплектования состава и деятельности Группы. Деятельность Группы будет осуществляться в рамках двухлетних Рабочих программ (РП) по четырем направлениям:

1) Планирование: включает в себя формирование Рабочей программы через полтора года после принятия Директивы (т.е. в феврале 2018 г.), а также последующую подготовку новой РП каждые два года.
2) Руководство: включает в себя инструктирование и консультации для Сети CSIRT, содействие государствам-членам ЕС в наращивании потенциалов и поддержку их работы по определению операторов жизненно важных услуг; обсуждение процедур уведомления об инцидентах и стандартов NIS; взаимодействие с профильными структурами и ведомствами ЕС; а также оценку национальных CSIRT и национальных стратегий государств-членов ЕС (на добровольной основе).
3) Обмен информацией и лучшими практиками по вопросам рисков, инцидентов, повышения осведомленности, тренинговой деятельности, исследований и разработок.
4) Предоставление отчетности: каждые полтора года Группа готовит отчет, содержащий оценку опыта, полученного в ходе взаимодействия в течение отчетного периода. Отчет направляется Еврокомиссии и включается в процедуру обзора выполнения Директивы.

Помимо Группы по взаимодействию, к механизмам общеевропейского уровня в рамках Директивы относится Сеть CSIRT, включающая представителей национальных групп реагирования на компьютерные инциденты стран ЕС и CERT–iEU (общеевропейского CERT). Секретариат Сети CSIRT создается на базе ENISA (которая также активно поддерживает взаимодействие между членами Сети), Еврокомиссия участвует в ее работе в качестве наблюдателя. В задачи Сети входит:

- обмен информацией об услугах, операционной деятельности и ресурсной базе сотрудничества страновых CSIRT в рамках ЕС;
- обмен информацией и мнениями по вопросам инцидентов (по запросу или на добровольной основе);
- определение механизмов согласованного реагирования на инциденты (по запросу или на добровольной основе);
- поддержка трансграничного управления инцидентами (на добровольной основе);
- исследование и проработка дальнейших возможностей операционного взаимодействия;
- информирование Группы взаимодействия о деятельности Сети и запрос инструкций и консультаций у Группы;
- обсуждение опыта, полученного в ходе учений по обеспечению NIS;
- обсуждение вопросов, связанных с отдельными страновыми CSIRT государств-членов ЕС (по запросу);
- подготовка и публикация руководств по операционному взаимодействию.

Механизм отчетности для Сети схож с механизмом Группы по взаимодействию: по прошествии двух лет с момента принятия Директивы Сеть CSIRT каждые полтора года готовит отчет с оценкой опыта, полученного в рамках операционного взаимодействия, содержащий выводы и рекомендации; отчет рассматривается Еврокомиссией в рамках обзора выполнения Директивы.

В части регулирования КИИ ключевые нововведения Директивы связаны с третьим уровнем взаимодействия – установлением требований по управлению рисками и информированию об инцидентах для двух новых категорий субъектов, в основном

частного сектора (операторов ключевых услуг и провайдеров цифровых услуг). С принятием Директивы европейские регуляторы сделали существенный шаг в сторону от концепции КИИ в пользу подхода, в рамках которого регулирование и предписания устанавливаются исходя не из характеристик инфраструктурного объекта как такового, а из параметров услуг (сервисов), которые он обеспечивает/предоставляет. В частности, Директива вводит две новые категории субъектов: операторы жизненно важных услуг и провайдеры цифровых услуг; при этом первая категория по сути заменяет собой операторов КИИ.

Под оператором жизненно важных услуг (ОЖВУ) (operator of essential services) понимается государственная или частная организация, для определения и присвоения статуса которой применяются следующие критерии:

a) организация предоставляет услугу, которая жизненно важна для поддержания критически важной общественной либо экономической деятельности;
b) предоставление данной услуги зависит от информационных и сетевых систем;
c) инцидент информационной или сетевой безопасности окажет выраженное разрушительное воздействие на предоставление данной услуги.

Нужно особо отметить, что «выраженное разрушительное воздействие» в Доктрине рассматривается с помощью отдельного аппарата критериев, значимых, таким образом, и для определения ОЖВУ самих по себе. Во-первых, в документе приводится определение инцидента как «события, оказывающего выраженное разрушительное воздействие на безопасность сетей и информационных систем». Такое, воздействие, а значит и сам факт инцидентами, определяются следующими параметрами:

- число пользователей, пострадавших от инцидента;
- продолжительность инцидента;
- географические показатели распространения инцидента;
- степень нарушения функциональности систем;
- степень влияния на экономико-социальные сферы деятельности.

Пороговых значений по этим параметрам не приводится, но их разработки остается за государствами-членами ЕС.

В тексте документа отсутствует определение жизненно важных услуг как таковых, однако по сути речь идет именно о том понимании, которое было предложено в «Зеленой книге» 2005 г. и упоминалось в последующих документах по ЕР CIP. Для ОЖВУ также дается секторальная классификация с детализацией по подсекторам и типам организаций; перечислены восемь секторов, также преемственных по отношению к ранним документам по ЕР CIP (в тексте Директивы отмечается, что список не исчерпывающий): энергетика, транспорт, банковский сектор, инфраструктуры финансового рынка, здравоохранение, снабжение и распределение питьевой воды, а также цифровая инфраструктура, де-факто заменяющая сектор ИКТ из документов ЕР CIP. Список подсекторов для цифровой инфраструктуры не приводится, но перечисляются три типа организаций, подпадающих под статус ОЖВУ:

1. Точки обмена трафиком (IXPs). В Директиве IXPs определяются как объект сетевой инфраструктуры, который обеспечивает взаимоподключение более чем двух независимых автономных систем, прежде всего с целью осуществления обмена интернет-трафиком; IXP обеспечивает взаимоподключение только для автономных систем; сервис IXP не требует пропускания интернет-трафика,

передаваемого через пару взаимодействующих автономных систем, через какую-либо третью автономную систему; также использование сервиса IXP не ведет к преобразованию трафика или иному взаимодействию с ним. В Директиве подчеркивается, что IXP предоставляет доступ к сети и не выступает в качестве транзитного провайдера, не предоставляет услуг, не связанных с взаимоподключением технически и организационно обособленных друг от друга сетей. При этом под автономной системой понимается технически обособленная сеть, что не соответствует определению автономной системы, используемому в документах IETF (RFC 1771, RFC 1970). Вместе с тем, IXP по тексту Директивы могут оказывать дополнительные услуги, не связанные с пропуском трафика через взаимоподключение, однако такие услуги не влияют на статус ОЖВУ.

2. Провайдеры сервисов DNS: определяются как организации, предоставляющие сервисы DNS в Интернете.
3. Регистратуры доменных имен верхнего уровня: в тексте Доктрины определяются как организации, которые администрируют и поддерживают регистрацию доменных имен в доменных зонах верхнего уровня (TLD); таким образом, речь идет не о регистраторах, а именно о регистратурах.

Определение ОЖВУ возлагается на государства-члены ЕС, которые должны составить списки таких организаций в течение 27 месяцев с момента принятия Директивы (к октябрю 2018 г.). Такие списки подлежат регулярному пересмотру и обновлению. Трансграничные эффекты деятельности ОЖВУ также учитываются: определение тех операторов, которые предоставляют ЖВУ двум и более государствам, требует совместных консультаций таких государств. Кроме того, отдельные государства ЕС также формируют собственные списки жизненно важных услуг, в соответствии с которыми определяются их операторы. Начиная с октября 2018 г. и далее каждый два года государства-члены ЕС должны будут направлять Еврокомиссии информацию о проделанной работе по определению ОЖВУ. Такая информация должна включать:

(a) принятые на национальном уровне меры и механизмы, позволяющие составить перечень ОЖВУ;
(b) список жизненно важных услуг;
(c) количество операторов ЖВУ, выявленных по каждому из секторов с указанием их значимости для сектора;
(d) где применимо, пороговые показатели, позволяющие оценить уровень поставок на основе количества пользователей, зависящих от предоставления той или иной услуги, или на основе важности того или иного ОЖВУ.

Обмен лучшими практиками по определению ОЖВУ между государствами-членами ЕС, включая вопросы трансграничности жизненно важных услуг и межсекторальной взаимозависимости, также ведется в рамках Группы по взаимодействию при содействии ENISA.

Однако определение и составление государствами-членами списков ОЖВУ не является самоцелью Директивы – документ устанавливает комплексную сетку требований и предписаний для таких операторов, нацеленную на обеспечение ими повышенного уровня NIS. В рамках принципа субсидиарности полномочия и ответственность за

соблюдение операторами таких требований делегируется государствам-члена ЕС. Согласно Директиве, ОЖВУ обязаны:

1. Принимать надлежащие технические и организационные меры по управлению рисками, включая меры по предотвращению и минимизации влияния инцидентов на безопасность сетей и информационных систем, используемых в целях обеспечения непрерывности оказания жизненно важных услуг.
2. Своевременно уведомлять компетентные органы государства или национальные CSIRTs о существенных инцидентах. Для установления степени серьезности инцидента используется отдельный набор критериев, включающий количество пользователей, затронутых нарушением процесса предоставления необходимой услуги; продолжительность инцидента и его географический охват. В свою очередь, CSIRTs и компетентные национальные регуляторы, которым ОЖВУ сообщают об инцидентах, должны защищать безопасность и экономические интересы операторов, а также предоставить им необходимую информацию, в том числе по эффективному управлению инцидентами. Однако если инцидент приводит к значительному нарушению процесса предоставления необходимой услуги, национальный CSIRT должен сообщить о нем другим CSIRTs и компетентным госструктурам других государств-членов ЕС. Компетентные национальные регуляторы вместе с Группой по взаимодействию могут разрабатывать руководства и рекомендации для определения тех случаев, когда ОЖВУ обязаны информировать их и CSIRTs об инцидентах. В том числе речь идет об установлении точных параметров и пороговых значений для критериев, определяющих серьезность инцидента.
3. Предоставлять компетентным государственным органам информацию, необходимую для оценки сетевой и информационной безопасности в своих сетях, включая:
    - письменно закрепленные политики безопасности;
    - доказательства эффективности применения политик безопасности, в т.ч. результаты аудита безопасности, проведенного компетентным ОГВ или квалифицированной организацией.

В свою очередь, компетентные национальные регуляторы вправе оценивать полученную от ОЖВУ информацию, доказательства и результаты аудита безопасности, а также по итогам оценки издавать распорядительные акты, обязательные для исполнения операторами.

Вероятно, самой противоречивой новацией Директивы, вызвавшей обвинения в создании избыточной регуляторной нагрузки на частную ИТ-отрасль, является введение еще одной категории регулируемых субъектов: провайдеров цифровых услуг (ПЦУ) (digital service providers). Эту категорию также стоит упомянуть в контексте КИИ: хотя Директива подчеркивает, что, хотя ПЦУ не предоставляют жизненно важных услуг и не обеспечивают столь критические функции, как ОЖВУ, они тем не менее играют важную роль для общественной жизни и экономической деятельности, и потому к ним также устанавливаются повышенные требования в части обеспечения NIS.

После длительных дебатов и «войны поправок», продолжавшейся в течение 2014-2015 гг., к числу ПЦУ в итоговом тексте Директивы были отнесены:

- торговые онлайн-площадки (*online marketplace*);
- онлайн поисковики (*online search engine*);

- сервисы облачных вычислений (*cloud computing service*).

Производители аппаратных средств и разработчики ПО, включавшиеся в список ПЦУ на ранних стадиях разработки документа, в конечном счете были исключены из него.

Принципиальное отличие регулирования ПЦУ от ОЖВУ состоит в том, что на определение ПЦУ не распространяется принцип субсидиарности. Определение ПЦУ не является задачей государств-членов ЕС – под нормы Директивы напрямую попадают все организации, соответствующие установленным в Директиве видам деятельности.

В части определения цифровых услуг Директива ссылается на Директиву 2015/1535 Европарламента и Совета ЕС от 9 сентября 2015 г., устанавливающую процедуру предоставления информации в сфере в сфере технического регулированиям и другие нормы для сервисов информационного общества (OJ L 241, 17.9.2015, p. 1)[71]. Данный документ оперирует понятием сервисов, под которыми понимаются любые сервисы информационного общества, т.е. любые услуги, предоставляемые:

- как правило за вознаграждение,
- удаленно (без непосредственного взаимодействия сторон),
- электронными средствами (услуга изначально отправляется и приходит к получателю за счет использования электронного оборудования для обработки (включая цифровое сжатие) и хранения данных, а также полностью передается, доставляется и получается по проводным коммуникациям, радио, оптическими или иными электромагнитными средствами.

Т.е. этому определению сегодня соответствует любой сервис или субъект, бизнес-модель которого с предоставлением услуг через Интернет. С учетом столь широкого определения получается, что круг ПЦУ ограничивается исключительно наличием в тексте Директивы конечного их списка. При этом в плане юрисдикции ПЦУ может быть юридическое лицо, которые предоставляет цифровые услуги, если оно предоставляет их в пределах любого государства-члена ЕС. ПЦУ находится под юрисдикцией государства-члена ЕС, в котором он зарегистрирован и имеет головной офис. Однако если провайдер цифровых услуг создан за пределами ЕС, но предлагает услуги на территории государства-члена ЕС, он обязан вести деятельность через уполномоченного представителя, находящегося на территории и под юрисдикцией этого государства-члена ЕС.

В части требований по обеспечению повышенного уровня NIS Директива устанавливает для ПЦУ три блока требований и предписаний:

- Требования по управлению рисками и обеспечению надлежащего уровня безопасности включают обеспечение безопасности систем и технологических средств; управление инцидентами; управление устойчивостью функционирования предприятий и инфраструктуры; проведение оперативного контроля, аудита и диагностики; соблюдение международных стандартов сетевой и информационной безопасности.

[71] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN

- Требования по обеспечению непрерывности оказания услуг и минимизации воздействия инцидентов, влияющих на безопасность используемых сетей и информационных систем.
- Обязанность своевременно информировать любых инцидентах компетентные органы государств-членов или CSIRTs.

Кроме того, ПЦУ также обязаны предоставлять информацию в компетентные органы государства о безопасности своих сетей и информационных систем и обеспечивать соответствие требованиям стандартов, предусмотренных в Директиве. ПЦУ обязан предоставлять информацию и доказательства: компетентным органам своего государства; компетентным органам другого государства-члена ЕС и непосредственно пользователям услуг. В целом устанавливаемые для ПЦУ предписания и требования носят менее комплексный и обременительный характер, чем требования к ОЖВУ; однако нужно отметить, что, исходя из данного в Директиве крайне широкого определения, круг ПЦУ окажется существенно шире, чем национальные списки ОЖВУ. С одной стороны, это может способствовать масштабным изменениям в политиках и практиках обеспечения сетевой и информационной безопасности в ЕС. С другой стороны, на данный момент полностью не просчитаны административные и финансовые издержки, которые понесут ПЦУ, включая организации малого и среднего бизнеса.

*Терминологическая справка: перевод термина "essential services"*

Понятие Essential services в контексте защиты КИ и КИИ появилось в документах ЕС в 2005 г. в «Зеленой книге» по EP CIP. В настоящее время этот термин служит основой для определения круга операторов, подпадающих под требования по обеспечению сетевой и информационной безопасности в рамках Директивы о мерах обеспечения повышенного уровня безопасности сетевых и информационных систем от 6 июля 2016 г. Однако определение «Зеленой книги» не является официальным, т.к. документ не носит нормативного статуса; а в Директиве 2016 г. подробное определение essential services отсутствует. Таким образом, на уровне законодательства ЕС исчерпывающее определение не закреплено.

Вместе с тем, в соответствии с отсылкой из рабочего определения «Зеленой книги», понятие essential services достаточно широко используется в НПА и иных документах как в государствах ЕС, так и за их пределами вне контекста NIS и CIP. Можно выделить следующие группы источников, в которых употребляется этот термин:

- Законодательство в сфере трудовых отношений в ряде англоязычных государств, прежде всего в странах Содружества наций и США.
- Доклады и иные рабочие документы Международной организации труда (МОТ), посвященные вопросам соблюдения права трудящихся на забастовки.
- Экспертные доклады, неправительственные проекты документов по вопросам охраны труда и защиты прав трудящихся на забастовки.

Примеры национального регулирования essential services включают:

- Essential Services Commission Act 2001, принятый в штате Виктория, Австралия. Во исполнение закона в штате была создана Комиссия, задачи которой включают содействие и надзор за эффективностью, повышением

конкурентоспособности и качества услуг в секторах энергетики, транспорта, водоснабжения и местного самоуправления[72].

- Сходное законодательство (Essential Services Act 1979) принято в австралийском штате Квинслэнд. Согласно закону, к essential services относятся следующие объекты и службы, повседневно доступные для общественного пользования: общественный пассажирский и грузовой транспорт, пожаротушение, госпитали и службы неотложной медицинской помощи, энергоснабжение и водоснабжение, уборка мусора и санитарно-гигиенические службы[73].
- Essential Services Maintenance Act (1968) – закон федерального уровня в Индии, регулирующий порядок предоставления и поддержания непрерывности важных услуг, а также права работников соответствующих служб и отраслей на забастовки[74]. Согласно закону, essential services включают телеграфные, почтовые, и телефонные службы, ж/д-перевозки и иной массовый грузовой и пассажирский транспорт, службы, обеспечивающие работу аэродромов и эксплуатацию воздушных судов, таможню, службы портовой грузовой логистики и проч.
- Законодательство о занятости и охране труда в Канаде, включая принятые в 2014 г. поправки в Saskatchewan Employment Act[75], которые определяют essential services как услуги, обеспечиваемые государством и необходимые ему для того, чтобы предотвратить угрозы общественной безопасности, жизни и здоровью граждан, разрушение или серьезное нарушение функционирования механизмов, оборудования и помещений, серьезный ущерб окружающей среде или создание помех для деятельности любого из судов штата Сасквачеван.

Указанные НПА позволяют составить представление о том, что включается в понятие essential services в национальных регуляторных практиках. Однако практически ни один документ не был переведен на русский, поэтому вопрос русскоязычной терминологии остается. Некоторую ясность позволяет внести обращение к документам МО, прежде всего МОТ.

- Понятие essential services неоднократно упоминается в документах Комитета по свободе объединения Административного совета МОТ, включая часть С раздела «Случаи ограничения или запрещения забастовки гарантии компенсации» в Сборнике решений Комитета (2016). В русскоязычной версии Сборника essential services переводятся как «жизненно важные службы» (ЖВС), «в строгом значении термина» под ними понимаются службы, прекращение деятельности которых может создать угрозу жизни, личной безопасности или здоровью всего населения или его части[76].

---

[72] Essential Services Commissoion. What we do, http://www.esc.vic.gov.au/corporate/about-us/what-we-do/.
[73] См.: An Act relating to the protection of the community against the interruption or dislocation of essential services [ASSENTED TO 26TH OCTOBER, 1979], Elizabethae Secundae Reginae No. 45 of 1979, https://www.legislation.qld.gov.au/LEGISLTN/ACTS/1979/79AC045.pdf.
[74] ACT NO. 59 OF 1968 [ 28th December, 1968 1. An Act to provide for the maintenance of certain essential services and the normal life of the community, https://indiankanoon.org/doc/902835/.
[75] BILL No. 128 An Act to amend The Saskatchewan Employment Act and to repeal The Public Service Essential Services Act. http://docs.legassembly.sk.ca/legdocs/Bills/27L3S/Bill27-128.pdf.
[76] Свобода объединения. Сборник решений, принятых Комитетом по свободе объединения Административного совета МОТ, и выработанных им принципов. Пятое издание. Международное бюро труда. Женева, пп. 541, http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---normes/documents/publication/wcms_455269.pdf.

- Стоить отметить, что в других решениях в том же разделе Комитет признает, что право на забастовку может быть ограничено или запрещено в сфере государственной службы или в жизненно важных службах, поскольку забастовка в этих службах может нанести серьезный ущерб населению страны. При этом уточняется, что понятие ЖВС в значительной степени зависит от конкретных обстоятельств, существующих в стране, а сама концепция ЖВС не является абсолютной: «служба, не являющаяся жизненно важной, может стать таковой, если забастовка продлится дольше определенного периода времени или выйдет за определенные пределы, создав таким образом, угрозу для жизни, личной безопасности или здоровья всего населения или его части»[77].
- В решении 585[78] приводится нестрогий и не исчерпывающий перечень ЖВС, который включает больничный сектор, энергоснабжение, водоснабжение, телефонную связь, полиция и вооруженные силы, пожарные службы, государственные или частные тюремные службы, доставку продуктов питания учащимся школьного возраста и уборку школ, а также управление воздушным движением.
- Отдельно приводится перечень служб, которые **не** относятся к ЖВС в строгом значении термина: радио- и телевизионное вещание, нефтяной сектор, порты, банки, компьютерные службы по сбору акцизов и налогов, универмаги и парки отдыха; металлургическая и горнодобывающая отрасли, транспорт в целом, летчики гражданской авиации, производство, транспортировка и распределение топлива, железнодорожный транспорт[79].

Таким образом, в документах МОТ и НПА стран Содружества понятие essential services рассматривается в более узком контексте, чем в документах ЕС по CIP и NIS – речь идет исключительно о службах, поддержание которых может вести к ограничению прав трудящихся на проведение забастовок. Такой контекст не совпадает с пониманием, заложенным в Директиву и «Зеленой книги ЕС», и напрямую не связан с обеспечением БСО технологической инфраструктуры и предотвращением инцидентов. Кроме того, документы МОТ и национальные НПА в этой сфере никак не затрагивают Интернет и вообще ИТ-сектор. Отсюда встает вопрос, актуально ли понятие «жизненно важных служб» как перевод essential services в документах ЕС. С учетом рассмотренных выше документов уместно отметить следующее:

1. Применительно к регуляторным актам ЕС неактуальным выглядит употребление понятия «службы». Документы МОТ не отражают отраслевую специфику ИТ-сектора, для которого характерны именно услуги (сервисы), оказываемые сетевыми операторами и другими субъектами преимущественно частного сектора. В сфере охраны труда, которую регулируют национальные НПА и документы МОТ, под службами обычно понимаются организационно выделенные функции государства как работодателя и «общественного провайдера» тех или иных благ. Кроме того, само понятие «служба» в контексте деятельности МОТ оформилось еще до появления Интернета и связанной с ним модели взаимодействия различных субъектов, основанной прежде всего на рыночных услугах/сервисах. Кроме того, контекстуально понятие «услуга» гораздо лучше отражает ориентацию на клиента, конечного получателя такой

[77] Там же, пп. 582.
[78] Там же, пп. 585.
[79] Там же, пп. 587.

услуги, в то время как понятие «службы» в большей степени замкнуто на функционирование самого государства, а также общества в целом. В итоге, для регулирующих документов ЕС представляется уместным заменить термин «службы» на «услуги».

2. Критерии и признаки отнесения услуг к категории «essential» в документах ЕС и, с другой стороны, национальных и международных актах об охране труда явно отличаются. Различается и перечень секторов и отраслей деятельности, службы и услуги в которых относятся к essential. Но при этом базовый критерий в рамках двух подходов в целом остается прежним: остановка предоставления соответствующих служб/услуг создает угрозу общественной безопасности, экономической деятельности жизни и здоровья граждан/населения. В итоге. понятие «жизненно важные» адекватно передает смысл соответствующих услуг/служб как для сферы регулирования трудового права, так и для обеспечения безопасности в ИТ-секторе.

Соответственно, в тексте исследования “essential services” переводятся авторами как **«жизненно важные услуги»**.

## Швеция

Одним из примеров государства ЕС, регуляторный подход и практики которого развиваются с существенной ориентацией на подход, сформулированный в документах ЕС, является Швецией.

На данный момент в Швеции существует достаточно развитый подход к обеспечению безопасности КИ и жизненно важных общественных функций (Vital Social Functions, VSF), который в том числе охватывает непосредственно сектор передачи данных и телекоммуникаций и во многом отвечает современному подходу ЕС. Нормативной основой этого подхода выступает План действий по защите жизненно важных общественных функций и КИ, принятый в 2014 г. В рамках плана объединенное понятие «защита VSF и КИ» реализуется в рамках комплексного подхода по управлению чрезвычайными ситуациями и основывается на трех стратегических принципах:

- Системный подход к защите VSF и КИ, основанный на ранжировании инфраструктуры и задач по уровням от местного до национального и подразумевающий активное вовлечение частных операторов.
- Выработка и реализация мер по защите, обеспечению устойчивости и восстановлению систем на трех этапах – до нарушения функционирования, во время и после.
- Подход нацелен на охват и предупреждение всех возможных рисков и угроз, включая неизвестные на данный момент.

Согласно Плану действий, эти задачи предполагается решить до 2020 г. В шведском подходе под КИ понимаются активы, системы или их составляющие, расположенные на территории государств-членов ЕС, которые являются незаменимыми для исполнения жизненно важных функций, поддержания здравоохранения, безопасности, экономического и социального благополучия населения; нарушение функционирования или разрушение таких систем и активов и систем окажет существенное воздействие на государство-член ЕС в результате невозможности выполнения таких функций. Собственно, критически важный статус таких функций закрепляется двумя критериями:

1. Отказ или масштабный сбой в осуществлении такой функции сам по себе или в сочетании с другими сходными событиями быстро приводит к развитию серьезной чрезвычайной ситуации или кризиса.
2. Такой вид деятельности является необходимым или незаменимым, в силу чего предполагается максимально полное преодоление негативных последствий общественного кризиса, вызванного сбоем в выполнении такой деятельности.

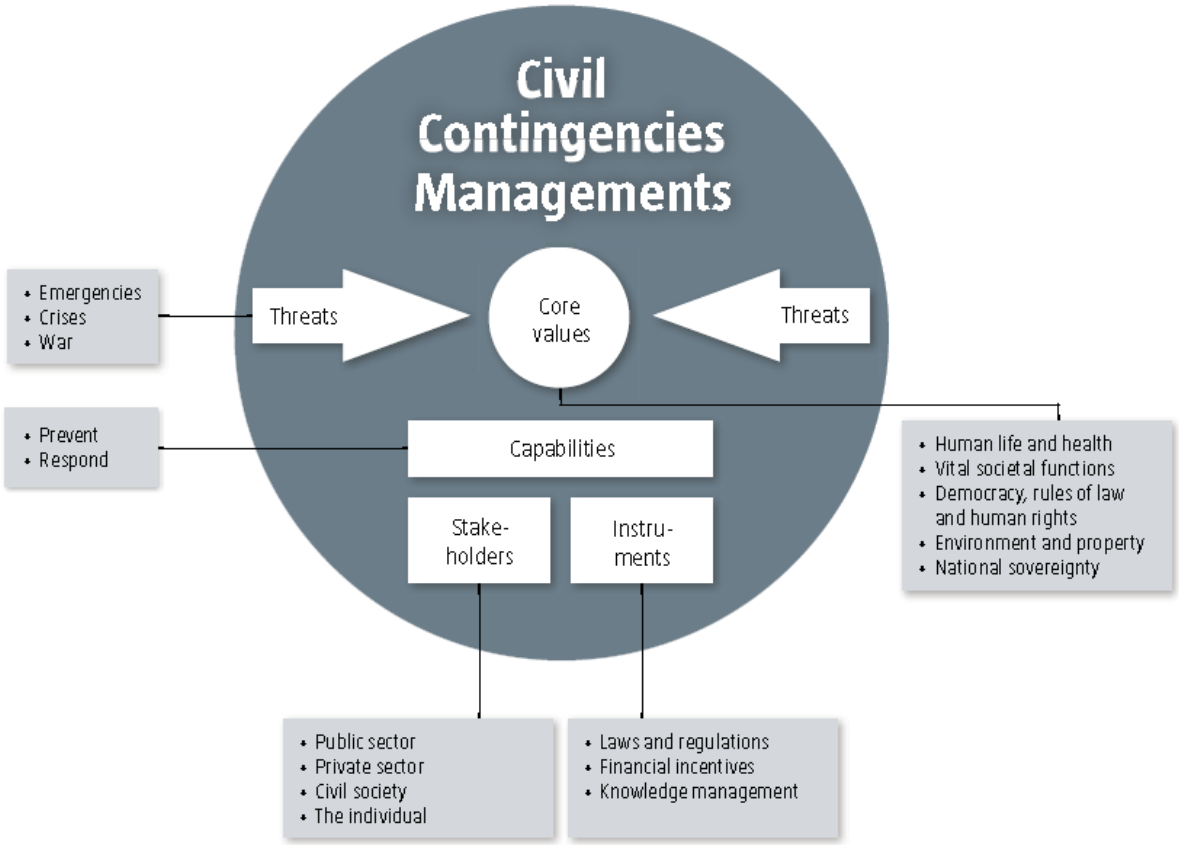
В свою очередь, под VSF понимаются виды деятельности, за счет которых решаются те или иные задачи; каждая жизненно важная функция включается в один из секторов общественной жизнедеятельности, а выполнение ее обеспечивается за счет той или иной КИ. В рамках секторального категорирования в Плане действий выделены 11 секторов, достаточно близких к классификации секторов КИ в рамках EPCIP, включая сектор информации и коммуникаций, в состав которого входят: мобильная и фиксированная телефонная связь, Интернет, радио-коммуникации, распределение почтовых отправлений, производство и распространение ежедневых газет, информационное наполнение вебсайтов, социальные медиа и проч.

Шведский систематический подход к защите КИ и VSF строится на комплексной модели безопасности, состоящей из трех компонентов:

- Управление рисками, включающее в себя выявление, обработку, оценку рисков и собственно управление рисками.
- Управление непрерывностью бизнеса ведется путем планирования того, как поддерживать процессы и виды деятельности, за счет которых обеспечивается исполнение необходимых функций вне зависимости от типов инцидентов и кризисных ситуаций.
- Планирование управлением различными событий от рядовых инцидентов до полномасштабных кризисных ситуаций, которое позволяет создать условия для эффективного управления событиями без ущерба для поддержания VSF и КИ.

Деятельность в этих направлениях прямо увязывается с международными стандартами, в частности, стандарту управления рисками ISO 31000 и стандарту управления непрерывностью бизнеса ISO 22301.

*Схема комплексной системы управления гражданскими ЧС в Швеции*




Источник: Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure. MSB (Swedish Civil Contingencies Agency), 2014. https://www.msb.se/RibData/Filer/pdf/27412.pdf

Что касается конкретно сектора телекоммуникаций и Интернета, наиболее любопытной составляющей шведского подхода выглядит практическая деятельность регуляторов по обеспечению защиты КИ, которая началась еще до принятия Плана действий. По состоянию на 2010 г. в Швеции Управление почты и телекоммуникаций

(PTS) реализовало программу по сокращению уязвимостей сетей линий электропередачи и сервисов ведущих телекоммуникационных операторов. После консультаций с операторами, национальными вооруженными силами и структурами гражданской обороны был запланирован ряд мер по обеспечению кризисной готовности и реагированию, включая направление по обеспечению устойчивости коммуникаций, которые были бы способны выдерживать сбои и продолжать функционировать, избегая падения качества или отказа предоставления услуг пользователям. За счет участия PTS каждому из трех крупнейших национальных операторов были поставлены 1600 малых резервных электрогенераторов, а также 10 мобильных базовых GSM-станций. PTS также запустила проект расширения сетей ВОЛС и закупила узловое оборудование для соединительных сетей, а также усилила инфраструктуру сетей линий электропередачи в крупнейших городах страны.

Кроме того, госрегулятор обустроил ряд защищенных подземных площадок и предложил использовать их телекоммуникационным операторам для размещения и установки критического оборудования, включая коммутаторы, инфраструктуру точек обмена трафиком (IXP), серверов DNS и проч. по себестоимости. Скальные бункеры оснащены автономными системами охлаждения, энерго- и водоснабжения, и даже защищены от применения ОМУ, включая биологическое, химическое и ядерное оружие, внешнего электромагнитного излучения и ракетно-бомбовых ударов. Использование таких объектов потенциально доступно для всех шведских телекоммуникационных операторов. По состоянию на 2010 г. государство также выделяло финансирование в размере 20 млн евро для содействия операторам в дальнейшем укреплении устойчивости и защищенности их инфраструктуры, закупке отказоустойчивого оборудования, строительства защищенных скальных объектов и выполнения учений и тренингов. Одним из пользователей этой инфраструктуры по состоянию на 2014 г. являлся один из крупнейших интернет- и телекоммуникационных шведских операторов IP-Only Telecommunication AB. В частности, для размещения одного из дата-центров компания использовала бывшее здание военного командного центра к югу от Стокгольгма, уходящее на 20 метров вглубь скальных пород. Согласно собственной оценке компании, жизненный цикл эксплуатации такого объекта составляет порядка 40-50 лет[80].

При оценке этих мер необходимо учитывать, что помимо инфраструктур национального значения шведские телекоммуникационные компании также обслуживают некоторые элементы глобальной системы УИИ. Так, независимая техническая инфраструктурная организация Netnod Internet Exchange i Sverige (Netnod) является оператором 5 точек обмена трафиком (IXPs) в Швеции и одной точки в Дании и предоставляет иные услуги в качестве провайдера, также управляет одним из авторитативных корневых серверов глобальной DNS (сервер I). Таким образом, шведские регуляторные наработки и лучшие практики, развивающиеся в русле общего подхода ЕС, привносят вклад в обеспечение БСО не только европейской, но и глобальной КИИ.

[80] IP-Only. Annual Report 2014 Full speed ahead! http://www.ip-only.com/wp-content/uploads/2015/10/IP-Only_annual_report_2014.pdf.

## США

Официальное определение термина «критическая инфраструктура» (Critical Infrastructure) в США содержится в Патриотическом акте[81]: системы и активы, физические или виртуальные, столь жизненно-важные для Соединенных Штатов, что приостановка их работы или их разрушение окажет разрушительные последствия для безопасности, национальной экономической безопасности, национальной системы общественного здравоохранения, системы общественной безопасности или нескольких из этих систем одновременно.
Главным американским государственным органом, руководящим и координирующим усилия по защите критической инфраструктуры, является Министерство внутренней безопасности, созданное в 2002 г. в соответствии с Актом о внутренней безопасности (Homeland Security Act). В продолжение Патриотического акта Акт о внутренней безопасности добавляет вторую составляющую к базовой терминологии США в сфере КИ, вводя понятие «ключевых ресурсов» (key resources), под которыми понимаются контролируемые государством или частным сектором ресурсы, жизненно важные для обеспечения минимальной функциональности экономики и системы государственного управления[82]. В более поздних законах и других НПА достаточно часто используется комбинированное понятие «критические инфраструктуры и ключевые ресурсы (КИ и КР, CIKR). При этом подробной системы категорирования и параметров КР ни в Акте 2002 г., ни в других открытых НПА не приводится.

Акт о внутренней безопасности от 2002 г. остается основой для выработки новых НПА, в том числе развивающих и конкретизирующих его положения в части защиты КИ в формате ГЧП. В марте 2016 г. в Сенат был внесен проект Акта о Национальном консорциуме по обеспечению готовности в сфере кибербезопасности (NCPC)[83], который расширяет возможности взаимодействия DHS с консорциумом, который был учрежден в 2004 г. профильными институтами и исследовательскими центрами четырех американских университетов (Арканзасский, Техасский, Норвичский университеты, а также Университет Мемфиса) и государственным агентством Texas A&M Engineering Extension Service. Основная цель консорциума – развитие частно-государственного и исследовательского взаимодействия в сфере повышения устойчивости к инцидентам кибербезопасности, обмен информацией, лучшими практиками и организация тренингов для развития практик частного сектора и регуляторных подходов в этой области. Законопроект NCPC расширяет возможности сотрудничества между консорциумом и DHS (в рамках существующего при министерстве центра интеграции национальной кибербезопасности и связи). Конкретные направления сотрудничества в области защиты КИ могут включать в себя проведение межсекторальных тренингов по кибербезопасности, тестовых упражнений по организации ответа на инциденты с участием представителей госорганов и местных властей, владельцев и операторов КИ и представителей частного сектора. Одной из

[81] SEC. 1016. CRITICAL INFRASTRUCTURES PROTECTION. UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001. PUBLIC LAW 107–56—OCT. 26, 2001 (https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf)
[82] An Act to establish the Department of Homeland Security, and for other purposes. PUBLIC LAW 107–296—NOV. 25, 2002. Department of Homeland Security. Sec. 2 – Definitions. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.
[83] An Act to authorize the Secretary of Homeland Security to work with cybersecurity consortia for training, and for other purposes. H. R. 4743 — 114th Congress (2015-2016). https://www.congress.gov/bill/114th-congress/house-bill/4743/text.

задач такого взаимодействия признается повышение антитеррористической киберзащищенности КИ в соответствии с целями Акта о внутренней безопасности от 2002 г.

Одной из обязанностей министерства в отношении КИ является создание Плана защиты критической инфраструктуры (National Infrastructure Protection Plan, NIPP). Этот план определяет либо президент США, либо министр внутренней безопасности. Первый такой план был выпущен в 2006 г., последний на июль 2016 г. – в 2013 г.[84] с приложением в 2015 г.[85] NIPP-2013, в частности, сконцентрирован на развитии единого концепта информационной и физической безопасности КВО, взаимосвязи между разными критическими отраслями, определил роль операторов и владельцев инфраструктур как ключевую.

Основным документом, регулирующим безопасность КИ в США, является Президентская директива № 21 «Безопасность критической инфраструктуры и устойчивость»[86]. Она предусматривает 16 отраслей, инфраструктуры в которых могут являться критическими, вместе с контролирующими их ведомствами:

| Ведомство | Отрасль |
|---|---|
| Министерство внутренней безопасности | Химическая |
| | Коммерческие объекты |
| | Коммуникации |
| | Критическое производство |
| | Дамбы |
| | Аварийно-спасательные службы |
| | Информационные технологии |
| | Ядерные реакторы, материалы и отходы |
| Министерство внутренней безопасности и Администрация служб общего назначения | Государственные учреждения |
| Министерство внутренней безопасности и министерство транспорта | Транспортные системы |
| Агентство по охране окружающей среды | Система водоснабжения и водоочистки |
| Министерство здравоохранения и социальных служб | Медицинские услуги и здравоохранение |
| Министерство здравоохранения и социальных служб и министерство сельского хозяйства | Питание и сельское хозяйство |
| Министерство финансов | Финансовые услуги |
| Департамент обороны | Оборонная промышленность |

[84] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf)
[85] Communications Sector-Specific PIan 2015. An Annex to the NIPP 2013 (https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf...
[86] PRESIDENTIAL POLICY DIRECTIVE/PPD-21 -- Critical Infrastructure Security and Resilience. The White House. Office of the Press Secretary. February 12, 2013,https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

| | |
|---|---|
| Министерство энергетики | Энергетика |

В Президентской директиве № 21 две отрасли – коммуникации и энергетика – выделяются как особо критические, так как «предоставляют возможности» для других критических отраслей.

Согласно той же директиве, Федеральная комиссия по связи (FCC) вместе другими федеральными органами власти и ведомствами (Государственный департамент, Министерство внутренних дел, Министерство юстиции и ФБР, Министерство торговли, Разведывательное сообщество, Комиссия по ядерному регулированию, Администрация общих служб) участвует в регулировании профильных критических отраслей; в случае FCC таковой является отрасль связи. В обязанности Комиссии входит:

(1) определять инфраструктуру связи и выстраивать для нее приоритеты;
(2) выявлять уязвимости сектора связи и работать с отраслью и другими заинтересованными сторонами над их закрытием;
(3) взаимодействовать с заинтересованными сторонами, включая отрасль, и вовлекать правительства и МО в работу по повышению безопасности и устойчивости КИ в рамках сектора связи, а также способствовать развитию и внедрению лучших практик повышения безопасности и устойчивости КИ сектора связи.

Третья цель упоминается и в Стратегическом плане FCC на 2015-2018 гг., причем Комиссия ставит акцент на взаимодействие с коммерческими операторами связи, которые сталкиваются с угрозами «критическим инфраструктурам Интернета»[87].

NIPP-2013 предлагает следующие элементы оценки и анализа рисков для КИ:

- Угроза - естественные или антропогенные события, лица, объекты или действия, которые могут причинить вред жизни, информации, окружающей среде или частной собственности.
- Уязвимость– физические свойства или функциональные атрибуты, которые открывают объект для использования или подвергают его опасности
- Последствие – эффект события / инцидента.

Управление рисками осуществляется в следующих областях:

- Предотвращение угрозы.
- Защита от угрозы.
- Смягчение угрозы.
- Ответ на инцидент.
- Восстановление после инцидента.

В качестве приложения к NIPP-2013 в 2015 г. был опубликован отраслевой план для коммуникационной отрасли[88], в 2016 г. – для отрасли информационных технологий[89].

[87] Federal Communications Commission Strategic Plan 2015-2018. https://transition.fcc.gov/Reports/strategic-plan-2015-2018.pdf.
[88] Communications Sector-Specific Plan. An Annex to the NIPP 2013 2015, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf.

Соответствующий отраслевой план приводит следующие критические функции для отрасли информационных технологий:

- Предоставление ИТ-продуктов и сервисов;
- Предоставление возможностей для управления инцидентами;
- Предоставление сервисов разрешения доменного имени;
- Предоставление услуг управления учетными данными;
- Предоставление через Интернет контента, информации и коммуникационных сервисов;
- Предоставление услуг маршрутизации, доступа и соединения.

Риски, связанные с предоставлением сервисов разрешения доменных имен, включают в себя:

- Нарушение работы Интернета в связи с техногенной атакой и, как следствие, несостоятельность механизма управления;
- Масштабная сетевая Denial-of-Service атака (DoS-атака) на инфраструктуру системы доменных имен (DNS).
- В плане предложены следующие меры для уменьшения рисков:
- Внедрение процессов для усиления контроля за качеством и обеспечения постоянного мониторинга DNS-инфраструктуры;
- Внедрение технологии Anycast;
- Использование разнообразной инфраструктуры, дублирование каналов и увеличение их устойчивости.

Первые два пункта списка уже реализуются, а третий, согласно плану, еще предстоит развивать. Отдельного определения КИИ в американском законодательстве не содержится. В документах FCC встречается термин «КИ сектора связи» (critical communications infrastructure)[90]

В регулировании защиты КИ от киберугроз главными документами являются правительственные распоряжения президента США «Об улучшении кибербезопасности критической инфраструктуры» (Executive Order (EO) 13636, 2013)[91], «Продвижение обмена информацией о кибербезопасности в частном секторе» (2015)[92] и «Комиссия для повышения национальной кибербезопасности» (2016)[93].

Особую роль играет EO 13636, который обеспечивает систематизацию и координацию политики в сфере обеспечения кибербезопасности КИ. В распоряжении используется определение КИ из Патриотического акта, с учетом которого для разных федеральных регуляторов и иных субъектов прописывается ряд направлений деятельности:

- DHS, Министерство юстиции и Управление директора национальной разведки регулярно готовят и публикуют открытые отчеты об угрозах кибербезопасности США, с указанием конкретных структур и организаций, в отношении которых

[89] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf
[90] См. FCC Strategic Plan 2015-2018…
[91] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[92] https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari
[93] https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

выявлена угроза. Такие доклады оперативно доводятся до соответствующей организации.

- Для содействия владельцам и операторам КИ в защите их систем от неавторизованного доступа, злонамеренной эксплуатации и нанесения ущерба DHS и Министерство обороны обеспечивают расширение добровольной программы обмена информацией – Углубленной программы услуг в сфере кибербезопасности (Enhanced Cybersecurity Services) на все секторы КИ. Механизм программы включает добровольное предоставление правительством секретных данных о киберугрозах и технической информации отдельным владельцам и операторам КИ.
- DHS разрабатывает основанный на анализе рисков подход к определению нового подвида КИ США – критических инфраструктур, подверженных наибольшим рискам (Critical Infrastructure at Greatest Risk). К этой категории включаются КИ, на которых инцидент кибербезопасности может повлечь катастрофические последствия регионального или национального масштаба в сфере общественной безопасности и здоровья, экономической и национальной безопасности. Отдельно оговаривается, что при разработке и применении критериев для такой категории КИ в нее не могут включаться коммерческие ИТ-продукты или ИТ-сервисы для конечных пользователей. Список КИ, подверженных наибольшим рискам, ведется, ежегодно обновляется и предоставляется президенту США DHS.
- Минобороны и Администрация общих служб предоставляют президенту США рекомендации по целесообразности, возможных преимуществах для обеспечения безопасности и оценке внедрения стандартов безопасности в процесс управления контрактами и планирования закупок.

Также согласно президентскому распоряжению Национальный институт стандартов и технологий США (NIST) в сотрудничестве со всеми заинтересованными сторонами, основываясь на существующих стандартах, директивах и лучших практиках, разрабатывает добровольную Базовую рамочную программу для уменьшения рисков кибербезопасности КИ (NIST Cybersecurity Framework)[94]. В основе программы лежат базовые действия, направленные на обеспечение кибербезопасности: идентификация, защита, определение, ответ и восстановление. Функции разделяются на категории и следом на подкатегории, а к каждой подкатегории приводится описание и указывается, на какие отраслевые документы и стандарты она опирается[95].

Для 22 категорий мер защиты, выделенных в структуре базовых действий, проработана не только их дальнейшая детализация по подкатегориям и индивидуальным номерам, но и осуществлена систематизированная привязка к национальным и международным стандартам, включая стандарты самого NIST, COBIT S, ИСО/МСЭ серии 27001, ISA серии 62443. При этом по сравнению с пластом нормативно-методических документов NIST предыдущего поколения – серией Специальных публикаций NIST SP (SP) 800-53 – в нынешней базовой рамочной программе усилен акцент на вопросы (и соответствующие стандарты), связанные с управлением бизнес-процессами, включая

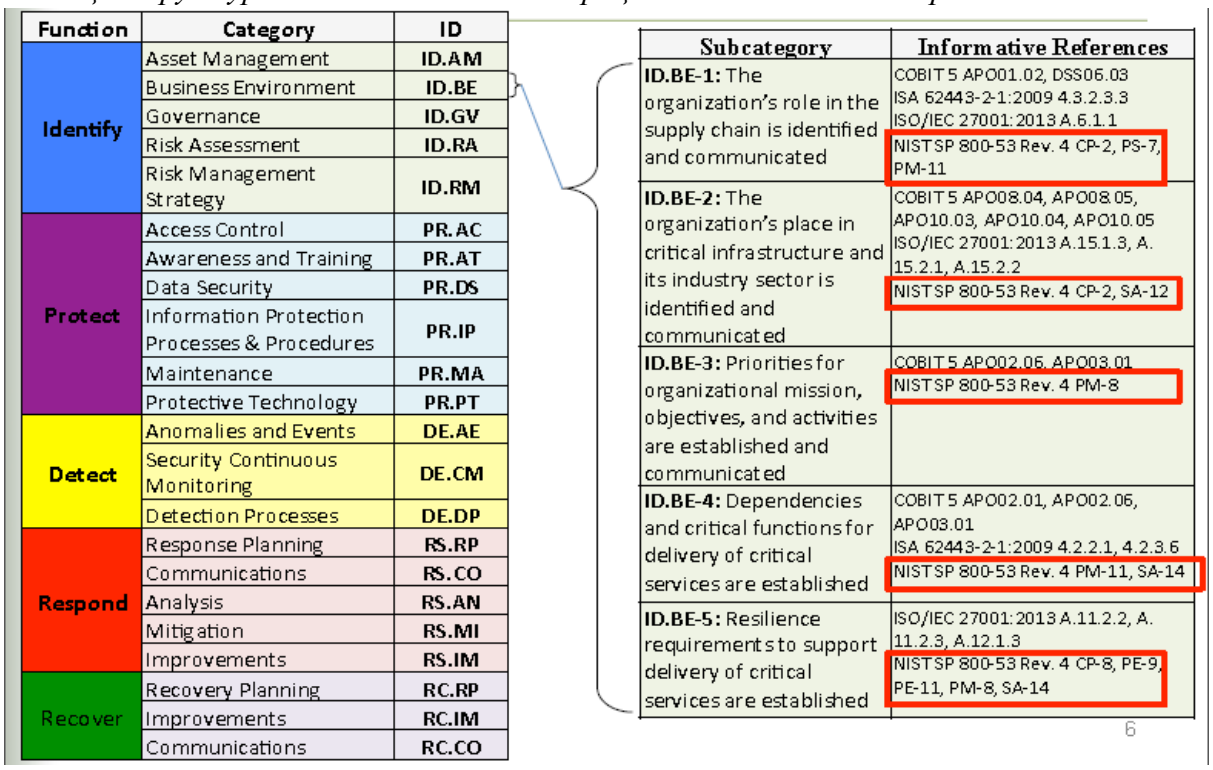
[94] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[95] Там же.

стратегии управления активами, оценки и управления рисками, корпоративного управления, поддержания бизнес-окружения.

К примеру, в категории «Бизнес-окружение» (ID.BE-01) выделяются пять подкатегорий:

- ID.BE-1: Определение роли организации в цепочке поставок и налаживание коммуникации по данному вопросу. Профильные стандарты: COBIT 5 APO01.02, DSS06.03, ISA 62443-2-1:2009 4.3.2.3.3, ISO/IEC 27001:2013 A.6.1.1, NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11.
- ID.BE-2: Определение места организации среди КИ и ее секторальной категории, налаживание коммуникации по данному вопросу. Профильные стандарты: COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2, NIST SP 800-53 Rev. 4 CP-2, SA-12.
- ID.BE-3: Определение организационной миссий, целей и видов деятельности организации, налаживание коммуникации по данным вопросам. Профильные стандарты: COBIT 5 APO02.06, APO03.01, NIST SP 800-53 Rev. 4 PM-8
- ID.BE-4: Установление зависимостей и критических функций, необходимых для предоставления критически важных услуг. Профильные стандарты: COBIT 5 APO02.01, APO02.06, APO03.01, ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6, NIST SP 800-53 Rev. 4 PM-11, SA-14.
- ID.BE-5: Установление требований по обеспечению устойчивости, необходимых для поддержания процессов, связанных с предоставлением критически важных услуг. Профильные стандарты: ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3, NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14.

*Таблица структуры базовых действий в процессе обеспечения кибербезопасности*



| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| Protect | Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

| Subcategory | Informative References |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | COBIT 5 APO01.02, DSS06.03<br>ISA 62443-2-1:2009 4.3.2.3.3<br>ISO/IEC 27001:2013 A.6.1.1<br>NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2<br>NIST SP 800-53 Rev. 4 CP-2, SA-12 |
| **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | COBIT 5 APO02.06, APO03.01<br>NIST SP 800-53 Rev. 4 PM-8 |
| **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | COBIT 5 APO02.01, APO02.06, APO03.01<br>ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6<br>NIST SP 800-53 Rev. 4 PM-11, SA-14 |
| **ID.BE-5:** Resilience requirements to support delivery of critical services are established | ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3<br>NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 |

Источник: Framework for Improving Critical Infrastructure Cybersecurity, January 2016. NIST, U.S. Department of Commerce, http://www.nist.gov/cyberframework/upload/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf.

Доработка публикаций NIST от 2013 г. и выработка итоговой версии Базовой рамочной структуры продолжаются по настоящий момент, но уже на нынешнем этапе ее проект представляет собой один из наиболее масштабных примеров систематизации и взаимоувязки политик, практик и стандартов в ИБ, БСО, управлении рисками, обеспечении непрерывности бизнеса и ряде других областей.

Одним из основных рабочих механизмов, обеспечивающих координацию работы DHS по обеспечению кибербезопасности КИ с другими регуляторами, а также с операторами КИ, вендорами ИТ-продукции и другими заинтересованными сторонами, является система секторальных партнерств КИ. В нее входят секторальные координирующие советы (SCC, объединяют владельцев и операторов КИ и представителей их торговых ассоциаций), (GCC, правительственные координирующие советы (по каждому сектору включают представителей профильных федеральных регуляторов, выступают как диалоговые партнеры для секторальных операторских советов).

В структуре секторов партнерства (как и вообще в регуляторной практике США) отдельно выделены сектор ИТ (IT Sector) и сектор связи (Communications Sector). В состав GCC ИТ-сектора входят представители Администрации общих служб, Минобороны, Минторговли, Министерства энергетики, Министерства юстиции, МВД, Госдепартамента и самого DHS; участниками соответствующего SCC являются более 90 крупнейших компаний сектора ИТ, телекоммуникаций, обороны и проч., включая Adobe, Microsoft Systems, Verizon, Northrop Grumman и проч.[96] GCC сектора связи включает 13 федеральных регуляторов, в т.ч. Комиссию по ядерному регулированию, а секторальный совет операторов – практически всех крупнейших американских телеком-провайдеров[97].

Базовой платформой для развития и координации секторальных партнерств служит Консультативный совет партнерства по КИ (CIPAC), деятельность которого ведется в соответствии с целями Национального плана по защите КИ (NIPP-21). Партнерства и советы по отдельным секторам действуют в рамках общей структуры CIPAC, но для всех секторов, включая ИТ и связь, форматы работы включают государственно-частное взаимодействие, общение операторов КИ с госрегуляторами, добровольный обмен информацией и наработками по совершенствованию защиты КИ.

В2015 г. DHS опубликовал документ «Установки безопасности для жизненно важных встроенных систем»[98], разработанный несколькими рабочими группами по критическим инфраструктурам. Хотя документ не является обязательным для операторов и владельцев КИ, он показывает позицию в отношении устройства информационных систем управления КВО.

[96] См. подробнее: Information Technology Sector: Council Charters and Membership. Department of Homeland Security. https://www.dhs.gov/information-technology-sector-council-charters-and-membership.
[97] Communications Sector: Council Charters and Membership. Department of Homeland Security. https://www.dhs.gov/communications-sector-council-charters-and-membership.
[98] Security Tenets for Life Critical Embedded Systems. November 20, 2015, https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf.

24 июня 2016 г. последовали регуляторные нововведения FCC в сфере обеспечения БСО критических коммуникационных инфраструктур, предложения по которым были опубликованы в августе 2015 г.[99] После обсуждения Комиссия приняла Приказ и доклад по вопросу улучшения и расширения данных отчетности о перебоях при эксплуатации подводных морских кабелей[100]. Приказ вносит в свод правил и регулирующих норм FCC поправки, включая новый раздел 4.15[101], согласно которому владельцы лицензий на эксплуатацию подводных морских кабелей обязаны отчитываться о перебоях при эксплуатации в случаях, когда:

(i) перебои, в том числе вызванные плановыми работами, на участке между оконечным оборудованием подводной линии (SLTE) на одном и на другом конце кабеля продолжаются более 30 минут;
(ii) на участке кабеля происходит потеря доступа к какой-либо оптической паре, включая потери доступа в связи с работой оконечного оборудования, продолжающаяся четыре часа и более, вне зависимости от количества от общего количества оптических пар на данном участке кабеля.

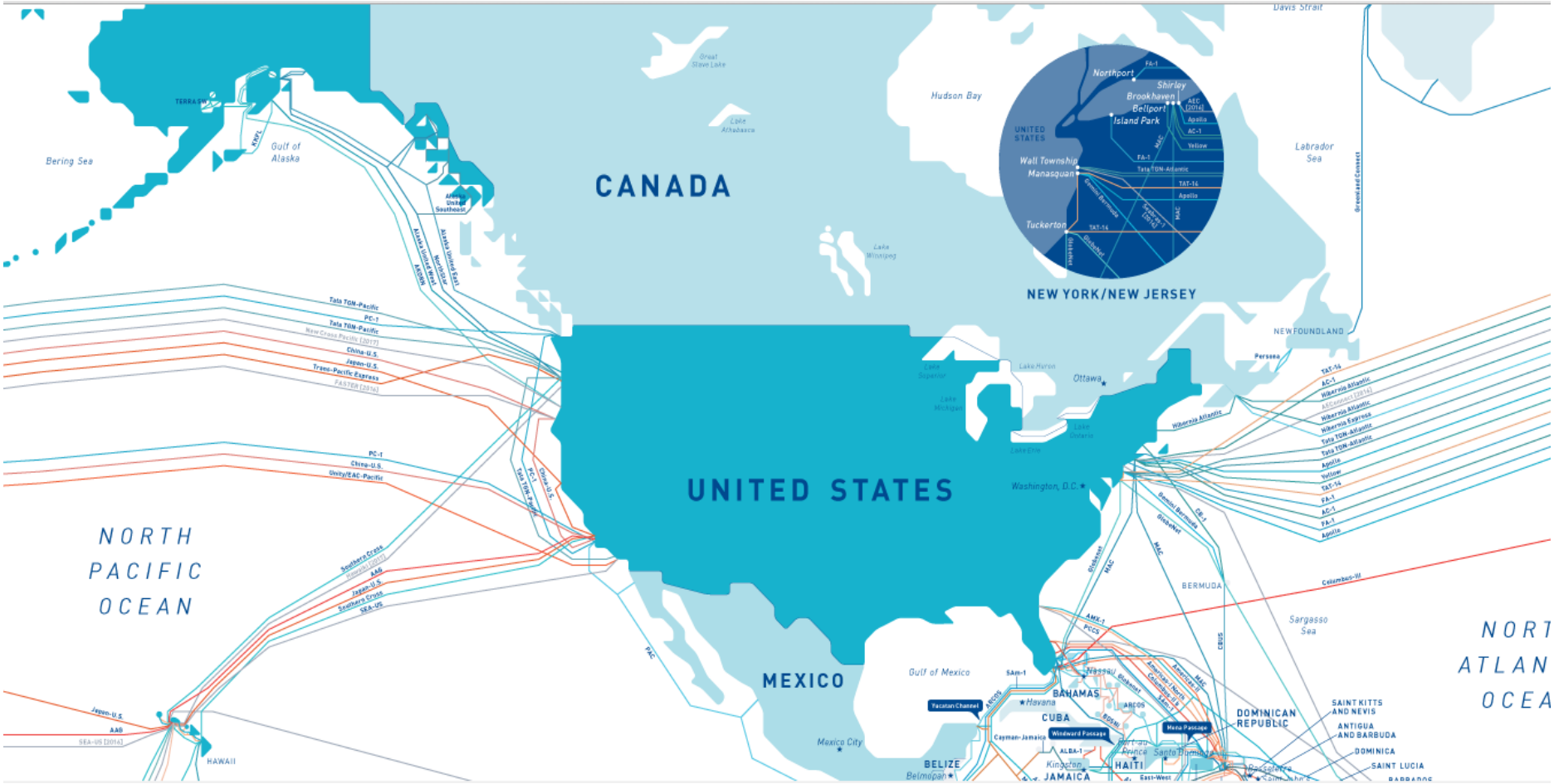
«Перебой» в контексте приказа определяется как отказ или значительное ухудшение качества предоставляемой лицензиатом услуги кабельной сети, вне зависимости от того, может ли лицензиат перенаправить трафик по альтернативному маршруту. Лицензиат обязан направить FCC первичное уведомление о перебое в течение восьми часов с момента выявления перебоя, который соответствует установленным критериям для предоставления отчетности. Если перебой является внеплановым, далее оператор направляет FCC предварительный и итоговый отчет, в котором указывается подробная информация о самом лицензиате, причине, локализации и продолжительности перебоя и его влиянии на предоставляемые услуги кабельной сети, а также мерах, предпринятых для устранения перебоя и временных параметрах его устранения.

В сопроводительных документах к приказу подчеркивается критическая важность морских подводных кабелей как составляющей коммуникационной инфраструктуры США. По информации, приведенной в документах FCC, порядка 60 подводных кабелей обеспечивают трансграничную передачу от 95 до 99% всего трафика сетей голосовой связи и передачи данных из США и обеспечивают инфраструктурный фундамент для совершения электронных транзакций на сумму 10 трлн USD ежедневно[102]. Потребность в улучшении практик отчетности возникла в силу того, что ранее операторы морских подводных кабелей, в отличие от провайдеров беспроводных, проводных наземных и спутниковых коммуникаций, не подпадали под требования обязательной отчетности о текущем состоянии эксплуатации своей инфраструктуры в Систему информирования о сетевых перебоях (NORS) при FCC. Такая отчетность была добровольной, обязательно было лишь предоставлять в FCC данные об общих эксплуатационных характеристиках инфраструктуры. В качестве

[99] Notice of Proposed Rulemaking In the Matter of Improving Outage Reporting for Submarine Cables and Enhancing Submarine Cable Outage Data. GN Docket No. 15-206. FCC 15-119. Federal Communications Commission. https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-119A1.pdf.
[100] Report and Order Before the Federal Communications Commission Washington, D.C. 20554 In the Matter of Improving Outage Reporting for Submarine Cables and Enhanced Submarine Cable Outage Data ) ) ) ) GN Docket No. 15-206. June 24, 2016. http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0712/FCC-16-81A1.pdf.
[101]Electronic Code of Federal Regulations. Title 47 Telecommunication. U.S. Government Publishing Office. http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title47/47tab_02.tpl.
[102] Там же, м. раздел II. The Need for Rules.

примера несовершенства системы отчетности и нехватки у регулятора полномочий по мониторингу перебоев и доступу к морской кабельной инфраструктуре в ряде серьезных инцидентов, включая повреждение тайфуном морского кабеля между островом Гуам и Сообществом Северных Марианских островов в июле 2015 г., ликвидация последствий которого растянулась на три недели.

*Карта трансконтинентальных подводных волоконно-оптических кабельных систем США в 2016 г.*




Источник: Submarine Cable Map 2016. TeleGeography. Authoritative Telecom Data, https://www.telegeography.com/assets/website/images/maps/submarine-cable-map-2016/submarine-cable-map-2016-x.png.