О кибербезопасности критической инфраструктуры государства

М.А. Шнепс-Шнеппе, С.П. Селезнев, Д.Е. Намиот, В.П. Куприяновский

***Аннотация*—Данная статья является первой попыткой систематизации и описания предложений по киберзащите объектов критической инфраструктуры в мире. В работе показывается ведущая роль телекоммуникаций в этом процессе. Представлены стандарты кибербезопасности в США, особенно касающиеся кибербезопасности систем связи США. Особое внимание обращается на защиту баз данных, что иллюстрируется примером тестирования сети DISN. Даны соображения о защите объектов критической инфраструктуры в России.**

***Ключевые слова*—киберзащита, кибербезопасность, критическая инфраструктура.**

I. Введение

Обеспечение безопасности критической инфраструктуры (Critical Infrastructure Protection, CIP) представляет собой концепцию готовности противодействовать серьезным угрозам работы важных объектов инфраструктуры и объектов повышенной опасности в регионе или стране, особенно в условиях распространения информационных технологий и связанных с ними киберугроз.

Исторически, первым шагом в этом направлении было создание в 1996 году Комиссии по защите жизненно важной инфраструктуры при президенте США: была поставлена задача разработать всеобъемлющую национальную стратегию по защите инфраструктуры от физических и кибернетических угроз. Похожая же директива издана в Европейском Союзе в 2008 году [1]. В России основные направления государственной политики по защите критически важных объектов инфраструктуры утверждены в 2012 г. [2]. В этом документе поставлена цель совершенствовать безопасность информационных и телекоммуникационных систем критической инфраструктуры, и объявлен план работ до 2020 года. Практически на сегодня наибольшая активность в России сосредоточена в направлении «Безопасный город» [3].

Настоящая статья является продолжением нашей работы по анализу телекоммуникационной инфраструктуры аппаратно-программного комплекса «Безопасный город» [3], где также детально обсуждалась Система-112, считая ее частью «Безопасного города». АПК «Безопасный город» должен объединить в себе любые системы (информационные, мониторинговые, оповещающие, приемопередающие) любого муниципального образования, а в перспективе – и всей страны. И, самое главное, АПК «Безопасный город» должен иметь высокий уровень собственной информационной безопасности. Поэтому при его создании необходимо использовать российское аппаратное и программное обеспечение, изначально разрабатываемое под российские стандарты безопасности.

Отметим, что ведущая роль в обеспечении кибербезопасности критической инфраструктуры принадлежит телекоммуникациям – как в обеспечении собственной безопасности, так и всех важных объектов. К сожалению, следует отметить, что российские сети связи построены в основном на базе иностранного оборудования. Гордостью «Ростелекома» является сеть IP/MPLS, объединяющая всю страну и имеющая многие выходы на международные IP сети (рис. 1). Она построена на базе маршрутизаторов компании Juniper. Всего имеется 150 узлов: несколько мощнейших Juniper router T1600 (1,6 Tb/s) и множество меньших. Но в условиях кибервойны, возникает провокационный вопрос: не является ли эта сеть американским кибероружием?

Благодаря разоблачениям Э. Сноудена (Washington Post, 30.98.2013), стало известно о шпионской программе GENIE, разработанной Агентством национальной безопасности (АНБ), которая проникает в зарубежные сети и ставит их под контроль США. К концу 2013 года было заражено как минимум 85 тыс. стратегических серверов. Сейчас АНБ внедряет более мощную систему – TURBINE, которая будет управлять имплантами для сбора разведывательной информации в автоматическом режиме. К началу 2014 года она заразила до 100 тыс. серверов [4]. Система TURBINE составляет основу крупнейшей программы кибервойны Quantum, которую АНБ реализует в содружестве с телефонными операторами и пользуясь услугами мощной серверной сети. Головной офис Quantum находится в штаб-квартире АНБ (Форт Мид, штат Мэриленд), а отделения - в Японии и Великобритании.

Статья получена 6 июня 2016.

М.А. Шнепс-Шнеппе, AbavaNet (e-mail: sneps@mail.ru)
С.П. Селезнев, Фактор-ТС (e-mail: sergei.seleznev@gmail.com)
Д.Е. Намиот, МГУ имени М.В. Ломоносова (e-mail: dnamiot@gmail.com)
В.П. Куприяновский, МГУ имени М.В. Ломоносова (e-mail: vpkupriyanovsky@gmail.com)

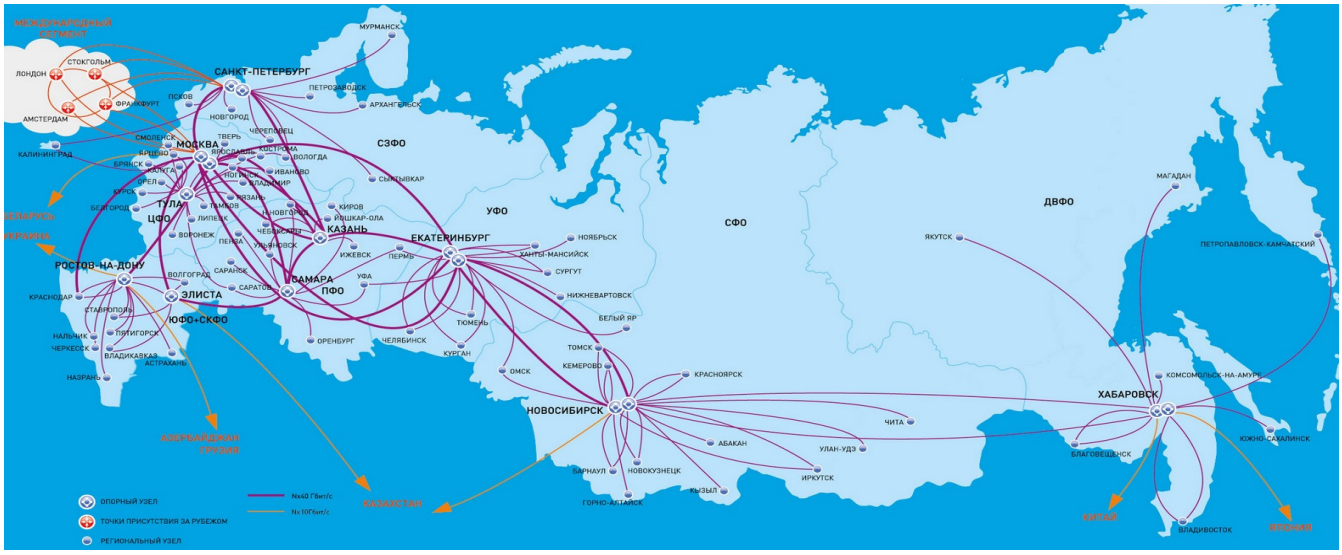
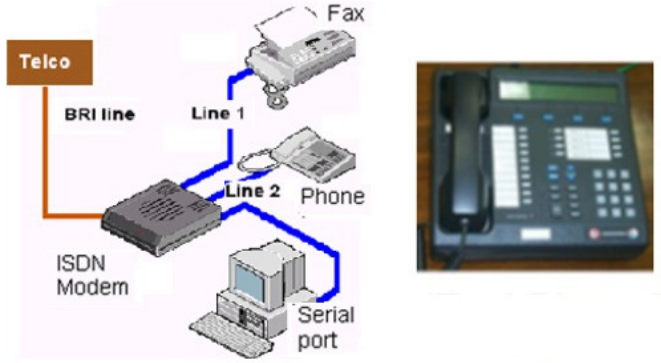


Рис. 1 Сеть IP/MPLS – гордость «Ростелекома».

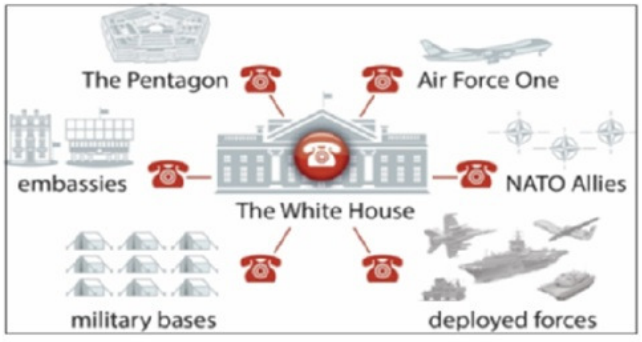
Кроме того, имеется множество хакеров-любителей. Например, в 2013 году телекоммуникационные компании Германии зарегистрировали небывалое количество хакерских атак - до одного миллиона ежедневно [5]. Два года назад это число было только 300 тысяч. Экономические потери, вызванные хакерскими атаками, в 2013 году составили около 575 млн. долл.

Угрозы кибервойны привели к поразительному факту в США: правительственная сеть США отказалась от установки IP телефонов [3]. Сверхсекретная сеть DRSN (Defense RED Switched Network) — это выделенная телефонная сеть, которая обеспечивает управление вооруженными силами США (рис. 2B). Вопреки желанию идеологов строящейся военной инфокоммуникационной системы DISN (Defense Information System Network), где предполагается переход от существующей телефонной сигнализации SS7 на новый интернет-протокол AS-SIP, сеть DRSN, сохраняет «старую» технологию коммутации каналов, точнее, ISDN (Integrated Services Digital Network) каналы (рис. 2A). Поэтому маршрутизаторы строящейся сети DISN будут вынуждены работать не только на сети коммутации пакетов, но и на сети коммутации каналов.



А)

Б)



В)

Рис. 2. А) Иллюстрация использования ISDN линии. Б) «Красный» телефон. (Обратите внимание на щель справа внизу – для криптокарты и на 4 кнопки наверху – для выбора приоритетности разговора.) В) Схема правительственной сети DRSN.

Настоящая статья посвящена краткому описанию работ по киберзащите критической инфраструктуры в мире (Раздел 2), имея целью показать ведущую роль телекоммуникаций. В Разделе 3 рассказано о стандартах кибербезопасности в США, а в Разделе 4 – о кибербезопасности систем связи США. Особое внимание обращается на защиту баз данных, что иллюстрирует пример тестирования сети DISN (Раздел 5). Статья завершается соображениями о защите объектов критической инфраструктуры в России (Раздел 6).

II О ЗАЩИТЕ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

США. Поворотным моментом послужил теракт в Нью-Йорке 11 сентября 2001 года, и, как мера противоборства, в 2003 году была образована мощнейшая структура - Министерство внутренней безопасности США (Department of Homeland Security), хотя борьба с терроризмом началась значительно раньше. Уже в 1996 была создана Комиссия президента по защите жизненно важной инфраструктуры (PCCIP, President's Commission on Critical Infrastructure Protection). Была поставлена задача разработать всеобъемлющую национальную стратегию по защите инфраструктуры от физических и киберугроз.

Комиссия была разделена на пять команд,

представляющих девять критических инфраструктур. Каждая команда оценивала растущие риски, угрозы и уязвимости. Работа комиссия PCCIP имеет пять направлений:

• Information & Communications: телекоммуникации, компьютеры и программное обеспечение, Интернет, спутники, оптоволокно

• Physical Distribution: железные дороги, воздушное и морское сообщение, трубопроводы

• Energy: электроэнергия, природный газ, нефть, производство, распространение и хранение

• Banking & Finance: финансовые операции, фондовые и рынки облигаций, Федеральная резервная система

• Vital Human Services: вода, аварийные службы, государственные службы

Федеральное правительство США разработало стандартизированное описание критической инфраструктуры, чтобы облегчить контроль и подготовку к ликвидации ЧС:

• Правительство требует от частных компаний в каждом критическом секторе экономики оценки его уязвимости от физических и/или кибер атак,

• Планы устранения слабых мест и планов реагирования;

• Разработку системы идентификации и предотвращения попыток нападения; объявить тревогу, быть способным отбить нападение и затем, с Федеральным агентством по управлению в чрезвычайных ситуациях(FEMA), восстановить нарушенные существенные функции объекта.

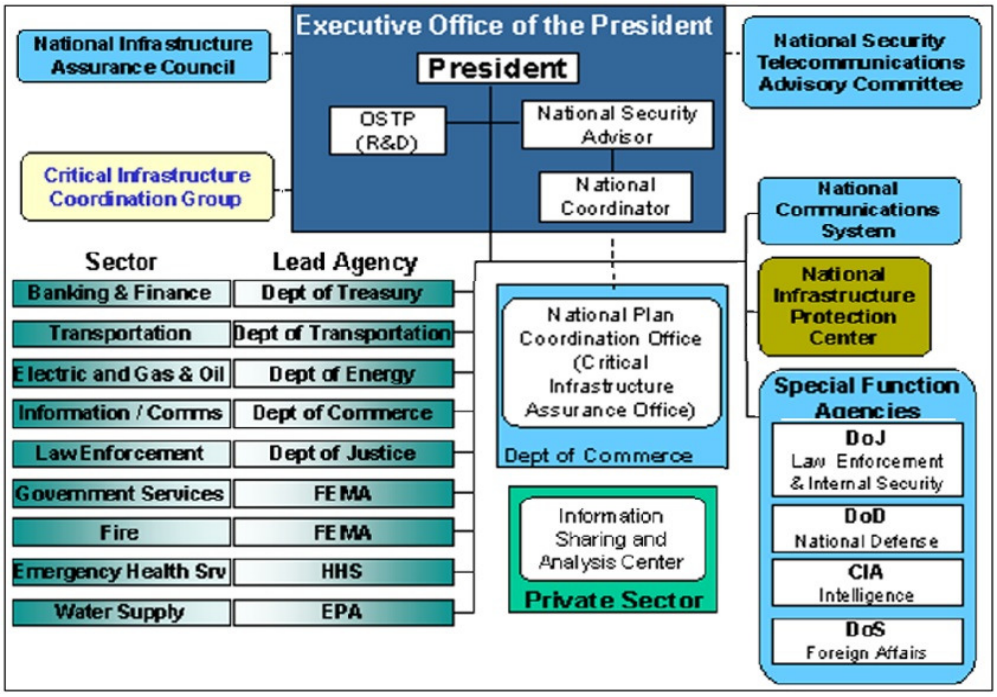


Рис. 3. Структура защиты критической инфраструктуры США.

Европейский Союз. На перспективу предусмотрено расширение забот по защите критической инфраструктуры (CIP) [6]. Эту работу курирует ERNCIP (European Reference Network for Critical Infrastructure Protection) Office. Работа ведется в восьми тематических группах:

- Прикладная биометрия для CIP
- Безопасность авиационной техники
- Промышленная автоматизация и системы управления
- Химические и биологические риски в водном секторе
- Оборудование для обнаружения взрывчатых веществ (неавиационных)
- Радиологические угрозы критической инфраструктуры
- Устойчивость конструкций к взрывному воздействию
- Видео аналитика и наблюдения.

Пример Германии: телекоммуникации и атомные электростанции одинаково важны. В качестве примера реализации программы ERNCIP укажем на опыт Германии в области кибербезопасности [7]. В феврале 2016 г. принят новый Закон «IT SECURITY ACT», который имеет шесть разделов: (1) Энергетика, (2) IT и телекоммуникации, (3) Транспорт и перевозки, (4) Здравоохранение, (5) Пища и вода, (6) Финансы и страхование.

Согласно новому закону, 2000 немецких компаний имеют критически важные объекты инфраструктуры и подлежат государственному регулированию силами BSI (IT security department of the Bundestag and the Federal Office for Information Security). Закон об информационной безопасности не только обязует защитить свои веб-сайты, но и защищать другие свои ИТ-системы. Закон предписывает внедрять законом предусмотренные меры безопасности ИТ-систем в течение двух лет, а их выполнение будет проверяться не реже одного раза в два года.

Кроме того, в течение шести месяцев необходимо создать внутреннюю структуру отчетности, чтобы в BSI сообщать об инцидентах IT-безопасности. В настоящее время эта отчетность является обязательной только для операторов атомных электростанций и телекоммуникационных компаний. Невыполнение предписаний по IT-безопасности подлежат штрафным санкциям. Штрафы в размере до 100 000 евро могут быть наложены на операторов критической инфраструктуры, которые допускают ИТ-инциденты в сфере безопасности, не сумев реализовать предписанные меры ИТ-безопасности.

III О стандартах кибербезопасности в США

Национальные стандарты США разрабатывает Национальный институт стандартов и технологий (NIST, National Institute of Standards and Technology). В соответствии с Распоряжением Правительства "Улучшение кибербезопасности критической инфраструктуры", разработана Рамочная концепция (Framework), которая состоит из множества документов: стандартов, методик, процедур и процессов [8]. Меропрятия по киберзащите подробно изложены в [9].

Общий поток информации и решений о кибербезопасности в рамках любой организации состоит из трех уровней (рис. 4):

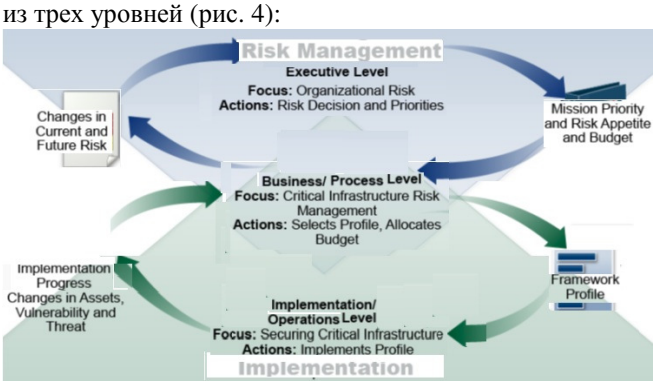


Рис. 4. Потоки информации и решений о кибербезопасности в рамках организации.

- Руководство (Executive): уровень определяет приоритеты, доступные ресурсы и общие риски,
- Бизнес-процессы: уровень использует информацию в процессе управления рисками, сотрудничает с исполнителями,
- Исполнительный уровень: здесь сообщается ход реализации бизнес-процессам.

Рамочная концепция [8] состоит из пяти функций киберзащиты:

• Выявить (Identify) - разработать понимания рисков и управления ими для кибербезопасности системы в целом, ее активов, данных и функциональных возможностей.

• Защитить (Protect) - разработать мероприятия по доставке сервисов для обеспечения киберзащиты важнейших объектов инфраструктуры.

• Обнаружить (Detect) – разработать и внедрить соответствующие мероприятия по выявлению событий кибербезопасности.

• Ответить (Respond) - осуществить соответствующие мероприятия киберзащиты при обнаружении событий кибербезопасности.

• Восстановить (Recover) – восстановить нарушенные функции из-за события кибербезопасности и обеспечить устойчивость работы системы.

Эти пять функций состоят из 22 мероприятий по обеспечению кибербезопасности (Таблица 1), которые детально описаны в стандарте [9].

IV Кибербезопасность систем связи США

В 2015 г. NIST организовал Рабочую группу РГ4 по применению Cybersecurity Framework для нужд поставщиков услуг связи [10]. Работа РГ4 велась по пяти подгруппам в соответствии с пятью ключевыми частями отрасли связи (рис. 5):

- Вещание (Broadcast): В США имеется более 15000 радиостанций и 1700 станций телевещания, которые предоставляют новости, информацию по чрезвычайным ситуациям и другие услуги по радио- и ТВ-каналам.
- Кабельная сеть (Cable): Кабельная сеть состоит из около 7791 кабельных систем, которые предлагают аналоговые и цифровые видеопрограммы, телефонную связь и высокоскоростной доступ к Интернету.
- Спутниковая связь (Satellite): спутниковые системы связи используют наземное оборудование для доставки данных, голоса, видео и широковещательной связи любому лицу на территории США и в любом месте мира.
- Беспроводная связь (Wireless): Беспроводная индустрия обеспечивает беспроводные широкополосные услуги, которые включают передачу данных, голоса и видео для более чем 335 миллионов активных беспроводных устройств по всей стране, в том числе более 175 миллионов смартфонов, 25 миллионов таблетов и 51 миллионов устройств приема данных. В США имеется около 160 операторов беспроводной связи, которые управляют и поддерживают работу более 304 тысяч базовых станций.
- Проводная связь (Wireline): Более 1000 компаний предлагают проводные услуги, служат основой сети Интернета.

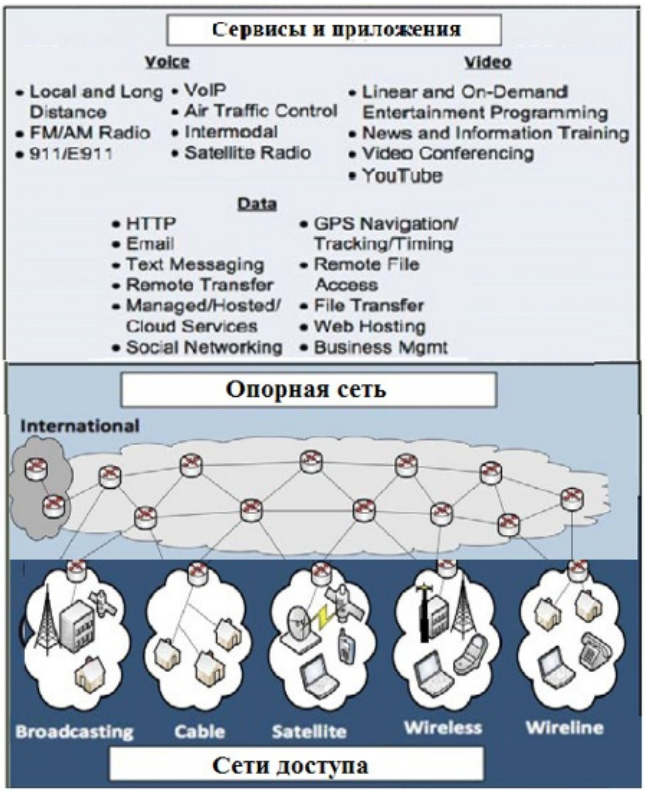


Рис. 5. Архитектурная модель телекоммуникаций.

Рассмотрим детальнее кибербезопасность двух сегментов сетей связи: местных радиостанций и беспроводных сетей.

Местные радиостанции (рис. 6) имеют множество уязвимых мест, что требует повышенной киберзащиты. Это включает: источники контента, поставляемого через IP область, коммерческие услуги, такие производственные ресурсы, как лента новостей Associated Press, удаленные операции, протокол оповещения о природных катаклизмах CAP (Common Alerting Protocol), каналы удаленной передачи программ (STL, Studio Transmitter Links), передачи телеметрии и управления.

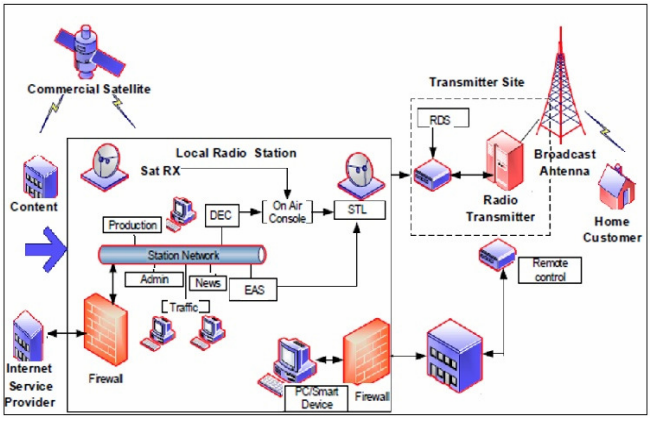


Рис. 6. Схема местной радиостанции.

Таблица 1. Мероприятия кибербезопасности в США.

Function	Category
Identify Выявить	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect Защитить	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes
	Maintenance
	Protective Technology
Detect Обнаружить	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond Ответить	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover Восстановить	Recovery Planning
	Improvements
	Communications

Беспроводные сети состоят из множества физических и логических объектов, которые обеспечивают поддержку мобильных устройств, сетевые функции и телекоммуникационные услуги. Поддержка включает обеспечение бесперебойной работы сети и контроль ее характеристик, управление мобильными информационными устройствами, контроль качества услуг, обеспечение механизмов сигнализации и передачи пользовательской информации. На рис. 7 представлена архитектура трех поколений мобильных сетей: сеть 2го поколения (она же GSM), построенная на средствах коммутации каналов, сеть 3го поколения, сочетающая коммутацию каналов и пакетов (особенно для передачи сообщений GPRS) и новейшая сеть 4го поколения - LTE, построенная исключительно на средствах коммутации пакетов и SIP сигнализации.

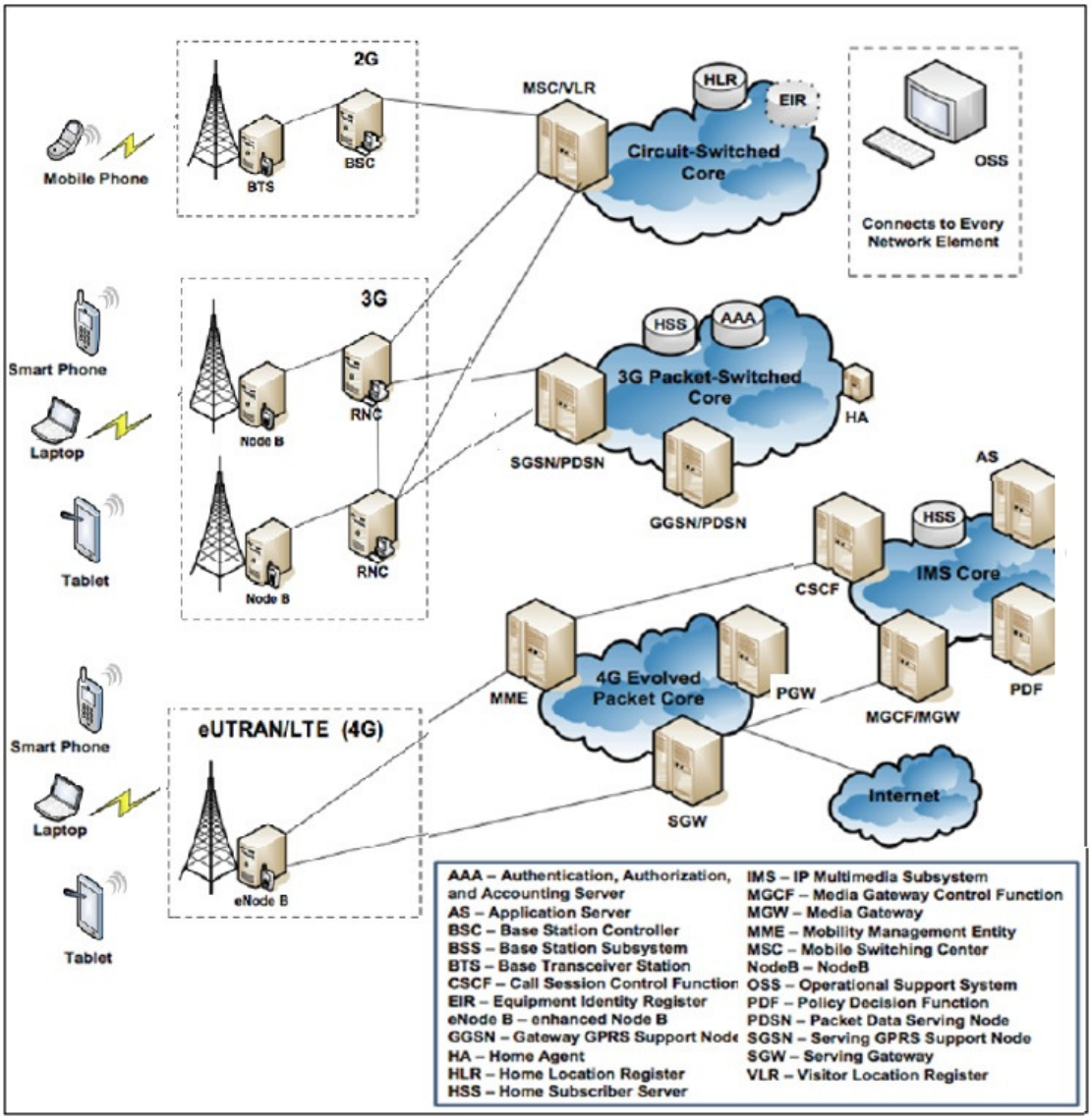


Рис. 7. Архитектура трех поколений мобильных сетей.

Мобильные сети составляют важнейшую часть охраны критической инфраструктуры и требуют повышенных мер кибербезопасности. Наиболее уязвимыми узлами мобильных сетей являются базы данных:

- Регистры местоположения. Они обеспечивают информацию о местоположении мобильных устройств. Это – «домашний» регистр HLR (Home Location Регистр) и регистр местонахождения визитеров VLR (Visitor Location Register).
- Регистры идентификации и аутентификации. Устройства идентификации и аутентификации (AAA) являются основными для правильной и надежной работы сети мобильной связи. Кроме того, критическим элементом является база данных абонентов HSS (Home Subscriber Server).
- Управление мобильностью (Mobility Management Entity). Управление мобильностью является одной из основных функций новейшей сети LTE. Узел MME является ключевым узлом управления и участвует в таких функциях, как процесс активации/деактивации процессов передачи потоков пакетов, отвечает за подключение к сети мобильной связи и оперативный контроль.
- Системы сигнализации (общие с проводными сетями). Узлы сигнализации обеспечивают управление сетью и предоставление услуг связи, точнее, обеспечивают координацию, надежность и аутентификацию для выполнения всех основных функций: работу регистров местоположения, регистров идентификации и аутентификации, коммутации мобильной связи и управления мобильностью терминалов. Базовыми протоколами сигнализации являются: система сигнализации № 7 (SS7), протокол ISUP пользователей ISDN, протокол GSM-MAP пользователей GSM-приложений и другие.

К настоящему времени наиболее изучены приемы предупреждения кибератак на протоколы SS7 в проводных сетях [11].

Экстренные вызовы в мобильных сетях. Широкое распространение мобильных устройств, их доступность для пользователей становится решающим фактором для

обеспечения связи во время стихийных бедствий и других чрезвычайных ситуаций. Это привело к разработке ряда специальных услуг, где ключевую роль играют базы данных.

1) Беспроводные оповещения в чрезвычайных ситуациях WEA (Wireless Emergency Alerts): текстовые сообщения - оповещения, которые появляются на экранах мобильных устройств о чрезвычайных ситуациях. Сообщения WEA имеют две особенности: (1) WEA используют различные виды технологий, чтобы обеспечить немедленную доставку этих предупреждений вне зависимости от загрузки сети, (2) WEA использует режим точка-многоточка, т.е. предупредительные сообщения будут отправляться всем мобильным пользователям в пределах заданной территории.

2) Экстренные вызовы E911 и NG911. Мобильная сеть обеспечивает пропуск экстренных вызовов к Центрам обслуживания вызовов PSAP (Public Safety Answering Point). Мобильное устройство, независимо от того, зарегистрировано ли оно на сети, имеет возможность поддерживать вызов, когда пользователь называет цифры "911". В дополнение к голосовой связи, в настоящее время внедряется передача текстовые сообщения, что важно для лиц с дефектами слуха.

Новейшее поколение службы 911 - NG911 (Next Generation 911) обеспечит передачу разной дополнительной информации о происшествии, включая фотографии и видео.

3) Беспроводные приоритетные услуги (WPS, Wireless Priority Services). WPS является программой Министерства внутренней безопасности США (Department of Homeland Security, DHS) для обеспечения национальной безопасности и готовности к чрезвычайным ситуациям. Услуга WPS предназначена для использования в чрезвычайных или кризисных ситуациях, когда беспроводная сеть может быть перегружена и вероятность завершения обычного вызова уменьшена. К этому ряду экстренных вызовов примыкает Правительственный экстренный телекоммуникационный сервис GETS (Government Emergency Telecommunications Service).

Этот краткий перечень новых типов экстренных вызовов (WEA, NG911, WPS, GETS) иллюстрирует актуальность области, в том числе в смысле киберзащиты, но и являет собой пример сложностей смены парадигмы телекоммуникаций: организаторы экстренных служб никак не желают переходить на коммутацию пакетов (вместо традиционной телефонной связи).

Принципы киберзащиты по документам ITU. ITU особое внимание уделяет унификации методов доступа к сети [12]. Согласно Рекомендации ITU-T X.1205, термин "управление доступа" определяет системы аутентификации и авторизации услуг, что и контролирует использование ресурсов сети. Аутентификация представляет собой процесс, в котором пользователь или организация запрашивает создание идентификатора. Авторизация же определяет уровень допустимых привилегий абонента на основании контроля доступа. Права доступа зависят от правил (политики) управления. На рис. 8 изображена эталонная модель ITU-T X.1205 для безопасной аутентификации и авторизации с множеством баз данных.

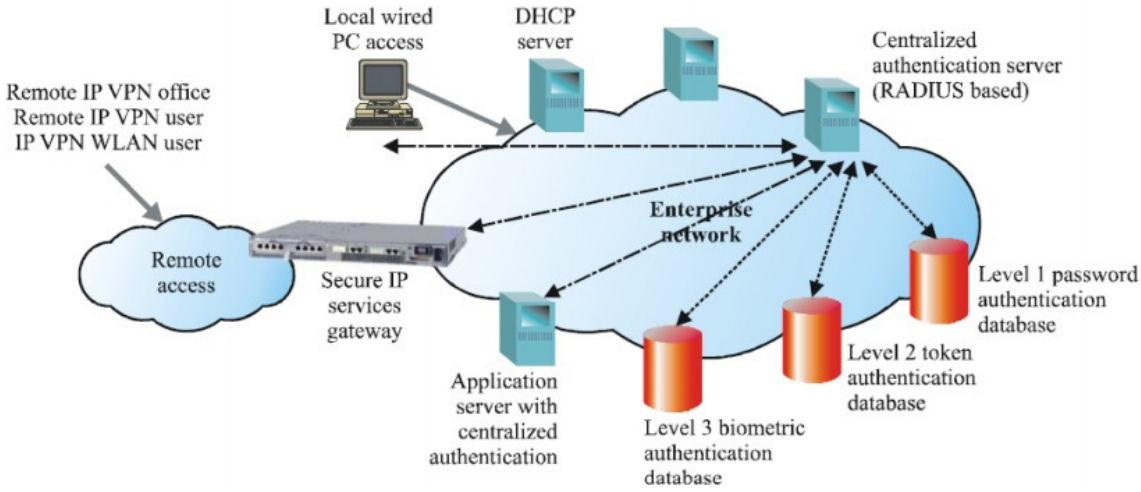


Рис. 8. Эталонная модель ITU-T X.1205 для безопасной аутентификации и авторизации.

В соответствии с эталонной моделью, администрации стран должны получать решения, которые отвечают следующим целям:

- Централизованная аутентификация - механизм облегчает администрирование и устраняет необходимость в локальном хранении учетных данных (паролей или сертификатов);
- Централизованная авторизация - совместно с аутентификацией, такой подход гарантирует, что доступ к системным ресурсам осуществляется прозрачным и проверяемым способом;
- Применение сложных паролей;
- Безопасное хранение всех паролей в односторонне зашифрованном (хэшированном) формате;
- Простота - принцип заключается в обеспечении простоты использования и администрирования; и
- Безопасное протоколирование всех событий по аутентификации и авторизации.

V Пример тестирования базы данных

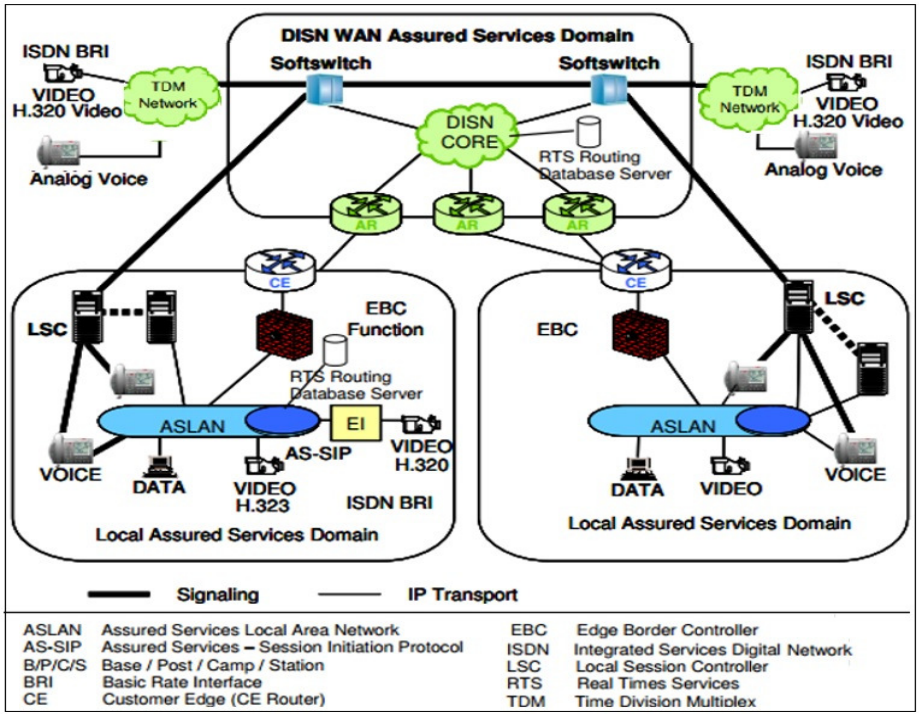


Рис. 9. Архитектура предоставления сервисов на сети DISN.

В качестве примера приведем тестирование одной из баз данных оборонной сети DISN [13]. Речь идет о тестировании базы данных компании Avaya. База DB работает по протоколу LDAP (Lightweight Directory Access Protocol) и использует сервер IBM 3550. Эта база данных определяет маршрутизацию сервисов реального времени RTS (Real Times Services) в соответствии с требованиями унифицированных свойств UC (Unified Capabilities). Вопросы программирования сервисов RTS и требованиям к унифицированным свойствам UC подробно изложены в [14,15].

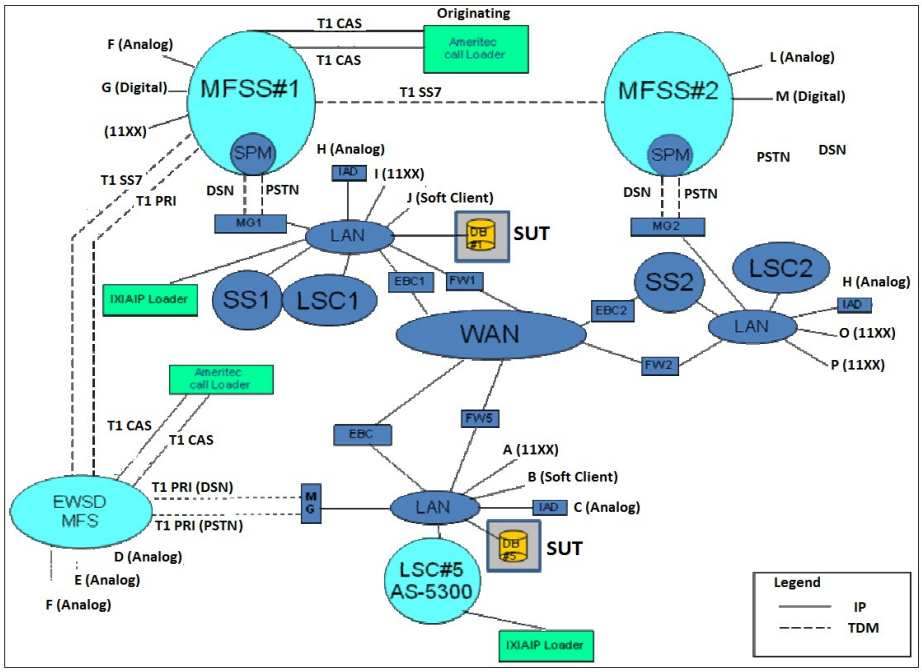


Рис. 10. Диаграмма тестирования баз данных DB.

Тестируемые базы данных DB на рис. 10 обозначены как System Under Test (SUT). Заметим, что компания Avaya установила на сети DISN не только собственные базы данных маршрутизации (Routing Database), но и многофункциональные софтсвичи Avaya CS2100 MFSS и локальные контроллеры Avaya Aura AS5300 LSC.

Как следует из вышеизложенного, ключевую роль в киберзащите систем связи имеет безопасность баз данных.

VI О защите объектов критической инфраструктуры в России

Сравнение состояния проблемы комплексной безопасности объектов критической инфраструктуры в России и в других промышленно развитых странах по показателю «социальный риск» (частота ЧС, приводящих к поражению определенного числа людей) показывает, что в России значение этого показателя в 10-100 раз выше, чем в развитых странах.

По данным МЧС Российской Федерации в 2010 г. на территории страны произошли 338 чрезвычайных ситуаций (ЧС) природного, техногенного и биолого-социального характера, а также 12 крупных террористических актов. Анализ общего количества ЧС природного, техногенного и биолого-социального характера показывает, что по количеству доминируют техногенные ЧС — 199. При этом наиболее проблемной отраслью является электроэнергетика. Так, количество аварий на объектах электроэнергетики за первые восемь месяцев 2010 г. выросло, в среднем, на 20%, по сравнению с аналогичным периодом 2009г. Аналогичная, неблагоприятная картина наблюдается, практически, во всех отраслях российской экономики, хотя, справедливости ради, надо сказать, что во всех секторах есть контрольные органы, деятельность которых координирует правительство РФ: Ростехнадзор – Опасные Производственные Объекты, Ространснадзор – объекты транспорта, Россвязьнадзор – связь, информация и коммуникации, Россельхознадзор, Росфиннадзор, Роспожнадзор, Роспотребнадзор, Росздравнадзор, надзорные органы в МЧС, МВД, ФСБ, Минобороны.

Анализ российского законодательства показывает, что кибербезопасностью критически важных объектов занимается множество ведомств. Следует отметить несовершенство законодательной базы в России, ее ведомственность. Только в последнее время начинается разработка технологий оценки ситуаций и планов реагирования, паспортов безопасности. Происходящие события характеризуются слабой координацией ведомств по вопросам безопасности объектов критической инфраструктуры, в том числе, их взаимодействие с АПК «БЕЗОПАСНЫЙ ГОРОД».

Справедливости ради, следует отметить, что после чернобыльской аварии, по рекомендациям и при участии МАГАТЭ были разработаны и функционируют защищённая сеть передачи данных и система мониторинга атомных электростанций, ситуационный центр которой размещён в Ростехнадзоре и позволяет отслеживать все технологические процессы на станциях. Чем не пример для подражания?

Тем не менее, до сих пор Россия не имеет национальной программы аналогичного масштаба и значимости, как в США и ЕС. Есть только ведомственные законы, СНИПы и другие, не гармонизированные нормативно-правовые документы, регламентирующие процесс создания систем комплексной безопасности объектов критической инфраструктуры.

Библиография

[1] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[2] 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. http://www.scrf.gov.ru/documents/6/113.html

[3] Шнепс-Шнеппе М.А., Селезнев С.П., Намиот Д.Е., Куприяновский В.П. О телекоммуникационной инфраструктуре комплекса «Безопасный город» // International Journal of Open Information Technologies. 2016.-Т.4.- №6 С.17-31.

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

[5] One million cyber attacks a day on Deutsche Telekom network http://www.euractiv.com/section/digital/news/one-million-cyber-attacks-a-day-on-deutsche-telekom-network/ Retrieved: Jun, 2016

[6] A. Poustourli, N. Kourti STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION (CIP) - THE CONTRIBUTION OF ERNCIP http://www.euras.org/uploads/euras2014/paper_cip_erncip_pusturli_final.pdf Retrieved: Jun, 2016

[7] THE NEW GERMAN IT SECURITY ACT, FEBRUARY 2016, http://www.wfw.com/wp-content/uploads/2016/02/WFW-Briefing-Germany-IT-Security-Feb-2016-EN-15-Feb.pdf Retrieved: Jun, 2016

[8] Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology. February 12, 2014

[9] 9 NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[10] CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES, The Communications Security, Reliability and Interoperability Council, NIST, WORKING GROUP 4: Final Report, March 2015

[11] Шнепс-Шнеппе М. А. Система сигнализации SS7 и ее уязвимость //International Journal of Open Information Technologies. – 2015. – Т. 3. – №. 5. – С. 1-11.

[12] THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf Retrieved: Jun, 2016

[13] Special Interoperability Test Certification of the Avaya Lightweight Directory Access Protocol (LDAP) Database (DB), DISA, 16 Dec 2011 http://www.avaya.com/usa/documents/avaya-_ibm-3550_dec11.pdf Retrieved: Jun, 2016

[14] Шнепс-Шнеппе М. А., Намиот Д. Е. Об эволюции телекоммуникационных сервисов на примере GIG //International Journal of Open Information Technologies. – 2015. – Т. 3. – №. 1. – С. 1-13.

[15] Шнепс-Шнеппе М. А., Намиот Д. Е., Сухомлин В. А. О создании единого информационного пространства общества //International Journal of Open Information Technologies. – 2015. – Т. 3. – №. 2. – С. 1-10.

About the status of cybersecurity of critical infrastructure of the state

Manfred Sneps-Sneppe, Sergey Seleznev, Dmitry Namiot, Vasily Kupriyanovsky

Abstract — **This article is the first attempt to analyze and describe the proposals on the cyber defense of critical infrastructures in the world. The paper shows the key role of telecommunications in this process. This article presents cyber security standards in the United States, especially regarding cyber security for US communication systems. Particular attention is drawn to the protection of databases, as illustrated by the example of DISN network testing. We provide concerns about the protection of critical infrastructure in Russia.**

Keywords— **cyber defense, cyber security, critical infrastructure.**