Доверенные сети связи как основа информационной безопасности государства

Статья рекомендована А. А. Стрельцовым 27.10.2014 г.

ЯКУБОВ Тагир Ягудович
Генеральный директор ОАО НПП «Полигон»

ИСХАКОВ Алмаз Раилевич
Ведущий научно-технический эксперт ОАО НПП «Полигон»

МАННАПОВ Альберт Раисович
Начальник Управления по интеллектуальным активам ОАО НПП «Полигон»

Аннотация
В статье рассмотрены актуальные угрозы национальным интересам в области информационной безопасности, анализируются текущее состояние и перспективы развития отечественного производства телекоммуникационного оборудования. Предлагается концепция доверенных сетей связи, описывается информационная система анализа медиаконтента, реализующая функцию монитора обращений для ядра безопасности доверенной сети связи. Показан опыт практической реализации доверенной сети связи на базе государственной мультисервисной сети передачи данных Республики Башкортостан.

Ключевые слова:
доверенная сеть связи, информационная безопасность, национальные интересы, телекоммуникационное оборудование.

Есть нечто, имеющее общую значимость для каждого человека, для любых отношений, для каждой команды, семьи, организации, для каждого народа и для всей человеческой цивилизации. Нечто, без чего будет разрушено самое могущественное правительство и самый успешный бизнес, самая процветающая экономика и самое влиятельное руководство, крепчайшая дружба, самая сильная личность и самая глубокая любовь. В то же время, если это нечто развивать и использовать, оно способно принести беспрецедентный успех и процветание во всех сферах жизни. И именно эту возможность в наше время, как правило, не понимают, её недооценивают и больше всего ею пренебрегают.

Это нечто — доверие.

Кови-мл. С., Меррилл Р. «Скорость доверия. То, что меняет всё» [13].

Актуальные угрозы национальным интересам в области информационной безопасности

Стремительное развитие уровня информатизации общества приводит к накоплению огромных массивов информации, снижению затрат на ее передачу и хранение, в то же время создаются все новые угрозы национальным интересам. К числу наиболее опасных современных информационных угроз можно отнести: материалы

экстремистского и террористического содержания с призывами к войне, убийствам политических деятелей и представителей различных религиозных конфессий; обнародование информации порнографического характера, которая противоречит устоям современного общества и традиционным взглядам на семью; призывы к суициду; распространение компьютерных вирусов и пиратских копий оригинальных цифровых работ. Таким образом, контент глобальной сети может не только содержать полезные сведения, но и нести в мировое сообщество информацию асоциального и деструктивного характера, поддерживая тем самым радикальные социальные, политические и религиозные группы и движения, в том числе экстремистского и террористического толка. Такие образования с течением времени могут развиваться и создавать угрозы мирового масштаба. В теории информационного общества это явление называют *потерей устойчивости*.

Развитие негативных явлений в современном информационном обществе тут же отражается в материалах интернет-ресурсов. В статье [5] отмечается, что в интернете происходит интенсивное распространение социально вредной информации — фашистского и сектантского толка, порнографического характера. В публикации [28] приводятся результаты исследования по систематизации такого феномена, как информационная война. В другой работе [27] того же автора доказывается существование способов индивидуального и массового «перепрограммирования» людей. Наличие в поведении системы приемов, в основе которых лежат эти утверждения и следствия, является одним из признаков информационного нападения, что подтверждает факт ведения информационных войн в сети. К настоящему времени проведены многочисленные исследования и опубликовано множество работ научного, научно-популярного и технического характера, в которых освещаются эти и другие аспекты информационной безопасности РФ [4, 7, 12].

На государственном уровне информационная безопасность является одной из составляющих национальной безопасности. Информационная безопасность нашего государства основывается на целом ряде документов, принятых Советом безопасности РФ [10]. В них официально констатируется наличие проблемы обеспечения безопасности индивидуального, группового и массового сознания в современном мире. В стратегии развития информационного общества в РФ поставлена, в частности, задача противодействия использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам страны, что предполагает противодействие распространению идеологии терроризма и экстремизма, пропаганде насилия [12]. Поэтому утверждается, что «обезопасить интернет от внутренних и внешних угроз станет в ближайшее время приоритетной задачей, однако для этого операторам связи придется устанавливать новое оборудование для фильтрации и анализа трафика» [30]. Это рациональное решение, но следует принимать во внимание, что «отставание отечественных информационных технологий вынуждает… идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения» [31].

В Доктрине информационной безопасности РФ [31] сформулированы четыре основных вектора обеспечения безопасности по этому направлению. Для нас представляет интерес четвертый вектор — защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России. В этих целях необходимо повысить безопасность сетей связи и информационных систем и интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля их эффективности.

Разработки программного обеспечения для фильтрации и анализа трафика на аппаратном и программном уровнях уже ведутся отечественными производителями телекоммуникационного оборудования и сетевого программного обеспечения. Например, компания ТКБ [14] предлагает систему анализа информационных потоков в корпоративных сетях и программно-аппаратный комплекс для анализа больших объемов трафика. Сервисы блокировки доступа к нежелательному контенту для операторов мобильного и широкополосного интернета разрабатываются ее дочерним предприятием ООО «Безопасный Интернет» [3]. Однако подходы, применяемые в разработках этих компаний, являются достаточно жесткими. В современном неустойчивом мире наибольший эффект можно получить только с применением «мягкой силы». Жесткий подход всегда обусловливает дальнейшую эскалацию ужесточения используемых инструментов для контроля действий пользователей, что чревато установлением тотального контроля их деятельности в интернете.

Предлагаемый нами подход к решению проблемы обеспечения информационной безопасности государства основывается на построении доверенных сетей связи, использующих технологии «мягкой силы». Для создания таких сетей необходимы следующие элементы:

- доверенные средства построения сети, которые реализуют функции передачи и обработки потоков данных в соответствии с выработанной политикой безопасности;
- средства анализа потоков данных, результатом деятельности которых является политика безопасности;
- элементы сетевой инфраструктуры (коммутаторы, маршрутизаторы, шлюзы) с поддержкой технологии программно-конфигурируемых сетей[1].

Другими словами, для построения доверенной сети связи необходимо доверенное телекоммуникационное оборудование.

Доверенное телекоммуникационное оборудование

Сейчас в России приблизительный ежегодный объем закупок оборудования в телекоммуникационной отрасли оценивается более чем в 300 млрд руб.,

[1] За рубежом эта технология называется Software Defined Networking, или коротко SDN. Она позволяет решать задачи динамического конфигурирования сетей, внесения оперативных изменений в работу сетевой инфраструктуры (причем приложения способны делать это автоматически), решает ряд задач, включая приоритезацию трафика, назначение правил реагирования на проблемы в сети и управление группами коммутаторов и маршрутизаторов.

доля импортного оборудования в российских информационно-телекоммуникационных сетях в настоящее время составляет 90% [9]. В связи с этим «сложившаяся ситуация может привести к потере контроля и управляемости национальных информационно-телекоммуникационных сетей, что, в свою очередь, влечет серьезные и даже катастрофические последствия для экономики РФ, а также снижение обороноспособности до критически опасного уровня» [там же].

Как известно, спецслужбы иностранных государств используют различные способы получения несанкционированного доступа к сетям связи для ведения информационной войны, шпионажа и совершения кибератак, о чем неоднократно сообщалось в СМИ [1]. То, что в оборудовании американских и китайских производителей (Cisco, Huawei и Juniper) используются специальные программные и аппаратные «закладки», предназначенные для перехвата данных и контроля работы оборудования, уже не секрет [26]. Эти «жучки» созданы таким образом, чтобы они могли продолжать работать после перезагрузки и даже обновления прошивки оборудования. Д. О. Рогозин справедливо отмечал, что «на самом деле кибербезопасность на Западе понимается как закладки в чипы и программное обеспечение, поставляемое в другие страны, закладки, которые активируются в определенный момент» [37].

Сейчас информационно-телекоммуникационные сети России построены в основном на оборудовании американской компании Cisco, относительно небольшая доля приходится на оборудование других американских и китайских производителей. Это действительно серьезная угроза национальной безопасности, и данную ситуацию необходимо кардинально изменить в ближайшие годы.

С этой целью в начале 2014 г. ОАО НПП «Полигон» [18] совместно с компаниями ООО «АйТиФай» и ЗАО «ИнформИнвестГрупп» инициировало системный проект[1] «Развитие производства телекоммуникационного оборудования средними компаниями» [25]. Этот проект был одобрен 8 апреля 2014 г. на заседании наблюдательного совета Агентства стратегических инициатив под председательством В. В. Путина [8]. Согласно протоколу заседания наблюдательного совета [23] было принято решение оказать содействие малым и средним компаниям, производящим телекоммуникационное оборудование, во взаимодействии с крупными компаниями с государственным участием, федеральным органам исполнительной власти в целях технологического обеспечения построения доверенных сетей, обеспечивающих высокий уровень информационной безопасности передаваемых данных, рекомендовано проработать вопрос создания центра компетенции в области доверенного телекоммуникационного оборудования.

ОАО НПП «Полигон» на протяжении достаточно продолжительного времени самостоятельно разрабатывает и производит сложное телекоммуникационное оборудование [32, 33], которое можно отнести к категории доверенного. Это подтверждено многочисленными экспертизами. В конце 2013 г. продукция компании получила статус «телекоммуникационного оборудования российского происхождения». Конкретные параметры, при соблюдении

[1] Согласно принятому в Агентстве стратегических инициатив подходу, к «системным проектам» относятся те, которые направлены на решение масштабных, системных проблем, устранение которых создает возможность для дальнейшего развития отраслей и экономики РФ в целом.

которых оборудованию может быть присвоен такой статус, перечислены в совместном приказе Минэкономразвития и Минпромторга РФ от 17 августа 2011 г. [24]. В 2013 г. в этот приказ были внесены изменения [11, 17]. Важно, что при присвоении оборудованию статуса российского комиссия Минпромторга учитывает уровень локализации производства на территории России, долю российских налоговых резидентов в уставном капитале компании, наличие у компании прав на конструкторскую документацию и программное обеспечение, используемые в телекоммуникационном оборудовании. Для получения статуса компании необходимо обладать научно-производственной базой на территории России для организации производства, гарантийного и послегарантийного обслуживания, а также осуществлять в стране полный цикл сборки печатных плат и финишную сборку оборудования [11, 17, 19].

К настоящему моменту статус «российской» на свою продукцию получили только семь компаний: ООО «Т 8», ОАО НПП «Полигон», ОАО «Супертел», ЗАО «НПФ «Микран», ЗАО «НПП «Цифровые технологии», ОАО «МАРТ» и ЗАО «РОН-Телеком» [19][1]. Оборудование этих компаний можно по праву считать обладающим высоким уровнем доверия.

Есть и другие компании, которые заявляют о том, что производят «доверенное телекоммуникационное оборудование» [16, 20]. Однако, по нашему мнению, создание оборудования «по технологии зарубежного производителя на российских предприятиях под контролем отечественных специалистов с обязательной сертификацией на территории России» [20] не может обладать достаточной степенью доверия. Такие заявления видятся, скорее, неким маркетинговым ходом, искажающим реальное положение дел. В данном контексте фраза «доверие является основным корнем и источником нашего влияния» [13] обретает для предприятий — производителей доверенного телекоммуникационного оборудования новый смысл.

В интересах обеспечения национальной безопасности представляется целесообразным серьезным образом ограничить использование телекоммуникационного оборудования иностранного происхождения при построении сетей органов государственной власти всех уровней, силовых и ведомственных структур, государственных корпораций и предприятий, а также хозяйственных обществ вплоть до полного запрета его импорта.

Подобные действия уже практикуются за рубежом. Например, в 2013 г. США ввели запрет на закупку китайского телекоммуникационного оборудования (компаний Huawei и ZTE) для своих ведомств и правительственных организаций [2]. При этом американские власти рекомендовали местным компаниям также воздержаться от приобретения телекоммуникационного оборудования из Поднебесной. Кроме того, было принято решение отстранить упомянутые китайские компании от любых сделок по слияниям и поглощениям в США. Принятые меры стали логичным следствием многочисленных обвинений китайских производителей в шпионаже и кибератаках [15, 34]. В данном случае не так важно, было ли это действительно реакцией на угрозу национальной безопасности или просто лоббированием

[1] Наибольшее количество наименований телекоммуникационного оборудования, получившего статус российского, — у ОАО НПП «Полигон» — 23 (всего выпускается 66 наименований).

интересов американских производителей телекоммуникационного оборудования. В любом случае, от этих запретов Соединенные Штаты только выиграли. Надо сказать, что существенные ограничения на деятельность иностранных производителей ввели также Великобритания, Австралия, Индия и ряд других стран. В 2010 г. Правительство РФ подписало распоряжение о приоритетном использовании телекоммуникационного оборудования отечественного производства в национальных проектах в области связи. Однако данный документ является лишь рекомендацией [19].

Постановлением Правительства РФ от 24 декабря 2013 г. № 1224 установлен «запрет на допуск товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок товаров, работ (услуг) для нужд обороны страны и безопасности государства, за исключением случаев, когда производство таких товаров, выполнение работ и оказание услуг на территории РФ отсутствуют или не соответствуют требованиям государственных заказчиков» [21]. Но, как показывает практика, не все руководствуются этим указанием.

Законопроект, согласно которому иностранное оборудование может использоваться на территории РФ в сетях связи всех форм собственности только в том случае, если аналогичное оборудование связи российского производства отсутствует, был предложен в начале 2014 г. [9, 29]. В нем приводится ряд условий, одновременное соблюдение которых требуется, чтобы отнести оборудование связи к категории «российского производства». В частности, производитель оборудования должен быть: налоговым резидентом РФ, обладать исключительными правами на схемотехническое решение и конструкторскую документацию, использовать микропрограммы с открытым исходным кодом или те, на которые обладает исключительными правами, использовать открытую операционную систему и быть исключительным собственником на программы и их тексты, запускаемые на оборудовании [39]. Несмотря на свою актуальность и насущную необходимость, к настоящему моменту этот закон еще не принят.

В свете обострения отношений России с рядом западных стран и введением экономических санкций, тема импортозамещения, обеспечения информационной и технологической безопасности страны, в особенности ее ОПК, госсектора, а также организаций-операторов персональных данных, приобрела особую актуальность. На пленарном заседании Петербургского международного экономического форума 23 мая 2014 г. Президент РФ В. В. Путин поставил задачу обеспечить импортозамещение как важнейший элемент технологического перевооружения российской промышленности [38].

С учетом текущих поручений Правительства РФ по разработке программы импортозамещения для предприятий ОПК России, осуществляемой Минкомсвязи РФ и Минпромторгом РФ, считаем целесообразным установить запрет на закупку отдельных видов телекоммуникационного оборудования, происходящего из иностранных государств, для обеспечения государственных и муниципальных нужд. Прецедент уже имеется: 14 июня 2014 г. утверждено Постановление Правительства РФ № 656 [22] аналогичного содержания на отдельные виды товаров машиностроения.

Подобные меры будут способствовать обеспечению информационной, экономической и технологической безопасности, защите внутреннего рынка и развития национальной экономики, а также поддержке российских производителей телекоммуникационного оборудования.

В поисках российской концепции доверенных сетей связи

Ввиду того, что нефункциональные требования, такие как надежность и безопасность, должны учитываться на ранних стадиях процесса проектирования и реализации будущих систем, для создания доверенных сетей связи целесообразным является построение новых сетей передачи данных, в которых будут учтены указанные требования.

Концепция доверенной сети связи[1] предполагает разбиение всей сети по территориальному признаку на сегменты и организацию доверенной

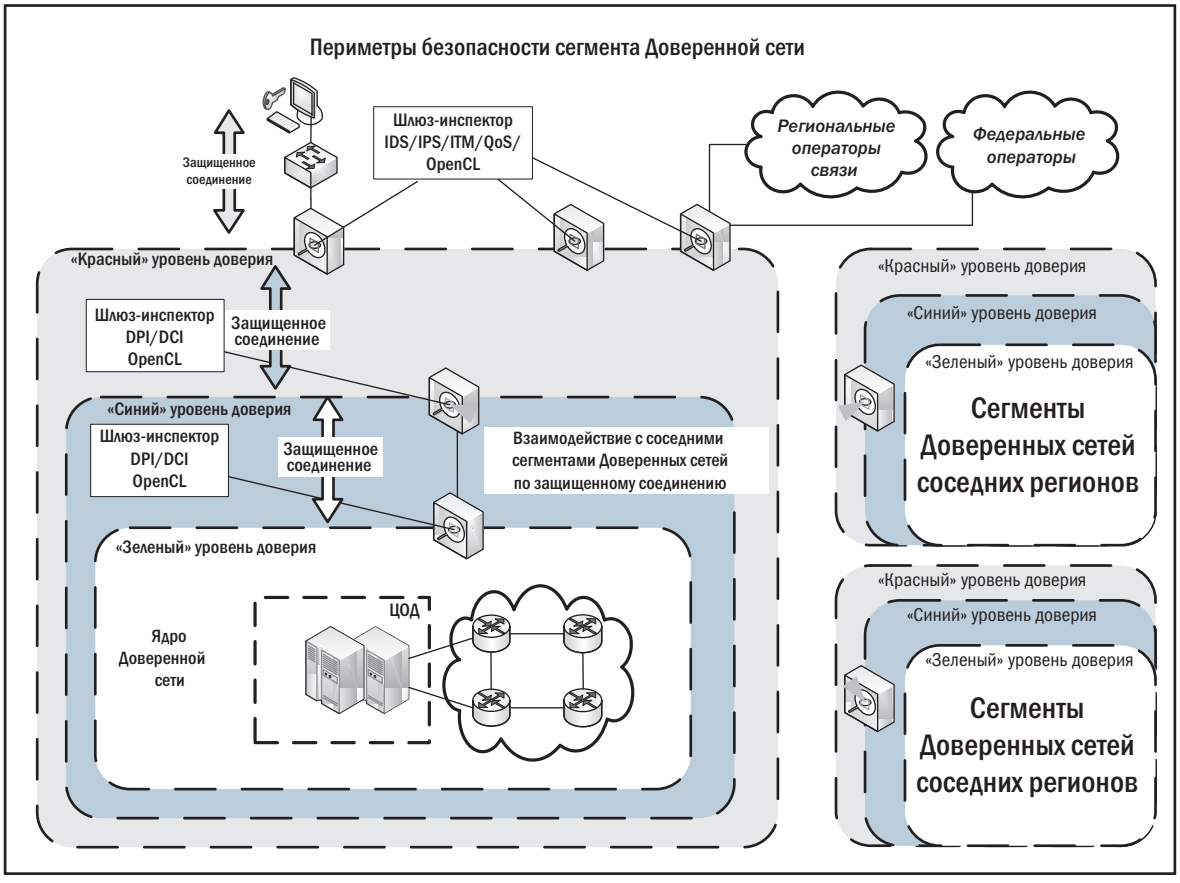

Рис. 1. Сегментное представление доверенной сети связи

[1] Разработана специалистами ОАО НПП «Полигон» и ГУП Центр информационно-коммуникационных технологий Республики Башкортостан.

сети на их уровне. Сегменты как структурные элементы доверенной сети будут взаимодействовать по защищенному каналу соединения (рис. 1).

Согласно международному стандарту ISO/IEC 15408 [4, 35] каждый из этих сегментов является доверенной системой. Сегменты условно разбиваются на динамические во времени субсегменты уже не по территориальному признаку. В качестве принципа разбиения выбрана степень доверия к составляющим их субсегментам. Под субсегментом сегмента доверенной сети понимается совокупность узлов, функционирующих в рамках одинаковой политики безопасности. Субсегменты в некотором смысле аналогичны классам безопасности из «Оранжевой книги» [4, 6, 36], так как направлены на достижение тех же целей, что и эти классы. Субсегменты подразделяются на три уровня доверия: зеленый, синий и красный. Наивысшую безопасность обеспечивает зеленый уровень, который обладает «наисильнейшей» политикой безопасности. Для проведения границ между уровнями доверия используются такие элементы сетевой инфраструктуры, как шлюзы-инспекторы.

В данном случае под шлюзом-инспектором понимается программно-аппаратный комплекс отечественного производства, основанный на технологиях Deep Packet Inspection (DPI) и Deep Content Inspection (DCI). Он предназначен для контроля и управления контентом. Предполагается функционирование шлюз-инспектора, начиная с канального уровня OSI модели и выше. Именно по таким шлюз-инспекторам планируется определение периметров субсегментов. Подсеть синего уровня доверия будет защищена двусторонним кольцом шлюз-инспекторов. Первые из них должны реализовывать «слабую» политику безопасности субсегмента с красным уровнем доверия, а вторые — более «сильную» политику безопасности зеленого уровня. Предполагается реализация защищенных соединений между субсегментами. В ядро доверенной сети будут входить те узлы, в которых хранятся и обрабатываются данные государственной, коммерческой и частной значимости, именуемые в данной концепции центрами обработки данных (ЦОД). Последние будут продублированы резервными ЦОД.

Анализ видеоресурсов сети монитора обращений

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. В соответствии с международным стандартом ISO/IEC 15408 степень доверия оценивается по двум следующим критериям: по политике безопасности и по уровню гарантированности [4]. В предлагаемой нами концепции доверенной сети связи политика безопасности полностью основывается на средствах анализа потоков данных — технологиях глубокого анализа DPI и DCI. Как известно, в пределах сети пользователи работают с данными разной модальности. Обработка одних (например, текста) требует небольших вычислительных ресурсов, что позволяет запускать их на базе шлюз-инспекторов. Другие же, в силу сложности алгоритмического обеспечения, могут быть запущены только на специализированных узлах ЦОД. К числу последних можно отнести обработку и анализ видео контента сети как функции монитора обращений.

Таким образом, разрабатываемый механизм монитора обращений должен будет располагаться в ядре доверенной сети и запущен на базе ЦОД. Такое расположение должно гарантировать его изолированность. Обеспечить его работу в масштабе реального времени для каждого пользовательского обращения невозможно в силу сложности программного обеспечения. Поэтому требование полноты данный механизм будет обеспечивать в квазистационарном режиме работы: периодически составлять карту узлов сегмента доверенной сети с указанием их уровней доверия. Однако это требует постоянного контроля изменений контента сайтов по появлению новых ссылок на видеоресурсы. Следовательно, механизм должен функционировать совместно с веб-сервером, своевременно получая информацию об обновлении содержания страниц сайтов, в которых присутствуют теги подключения изображений или видео. Другим аналогичным вариантом является полный контроль ресурсов видеохостинга. Верифицируемость данного механизма обращений будет обеспечивать сервисы безопасности ЦОД в автоматическом режиме. В свою очередь, создаваемый механизм анализа видеоконтента сегмента монитора обращений должен своевременно предоставлять ядру безопасности актуализированную карту уровней доверия узлов сегмента.

Вернемся к задачам Доктрины информационной безопасности РФ. Согласно второму пункту статьи 29 Конституции РФ «не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства». Таким образом, подобная информация подлежит законному удалению. Система анализа видеоконтента и изображений изначально направлена на обнаружение в них или в их последовательности нарушений, которые противоречат упомянутой статье Конституции. Описываемая система позволяет проводить классификацию изображений или видео на уровне абстрактных понятий, что соответствует ее прямому назначению (например, отделять людей от техники). Но она не обладает возможностью проводить более детальную классификацию из-за специфичности своего алгоритмического обеспечения. Согласно теории распознавания образов, это процедура является распознаванием классов (категоризацией), но не их элементов.

Что касается второй составляющей национальных интересов РФ в информационной сфере, то система анализа видеоконтента и изображений может применяться в качестве инструмента для более сложных информационных систем принятия решений о доверенности сетевых ресурсов. Констатируя наличие информационных угроз в ресурсах, указанных в политике безопасности, данная система вполне может обеспечить ядро безопасности доверенной сети актуальной информацией о распределении уровней доверия в сегменте для анализируемых активов. Например, именно система анализа видео и изображений позволит частично разрешить проблему «аргументации ложными фактами», обеспечив сокращение числа недоверенных источников сети путем определения новизны выставленного ресурса и его проверки на соответствие требованиям политики безопасности. Тем самым можно содействовать решению такой задачи, как «укрепление государственных средств массовой информации, расширение их возможности

по своевременному доведению достоверной информации до российских и иностранных граждан» [31].

Третья составляющая национальных интересов РФ в информационной сфере требует развития и совершенствования инфраструктуры информационного пространства за счет нового поколения телекоммуникационного оборудования и комплектующих отечественного производства. Переосмысление принципов построения сетей связи и разработка новых технологий для доверенных сетей, повышающих «живучесть» и стойкость к активным информационных атакам, позволят новому поколению сетевой инфраструктуры оперативно и полноценно локализовать уже существующие и новые источники информационных угроз. К настоящему времени система анализа изображений и видео позволяет обнаружить в них объекты указанных классов, которые относятся к числу информационных угроз. На стадии проектирования находится система анализа речи и звуков. Она в комплексе с системой анализа изображений и видео позволит не только проводить поиск информационных угроз по изображениям, но и анализировать речь, передаваемую через видео. Такой комплексный подход к анализу мультимедийных ресурсов на порядок повышает достоверность обнаружения информационных угроз. Система анализа речи основана на технологиях распознавания и идентификации с применением вейвлетных вычислений и нейронных сетей.

Наиболее полно доверенные сети связи решают задачи четвертой составляющей национальных интересов Российской Федерации в информационной сфере:

- повышение безопасности информационных систем и сетей связи планируется провести за счет использования технологий DPI и DCI анализа;
- новое поколение российского сетевого оборудования полностью основано на отечественных комплектующих, что исключает несанкционированные «закладки»;
- задачи информационной безопасности, которые не могут быть решены в масштабе реального времени и требуют проведения DPI и DCI-анализа фрагментов трафика, будут вынесены за аппаратную платформу шлюз-инспекторов сети.

Таким образом, технология анализа изображений и видеоресурсов является неотъемлемым инструментом DCI-анализа контента. Увеличение технических характеристик каналов передачи сетевой инфраструктуры требует разработки быстрых алгоритмов анализа и распознавания информационных угроз в контенте. Это обусловливает реализацию системы анализа изображений и видео на базе многоядерных платформ и их расположения на территории ЦОД, что позволит обеспечить эффективную работу этой системы.

Опыт построения прототипа доверенной сети связи

Государственная мультисервисная сеть передачи данных (ГМСПД) Республики Башкортостан (РБ) является закрытой телекоммуникационной

инфраструктурой, обеспечивающей единое пространство электронного взаимодействия на основе специальных информационных и информационно-технологических систем обеспечения деятельности государственных органов РБ. ГМСПД построена как телекоммуникационная сеть с интеграцией услуг, обеспечивающая передачу различных типов информации. Целью ГМСПД является создание управляемого информационного пространства с единой информационной структурой и сервисами для обеспечения надежного и защищенного информационного обмена между государственными органами РБ. На базе ГМСПД в Уфе развернут действующий прототип регионального сегмента доверенной сети связи на основе архитектурных и платформенных решений ОАО НПП «Полигон» и ГУП «Центр ИКТ» [40]. Ядро доверенной сети организовано в Уфе на базе оборудования ОАО НПП «Полигон» с кольцевой топологией пропускной способности в 10 Гбит/сек.

В заключение подчеркнем, что современное общество имеет право на качественный интернет-контент, свободный от информации, нарушающей эмоционально-психологическое, духовное и интеллектуальное здоровье людей. Доверенные сети помогают обеспечить эту потребность.

ЛИТЕРАТУРА

1. **Американская разведка «взломала» компьютеры Минобороны РФ.** URL: http://www.rosbalt.ru/main/2014/01/15/1221086.html (дата обращения: 23.09.2014).

2. **Барак Обама запретил НАСА и другим ведомствам покупать оборудование из Китая.** URL: http://www.cnews.ru/top/2013/03/29/barak_obama_zapretil_nasa_i_drugim_vedomstvam_pokupat_oborudovanie_iz_kitaya_524119 (дата обращения: 23.09.2014).

3. **Безопасный Интернет** / Решения для глубокого анализа информационных потоков в реальном масштабе времени. URL: http://safeinet.ru (дата обращения: 23.09.2014).

4. БЛИНОВ А. М. **Информационная безопасность.** СПб.: Изд-во СПбГУЭФ, 2010.

5. БУКРЕЕВ И. Н. **Социальные аспекты информационной безопасности** // Информационное общество. 1998. № 6. С. 42–45.

6. **Введена в действие «Оранжевая книга».** URL: http://www.securitylab.ru/informer/240650.php (дата обращения: 23.09.2014).

7. ВЛАДИМИРОВА Т. В. **Информационная безопасность: к методологическим основаниям анализа вопроса** // Информационное общество. 2012. № 5. С. 47–52.

8. **Заседание наблюдательного совета Агентства стратегических инициатив.** 8 апреля 2014 года. URL: http://www.kremlin.ru/news/20737 (дата обращения: 23.09.2014).

9. **Иностранное оборудование связи в России могут запретить в июле.** URL: http://lenta.ru/news/2014/04/15/zakonooborudovanie (дата обращения: 23.09.2014).

10. **Информационная безопасность** / Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6 (дата обращения: 23.09.2014).

11. КАЛИГИН А. **Производственная необходимость** // Стандарт. 2014. № 5. С. 62–69.

12. КАРПОВА А. Ю. **Императивы информационной политики** // Информационное общество. 2 014. № 2. С. 10–16.

13. КОВИ-МЛ. С., МЕРРИЛЛ Р. **Скорость доверия. То, что меняет всё.** М.: Альпина Паблишер, 2012.

14. **Компания ТКБ — Технологии корпоративной безопасности.** URL: http://www.cstech.ru (дата обращения: 23.09.2014).

15. **Конгрессмены предлагают запретить деятельность Huawei и ZTE в США.** URL: http://www.forbes.ru/news/156241-komitet-kongressa-ssha-predlagaet-zapretit-deyatelnost-v-strane-huawei-i-zte (дата обращения: 23.09.2014).

16. **Концепция доверенного оборудования как отражение воли рынка** // Электросвязь. 2011. № 8. С. 3–4.

17. **Приказ Министерства промышленности и торговли РФ и Министерства экономического развития РФ от 29 октября 2013 г. № 1675/628 «О внесении изменений в приказ Министерства промышленности и торговли Российской Федерации и Министерства экономического развития Российской Федерации от 17 августа 2011 г. № 1032/397».**

18. **ОАО НПП «Полигон».** URL: http://www.plgn.ru (дата обращения: 23.09.2014).

19. **Оборудование Т 8, «Микран» и «Полигон» получило статус отечественного.** URL: http://biz.cnews.ru/news/top/index.shtml?2014/01/29/558435 (дата обращения: 23.09.2014).

20. ПОНОМАРЕНКО Б. Ф. **Обеспечение информационной безопасности РФ в ходе реализации стратегических национальных задач** // Век качества. 2013. № 4. С. 38–40.

21. **Постановление Правительства РФ от 24 декабря 2013 года № 1224 «Об установлении запрета и ограничений на допуск товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок товаров, работ (услуг) для нужд обороны страны и безопасности государства».**

22. **Постановление Правительства РФ от 14 июня 2014 года № 656 «Об установлении запрета на допуск отдельных видов товаров машиностроения, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».**

23. **Протокол заседания наблюдательного совета автономной некоммерческой организации «Агентство стратегических инициатив по продвижению новых проектов» от 08 апреля 2014 г., № 1.**

24. **Приказ Минпромторга России № 1032, Минэкономразвития России № 397 от 17 августа 2011 года.**

25. **Развитие производства телекоммуникационного оборудования средними компаниями.** URL: http://asi.ru/projects/9616 (дата обращения: 23.09.2014).

26. **Раскрыт список «жучков» АНБ США для техники Cisco, Huawei и Juniper.** URL: http://www.cnews.ru/top/2014/01/10/raskryt_spisok_zhuchkov_anb_ssha_dlya_tehniki_cisco_huawei_i_juniper_foto_556040 (дата обращения: 23.09.2014).

27. РАСТОРГУЕВ С. П. **Информационная война.** М.: Радио и связь, 1999.

28. РАСТОРГУЕВ С. П. **Информационная война как целенаправленное информационное воздействие информационных систем** // Информационное общество. 1997. № 1. С. 64–66.

29. **Российским компаниям могут запретить покупать иностранное оборудование связи при наличии отечественных аналогов.** URL: http://biz.cnews.ru/news/top/index.shtml?2014/02/12/560302 (дата обращения: 23.09.2014).

30. **Совет безопасности обсудит отключение России от глобального интернета.** URL: http://www.vedomosti.ru/politics/news/33610271/suverennyj-internet#ixzz3Djqg4Oa5 (дата обращения: 23.09.2014).

31. **Доктрина информационной безопасности Российской Федерации.** URL: http://www.scrf.gov.ru/documents/6/5.html (дата обращения: 02.10.2014).

32. ЯКУБОВ Т. Я. **Мы всё разрабатываем сами** // Первая миля. 2011. Т. 23. № 2. С. 2–9.

33. ЯКУБОВ Т. Я. **Современные концепции разработки оборудования: от системной модели до микросхем. Подход компании «НПП «Полигон»** // Первая миля. 2011. Т. 25. № 4. С. 8–13.

34. **Huawei уходит из США.** URL: http://www.vestifinance.ru/articles/26804 (дата обращения: 23.09.2014).

35. **International Standard ISO/IEC 15408.** Information technology. Security techniques. Evaluation criteria for IT security.

36. **Критерии определения безопасности компьютерных систем.** URL: https://ru.wikipedia.org/wiki/Критерии_определения_безопасности_компьютерных_систем (дата обращения: 23.09.2014).

37. **Рогозин обещает появление в России первых прорывов в военных технологиях к концу нынешнего года.** URL: http://itar-tass.com/politika/552700 (дата обращения: 23.09.2014).

38. **Предложения по импортозамещению для российских предприятий.** URL: http://www.it-world.ru/categories/releases/63177.html (дата обращения: 23.09.2014).

39. **Проект федерального закона «О внесении изменения в статью 12 Федерального закона «О связи».** URL: http://asozd2c.duma.gov.ru/addwork/scans.nsf/ID/B0AD3A480282BE4843257C7C005B2CB8/$FILE/449120–6.PDF? OpenElement (дата обращения: 23.09.2014).

40. **Центр информационно-коммуникационных технологий.** URL: https://www.ciktrb.ru (дата обращения: 23.09.2014).