Описательная модель защищенной сетеориентированной системы информационного обеспечения для управления силами РЭБ ВМФ

Бухта
Сергей Иванович,
начальник научно-исследовательского отдела НИИ ОСИС ВМФ ВУНЦ ВМФ «ВМА», капитан 2 ранга

Сидоров
Степан Сергеевич,
помощник начальника НИИ ОСИС ВМФ ВУНЦ ВМФ «ВМА», капитан-лейтенант

В настоящее время ведущие иностранные государства добились существенного преимущества в информационной сфере, создав сетецентрические системы, которые имеют глобальный пространственный охват, объединяя в единое целое различные функциональные сети, обеспечивающие применение боевых систем и оружия в едином информационном пространстве.

Мировая инновационная тенденция состоит во всеобъемлющем внедрении информационных сетей в процессы управления, жизнеобеспечения и военной деятельности.

В данный период в ВС РФ прилагаются значительные усилия для того, чтобы создать интегрированные информационные сети для решения задач управления, включая задачи организации сетей связи и передачи данных. Такие сети обладают высокой защищенностью, однако в целом не покрывают все потребности управления силами, а по достигаемым значениям показателей не соответствуют мировому уровню в достаточной степени. Кроме технологических вопросов требуется значительное время для ликвидации существующего отставания.

Большую пользу общему процессу строительства сетеориентированных систем в ВС РФ может принести доработка и применение в военном деле информационно-телекоммуникационных сетей общего пользования (ИТКС ОП). Такие сети уже глобально развернуты и обладают высокими качественными показателями.

Недостатком, не позволяющим их применять в том виде, в котором они существуют, является незащищенность информации от несанкционированного доступа, разрушения и модификации. Речь идет о доработке ИТКС ОП до уровня требований ВС РФ и их информационном и техническом сопряжении с аналогичными сетевыми военными системами, то есть фактически о создании технологии военного и двойного назначения, или гибридных систем с удовлетворяющими ВС РФ требованиям и регламентом применения.

Такие сети без существенных затрат могли бы быть развернуты для применения в ВС РФ в кратчайшее время. При создании полноценных сетей в Вооружённых Силах нашей страны применение гибридных сетей могло бы выполнять функцию как минимум вспомогательных систем.

Следует отметить, что речь не идет, как это принято, об использовании (аренде) в военных целях каналов связи и передачи данных гражданского (коммерческого) назначения.

Суть предложения состоит в совместном применении военных систем с глобальными информационно-телекоммуникационными сетями общего пользования. Примером такой сети, которая может использоваться как прототип, является Интернет.

Авторы не предлагают использовать Интернет в военных целях. Это неразумно по причине незащищенности информации и негосударственной принадлежности глобальной сети по отношению к РФ. Главное — это запрещено руководящими документами МО РФ.

Кроме того, сейчас реализуется на практике новая технология криптографической защиты информации ViPNet, а также имеются научные, технологические, программно-технические и организационные возможности, позволяющие доработать Интернет до уровня специальных требований МО РФ и в том числе по обеспечению защищенности информации на местах применения.

В соответствии с государственной политикой в области информатизации к 2018 году весь трафик обмена информацией между российскими пользователями Интернета будет проходить только по территории России. Управление трафиком будет осуществляться через государственные сервера.

Инфраструктура сети в виде локальных сетей и отдельных компьютеров принадлежит внутренним пользователям, включая энергообеспеченность и регламенты работы сети. Используемые в военных целях технические средства сети проходят необходимые проверки в соответствии с нормативами МО РФ, ФСТЭК России и других компетентных органов.

Поэтому предпринимаемые действия позволяют считать Интернет только прототипом создаваемой внутренней глобальной информационной сетевой системы. С учетом того, что внутренняя сеть многопланово дорабатывается с применением специальных технологий и обеспечивается защитой, можно считать, что такая сеть общего применения становится интересной для использования в интересах МО РФ.

Особенность создания сети информационного обеспечения (ИО) для ВС состоит в том, что сеть образуется виртуально, «поверх» существующей сети Интернет, а программно-технически дорабатывается только на местах пользователей с помощью серийно выпускаемой продукции. При таком подходе снимаются значительные затраты на создание сети, ввиду ее наличия внутри страны, и сводится до минимума время на ее внедрение. Возможно, было бы правильно даже присвоить такой внутренней защищенной сети собственное наименование.

Данная мысль подтверждается реальными действиями руководства МО РФ по внедрению в войска информационных сетей с технологией VPN. Данные сети позволяют вести маскированный обмен информацией между элементами сети с использованием средств криптографической защиты информации.

Целью данной статьи является ознакомление с выработанными предложениями по возможностям доработки и внедрения ИТКС ОП в процесс информационного обеспечения системы РЭБ ВС РФ.

Назначение. Защищенная сетеориентированная система информационного обеспечения для управления силами РЭБ (ЗСС ИО РЭБ) предназначена для сбора, обработки и оперативного, безопасного обмена зашифрованной информацией между пространственно распределенными органами и пунктами управления, центрами, кораблями и частями, участвующими в ведении РЭБ, и применяемыми программными, аппаратными средствами.

Защищенная СС ИО РЭБ:

1. Глобальная территориально распределенная логическая сеть, отличающаяся высоким уровнем защиты данных, созданная на базе ИТКС ОП типа Интернет, и других систем, имеющих сходный набор услуг, с использованием средств криптографической защиты информации ViPNet.
2. Гибридная сеть, осуществляющая совместное, распределенное по доступу функционирование открытых и защищенных сетей общего применения, и АСУ военного назначения, обеспечивающие применение сил и средств системы РЭБ.
3. Универсальная сеть для сбора, обработки, передачи потоковой сигнальной, звуковой и видеоинформации, а также файловой текстовой, графической информации. Применяется в РЭБ для мониторинга и оценки обстановки, поддержки принятия решений, репликации баз данных распределенных пунктов управления, передачи команд управления, проведения видеоконференций и реализации обмена электронного документооборота.

Возможности

1. Неограниченный по числу (полный) охват пользователей, независимо от удаленности.
2. Сетеориентированная система информационного обеспечения РЭБ — универсальная информационная телекоммуникационная решетка, фундамент для построения сетецентрической системы РЭБ.
3. Технические возможности организации ЗСС ИО РЭБ обеспечивают ее обособленное функционирование внутри территории РФ, не выходя за ее пределы, без использования серверов иностранных государств.
4. Перенос первичной и формализованной информации о текущей радиоэлектронной обстановке от средств добывания информации на пункты управления РЭБ.
5. Взаимодействие по зашифрованному каналу с вышестоящими межвидовыми, видовыми и специальными системами аналогичного назначения.
6. Безопасный обмен информацией с пометкой «для служебного пользования», с возможностью обработки информации, составляющей государственную тайну, при реализации гибридной схемы построения сети.
7. Альтернативные возможности функционирования ЗСС ИО РЭБ через проводные каналы передачи данных, спутниковые системы связи, сотовую связь.
8. Возможность применения существующих каналов передачи данных и сетевых устройств общего применения.
9. Высокая устойчивость сети, обусловленная ее избыточностью и резервированием, обеспечивает функционирование сети при преднамеренных воздействиях и отказах.
10. Развернутым правовым обеспечением проведения работ по созданию ЗСС ИО РЭБ на основе сетей общего пользования.

Правовое обеспечение

Работы по созданию защищенных сетей общего применения в МО РФ ведутся с 2013 года. В Министерстве обороны РФ имеются соответствующие правоустанавливающие документы.

Структура ЗСС ИО РЭБ

Защищенная СС ИО РЭБ представляет собой объединенную единым функциональным процессом, информационным обменом, управлением и технологией защиты совокупность сетей для полного, достоверного и всестороннего обеспечения данными о радиоэлектронной обстановке органов (пунктов) управления ВМФ и вышестоящих органов ВС РФ, в части РЭБ ВМФ, для последующего планирования и применения сил РЭБ ВМФ на оперативном (стратегическом) направлении.

Топология ЗСС ИО РЭБ характеризуется регулярным построением сети на основе использования однотипных защищенных VPN-туннелей, образующих информационно-телекоммуникационную решетку с оптимальным маршрутом передачи данных.

Туннель — процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.

Инкапсуляция — метод построения модульных сетевых протоколов на основе их размещения в некоторую единую для сети оболочку, обеспечивающий защиту и стандартизацию передачи данных в канале. Это упаковка пакетов разных протоколов передачи данных (видео, речь, текст, сигнал) в пакеты одного протокола, включая адрес.

VPN-туннель — формальное отображение виртуальной связи между клиентами ViPNet, являющейся актуальной логической, функциональной и информационной цепочкой взаимодействующих устройств сети с оптимизированным путем передачи данных. VPN-туннель является элементарным путем, связывающим средства системы РЭБ. Туннель характеризуется минимально необходимым составом его образующих устройств. На рис. 1 приведена схема элементарного туннеля.

Состав программно-аппаратного комплекса ViPNet, образующих VPN – туннель сети

Средства добывания информации — корабельные (авиационные, береговые) средства (подсистемы, системы) добывания, обработки распределения и передачи первичной пото-

Рис. 1

ковой сигнальной информации и формализованной файловой информации соответствующего назначения.

Универсальный модем — аппаратно-программное устройство, обеспечивающее следующие позиции:
- сбор первичной сигнальной информации о РЭС от средств добывания информации;
- проведение специальной обработки информации, предполагающей формирование массива данных из формуляров РЭС в форме, допустимой для сетевой транспортировки с помощью программно-аппаратного комплекса ViPNet;
- распознавание целей по выявленным данным (функция распознавания может быть передана системе поддержки принятия решения (СППР) органа (пункта) управления РЭБ.

VipNet Client — программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции шифрования.

Спутниковый модем — аппаратно-программное устройство, обеспечивающее на основе VipNet непосредственный прием (передачу) данных в сети через спутниковые каналы связи.

Глобальная территориально распределенная информационно-телекоммуникационная сеть общего пользования — глобальная сеть общего пользования для передачи информации различной формы представления, формализации и защиты, основанная на использовании спутниковых каналов связи, сотовой связи и средств проводной коммуникации, удовлетворяющая современным стандартам функциональности и защиты.

Граничный маршрутизатор — устройство обмена данными маршрутизации с маршрутизаторами, принадлежащими другим автономным системам.

ViPNet-координатор — программный сервер защищенной сети VipNet, позволяющий создавать защищенную доверенную среду передачи информации ограниченного доступа с использованием общих и выделенных каналов связи (Интернет, телефонные и беспроводные линии связи) путем организации виртуальной частной сети с одним или несколькими центрами управления, выполняющий следующие функции:
- сервер IP-адресов — сервер, выдающий адреса устройствам в сети;
- прокси-сервер защищенных соединений — служба (комплекс программ), позволяющая клиентам выполнять косвенные запросы другим сетевым службам;
- туннелирующий сервер — криптошлюз;
- отказоустойчивый сервер защищенной сети VipNet в конфигурации VipNet Failover (кластера).

Маршрутизатор — специализированный сетевой компьютер, имеющий два или более сетевых интерфейсов и пересылающий пакеты данных между различными сегментами сети на основе таблиц маршрутизации, которые содержат информацию о топологии сети. Маршрутизатор может связывать разнородные сети различных архитектур.

Однонаправленный шлюз — предназначен для гарантированной однонаправленной передачи информации из открытых сетей в сети, в которых циркулирует секретная информация.

Рабочее место оператора открытого сегмента сети — сетевой компьютер, выполняющий функции хранилища несекретных данных и управления репликацией открытых баз данных между органами (пунктами управления) системы РЭБ.

Система поддержки принятия решений (СППР) — компьютер со специальной периферией и проблемно-ориентированным программным обеспечением для моделирования сетецентрической системы противника по формулярам данных РЭС, полученных средствами добывания информации и внешними системами, привязанными к карте оперативной обстановки. Система поддержки принятия решений — рабочее место оператора-аналитика закрытого сегмента сети, вырабатывающего рациональные рекомендации по ведению РЭБ с сетецентрическими системами противника.

Функциональная подсистема РЭБ АСУ различных органов (пунктов) управления МО и ВМФ, объединенных единым контуром управления.

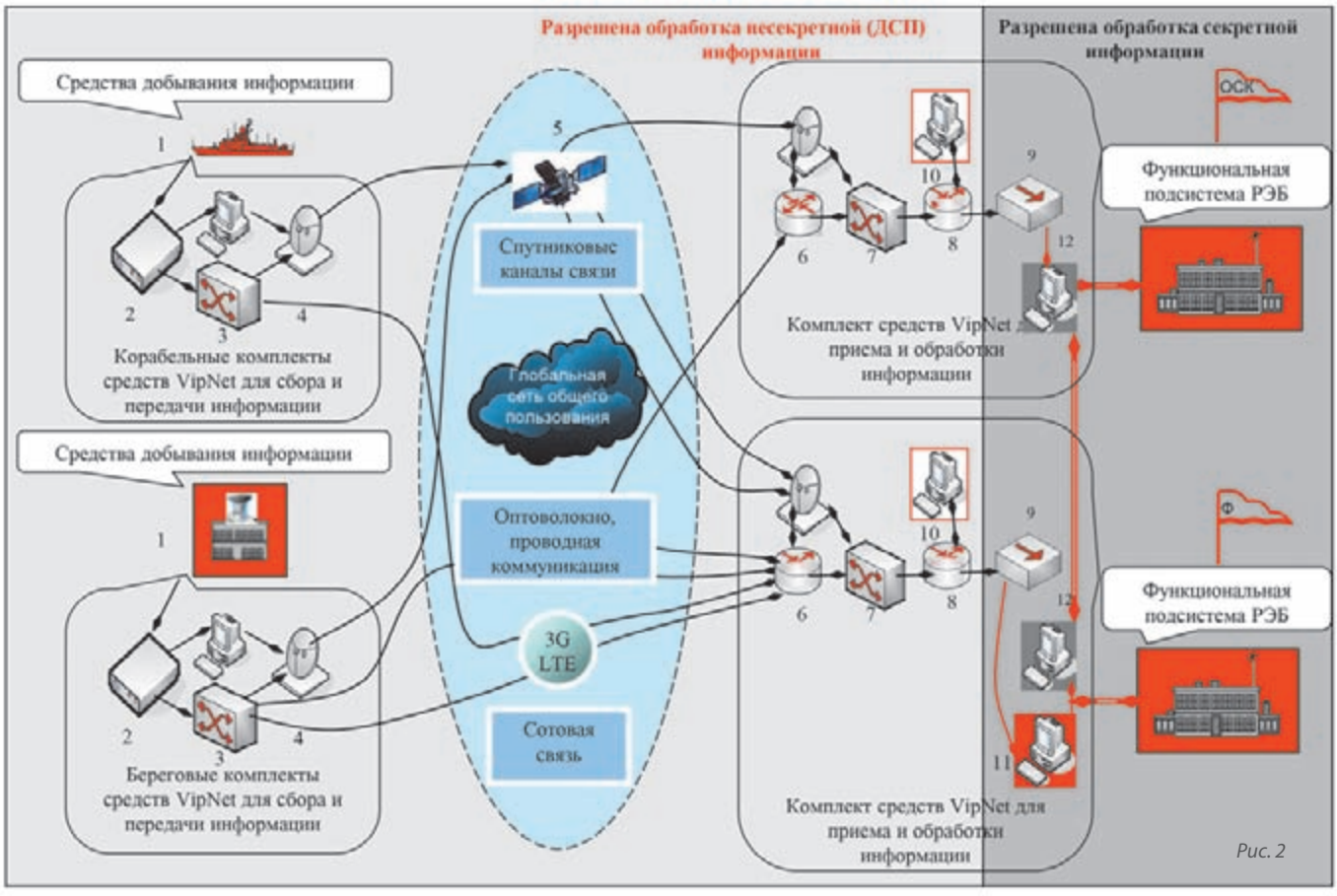

Рис. 2

Состав дополнительных средств программно-аппаратного комплекса ViPNet

Криптошлюз — аппаратно-программный (криптографический шлюз, VPN-шлюз, криптомаршрутизатор) — аппаратно-программный комплекс криптографической защиты трафика данных, голоса, видео на основе шифрования пакетов по протоколам IPsec при установлении соединения, соответствующий требованиям к средствам криптографической защиты информации (СКЗИ) ФСБ России и обеспечивающий базовую функциональность современного VPN-устройства.

Драйверы ViPNet взаимодействуют непосредственно с драйверами сетевых интерфейсов операционной системы (реальных или их имулирующих), что обеспечивает независимость программы от операционной системы и недокументированных возможностей в ней. VipNet-драйвер перехватывает и контролирует весь IP-трафик, поступающий и исходящий из компьютера.

Коммутатор — устройство для соединения нескольких узлов или сегментов вычислительной сети.

Межсетевой экран — комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Медиаконвертер — устройство, преобразующее среду распространения сигнала из одного типа в другой.

ViPNet осуществляет контроль и фильтрацию всего трафика с помощью специального ViPNet-драйвера.

ViPNet-драйвер позволяет вести обработку пакетов (дешифрование, контроль целостности, фильтрацию и блокирование) до того, как они будут переданы на транспортный уровень. Модули ViPNet обрабатывают весь TCP/IP-трафик, осуществляя его шифрование и дешифрование, контроль целостности и фильтрацию согласно установленной политике безопасности.

Принципы построения защищенной сетеориентированной системы информационного обеспечения РЭБ

Сетеориентированность — создание ЗСС ИО РЭБ по сетевым информационным технологиям.

Глобальность — способность всех определенных пользователей в свободной временной доступности использовать в виртуальном режиме ЗСС ИО РЭБ с контролируемой защищенностью информации.

Единое информационное пространство — пространство развертывания информационной сети с возможностями полного и своевременного получения пользователями однотипной информации одинаковой достоверности в соответствии с их полномочиями.

Защищенность информации в ЗСС ИО РЭБ, удовлетворяющая требованиям нормативных документов.

Гибкость — способность совершения быстрых перестроек топологии и маршрутизации информационных потоков ЗСС ИО РЭБ под типы выполняемых информационных задач.

Пространственная локализация — сосредоточение информации заданного типа защищенности (секретности) в границах локализации ЗСС ИО РЭБ с регулируемым режимом передачи информации на ее границах.

Гибридность — динамическое формирование ЗСС ИО РЭБ из пространственных локализаций различ-

ной защищенности под типы выполняемых информационных задач. Способность регламентированного функционального и информационного взаимодействия информационных сетей ЗСС ИО РЭБ и сетей ВС РФ.

Структура ЗСС ИО РЭБ (рис. 2) сетеориентированная, обусловленная созданием единого информационного пространства, и гибридная, так как интегрирует два взаимодействующих сегмента обработки информации: закрытый сегмент и открытый сегмент.

Общая модель функционирования ЗСС ИО РЭБ

Обнаружение сигналов РЭС, потенциальных объектов РЭБ на оперативном (стратегическом) направлении ведут корабельные, береговые и авиационные специализированные средства, комплексы, подсистемы. Полученная информация, в зависимости от конфигурации используемых средств, снимается в сигнальном или в файловом виде в форме формуляров.

На кораблях информацию об излучающих РЭС может давать АСУ или БИУС. Кроме того, от внешних источников — корабельных РЛС и пеленгаторов береговых частей — снимается информация о пространственных координатах целей, носителей излучающих РЭС. Всю перечисленную информацию собирает универсальный модем. Собрав информацию (потоковую, файловую), модем по установленной форме перекодирует ее в стандарт сети ViPNet для дальнейшей транспортировки по сети.

Передача формализованной информации осуществляется к VipNet Client — программному комплексу или к серверу с прикладным ПО функции VPN-клиента, которые с помощью криптодрайвера реализуют шифрование информации и ее последующую передачу на спутниковый модем или в каналы передачи данных.

Спутниковый модем обеспечивает непосредственный прием (передачу) данных в сети на основе VipNet через спутниковые каналы связи. Для каналов передачи данных (беспроводных и проводных) информация поступает на граничный маршрутизатор, обеспечивающий прием сигналов и обмен данными с другими маршрутизаторами сети.

Спутниковые каналы связи, каналы передачи данных, включая сотовую связь стандарта 3G (4G), являются глобальными сетями общего пользования, через которые переносятся обработанные шифром массивы обезличенных чисел о РЭС противника на оперативном (стратегическом) направлении. Никакой оперативной информации, приказаний боевого управления не передается. Информация собирается клиентами сети на региональном, территориальном уровне и в частях.

Принятая названными устройствами информация поступает на ViPNet координатор — программно-аппаратный сервер защищенной сети, создающий коммутацию виртуальной части сети (сети общего пользования) с центрами управления сети и с сервером. По организованным каналам полученная информация переносится в хранилище.

Таким образом формируется информационный ресурс открытого сегмента сети. Перечисленные средства сети имеют прямые и обратные связи, через которые данные с одного хранилища переносятся на хранилища других клиентов сети.

Часть сети, которая будет работать уже с проблемно-ориентированной информацией, с задачами и силами РЭБ и с оперативной и радиоэлектронной обстановкой, образует закрытый сегмент сети. Разделение между открытым и закрытым сегментами сети жесткое и обеспечивается использованием однонаправленного шлюза. У всех клиентов в соответствующих им участках сети используется однонаправленный шлюз.

Сетеориентированная организация ИО предполагает осуществление сетевого обмена данными между клиентами, что обеспечивает создание единого информационного пространства и наделение сил РЭБ одинаковой по полноте, достоверности и своевременности всесторонней информацией. Клиенты получают зашифрованную информацию с параметрами излучающих РЭС от глобальной сети общего пользования. Прием осуществляется типовым набором средств.

Таким образом, применение технологии и программно-аппаратных средств ViPNet обеспечивает скорейшее построение защищенной сетеориентированной системы информационного обеспечения системы РЭБ ВМФ. Данная сеть может рассматриваться как прототип и опытный участок для развертывания аналогичных сетей в МО РФ.