

БЕЗОПАСНОСТЬ

Предложения по построению сети Интернет для силовых структур Российской Федерации

Internet networking solutions for defense and law enforcement agencies of the Russian Federation

Ключевые слова: создание военного (боевого) Интернета – engineering of military (battlefield) Internet; формирование доменов и поддоменов – domaining and subdomaining; система адресования – addressing system; структура построения – forming structure.

В статье на основе анализа ведения современных военных действий и в рамках реформирования Вооруженных Сил Российской Федерации рассмотрены подходы и возможности создания военного (боевого) Интернета ВС РФ. Определена структура его построения, формирование доменов и поддоменов, система адресования.

This article proposes possible ways of designing a military Internet for the RF armed forces through the analysis of modern battle management within restructuring of the Armed Forces of the Russian Federation. It determines the architecture, domains, subdomains and addressing system of the network.

Нестабильность геополитической обстановки конца XX – начала XXI века и новые тенденции ее развития, связанные с прорывом в области информационных технологий в условиях применения новейших видов оружия и применения автоматизированных систем управления и связи, потребовали от военного руководства многих государств мира переосмыслить теорию и практику строительства и реформирования силовых структур. В современных условиях при быстро меняющейся обстановке высокий уровень информационного обеспечения боевых действий войск становится определяющим фактором достижения превосходства над противником. Намечился прогресс и во взглядах на развитие процесса управления в силовых структурах и ведомствах при выполнении ими различного рода задач как по прямому назначению, так и при совместном использовании сил и средств (МО, МЧС, МВД и т.д.). При этом требуется четкое и быстрое в реальном масштабе времени доведение необходимой информации от органов управления

АРТЮШЕНКО / ARTYUSHENKO A.
Александр Николаевич

адъюнкт научно-исследовательского центра
Военной академии связи им. С.М. Буденного.
Санкт-Петербург

до подчиненных (исполнителей). Однако различного рода информацией могут обладать только те силовые структуры, которым она присуща для выполнения задач по предназначению их деятельности в составе Российской Федерации.

Концептуальной основой концентрации действий сил и средств силовых структур является единое глобальное (региональное, локальное) боевое информационное поле, постоянно подпитываемое информацией посредством разветвленной системы связи и автоматизации. В современных условиях должностному лицу (командиру) для принятия адекватного решения необходима только обновленная и точная информация в реальном масштабе времени, отражающая сложившуюся оперативную обстановку. Сложность и динамичность информации требуют значительного количества времени для ее анализа, а современный характер выполнения боевых задач – принятия решений в возможно короткие сроки, а в отдельных случаях мгновенного.

Разрешение данной проблемы возможно на основе полной компьютеризации, комплексной автоматизации органов, сил, систем связи и средств управления, создания и развертывания боевого варианта информационной сети с интегрированными сервисами наподобие существующей и развивающейся глобальной сети общего доступа – Интернета. Создание и развитие сети Интернет выполнялось в основном частными компаниями и осуществлялось за счет государственного бюджета США. Такое решение было принято президентом Эйзенхауэром в ответ на запуск в СССР первого искусственного спутника Земли. На выделенные средства было создано Агентство перспективных научных исследований (ARPA), одной из важнейших задач которого стала разработка специальной информационно-вычислительной сети, связывающей сотни университетов и исследовательских организаций. В дальнейшем эта сеть была передана Национальному научному

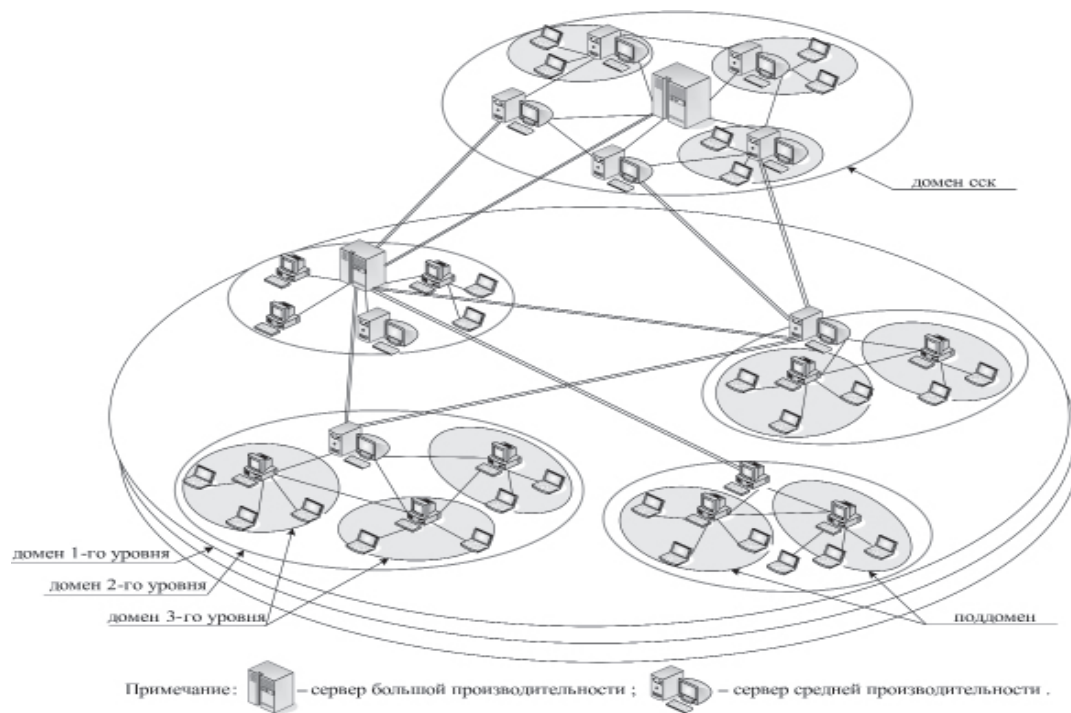


Рис 1. Структурный принцип построения "силового" Интернета

фонду США, а в ходе ее развития и возникла в результате Всемирная сеть Интернет. В этой работе активное участие принимали и другие государства, поэтому вполне можно считать, что создание сети Интернет – это результат международных усилий. Важная концепция, лежащая в основе развития сети Интернет: возможность предоставления любому пользователю любой информации в любое время и в любом месте. Последнее предполагает, что у пользователя совсем не обязательно должно быть под рукой устройство, включенное в проводную сеть. Так возникла новая проблема – обеспечение беспроводного доступа к универсальным услугам связи, предоставляемым через Интернет.

Сегодня Интернет представляет собой глобальную информационную сеть, обеспечивающую ее пользователям быстрый доступ к целому океану различной информации. Однако Интернет может быть подвержен воздействию извне, что может привести к сбоям или отказу в работе сетевого оборудования, серверов и автоматизированных рабочих мест должностных лиц. Каким бы совершенным и технически надежным он не был, компьютер может «зависнуть» в любой момент. А если представить картину, когда силовые ведомства выполняют боевые (специальные) задачи (поиск и обнаружение террористов, ведение локальных боевых действий и т.д.), а управляющий комплекс не функционирует? А если сеть не реагирует на

внешнее радиоэлектронное противодействие, она абсолютно беспомощна перед угрозой внутреннего вторжения. Уязвимости могут быть подвержены линии и каналы связи, обеспечивающие доступ управляющих и управляемых объектов к Интернету (порталам силовых структур). Командование ВС США пришло к выводу о необходимости изыскания путей совершенствования боевого Интернета, повышения его безопасности и защищенности от внутреннего и внешнего воздействия.

Одной из важнейших причин, оказывающих влияние на создание «силового» Интернета РФ, является его уязвимость, так как он может функционировать в глобальной (мировой) информационной паутине, на которую может воздействовать множество факторов. В настоящее время в Интернете функционируют силовые ведомства – прежде всего, военно-учебные заведения, органы управления военного образования, т.е. это, по существу, учебно-справочный Интернет, который не предназначен для управления силовыми структурами (доведения приказов, боевых распоряжений, обмена оперативной обстановкой и т.д.), а тем более – при выполнении боевых и специальных задач.

Создание Интернета для силовых структур РФ возможно на основе глобальной (мировой) информационной «паутины», но при этом должен быть

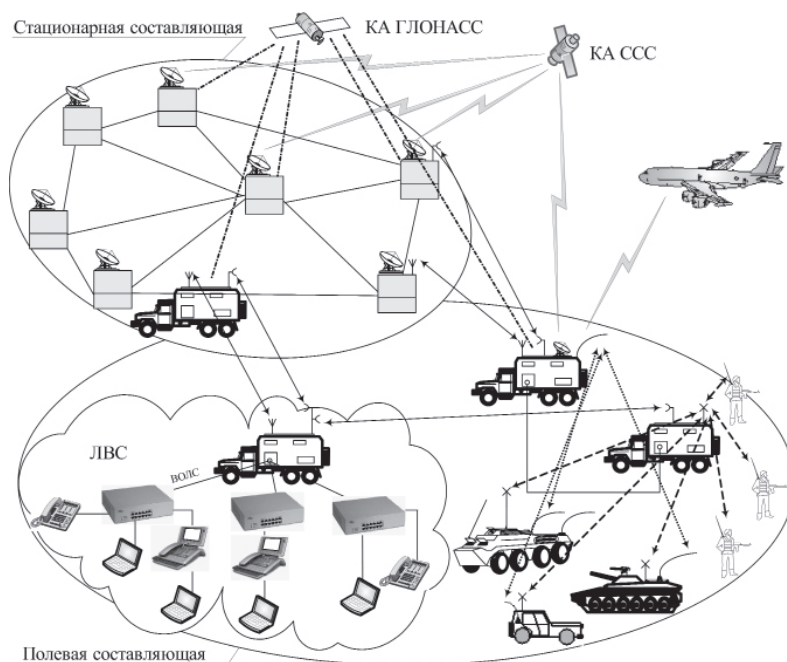


Рис 2. Применение сети "силового" Интернета в полевых условиях

выделен специальный сегмент (домен) закрытого типа, к которому бы обеспечивался доступ силовых структур РФ по определенному статусу (приоритету) пользователей. Однако так как глобальная информационная система по своей структуре является полносвязной, выделенный сегмент (домен) находится в глобальной (мировой) информационной паутине совместно с другими доменами и поддоменами, вследствие чего велика вероятность несанкционированного доступа, взлома сети и ее блокировка, ввод ложной информации и как результат – нарушение или потеря управления. Выходом из такой ситуации является создание «силового» Интернета РФ на основе сетей связи межвидового и межведомственного применения путем цифровизации и интеграции их в единое информационное пространство РФ.

Интернет для силовых структур РФ представляет собой информационную сеть закрытого типа (ограниченного доступа), предназначенную для управления силовыми структурами РФ в условиях мирного (в повседневной деятельности войск) и военного времени, обеспечивающую ее пользователям быстрый доступ к различной информации в режиме реального времени. Интернет силовых структур РФ должен создаваться как автономная сеть со своей операционной системой, специальной службой доменных имен и IP-адресами. С точки зрения оперативности управления и информационной доступности в сети возможен следующий

подход к созданию «силового» Интернета – формирование иерархии доменов по административно-территориальному делению (основной единицей является федеральный округ). В этом случае сеть может быть представлена в виде иерархии доменов (поддоменов) различного уровня, организуемых по территориальному признаку (рис. 1), в соответствии с границами федеральных округов. В соответствии с оперативной архитектурой должна создаваться специальная многоуровневая служба имен доменов для сопоставления IP-адресов и доменных имен, хранения и поиска адресов хост-компьютеров [1, 2]

Центральным органом в данном случае является домен верхнего уровня – «корневой» домен, включающий несколько серверов различной принадлежности, размещаемых на стационарных узлах связи пунктов управления, штабов силовых структур с условным именем «сск» («силовые структуры корневой»). Каждый из серверов связан друг с другом и центральным сервером линиями и каналами связи с использованием различных родов связи, что позволит создать сеть повышенной устойчивости и поддерживать информационный обмен между серверами при выходе из строя одного или нескольких серверов «корневого» домена. Доменами первого уровня являются федеральные округа РФ, доменами второго уровня – ВС РФ. К доменам третьего уровня относятся другие силовые структуры (МВД, МЧС, ФСБ и ФСО). Такое распределение доменов позволит обеспечить обмен инфор-

мацией силовых структур доменов нижних уровней (второго и третьего) с доменами первого уровня, территориально находящимися в одной зоне связи федерального округа.

При построении Интернета силовых структур возможны две системы распределения имен на серверах. В первом случае сервер может хранить отображения «доменное имя – IP-адрес» для всего домена первого уровня, включая его домены (поддомены) второго и третьего уровня. Во втором случае сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии, по сравнению с именем домена. При такой организации службы DNS нагрузка по разрешению имен распределяется равномерно между всеми DNS-серверами. Каждый DNS-сервер верхнего уровня, кроме таблицы отображений имен, содержит ссылки на DNS-серверы своих доменов (поддоменов) нижнего уровня. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена необходимо выделить несколько дублирующих друг друга DNS-серверов, чтобы обеспечить высокую живучесть, возможную расширяемость и масштабируемость сети, т.е. наращивание количества узлов связи, отдельных элементов сети (пользователей, компьютеров, приложений, служб и т.д.).

Для устойчивой работы важное значение имеет формирование единого адресного пространства в масштабе силовых структур РФ, обеспечивающего работу пользователей в сети на всех уровнях иерархии. Для этого должен быть создан специальный орган, ответственный за распределение IP-адресов. Управление адресами единого адресного домена организуется на основе формирования иерархии доменов в соответствии с подчиненностью. IP-адреса для удовлетворения внутренних потребностей в IP-адресах текущего уровня иерархии доменов и для нижележащих уровней выделяются из таблицы в соответствии с их потребностью. В своем составе «силовой» Интернет должен включать программно-аппаратные средства, предназначенные для построения телекоммуникационных сетей, функционирующих в постоянно меняющихся условиях обстановки во всех звеньях управления. Рабочие места должностных лиц должны включать средства спутниковой и радиорелейной связи, радиосвязи, беспроводного доступа, серверы, кросс-маршрутизаторы, терминальные устройства и другое оборудование. Так как подразделения и боевые расчеты, как правило, при выполнении боевых задач (в боевых условиях) будут действовать рассредоточено, в условиях частого перемещения, для организации связи необходимо использовать

средства беспроводного доступа (стандарта IEEE 802.11.x и 802.16.x).

Применение «силового» Интернета в условиях ведения боевых действий потребует развертывания полевой составляющей системы связи, которая должна представлять единое информационное пространство, взаимоувязанное со стационарной составляющей на основе внедрения новых информационных технологий, современных автоматизированных систем управления, слежения (наблюдения), разведки, сбора данных в совокупности с ударно-огневыми комплексами различного назначения (рис. 2). С помощью соответствующих сервисов, размещенных по уровням иерархии, пользователи смогут дополнять или уточнять соответствующие информационные файлы, а также «скачивать» необходимую информацию для решения тех или иных задач.

Достоинство Интернета для силовых структур РФ заключается в том, что создается единая разветвленная информационная сеть (типа «решетка»), обеспечивающая определенный санкционированный доступ к информации, повышается эффективность боевого управления силовыми структурами, их маневренность и взаимодействие в боевых условиях. Создаваемая сеть будет представлять три взаимоувязанных сферы (сегмента): информационную, физическую и когнитивную, что позволит обеспечить синхронизацию боевых действий и систем управления и тем самым повысить уровень боевых возможностей силовых структур и их взаимодействие. Сеть должна обеспечить непрерывный и единообразный обмен информацией для всех систем и средств, используемых в мирное время и при ведении боевых действий. Она объединяет в одно целое слагаемые процесса боевых действий путем создания цепочки «обнаружил – принял решение (обработал) – нанес удар (поразил)».

Реализация «силового» Интернета Российской Федерации может быть осуществлена на базе перспективной системы связи силовых структур РФ, созданной на основе применения современных информационно-телекоммуникационных технологий, средств автоматизации и обладающей высокими оперативно-техническими характеристиками, а также с использованием линий, каналов и трактов связи ЕСЭ РФ. Создание «силового» Интернета РФ позволит эффективно использовать силовые структуры при выполнении совместных задач в специальных операциях, в розыскной деятельности, в боевых условиях в режиме on-line.

Литература

1. Соломенчук В. Интернет: поиск работы, учеба, гранты. – СПб.: БХВ – Петербург, 2000.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. – СПб.: Питер, 2004.