Гигабитная сетевая структура ОИЯИ, сетевые сервисы, сетевая безопасность

К.Н. Ангелов, Б.А. Безруков, А.Э. Гущин, И.А. Емелин, В.В. Иванов, Л.А. Попов
Лаборатория информационных технологий, ОИЯИ
А.Г. Долбилов, С.В. Медведь
Лаборатория ядерных реакций, ОИЯИ

Гигабитная сетевая структура ОИЯИ представляет собой совокупность технических и программных средств, составляющих фундамент сетевой информационно–вычислительной инфраструктуры ОИЯИ, основу, на которой эта инфраструктура строится и развивается. Гигабитная сетевая структура решает следующие задачи: объединение в единое информационное пространство всех компьютерных ресурсов ОИЯИ; организация и предоставление сетевого доступа к информационно–вычислительным ресурсам для различных групп пользователей; обеспечение удаленного доступа к информационным ресурсам российских и зарубежных научных центров для исследователей всех подразделений ОИЯИ; создание единого информационного пространства для всех сотрудников ОИЯИ, обеспечивая возможность обмена данными, как между подразделениями института, так и между подразделениями и администрацией ОИЯИ; обеспечение сервисов удаленного доступа к ресурсам ОИЯИ с домашних персональных компьютеров сотрудников ОИЯИ.

Система адресации сетевой структуры
С 1991 года ОИЯИ, как научная организация, использует сеть реальных IP адресов класса “B”: 159.93.0.0/16 (256 сетей класса “C” по 256 адресов). Учетом и распределением сетевых адресов в ОИЯИ занимается Сетевая Служба ЛИТ. Для этого используется собственная программная разработка — реестр сетевых ресурсов IPDB. В реестре IPDB содержится информация о всех пользователях ОИЯИ, работающих с компьютерной сетью, о всех сетевых элементах (компьютерах и активном оборудовании) и о распределении IP адресов:

- за каждой лабораторией закреплен блок IP адресов, состоящий из 16-ти сетей класса “C” (256 адресов);
- за сервисом удаленного доступа (Dial-Up и VPN) закреплен блок адресов из 8-ми сетей класса “C”;
- за всеми отдельными подразделениями ОИЯИ, не входящими в состав лабораторий, но располагающими своими локальными сетями и достаточным количеством компьютеров, (например, УНЦ, Опытное производство, Научно–техническая библиотека, НЦПИ) закреплена персональная сеть класса “C”. За отдельными проектами или большими кластерами оборудования (GRID, фермы под управлением Linux) также закрепляются отдельные сети класса “C”;
- подсети меньшего размера (32 или 64 адреса) выделяются небольшим отдельным подразделениям, подключаемым с сети ОИЯИ по DSL;
- для части сетевого оборудования и технологических нужд используются частные (“private”) адреса сетей 192.168.xxx.xxx и 10.xx.xx.xxx .

Использование реальных IP адресов имеет как положительные, так и отрицательные стороны. Практически в каждом подразделении (лаборатории) применяется несколько серверов, которые принимают запросы из внешней сети и которым необходимы реальные IP адреса. Происходит постоянный обмен информацией и перекачка больших объемов данных между хостами сети ОИЯИ и хостами различных внешних научных российских и зарубежных организаций. Ряд протоколов передачи данных (например, NFS/AFS), широко используемых в научных сетях передачи данных, рассчитаны на использование только реальных адресов. Недостатки работы с реальным адресом — если на хосте установлен реальный IP адрес, то на этот хост возможно прямое входящее соединение из внешней сети. В случае, когда хост недостаточно защищен (не установлены обновления на операционную систему, не включен персональный брандмауэр) возможность прямого подключения извне может привести к взлому хоста. Поэтому при использовании в компьютерной сети реальных IP адресов, эту сеть надо защищать не только централизовано (задача Сетевой Службы ЛИТ), но и поддерживать защиту отдельных сетевых элементов (задача системных администраторов лабораторий/подразделений).

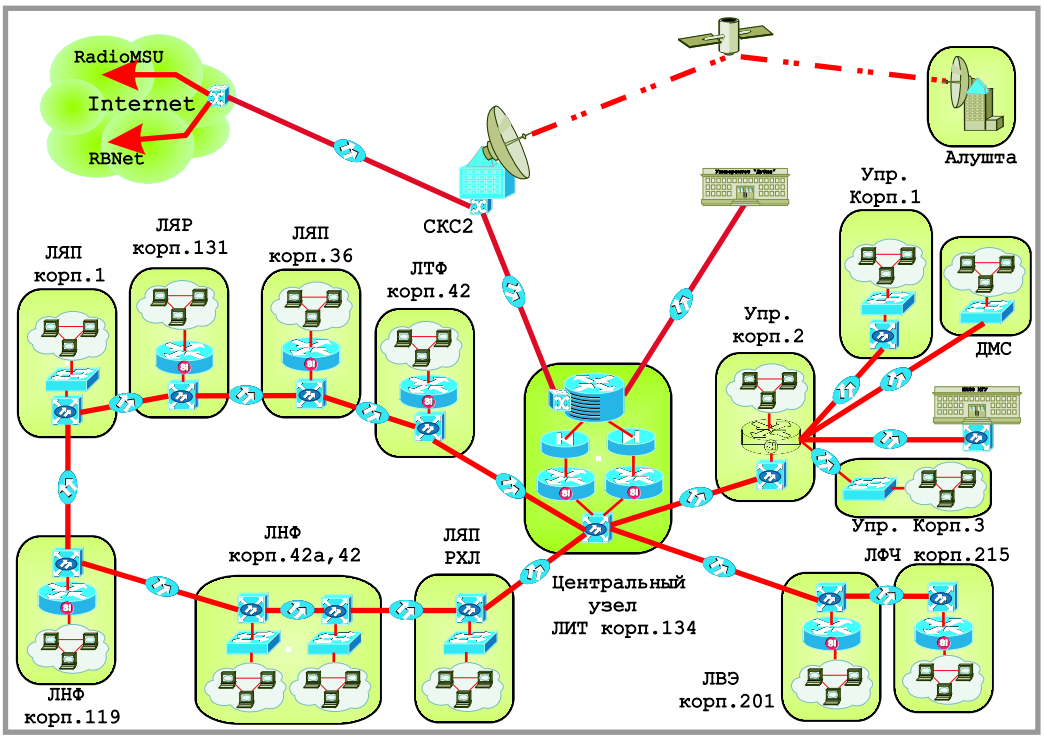

Рис. 1: Гигабитная сетевая структура ОИЯИ

Гигабитная сетевая структура состоит из оптической транспортной магистрали локальной вычислительной сети ОИЯИ, центрального телекоммуникационного узла связи, магистральных коммутаторов основных подразделений ОИЯИ (Рис.1).

Волоконно–оптическая кабельная структура локальной вычислительной сети включает: волоконно–оптическую линию связи с внешними каналами; одномодовую волоконно–оптическую кабельную структуру; многомодовую волоконно–оптическую кабельную структуру.

Связь с внешними каналами организована через волоконно–оптический канал между Интернет–маршрутизатором ОИЯИ и оборудованием ЦКС “Дубна”.

Центральный коммутационный узел связи
Центральный коммутационный узел связи предназначен для коммутации одномодовых и многомодовых волоконно–оптических линий связи транспортной магистрали ЛВС ОИЯИ; мультиплексирования пакетов данных, исходящих из локальной сети ОИЯИ, и передачи этих данных по волоконно–оптическому каналу связи в Москву Интернет–провайдеру РосНИИРОС сети RBNet и обратной процедуры — демультиплексирования пакетов данных, поступающих от Интернет–провайдера, передачи данных подсетям института и, наконец, конечным пользователям; кроме того, выполняется коммутация телефонных линий модемного пула и DSL–подключений.

Состав центрального коммутационного узла связи
Маршрутизирующее и коммутирующее оборудование фирмы Cisco Systems (США) является де-факто стандартом в ОИЯИ. Ниже приводится перечень оборудования центрального узла, которое произведено, в основном, компанией Cisco Systems.

- Многопротокольный Интернет—маршрутизатор Cisco 7505;
- Центральный коммутатор Cisco Catalyst 6509;
- Резервный коммутатор Cisco Catalyst 3550–12G;
- Межсетевой пакетный экран Cisco PIX–525;
- Многопротокольный маршрутизатор удаленных подключений Cisco 3640;
- Многопротокольный маршрутизатор сетей малых подразделений Cisco 2611;
- Промежуточный коммутатор Cisco Catalyst 3750–24TS–E;
- Промежуточный коммутатор Cisco Catalyst 2924M–XL–EN — 2 шт.;
- Промежуточный коммутатор Cisco Catalyst 2924M;
- Концентратор выделенных телефонных подключений AES100;
- Концентратор выделенных телефонных подключений IES1000;
- Модем Courier (компания US.Robotics) — 16 шт.;
- Оборудование волоконно–оптического цифрового линейного тракта T31.

Сетевые сервисы
Сетевые сервисы, к которым пользователи ОИЯИ имеют доступ, можно разделить на две группы: сервисы, предоставляемые пользователям ОИЯИ со стороны других сетей, то есть сервисы внешних сетей, и сервисы, предоставляемые собственными инфраструктураными ресурсами ОИЯИ.
Сервисы внешних сетей:

- почтовый транспортный сервис — Simple Mail Transport Protocol (SMTP);
- почтовые сервисы для работы почтового ящика: IMAPS, POP3S (расширение стандартных протоколов IMAP V4 и POP3 с криптованием аутентификации и потока данных);
- Secure Shell (SSH) — сервис удаленного терминала через криптованный канал;
- пересылка файлов по протоколам FTP, SCP, SFTP, HTTP, HTTPS;
- сервис доменных имен — Domain Name Service (DNS);
- работа с web–серверами (http, https);
- работа с RSS–серверами;
- работа с News–серверами;

- Webmail — сервис для удаленной работы с почтовой учетной записью и почтовым ящиком в зоне @jinr.ru;
- синхронизация времени по протоколу NTP;
- видеоконференции (ограниченно);
- пограничный протокол маршрутизации BGP.

Внутренние сетевые сервисы:

- все сервисы вышеуказанной группы;
- почтовые сервисы для работы с почтовым ящиком (IMAP, POP3);
- почтовые сервисы (SMTP, POP3);
- сервис динамического выделения сетевых адресов (DHCP);
- proxy–сервер;
- сервис печати;
- сервис аутентификации удаленных пользователей при коммутируемом и прямом доступе (TACACS);
- сбор сетевой статистики на базе NetFlow;
- Windows — протоколы (WINS, NETBIOS Name Service, NETBIOS Datagram Service, NETBIOS session service, microsoft–ds);
- Rdesktop — сервис удаленного "рабочего стола";
- Web–сервис для ведения единой учетной системы сетевых элементов, а также для управления сетевыми узлами и вывода статистических данных — IPDB;
- в качестве внутреннего протокола маршрутизации для повышения отказоустойчивости применяется протокол OSPF.

Сервис электронной почты является наиболее "старым" и значимым из Интернет–сервисов, используемых в ОИЯИ. Интенсивно используется как основной способ обмена информацией с внешними научными организациями. В настоящее время скорость обмена почтовыми электронными сообщениями (email) даже с зарубежными институтами CERN, FNAL, DESY, BNL такова, что сообщения доходят за 5–10 минут. В ОИЯИ используются два почтовых домена — **jinr.dubna.ru** и **jinr.ru**, с приоритетом на **jinr.ru** . Почтовый домен **jinr.dubna.su** сохраняется исторически и используется для совместимости. В каждой лаборатории есть свой почтовый сервер, сотрудники лаборатории получают почтовые адреса типа **xxxxx@yyyy.jinr.ru**, где **yyyy** — название лабораторного сервера. Существует центральный почтовый сервер, обслуживающий адреса типа **xxxx@jinr.ru** . На нем получают почтовые адреса сотрудники ЛИТ и Управления. Аппаратно он состоит из двух серверов: основного и резервного. При выходе из строя основного почтового сервера начинает работать резервный. Для того чтобы избежать потерь поступающих сообщений, когда какой–либо из почтовых серверов ОИЯИ становится недоступен, существуют, так называемые, "транзитные" (relay) сервера. Они принимают входящую почту и накапливают ее в своих очередях, периодически пробуя передать ее на тот почтовый сервер, которому она предназначена. Сетевая Служба поддерживает два таких relay–сервера: **relay** и **relay1**, которые при выходе из строя любого почтового сервера ОИЯИ будут принимать его входящую почту и хранить до восстановления этого сервера. Все почтовые сервера Сетевой Службы используют средства антивирусного контроля и фильтры рекламных рассылок для защиты от спама.

Статистика трафика

Для контроля использования внешнего канала в ОИЯИ используется система статистики трафика. Система состоит из программных модулей сбора, обсчета, визуализации и модуля базы данных. Сбор статистических данных основывается на использовании технологии NetFlow, встроенной в маршрутизаторы Cisco. После накопления на Cisco–маршрутизаторе очередного блока статистики трафика (примерно каждые 5 минут), сформированный блок пересылается на коллектор (технология "PUSH"). Учитывается как входящий, так и исходящий трафик. Коллектором в данном случае выступает выделенный сервер статистики под управлением операционной системы FreeBSD и установленным пакетом FlowTools. Далее, данные обсчитываются, отфильтровывается внутренний и служебный трафики; доли внешнего трафика распределяются по подсетям и подразделениям ОИЯИ, итоговые данные заносятся в базу данных MySQL. С помощью WWW–интерфейса реестра сетевых ресурсов IPDB, системные администраторы лабораторий могут просматривать статистику использования внешнего канала компьютерами своих подразделений с точностью до IP адреса. При необходимости система может быть настроена на автоматическое отключение потребителей, превысивших указанные нормы потребления трафика. Система сбора данных FlowTools — это бесплатно распространяемый пакет, а системы обсчета и визуализации — разработка Сетевой Службы ОИЯИ.

DNS сервис

Задача сервиса доменных имен DNS (Domain Name Service) — трансляция Интернет–имен (имен хостов) в соответствующие IP адреса. DNS сервис является ключевым сетевым сервисов, так как при нарушениях его работы ни одно сетевое приложение пользователей не сможет использовать обращения к ресурсам по имени. Например, вместо **www.jinr.ru** пришлось бы набирать IP адрес **159.93.39.7**. Схема размещения и распределения нагрузки DNS серверов похожа на схему размещения почтовых серверов. В каждой лаборатории на лабораторном сервере запущен DNS сервис, обслуживающий запросы пользователей этой лаборатории. В Сетевой Службе ЛИТ установлен центральный DNS–сервер, который поддерживает домены **jinr.ru** и **jinr.dubna.su**; есть резервный сервер, который настроен на обслуживание запросов пользователей всего института. Так, при сбое лабораторного DNS–сервиса запрос автоматически попадает на резервные центральные сервера. Домены (зоны) **jinr.ru** и **jinr.dubna.su** формируются на центральном сервере автоматически на основании данных реестра сетевых элементов ОИЯИ — IPDB. Например, если прописать в IPDB соответствие IP адрес **159.93.17.82=noc.jinr.ru**, то через 3 минуты эти данные уже попадут в DNS домены **jinr.ru** .

Сетевой доступ к ресурсам ОИЯИ

1) Высокоскоростные подключения. В связи с развитием городских скоростных сетей в 2005 году в институте был внедрен новый тип удаленного доступа — доступ через виртуальные частные сети (VPN — Virtual Private Network). Физически пользователь должен быть подключен к одному из городских Интернет–провайдеров, с которым у ОИЯИ есть договор об обмене трафиком и точка сопряжения сетей. Используя сеть провайдера как среду передачи, пользователь устанавливает соединение с VPN–сервером, находящимся в ОИЯИ, но имеющем подключение и к сети провайдера. После процедуры авторизации компьютеру пользователя присваивается IP адрес сети ОИЯИ, и пользователь на время сеанса становится частью сети ОИЯИ.

При этом передача данных между компьютером пользователя и VPN–сервером ведется через сеть провайдера, но по зашифрованному виртуальному каналу связи, передаваемые данные при этом защищены от подмены и перехвата.

2) Коммутируемые модемные телефонные линии организованы в модемный пул. Назначение модемного пула — предоставление услуги удаленного коммутируемого доступа к ресурсам локальной вычислительной сети института. Для удаленных (коммутируемых) пользователей предоставляются следующие сервисы: электронной почты (протоколы POP3/IMAP и SMTP); терминального соединения (TELNET/ SSH); передачи файлов (FTP/SCP и Microsoft file sharing); доступа к гипертексту (HTTP/HTTPS). На модемном пуле зарегистрировано около 800 пользователей. Недостатки модемного пула очевидны: 1) низкая скорость передачи данных; 2) большие входные очереди; 3) длительное время вхождения в связь.

3) Модемные соединения по выделенным телефонным линиям организованы для ряда подразделений ОИЯИ, которые располагаются на площадках в удалении от основных корпусов или на территории города. Для этих подразделений также требуется Интернет–подключение, но они потребляют небольшой объем сетевого трафика, и поэтому подведение к ним оптоволоконных магистралей нерентабельно. В таких случаях самым оптимальным решением является использование технологий цифровых абонентских окончаний xDSL (Digital Subscriber Line). В качестве среды передачи xDSL использует телефонные линии и может работать на расстояниях до 5 — 7 км.

Это более дорогой способ доступа, чем при коммутации телефонной линии, так как используется выделенная линия связи, но более эффективный, так как не нужно делить имеющуюся полосу пропускания с другими абонентами. Для небольших организаций используются устройства DSLAM (Digital Subscriber Line Access Multiplexer) — мультиплексоры цифровых абонентских окончаний в качестве концентраторов линий связи. У нас применяется два типа модульных мультиплексоров тайваньской фирмы Zyxel: AES–100 на 8 портов, IES–1000 на 16 портов. На абонентской стороне устанавливаются ADSL–модемы. Это оборудование позволяет подключать абонентов на скорости до 8 Мбит/с в сторону абонента, и до 900 Кбит/с от абонента.

4) Беспроводные подключения в ОИЯИ используются при проведении совещаний и конференций для предоставления возможности подключений ноутбуков участников совещаний. Так сделано, например, в ДМС, в ЛИТ и в других лабораториях. В ДМС используется простейшая схема: беспроводная точка доступа/маршрутизатор Trendnet TEW–411BRP. Когда есть потребность — она включается в большом зале в сетевую розетку. Беспроводный маршрутизатор настроен таким образом, что входной адрес берется по протоколу DHCP (как и всеми компьютерами в ДМС) от магистрального маршрутизатора Управления Cisco 3550–12T, находящегося во 2-ом корпусе Управления, и обеспечивающего маршрутизацию ДМС. Далее “точка доступа” сама осуществляет маршрутизацию в частную сеть 192.168.0.x/24, которую раздает по беспроводной технологии WiFi в зал. Шифрование на ней отключено для удобства работы пользователей.

Организация сетевой безопасности

Один из наиболее важных и ответственных вопросов — вопрос защищенности сетевой и компьютерной инфраструктуры. Многие специалисты по системам сетевой защиты предлагают определить сетевую безопасность как динамическую сущность,

когда формулируются риски для информационно–вычислительной инфраструктуры и формируются механизмы и процедуры для организации защищенности бизнес–процессов конкретной организации. Для эффективного обеспечения безопасности нужно защищать каждый сетевой элемент, то есть, организовывать эшелонированную защиту инфраструктуры.

Наиболее характерные угрозы для компьютерной сети любой организации: нарушение функциональности сетевого оборудования и серверов из–за искусственно создаваемых либо естественных перегрузок, либо направленных атак; несанкционированный доступ к ресурсам сети и к конфиденциальной информации; использование ресурсов сети с целями, не соответствующими профилю работы организации и неквалифицированные действия при настройке сети и сервисов.

За годы существования сетевой структуры ОИЯИ Сетевая Служба наработала значительный опыт в применении организационных и технических мер повышения уровня сетевой безопасности; были разработаны средства анализа и локализации сетевых проблем и источников угроз. Ниже описан методологический подход и процедуры, нацеленные на повышение уровня безопасности при работе в сети ОИЯИ. Постоянное совершенствование этого накопленного опыта особенно важно при работе с высокоскоростными гигабитными структурами.

Регистрация сетевых элементов

При любых инцидентах, когда источник находится внутри сети, первостепенное значение имеет скорость и точность локализации этого источника. Для ОИЯИ это особенно критично, так как сеть топографически очень разветвленная. При возникновении проблем, как правило, единственными известными данными являются IP адрес или MAC–адрес источника. Около 10 лет в ОИЯИ работает реестр Сетевой Службы — IPDB. Это программный комплекс, состоящий из базы данных и интерфейса, к которому имеют доступ администраторы Сетевой Службы и системные администраторы подразделений. По правилам сетевой политики, действующей в ОИЯИ, каждый сетевой элемент (компьютер или оборудование) должен быть зарегистрирован в IPDB. При регистрации указывается местоположение сетевого элемента, его IP и MAC адреса, а также контактные данные пользователя, ответственного за этот сетевой элемент. При помощи IPDB по IP или MAC адресам можно в считанные секунды получить необходимые данные о местонахождении этого сетевого элемента и координаты ответственного за него сотрудника.

Внедрение управляемого коммутируемого оборудования

Существует ряд ситуаций, когда источник должен быть незамедлительно и полностью отключен от сети. На старом сетевом оборудовании класса концентратор/неуправляемый коммутатор не было возможности удаленно отключать конкретные порты, а значит, и компьютеры. Зачастую приходилось отключать целый сегмент сети. Кроме того, оборудование класса концентратор транслировало все пакеты на все порты, что позволяло любому пользователю “прослушивать” сеть, получая доступ к информации, для него не предназначенной. Современное оборудование (управляемые коммутаторы) лишено таких недостатков, передача пакетов ведется между портами на основании таблицы MAC–адресов, пакеты попадают только по назначению, и возможность “прослушивания” исключена. Кроме того, они позволяют произвести удаленное отключение любого порта. В ЛИТ (и в большинстве лабораторий) в 2005

году практически полностью произведена замена старого сетевого оборудования на управляемые коммутаторы.

Автономные сети и временные отключения
Сети жизненно–важных подразделений, обслуживающих энергетическое и радиационное оборудование, по соображениям безопасности полностью автономны, и не подключены к общей сети. В других случаях, во время проведения экспериментов сеть, обслуживающая физическую установку, отключается от общей сети для снижения риска внешних воздействий.

Заражение компьютеров Интернет–червями
Ввиду высокой производительности современной компьютерной техники, заражение даже одного компьютера вирусом класса I — Worm создает существенную нагрузку на сетевые ресурсы. Зараженный компьютер начинает сканировать другие компьютеры локальной сети, рассылать по сети широковещательные сообщения, рассылать по адресам из адресной книги копии зараженного сообщения. Если сеть не защищена надлежащим образом, то количество зараженных компьютеров лавинообразно возрастает, и нагрузки принимают пиковые значения, парализуя работу почтовых серверов и коммутирующего оборудования.

В сети ОИЯИ для борьбы с вирусами приняты следующие меры:

- Возможность прямого почтового обмена с внешними сетями имеют только те почтовые сервера, на которых установлено антивирусное программное обеспечение, и включен постоянный антивирусный контроль почтового потока. Почта остальных серверов принудительно перенаправлена через сервера с антивирусным контролем.
- Идет процесс постепенной централизации почтовых серверов — снижение общего количества, но повышение защищенности;
- На серверах Сетевой Службы установлены системы анализа и оповещения, проверяющие почтовый и сетевой трафик, и автоматически рапортующие о признаках вирусной активности, исходящей с IP–адресов сети ОИЯИ. При обнаружении такой активности с целью предотвращения дальнейшего распространения вируса операторы Сетевой Службы блокируют доступ к сети для подозреваемого хоста и отправляют уведомление системному администратору лаборатории/подразделения.
- Приобретается легальное антивирусное программное обеспечение; наличие антивирусной программы на каждом компьютере обязательно.

Неквалифицированные действия пользователей
Допускаемые ошибки при настройке сетевого подключения (например, неправильно указанный IP адрес) могут привести к сбоям в работе сети и сетевых сервисов. Влияние таких инцидентов на всю сеть уменьшается при сегментировании сети. Чем выше степень сегментирования, тем меньшее количество пользователей может пострадать (только те, кто находится с источником в одном сегменте). В ОИЯИ к 2005 году при использовании коммутаторов 3-го уровня (Cisco Catalyst 3550, Cisco Catalyst 3750) создано восемь подсетей. Старый логический опорный сегмент (магистраль), состоявший из 32 сетей класса C (8160 адресов) был ликвидирован. Также, в центральных сегментах сети используются системы анализа и оповещения, которые реагируют

на изменения соответствий MAC–IP, появление незарегистрированных или просто некорректных IP адресов.

Безопасность уровня ключевых объектов и серверов
По соображениям безопасности все сетевое оборудование, обеспечивающее внутреннюю работу сети ОИЯИ, работает на немаршрутизируемых адресах частных (private) сетей
192.168.xx.xx и 10.xx.xx.xx. Таким образом, извне сети ОИЯИ невозможно установить сеанс связи с этим сетевым оборудованием, как и провести на него атаку. На кластере серверов Сетевой Службы, предоставляющем центральные сетевые сервисы, почту, DNS, авторизацию, статистику, установлены брандмауэры, регламентирующие доступ к этим службам.

Безопасность уровня приложений
В связи с открытостью протоколов TELNET, IMAP и POP3 для увеличения степени защищенности передачи паролей на пограничном маршрутизаторе ОИЯИ эти протоколы заблокированы. Используются альтернативные варианты с шифрованием данных: SSH, IMAP+SSL, POP3+SSL, что исключает возможность "подслушивания" паролей при соединениях между сетью ОИЯИ и внешними сетями.

На внешнем маршрутизаторе (Cisco 7505) настроены списки доступа ACLs (Access Control Lists) для некоторых приложений, сопряженных с повышенным риском сетевых атак. Заблокированы входящие соединения на порты, обслуживающие почтовые соединения, базы данных, прокси–сервис, сервис удаленного доступа.

Существенной проблемой является уровень поддержки самостоятельно устанавливаемых сервисных приложений. "Продвинутые" (более квалифицированные) пользователи любят устанавливать сервисные приложения типа DHCP, FTP, HTTP, также настраивать сетевой доступ к дисковым ресурсам и т.д. При этом в большинстве случаев, установленные сервисы не поддерживаются должным образом, не устанавливается политика безопасности, некорректно формируются списки доступа, не устанавливаются обновления прикладного ПО. Подобные сервисы и являются основными "дырами", через которые злоумышленники получают доступ к системе.

С серверов Сетевой Службы в автоматическом режиме проводится сканирование сети с целью выявления установленных сервисов, после чего обнаруженные сервисы проверяются администраторами Сетевой Службы, и при выявлении нарушений политики безопасности сервис блокируется, а ответственный пользователь получает уведомление.

Тематический контроль и ограничение трафика
Системным администраторам лабораторий и подразделений доступна система статистики внешнего трафика. При помощи этой системы администраторы выявляют наибольших потребителей в своей лаборатории и могут их блокировать. В некоторых подразделениях существует квота на потребление трафика пользователями. Если подразделение, не входящее в список основных лабораторий, начинает потреблять трафик на уровне лаборатории, то скорость подключения этого подразделения ограничивается. В целях ограничения потребления трафика и снижения нагрузки на внешний канал также используется система тематического контроля. Например, http–трафик сетей модемного пула принудительно завернут через прокси–сервер

proxy.jinr.ru . На прокси–сервере с помощью списков доступа заблокирован “ненаучный” развлекательный трафик, также заблокирована загрузка мультимедийных файлов большого объема. Для доступа к некоторым внешним ресурсам требуется пройти предварительную авторизацию. В результате появляется возможность индивидуального учета трафика пользователей с этих ресурсов.

Список литературы

[1] О.С.Алдышев, А.А.Мохнатюк, Б.М.Шабанов “Локальная вычислительная сеть вычислительного комплекса”, 2001 г.

[2] О.С.Алдышев, А.П.Овсянников, Б.М.Шабанов “Развитие корпоративной сети Межведомственного суперкомпьютерного центра”, 2002 г.

[3] Annual Report, 2003; Joint Institute for Nuclear Research; Laboratory of Information Technologies; Опорная сеть ОИЯИ на технологии Gigabit Ethernet.

[4] Стратегическое планирование сетей масштаба предприятия; ЦИТ, 1997 г.

[5] Джо Хабракен, “Маршрутизаторы Cisco. Практическое применение”, 2001 г., “ДМК–Пресс”.

[6] Кесрин Пакет, Дайана Тир “Создание масштабируемых сетей Cisco”.