Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 5 (108)/2002

Jet infosystems

Компания «Инфосистемы Джет»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Компания «Инфосистемы Джет»

Компания «Инфосистемы Джет» — ведущий российский системный интегратор и поставщик ключевых компонентов информационных систем для крупных организаций и предприятий.

О компании

Компания «Инфосистемы Джет» работает на российском рынке с 1991 года.

Компания выполняет крупномасштабные проекты по созданию и внедрению законченных информационных систем высокого уровня сложности. Разработка таких систем требует от компании-интегратора сочетания множества качеств — высокой культуры организации производственных процессов, глубоких знаний современных информационных технологий и солидного опыта применения этих технологий на практике, понимания бизнес-задач заказчиков, высокой квалификации специалистов.

Компания реализует проекты по созданию информационных систем заказчиков «под ключ».

Основные направления деятельности

Основными направлениями деятельности компании являются:

- Системное проектирование, разработка концепции и архитектуры больших информационных систем;
- Проектирование и построение серверных вычислительных комплексов;
- Аудит, проектирование, построение и оптимизация компьютерных сетей;
- Проектирование и построение комплексных систем защиты информации;
- Проектирование и построение централизованных систем управления информационными ресурсами;
- Разработка и интеграция прикладных систем на основе промышленных интернет-технологий;
- Сервисное обслуживание, техническая поддержка, внешняя эксплуатация.

Информационная безопасность – одно из основных направлений деятельности компании

Компания «Инфосистемы Джет» ведет работы в области информационной безопасности с 1994 года. За время своей деятельности компания осуществила более 200 проектных разработок по защите информации в государственных и коммерческих организациях. Опираясь на собственный опыт ведения проектов по защите информационных систем, компания проектирует и реализует комплексные системы защиты.

Компания осуществляет полный комплекс услуг по обеспечению информационной безопасности.

В основе подхода компании — сочетание первоочередных мер по устранению уязвимых мест в защите, всестороннего анализа рисков, разработки и реализации долгосрочной политики информационной безопасности.

Преимущества решений нашей компании

Команда высококвалифицированных специалистов

В нашей компании работает около 200 человек, в том числе более 100 инженеров, консультантов, разработчиков и руководителей проектов.

Компания располагает персоналом с высоким уровнем профессиональной подготовки, прошедшим обучение у фирм-производителей оборудования и программного обеспечения.

Большой практический опыт и высокое качество ведения проектов

С 1994 года компания выполнила более 200 проектов по защите информации в государственных и коммерческих организациях — в федеральных и муниципальных структурах, банках и финансовых учреждениях, крупных торговых и промышленных предприятиях.

Комплексный подход обеспечения информационной безопасности

В обеспечении информационной безопасности важен комплексный подход. Наша компания

гарантирует полноту и высокое качество поставляемых решений.

Компания осуществляет полный комплекс мероприятий по обеспечению информационной безопасности, включающий:

- Обследование защищенности информационных систем;
- Анализ рисков;
- Разработку политики ИБ;
- Проектирование и развертывание подсистемы ИБ, включая управление доступом и внешней защитой, мониторинг, аудит на основе продуктов наших партнеров и уникальных собственных разработок;
- Подготовку сертификационных испытаний СВТ и проведение аттестации АС на соответствие требованиям по защите информации;
- Техническую поддержку подсистем ИБ, развернутых у Заказчика;
- Консультации специалистов в области защиты информации.

Использование в своих решениях новейших технологий

Развитие и стремительное распространение информационных технологий заставляет специалистов компании быстро реагировать на происходящие изменения, постоянно быть в курсе последних событий.

У компании сложились тесные партнерские отношения с компаниями — Sun Microsystems, Hewlett-Packard Company, VERITAS Software Corporation, Symantec, Novell, RSA Security, Entrust Technologies, Nortel Networks, Cisco Systems, AVAYA Communication, Oracle Corporation, Legato Systems, IONA Technologies, Baltimore Technologies.

Компания также активно сотрудничает с ведущими российскими компаниями — разработчиками программного обеспечения, поставщиками решений, системными интеграторами. При выборе своих поставщиков и партнеров компания ориентируется на долгосрочные партнерские отношения.

Использование собственных разработок

Помимо продуктов своих партнеров, наша компания использует в проектах собственные разработки: межсетевые экраны «Застава-Джет» и Z-2, комплекс кодирования межсетевых потоков «Тропа-Джет», систему мониторинга и архивирования почтовых сообщений «Дозор-Джет». Эти комплексы установлены и успешно работают как во многих российских компаниях, так и в зарубежных.

Индивидуальный подход к задачам каждого Заказчика

Наши заказчики, как правило, имеют сложную информационную инфраструктуру, уникальные модели организации работ, большое количество географически распределенных подразделений. В своей работе компания ориентируется на адаптацию своих методов к подходам, принятым у заказчика — задача управления работами и проектами максимально приближена к заказчику.

Разработка типовых решений

На базе нашей испытательной лаборатории разрабатываются типовые решения по созданию ключевых подсистем корпоративных ИС по всем направлениям деятельности компании.

Разработка типовых решений позволяет уменьшить сроки исполнения проектных работ и повысить их качество.

Сервисное обслуживание

Сервисный центр, авторизованный многими известными производителями сетевого и телекоммуникационного оборудования, обеспечивает гарантийное и послегарантийное обслуживание средств защиты, поставляемых компанией.

Высокий уровень инженеров и технических специалистов, подтвержденный сертификатами фирм-производителей, позволяет успешно внедрять и осуществлять поддержку решений на базе современных информационных технологий.

Использование большого опыта наших специалистов, специально разработанных методик, современного сертифицированного аппаратного и программного обеспечения и собственных разработок является надежной гарантией при построении защищенной информационной системы.

Издательская деятельность

Корпоративный ежемесячный информационный бюллетень **«Jet Info»** — уникальное собрание актуальных материалов — издается регулярно с 1995 года.

С марта 1999 года бюллетень издается также в электронном виде.

Бюллетень рассчитан на руководителей высшего и среднего звеньев управления — руководителей IT-подразделений (отделов, департаментов), которые и являются основными подписчиками. Подписной индекс по каталогу — **32555**.

Специалистами компании опубликовано большое количество материалов, посвященных вопросам деятельности компании, во многих периодических компьютерных изданиях.

Контроль над корпоративной электронной почтой: система «Дозор-Джет»

С ростом популярности Интернета, электронная почта остается важнейшим средством коммуникаций. На ее долю приходится более половины всего сетевого трафика. Электронная почта имеет все необходимые качества для того, чтобы быть самым популярным средством связи: низкая стоимость, простота использования, большое количество пользователей. Удобство обмена информацией с помощью электронной почты сделали это средство коммуникации самым распространенным видом связи для большинства организаций.

Однако, наряду с многочисленными преимуществами, существует ряд рисков, связанных с использованием электронной почты, которые могут привести к значительному снижению эффективности работы организации, потере значимой информации.

Система мониторинга и архивирования почтовых сообщений (СМАП) «Дозор-Джет» представляет собой специализированное программное средство, позволяющее реализовать корпоративную политику использования электронной почты в части обеспечения информационной безопасности.

«Дозор-Джет» позволяет решить ряд проблем, связанных с неконтролируемым использованием электронной почты, таких как:

- Утечка конфиденциальной информации;
- Передача сообщений неприемлемого содержания;
- Передача потенциально опасных вложений, вирусов и вредоносных кодов;
- Передача неприемлемых вложений — большого размера, нежелательного формата и т.д.;
- Несанкционированные почтовые рассылки («спам»);
- Ошибочное направление писем;
- Потери рабочего времени, ресурсов или блокирование почтового сервиса.

Система «Дозор-Джет» осуществляет мониторинг и контроль всех входящих, исходящих и внутренних почтовых сообщений. Мониторинг включает в себя анализ заголовков и структуры сообщений и проверку на наличие в тексте сообщения или прикрепленных файлах разрешенных или запрещенных к использованию в почтовых сообщениях слов или последовательностей слов. Результатом мониторинга может стать, например, задержание подозрительных писем. «Дозор-Джет» позволяет задавать корпоративные правила обработки входящей и исходящей почты, в зависимости от тех или иных предопределенных событий, например:

- Запрет пересылки файлов формата EXE всем, кроме разработчиков программного обеспечения;
- Запрет пересылки картинок формата GIF и JPEG всем, кроме сотрудников рекламного отдела;
- Ограничение на объем и количество присоединенных файлов, направляемых отдельным адресатам;
- Автоматическое уведомление руководителя подразделения о письмах с определенными пометками или отвечающих поставленным условиям.

Использование гибкой системы фильтрации сообщений позволяет реализовать практически любую схему прохождения электронной почты. Например, возможна так называемая отложенная доставка почтового сообщения, когда решение о доставке конечному пользователю предпринимается только после дополнительного анализа Администратором безопасности и другими системами безопасности (проверка на наличие вирусов, контроль массовой рассылки сообщений рекламного характера, наличие неопознанных (закодированных) вложений и пр.).

Состав системы «Дозор-Джет»

Система «Дозор-Джет» представляет собой набор программных модулей, которые обеспечивают потоковый анализ SMTP-трафика почтовых сообщений как между локальной сетью компании и внешним миром, так и внутри локальной вычис-

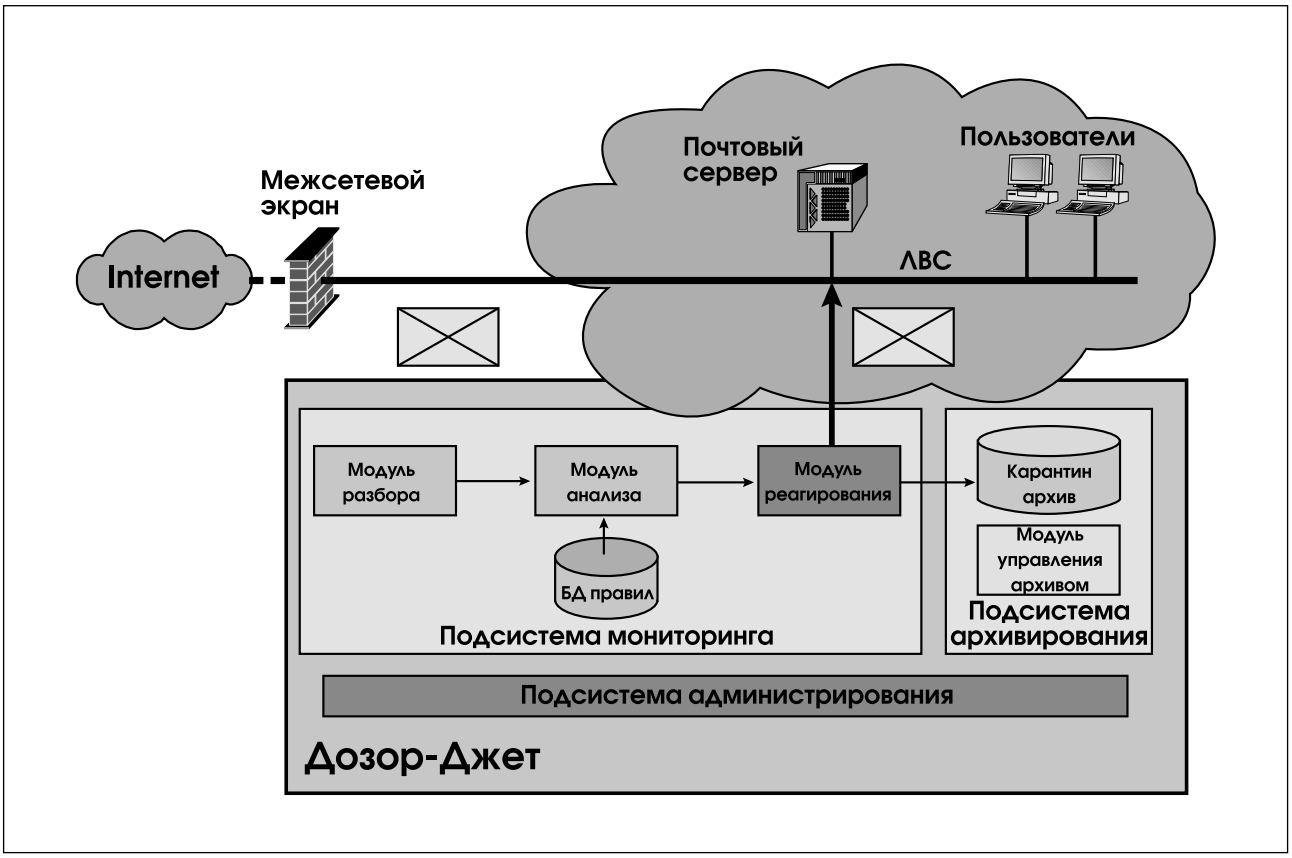

Рис. 1. Состав системы «Дозор-Джет»

лительной сети компании, а также ведение архива почтовых сообщений.

"Дозор-Джет" состоит из следующих основных подсистем:

- подсистемы мониторинга, включающей в свой состав три модуля - модуль разбора сообщений, модуль анализа и модуль реагирования;
- подсистемы архивирования;
- подсистемы администрирования.

Все почтовые сообщения, поступающие из внешней среды (Интернет) или из локальной сети компании, обрабатываются системой «Дозор-Джет». В процессе обработки система принимает решение о дальнейшей отправке сообщения адресату или о его задержке, архивировании сообщения, а также уведомлении Администратора безопасности о прохождении сообщения определенного типа. Вся почта, успешно прошедшая проверку системы, перенаправляется почтовому серверу для дальнейшей отправки по назначению.

Анализ содержимого почтовых сообщений

Все попадающие в «Дозор-Джет» почтовые сообщения проходят процедуру разбора на составляющие компоненты. При этом происходит разбор как заголовков сообщения (отправитель, получатель, скрытая копия, тело сообщения и пр.), так и всей его структуры, вне зависимости от количества уровней вложенности. Это позволяет анализировать сообщения, содержащие прикрепленные файлы, а также сообщения, которые были несколько раз перенаправлены корреспондентами.

Анализ разобранных сообщений включает:

- Определение характеристик сообщения — отправитель, получатель, дата, размер, структура;
- Определение характеристик вложений — имя, размер, тип, количество;
- Распознавание форматов вложений — сжатия/архивирования, документов, исполнимых файлов, графических, аудио- и видеофайлов;
- Анализ текста в заголовках сообщения, теме, теле письма и вложенных файлах.

Варианты реагирования по результатам проверок

При обнаружении соответствия почтовых сообщений заданным в правилах фильтрации критериям, система осуществляет одно или несколько из заранее предписанных действий:

- Отправка сообщения получателю;
- Отказ в передаче (блокировка сообщения);
- Задержка сообщения для последующего анализа;
- Помещение в карантинную зону;
- Регистрация сообщения;
- Архивирование сообщения;
- Проставление пометок;
- Отправка уведомления (оповещение администратора системы и др.) .

При этом обязательно осуществляется протоколирование всех производимых действий.

Архивирование сообщений и поиск по архиву

Архивирование почтовых сообщений позволяет хранить, учитывать и систематизировать сообщения и документы, передаваемые посредством корпоративной электронной почты. В архиве может осуществляться хранение либо регистрационной информации либо сообщения целиком.

Система «Дозор-Джет» предоставляет возможность как краткосрочного, так и долговременного хранения почтовых сообщений, удовлетворяющих определенным критериям. Кроме того, подотчетность и невозможность отказа от совершенных действий является немаловажным фактором повышения ответственности пользователей корпоративной почты за содержание передаваемой информации.

На каждое сообщение заводится учетная карточка, которая содержит всю идентификационную информацию сообщения и описание его структуры. В дальнейшем в учетную карточку попадает информация, связанная с жизненным циклом данного сообщения в системе (причина и сроки задержки, дальнейшие административные действия, время хранения в архиве и пр.). Для реализации модуля архивирования используется СУБД Oracle.

Система архивирования позволяет осуществлять просмотр сообщений в архиве и поиск по любым критериям, (в т.ч. контекстный поиск), выполнять различные действия с хранимыми сообщениями, предоставляет возможность получения статистики использования почтового сервиса.

Получение статистики

Статистическая обработка накопленной в системе «Дозор-Джет» информации предоставляет возможность анализа эффективности использования почтового сервиса компании: насколько активно ведется переписка с партнерами и клиентами, как часто пользователи передают по почте файлы большого размера или определенного типа — графические, аудио- или видео-файлы. Также появляется возможность анализа эффективности и качества работы отдельных подразделений компании: средние сроки обработки запросов клиентов, количество обращений, поступающих в подразделения компании и многое другое.

Администрирование системы

Обслуживание системы «Дозор-Джет» осуществляется Администратором безопасности, в задачи которого входит обеспечение надежного функционирования системы, настройка фильтров, управление подсистемой архивирования. В обязанности Администратора безопасности могут быть включены, кроме этого, регулярный контроль и анализ задержанных писем, осуществление поисковых запросов и реагирование на сообщения системы.

Разграничение доступа к компонентам системы

Доступ к элементам системы «Дозор-Джет» определяется на основе использования списков прав доступа для каждой категории объектов. Например, имеются списки для работы с условиями, с поисковыми запросами, с шаблонами уведомлений.

Существуют также списки прав на выполнение определенных функций администрирования.

Особенности системы

Использование открытых стандартов

В системе «Дозор-Джет» для ведения архива электронных сообщений используется СУБД Oracle, что позволяет, во-первых, использовать стандартные средства обработки, поиска и анализа накопленной информации, а, во-вторых, достаточно легко интегрировать базу почтовых сообщений с

уже существующими в компании системами с целью ее более широкого использования.

Применение в качестве пользовательского интерфейса Web-навигатора унифицирует рабочее место Администратора безопасности, что значительно упрощает как работу по настройке модулей системы, так и текущую работу Администратора безопасности.

Анализ русскоязычных текстов

В отличие от зарубежных аналогов «Дозор-Джет» осуществляет морфологический анализ русскоязычных текстов и поддерживает поиск последовательности символов (слов) как латиницы, так и кириллицы в кодировках Win-1251, DOS-866, ISO-8859.5, KOI-8, Mac.

Сертификация в Гостехкомиссии России

«Дозор-Джет» имеет сертификат Гостехкомиссии России № 465 от 14.06.01 на соответствие Техническим условиям и требованиям руководящего документа «Классификация средств защиты информации по уровню контроля недекларированных возможностей», что обеспечивает выполнение требований действующего законодательства в данной области.

Надежность и безопасность

Использование UNIX платформы (SPARC/ Solaris, HP-Unix, Linux) и современной промышленной СУБД (Oracle) для работы системы «Дозор-Джет» позволяет удовлетворить самым высоким требованиям по надежности, доступности и масштабируемости системы.

Размещение системы «Дозор-Джет»

Система «Дозор-Джет» размещается на выделенном сервере, располагаемом, как правило, в демилитаризованной зоне сети. Архив почтовых сообщений системы «Дозор-Джет» в случае большого количества почтовых адресов предпочтительно разместить на отдельном сервере.

Конкретная схема размещения и требования к аппаратной платформе для установки компонентов системы «Дозор-Джет» разрабатывается на основе результатов обследования почтовой системы и сбора информации о реализации почтового сервиса и почтового трафика.

Во время подготовки материала для этого номера выпущена новая версия системы мониторинга и архивирования почтовых сообщений Дозор/LX, которая функционирует под управлением ОС Linux на процессорах с архитектурой Intel.

Для хранения архива писем данная версия использует свободно распространяемую СУБД PostgreSQL, которая является стандартом "де-факто" для операционной системы Linux.

Эта версия системы обладает той же функциональностью, что и полная версия (платформы SPARC-Solaris и HP-UX), за исключением функции полнотекстового поиска в архиве писем.

Новая версия прошла тестирование на дистрибутивах Red Hat Linux версий 7.1 и 7.2, а также на Mandrake Linux версии 8.1.

Система Дозор/LX обладает следующими достоинствами: простота установки системы, отсутствие необходимости в дорогостоящей СУБД, возможность установки на персональный компьютер.

Однако Дозор/LX не используется для обработки больших архивов (более 10000 писем) или больших потоков (более 1000 писем в час) и позиционируется как «облегченная версия».

«Облегченная версия» может быть модернизирована до полнофункциональной версии системы, работающей с СУБД Oracle с сохранением накопленного архива.

На основе версии Дозор/LX разработана демонстрационная версия Дозора, предназначенная для знакомства с рабочей системой.

Z-2 – универсальный межсетевой экран высшего уровня защиты

Практически все современные корпоративные информационные системы используют сети общего пользования для получения доступа к внешним ресурсам, предоставления собственных ресурсов внешним пользователям, а зачастую используют публичные сети как средство организации информационного взаимодействия территориально-распределенных участков корпоративной сети.

В такой ситуации с одной стороны возникает необходимость обеспечения доступности части корпоративных информационных ресурсов извне, а также ресурсов внешних открытых сетей для внутренних пользователей Компании, с другой — остро встает проблема контроля информационного взаимодействия с внешним миром и обеспечения защиты корпоративной информационной системы от угроз информационной безопасности извне.

Для разграничения доступа к ресурсам и контроля информационных потоков между защищаемой сетью Компании и внешними сетями, а также между сегментами корпоративной сети, необходимо использовать специальные средства защиты — **межсетевые экраны**.

Межсетевой экран Z-2

Межсетевой экран (МЭ) Z-2 предназначен для защиты внутреннего информационного пространства корпоративных информационных систем (в том числе территориально-распределенных) при информационном взаимодействии с внешним миром в соответствии с принятой в Компании политикой информационной безопасности.

МЭ Z-2 устанавливается на границе между защищаемой сетью Компании и внешними «открытыми» сетями либо между сегментами защищаемой сети (разного уровня конфиденциальности или служащих для решения различных задач и потому требующих изоляции) и осуществляет контроль входящих/исходящих информационных потоков на основе заданных правил управления доступом.

Типовая схема подключения Z-2 представлена на Рис. 2.

Основные функциональные возможности

Основные возможности МЭ Z-2 по обеспечению информационной безопасности корпоративной информационной системы включают:

- Контроль входящих/исходящих информационных потоков на нескольких уровнях модели информационного обмена OSI/ISO;
- Идентификацию и аутентификацию пользователей с защитой от прослушивания сетевого трафика;
- Трансляцию сетевых адресов и сокрытие структуры защищаемой сети;
- Обеспечение доступности сетевых сервисов;
- Регистрацию запросов на доступ к ресурсам и результатов их выполнения;
- Обнаружение и реагирование на нарушения политики информационной безопасности.

Состав МЭ Z-2

МЭ Z-2 представляет собой программный комплекс, функционирующий под управлением операционной системы Solaris компании Sun Microsystems на аппаратной платформе SPARC или Intel, что позволяет подбирать оптимальную конфигурацию по производительности и цене.

В состав комплекса МЭ Z-2 входят следующие программные компоненты (Рис. 3):

- Фильтр сетевых пакетов;
- Шлюзы прикладного уровня;
- Средства идентификации и аутентификации пользователей;
- Средства регистрации и учета запрашиваемых сервисов;
- Средства оповещения и сигнализации о случаях нарушения правил фильтрации;
- Средства динамического контроля целостности программной и информационной среды МЭ;
- Средства управления программным комплексом МЭ.

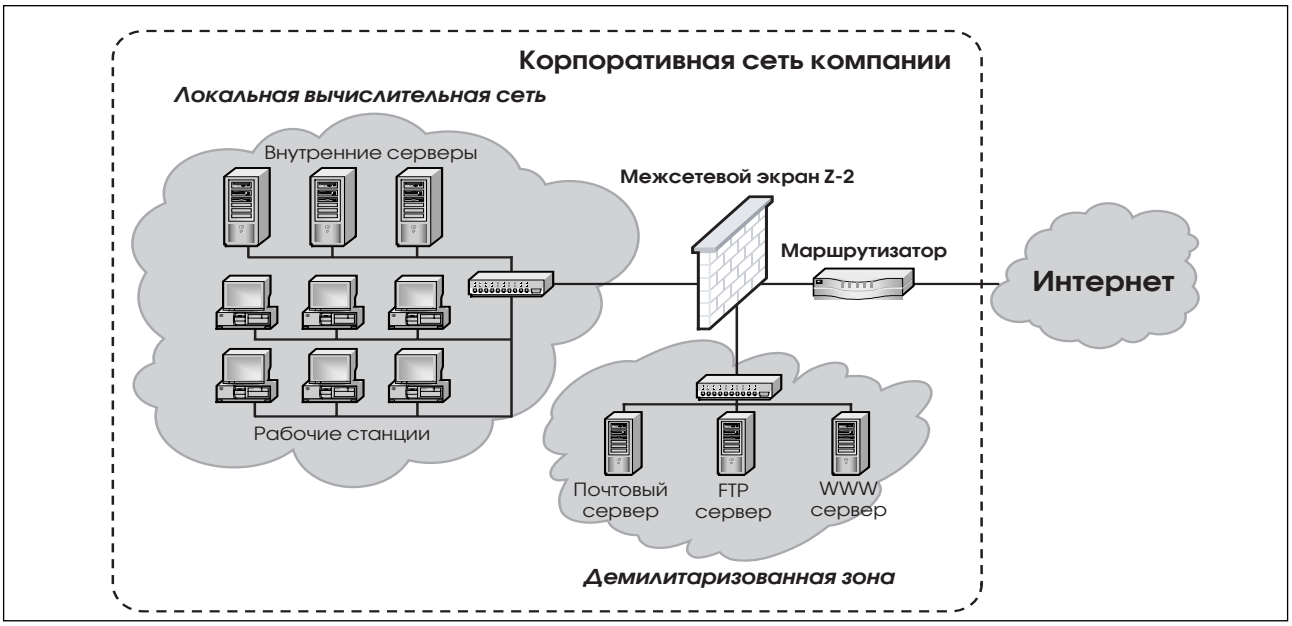

Рис. 2. Схема подключения межсетевого экрана Z-2

Функционирование МЭ Z-2

Фильтрация информационных потоков

Разграничение доступа и контроль входящих/исходящих информационных потоков осуществляется путем фильтрации данных, т.е. их анализа по совокупности критериев и принятия решения об их распространении в (из) защищаемой сети или сегмента.

Фильтрация производится на основе правил, задаваемых администратором, в соответствии с принятой в Компании политикой информационной безопасности.

На сетевом и транспортном уровнях фильтрация соединений осуществляется пакетным фильтром на основе транспортных адресов отправителя и получателя с сохранением состояния сессии. При этом осуществляется контроль доступа в соответствии с установленными правилами разграничения доступа к сетевым ресурсам и сервисам.

Фильтрация на уровне приложений осуществляется набором фильтров прикладного уровня, каждый из которых отвечает за фильтрацию информационного обмена по одному отдельному протоколу и между одним определенным типом приложений. Фильтрация осуществляется по дате и времени запроса, IP-адресам источников запроса, типу протокола, отдельным командам и другим атрибутам, характерным для данного протокола.

МЭ Z-2 включает шлюзы прикладного уровня для протоколов HTTP, FTP, SMTP, TELNET и SNMP.

МЭ также включает в себя прикладные шлюзы общего назначения, которые являются нейтральными по отношению к содержимому протокола и могут быть использованы для различных типов приложений, применяющих в качестве транспорта протоколы TCP и UDP. Универсальные шлюзы Generic TCP и Generic UDP обеспечивают фильтрацию по сетевым адресам и портам источника и получателя запроса и протоколирование соединений.

Шлюзы приложений могут также производить аутентификацию запроса на установление соединения на сервере аутентификации и авторизации.

МЭ может также проводить фильтрацию запросов к прикладным сервисам путем создания шлюзов приложений на уровне ядра ОС, для чего в его состав входят шлюзы приложений на уровне ядра ОС. Основная их задача — пропустить протокол, который они обслуживают, через МЭ на уровне пакетного фильтра, что позволяет существенно повысить быстродействие МЭ. В состав МЭ Z-2 входят шлюзы приложений на уровне ядра для протоколов FTP, Rlogin/Rsh и RealAudio (протокол PNA).

Разграничение доступа к шлюзам приложений производится с помощью списков управления доступом (Access Control Lists) на основании заданного диапазона IP-адресов и портов разрешенных источников запросов.

Верификация правил фильтрации

Для проверки списка правил фильтрации на избыточность и непротиворечивость МЭ Z-2 включает в состав средства проверки правил по адресам, портам и протоколам источника или точки назначения пакета.

Трансляция сетевых адресов

Помимо фильтрации информационных потоков МЭ Z-2 позволяет проводить трансляцию сетевых

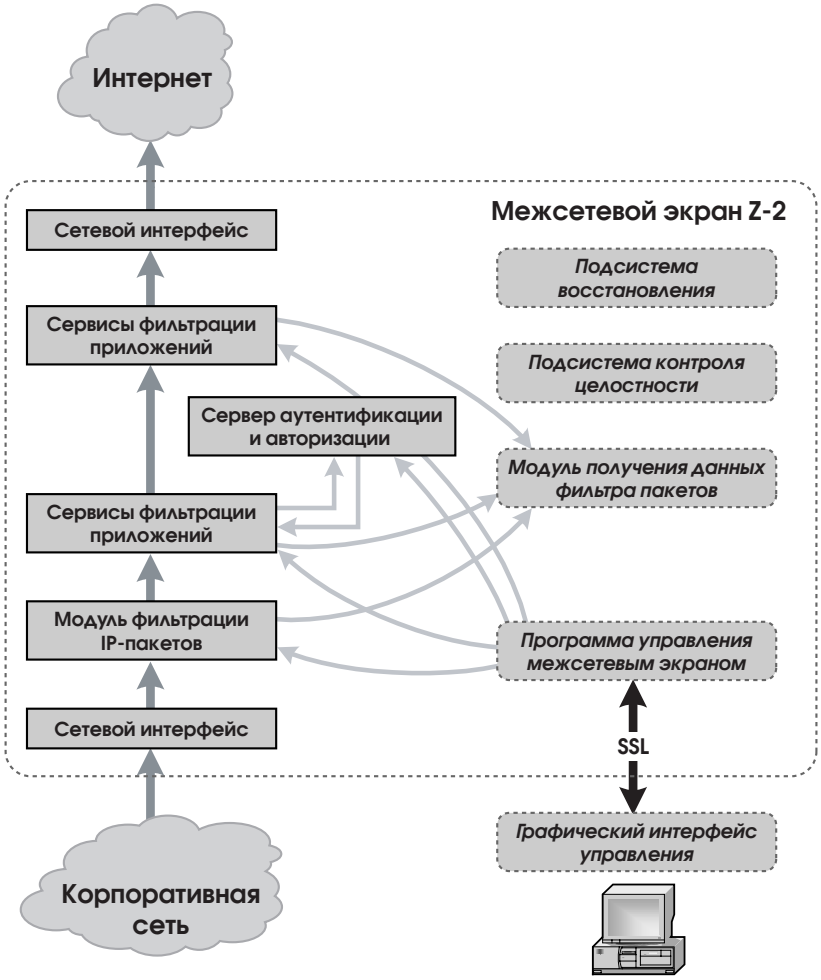

Рис 3. Схема меежсетевого экрана Z-2

адресов (Network Address Translation, NAT) на основании заданного набора правил. Это позволяет скрыть структуру внутренней сети от внешних субъектов и расширить возможность использования произвольных внутренних IP-адресов.

Обеспечение доступности ресурсов

Для предотвращения угроз доступности сервисов внешнего информационного обмена МЭ Z-2 осуществляет управление информационными потоками. В качестве атрибутов безопасности выступает количество одновременно обрабатываемых запросов на предоставление сервисов в зависимости от приоритета сервиса, определенного политикой безопасности компании.

Идентификация и аутентификация пользователей МЭ Z-2

МЭ Z-2 включает две схемы аутентификации пользователей — по простому паролю и паролю временного действия. Использование временных паролей позволяет обеспечить защиту от пассивных атак, таких как прослушивание сетевого трафика и перехват идентификаторов и паролей пользователей, т.к. информация, которая потенциально может быть использована для попыток получения несанкционированного доступа, не передается по сети, а используемые для аутентификации пароли не хранятся на каком-либо компьютере.

Аутентификация и проверка прав доступа пользователей при обращении к прикладным сервисам реализуется с помощью сервера аутентификации и авторизации, к которому обращаются шлюзы приложений МЭ Z-2. Доступ к запрашиваемому сервису может быть разрешен только в случае успешной проверки подлинности на сервере аутентификации.

Схема аутентификации каждого конкретного пользователя и иная необходимая информация хранится в базе данных пользователей на сервере аутентификации и авторизации МЭ Z-2.

Благодаря использованию встраиваемых модулей аутентификации (PAM-модулей), МЭ Z-2 до-

пускает подключение других схем аутентификации без изменения программного кода сервера аутентификации и авторизации межсетевого экрана.

Доступ к серверу аутентификации разрешен только шлюзам приложений в соответствии со списками управления доступом на основании IP-адресов и портов разрешенных источников запросов на аутентификацию.

Настройка и администрирование МЭ Z-2

Средства управления

Управление компонентами одного или нескольких межсетевых экранов Z-2 осуществляется централизованно с рабочего места Администратора на основе технологии «клиент-сервер», где в качестве сервера выступает программа управления, запускаемая на МЭ Z-2, а в качестве клиента — графический интерфейс управления МЭ Z-2, установленный на рабочем месте Администратора.

Графический интерфейс и программа управления написаны на языке Java, что обеспечивает многоплатформенность интерфейса управления МЭ.

Графический интерфейс управления позволяет:

- Производить настройку фильтра сетевых пакетов МЭ;
- Проводить настройки сервисов фильтрации, осуществлять их запуск и остановку, а также передачу статуса их работы;
- Редактировать базы данных пользователей сервера аутентификации;
- Производить полный или выборочный просмотр системных журналов в реальном времени;
- Производить настройку системного планировщика задач (cron).

Разграничение доступа и защита функций администрирования МЭ

Доступ к функциям конфигурирования и администрирования МЭ Z-2 предоставляется только уполномоченному Администратору, который должен пройти процедуру проверки подлинности.

Кроме того, осуществляется защита данных и команд управления, передаваемых между МЭ Z-2 и рабочим местом Администратора.

В качестве аутентификационной информации для задач администрирования МЭ Z-2 используется сертификат открытого ключа X.509 и одноразовый пароль S/key. Конфиденциальность и целостность информации управления обеспечивается средствами протокола SSLv3.

Обеспечение надежности функционирования МЭ

Надежность работы МЭ Z-2 обеспечивается комплексом мер по внутреннему аудиту, регистрацией событий и своевременным оповещением Администратора МЭ о нарушениях политики безопасности, а также средствами контроля целостности компонентов, резервного копирования и восстановления МЭ в случае сбоев.

Регистрация событий

МЭ Z-2 осуществляет регистрацию событий, связанных с его функционированием, включая все виды входящих/исходящих запросов и процессов их обработки, изменения конфигурации МЭ и прочие административные действия, события загрузки и останова МЭ, регистрации и выхода из системы Администратора и других пользователей. При этом обеспечивается защита хранимых данных аудита от несанкционированного удаления.

Полный или выборочный просмотр протоколов регистрации осуществляется только уполномоченным Администратором.

МЭ Z-2 включает также средства анализа регистрационной информации и генерации отчетов на ее основе.

Оповещение Администратора МЭ о попытках НСД

Для обеспечения оперативного реагирования на нарушения политики информационной безопасности компании при обнаружении событий, отвечающих определенным критериям (например, интерпретируемых как попытки НСД), МЭ Z-2 осуществляет одно из заданных действий, например:

- локальное оповещение Администратора, осуществляющего мониторинг работы МЭ;
- удаленное оповещение — посылка Администратору сообщения по электронной почте;
- другие настраиваемые Администратором действия.

Контроль целостности МЭ Z-2

МЭ Z-2 обеспечивает динамический контроль целостности своей программной части (исполняемых модулей и компонентов операционной системы) и информационной среды (конфигурационных файлов, баз данных пользователей и аутентификационной информации).

Возможность проверки целостности компонентов МЭ Z-2 предоставляется только уполномоченному Администратору.

Состав программного обеспечения	Серия «С»	Серия «В»	Серия «А»
Модуль фильтрации IP-пакетов на уровне ядра ОС	+	+	+
Минимальный набор шлюзов приложений (HTTP, FTP, SMTP)	+	+	+
Расширенный набор шлюзов приложений (TELNET, SNMP, Generic TCP/UDP)	-	+	+
Набор шлюзов приложений на уровне ядра ОС	+	+	+
Сервер аутентификации и авторизации	+	+	+
Подсистема контроля целостности	+	+	+
Графический интерфейс Администратора	+	+	+
Подсистема мониторинга и регистрации событий	+	+	+
Средства обеспечения отказоустойчивости	-	-	+
Подсистема биометрической аутентификации Администратора	-	-	+
Класс защищенности в соответствии с РД Гостехкомиссии[1]	3 класс	2 класс	1 класс

Табл. 1. Варианты поставки МЭ Z-2

[1] МЭ Z-2 серии «С» получил сертификат Гостехкомиссии РФ № 555 от 27.12.2001 г. Сертификация МЭ Z-2 серии «В» и «А» в Гостехкомиссии РФ проводится в настоящее время.

Резервное копирование и восстановление МЭ

При выходе из строя компонентов фильтрации МЭ в результате сбоя или отказа происходит приостановка связи по соответствующему протоколу и прекращение доступа к защищаемым ресурсам. Тем самым реализован принцип невозможности перехода в небезопасное состояние защищаемой информационной системы.

Для быстрого возобновления выполнения функций защиты корпоративной сети в случае сбоев и отказов программно-аппаратного обеспечения МЭ Z-2 предусмотрена возможность резервного копирования компонентов самого МЭ (конфигурационных файлов, файлов протоколирования, баз данных пользователей), файловой системы (средствами операционной системы), а также оперативного восстановления работоспособности МЭ.

МЭ Z-2 также выполняет набор операций самотестирования при запуске, восстановлении после сбоев и при запросах уполномоченного Администратора.

Основные особенности МЭ Z-2

Отличительными особенностями МЭ Z-2 являются:

- Гибкая система контроля информационных потоков на нескольких уровнях сетевых протоколов;
- Возможность функционирования шлюзов в специальном режиме работы на быстрых каналах связи;
- Трансляция адресов и сокрытие структуры защищаемой сети;
- Наличие встроенного расширяемого сервера аутентификации и авторизации;
- Возможность централизованного управления корпоративной политикой безопасности;
- Мультиплатформенный графический интерфейс управления произвольным количеством МЭ;
- Возможность аутентификации Администратора МЭ на основании биометрических характеристик;
- Контроль действий Администратора;
- Возможность мониторинга и автоматического реагирования на нарушения политики безопасности;
- Высокая степень собственной защищенности;
- Возможность интеграции с антивирусными решениями и системами блокировки "спам";
- Гибкий баланс уровня защиты корпоративной сети и производительности.

Варианты поставки МЭ Z-2

В зависимости от особенностей защищаемой информационной системы компании МЭ Z-2 может быть поставлен в трех различных вариантах комплектации (Табл. 1).

Заключение

Использование МЭ Z-2 для защиты корпоративной информационной системы позволит обеспечить высокий уровень безопасности внутреннего информационного пространства компании и возможность детального разграничения доступа к ресурсам и сервисам на основании корпоративной политики информационной безопасности. Развитые средства управления МЭ Z-2 делают реальной и практичной защиту сети любого назначения и масштаба, позволяют наращивать механизмы безопасности параллельно с развитием корпоративной информационной системы.

Комплекс кодирования межсетевых потоков «Тропа-Джет»

Одной из важнейших задач обеспечения информационной безопасности является защита потоков корпоративных данных, передаваемых по каналам общего пользования, в том числе и через Internet. Перспективным методом надежной защиты информации является метод кодирования данных.

Для решения этой задачи необходимо осуществить кодирование информации на выходе из локальной сети и декодирование поступающих в нее данных. Эти функции реализуются специальными программными или программно-аппаратными средствами. Если защита сегмента корпоративной сети уже обеспечена межсетевым экраном, естественно возложить на него также выполнение функций кодирования и декодирования.

Для реализации возможностей кодирования/декодирования должно быть выполнено предварительное (начальное) распределение ключей. Современные технологии предлагают для этого целый ряд методов. После распределения ключей появляется возможность осуществления процесса выработки совместных секретных ключей, обслуживающих сеанс общения абонентов.

В результате кодирования весь обмен данными между территориально-удаленными локальными сетями является защищенным и для пользователей выглядит как обмен внутри одной локальной сети, при этом от пользователей не требуется применение каких-либо дополнительных защитных средств.

Комплекс кодирования межсетевых потоков (ККМП) «Тропа-Джет»

Программный комплекс кодирования межсетевых потоков (ККМП) «Тропа-Джет» реализует функции кодирования межсетевых информационных потоков в сетях передачи данных протокола TCP/IP для обеспечения обмена информацией между территориально-удаленными локальными сетями. Это обеспечивается посредством организации виртуальных защищенных сетей (Virtual Private Networks — VPN).

Комплекс «Тропа-Джет» выполняет следующие функции:

- **Кодирование межсетевых потоков**
  Функции кодирования межсетевых информационных потоков в открытых сетях передачи данных выполняются путем организации VPN. Каждая сеть в составе VPN защищена своим кодирующим модулем, устанавливаемым в точке ее соединения с внешними сетями. Защищаемая информация кодируется на передающем модуле и декодируется на принимающем, т.е. передается в открытом виде в пределах локальных сетей и в кодированном — за их пределами.
  Кодированный трафик передается по протоколу IPsec.
- **Создание контура безопасности**
  ККМП «Тропа-Джет» позволяет сформировать контур безопасности, объединяющий IP-адреса всех абонентов, имеющих доступ в виртуальную защищенную сеть. Абонентами VPN могут быть целые сети, подсети и отдельные рабочие станции. Кроме того, кодирующий модуль может быть установлен на отдельную рабочую станцию.
- **Выборочное кодирование трафика**
  Формирование контура безопасности служит для разделения трафика на кодируемый и некодируемый потоки. Кодирующий модуль ККМП «Тропа-Джет» производит выделение пакетов, которые необходимо кодировать, на основании IP-адресов отправителя пакета и получателя пакета и, кроме того, проверки интерфейса, через который проходит пакет.
- **Управление ключевой системой**
  В ККМП «Тропа-Джет» реализована несимметричная ключевая система, когда потенциальные участники обмена данными используют пары долговременных секретного и открытого ключей кодирования. Кодирование осуществляется на основе сеансовых ключей, автоматически формируемых при помощи долговременных ключей и имеющих ограниченное время жизни. Комплекс «Тропа-Джет» осуществляет все необходимые действия по управлению ключами: генерацию и распределение долговременных ключей, выработку сеансовых ключей абонентов, сертифика-

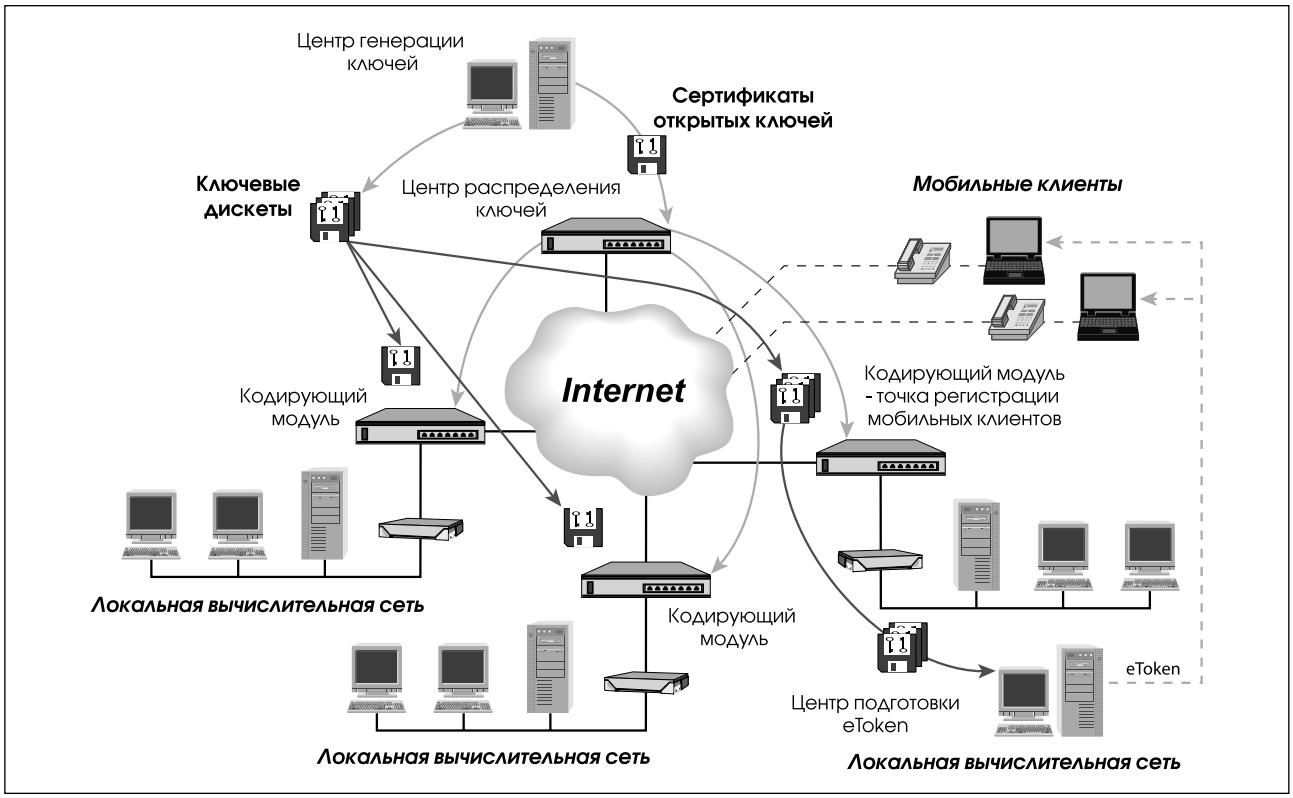

Рис. 4. Архитектура Комплекса кодирования межсетевых потоков «Тропа-Джет»

цию открытых ключей в доверенном центре, плановую и внештатную смену ключей кодирования.

- **Регистрация событий, мониторинг и управление межсетевыми потоками**
  ККМП «Тропа-Джет» осуществляет сбор и хранение статистической и служебной информации обо всех штатных и нештатных событиях, возникающих при аутентификации узлов, передаче кодированной информации, ограничении доступа абонентов ЛВС. Средства мониторинга проводят сбор и анализ протоколов регистрации от всех модулей комплекса по кодированному каналу.
- **Защита соединений с мобильными клиентами**
  В состав виртуальной защищенной сети могут входить мобильные пользователи — удаленные компьютеры, подключаемые по выделенным или коммутируемым каналам связи. Основным отличием Мобильного клиента является динамически-назначаемый IP-адрес. Носителем ключевой информации для них является электронный ключ eToken.

Состав Комплекса «Тропа-Джет»

Комплекс «Тропа-Джет» состоит из следующих компонентов:

1. Набор шлюзов кодирования;
2. Центр генерации ключей;
3. Центр распределения ключей;
4. Центр регистрации мобильных клиентов;
5. Центр подготовки электронных ключей мобильных клиентов;
6. Мобильный клиент;
7. Центр мониторинга;
8. Программа контроля целосности.

Архитектура Комплекса кодирования межсетевых потоков «Тропа-Джет» приведена на рис. 4.

Шлюз с кодирующим/декодирующим модулем

Шлюз является основным модулем комплекса, выполняющим функции маршрутизации, фильтрации и кодирования пакетов. Каждый Шлюз предназначен для закрытия определенной группы локальных сетей. На компьютере-шлюзе устанавливается ядерный модуль с функциями кодирования и декодирования и запускается программа аутентификации. Функциями шлюза являются:

- Фильтрация трафика (деление на кодируемый/некодируемый потоки);
- Кодирование трафика (кодируемый поток);
- Аутентификация с другими Шлюзами;
- Регистрация событий в Центре мониторинга;
- Обеспечение собственной защиты.

Центр распределения ключей

Центр распределения ключей осуществляет управление контуром безопасности, а также выполняет следующие функции:

- Получение со сменного носителя открытых ключей Шлюзов;
- Выдача любому Шлюзу открытых ключей любых других Шлюзов и информации о соответствующих сегментах структуры сети;
- Рассылка Шлюзам сообщений об изменениях структуры закрытой сети;
- Выработка и выполнение процедуры смены сеансовых ключей;
- Хранение информации о структуре сети.

Центр реализован в виде программного комплекса, выполняющего функции хранения и выдачи открытых ключей кодирования по сетевому запросу от модулей кодирования. Центр распределения ключей может быть установлен либо на отдельном (выделенном) компьютере, либо совместно с одним из Шлюзов кодирования.

Центр генерации ключей

Данный модуль служит для генерации пар комплементарных ключей, а также является репозитарием всех известных системе ключей. В функции Центра генерации ключей входит:

- генерация пар открытого и секретного ключей Кодирующих модулей;
- генерация пары ключей для сертификации (эталонного заверения) открытых ключей Кодирующих модулей;
- генерация сертификатов открытых ключей, подписанных секретным ключом сертификации;
- помещение подписанных сертификатов открытых ключей на сменные носители;
- хранение эталонных копий сертифицированных открытых ключей в архиве.

Центр генерации ключей — программа, выполняющаяся на изолированном автоматизированном рабочем месте.

Центр регистрации ключей

Центр регистрации ключей служит репозитарием всех известных системе ключей. В его функции входит:

- Ввод со сменного носителя открытого ключа;
- Ввод со сменного носителя закрытого ключа Администратора безопасности;
- Подпись нового ключа ключом Администратора безопасности;
- Помещение подписанного открытого ключа в архив долговременного хранения и на сменный носитель;
- Хранение эталонных копий сертифицированных (зарегистрированных) открытых ключей.

Центр регистрации ключей выполнен в виде программы, выполняющейся на изолированном автоматизированном рабочем месте и предназначенной для сертификации (эталонного заверения) открытых ключей.

Центр регистрации мобильных клиентов и Мобильный клиент

Для обеспечения доступа к защищаемым корпоративным данным мобильных абонентов, не подключенных к защищаемым локальным сетям, используется Центр регистрации мобильных клиентов и программное обеспечение мобильного клиента комплекса «Тропа-Джет».

Центр регистрации мобильных клиентов представляет собой специальный кодирующий модуль для подключения произвольного количества мобильных клиентов.

Мобильный клиент представляет собой программный модуль, работающий под управлением ОС Windows 98/2000 и использующий аппаратные ключи для аутентификации абонента в VPN.

Центр мониторинга

Центр мониторинга представляет собой сетевое автоматизированное рабочее место с установленным на нем набором программ, осуществляющих сбор и анализ протоколов, поступающих от всех модулей комплекса.

Программа контроля целостности

Комплекс «Тропа-Джет» включает в себя средства формирования и проверки контрольных сумм файлов. Эти средства реализованы в виде Программы контроля целостности, которая предназначена для определения и уведомления системного Администратора об изменении, добавлении и удалении файлов.

Администрирование комплекса

Настройка и администрирование компонентов комплекса «Тропа-Джет» осуществляется централизованно с рабочего места Администратора безопасности с помощью графического интерфейса или командной строки. Удаленное управление осуществляется по защищенному каналу.

Комплекс обеспечивает аутентификацию Администраторов и разграничение доступа к функциям администрирования.

Основные особенности комплекса

Основными особенностями ККМП «Тропа-Джет» являются:

- Полнофункциональная схема управления ключами, позволяющая осуществлять динамическое

распределение ключей с использованием доверенного центра сертификации, проверку подлинности ключевой информации и оповещение систем кодирования о компрометации ключей;
- Высокая надежность функционирования, обеспечиваемая средствами контроля целостности, протоколирования и аудита, устойчивости к сбоям и восстановления в случае сбоев и отказов;
- Прозрачность кодирования передаваемых данных для абонентов и используемого ими программного обеспечения;
- Высокая производительность (работа в сети 100 Мбит/с без существенного влияния на пропускную способность);
- Обеспечение требуемого качества сервиса (QoS) и поддержка работы с сервисами, предъявляющими высокие требования к величинам временных задержек (IP-телефония, видеоконференцсвязь);
- Различные варианты выбора платформ — функционирование под ОС Solaris на аппаратной платформе SPARC или Intel;
- Возможность использования в комплексе с межсетевыми экранами, антивирусными решениями и средствами контекстного анализа;
- Использование открытых стандартов — протокол туннелирования сетевых пакетов соответствует стандартам IETF IPsec.

Сертификация комплекса

ККМП "Тропа-Джет" имеет Сертификат N 00039743 от 22.12.1999 г. на соответствие требованиям ГОСТ Р ИСО/МЭК 9126-93, ГОСТ Р ИСО/МЭК ТО 9294-93 и Сертификат Гостехкомиссии N 466 от 14.06.2001 г. на соответствие Техническим условиям (создание защищенного информационного обмена между разнесенными локальными сетями) и отсутствие недекларированных возможностей.

Криптографическое ядро комплекса в настоящее время проходит сертификацию ФАПСИ на соответствие ГОСТ Р34.10-94 , ГОСТ Р34.11-94, ГОСТ 28147-89 (ожидается сертификат класса КС1 в июне 2002 г.).

НОВОСТИ КОМПАНИИ

СЕРВИСНЫЙ ЦЕНТР КОМПАНИИ «ИНФОСИСТЕМЫ ДЖЕТ» ПРОШЕЛ СЕРТИФИКАЦИЮ И ПОЛУЧИЛ НАИВЫСШИЙ ПАРТНЕРСКИЙ СТАТУС SUN MICROSYSTEMS В ОБЛАСТИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ

В апреле 2002 года Сервисный Центр компании «Инфосистемы Джет» получил официальное подтверждение от Sun Microsystems об успешном прохождении процедуры сертификации и присвоении наивысшего, на текущий момент, партнерского статуса в области технической поддержки – Sun Service Manager.

Согласно новой партнерской политике, объявленной компанией Sun Microsystems, с 1 марта 2002 года авторизованную техническую поддержку на территории России могут осуществлять только Сервисные Центры, квалификация и качество работы которых полностью соответствует общепринятым международным стандартам, что должно быть подтверждено специально разработанной процедурой сертификации.

«Наш Сервисный Центр, осуществляющий высокоуровневую техническую поддержку сложных информационных систем, еще раз подтвердил высокое качество своей работы успешным прохождением сертификации специалистов и собственной диспетчерской службы, – сказал руководитель Сервисного Центра компании «Инфосистемы Джет» Максим Папин. Однако, мы не собираемся останавливаться на достигнутом. Только постоянно совершенствуя свой профессиональный уровень, предлагая более разнообразные по содержанию и высокие по качеству исполнения услуги, можно завоевать полное доверие заказчиков. А это и является основным критерием успеха в нашей работе».

Сервисный Центр компании «Инфосистемы Джет» образован в 1994 году. За время своего существования он стал одним из крупнейших в России предприятий по комплексному сервисному обслуживанию сложных информационных систем.

Сегодня на постоянной технической поддержке в Сервисном Центре находятся более 100 государственных и коммерческих организаций, расположенных как по всей территории России, так и в странах СНГ. В число клиентов Сервисного Центра входят Центральный банк Российской Федерации, компании «Газпром», «Вымпелком», «Глобал Один», «Голден Лайн», Гута Банк, СОНИ СНГ, Тенгизшевройл.

Ключевыми элементами программ обслуживания Сервисного Центра являются услуги профилактического и консалтингового характера, позволяющие устранять причины потенциальных сбоев до возникновения серьезных аварий в системе и повышать общую надежность обслуживаемых систем.

Областью компетенции Сервисного Центра являются UNIX-системы (Sun Microsystems, Hewlett-Packard), сетевое оборудование (Nortel Networks, Cisco Systems), системы управления базами данных (Oracle, Informix), специализированное управляющее программное обеспечение (Veritas Software, Legato Systems, Hewlett-Packard), решения в области информационной безопасности и банковские SWIFT-системы.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555