Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 12 (139)/2004

Компания «Инфосистемы Джет»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Компания «Инфосистемы Джет»

Компания «Инфосистемы Джет» — системный интегратор и поставщик ключевых компонентов информационной инфраструктуры для крупных организаций и предприятий.

О Компании

Компания «Инфосистемы Джет» работает на российском рынке с 1991 года, работы в области информационной безопасности ведет с 1994 года.

За это время Компанией успешно реализовано более 300 проектов по защите информации в федеральных и муниципальных структурах, банках и финансовых учреждениях, крупных торговых и промышленных предприятиях. 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.

Основные направления деятельности

Основными направлениями деятельности Компании являются:

- высоконадежные вычислительные комплексы;
- системы и сети хранения данных;
- корпоративные сети и сети операторов связи;
- инженерные подсистемы ВЦ;
- системы управления информационными ресурсами;
- решения по информационнной безопасности;
- интеграционные прикладные решения и программные разработки;
- техническая поддержка и сервисное обслуживание.

По этим направлениям Компания осуществляет разработку концепции и архитектуры информационных систем, системное проектирование, внедрение и интеграцию систем, техническую поддержку и эксплуатацию, а также аудит и оптимизацию информационных ресурсов корпоративных заказчиков.

Компания обладает комплектом лицензий, дающим право работать в заявленных областях.

Информационная безопасность – одно из основных направлений деятельности Компании

Центр информационной безопасности компании «Инфосистемы Джет» объединяет более 50 высококвалифицированных инженеров и технических специалистов и выполняет полный комплекс работ по защите информационных систем для крупных государственных и коммерческих организаций.

Решения по защите информационных систем

Доступ к информационным ресурсам открытых сетей и информационный обмен с подразделениями компании, клиентами и партнерами с использованием Интернет является неотъемлемой частью бизнес-процессов любой компании.

Однако подключение корпоративной сети к Интернет и другим общедоступным сетям приводит к возникновению угроз информационной безопасности организации, таких как:

- Несанкционированный доступ (НСД) к информационным ресурсам компании (базам данных, внутренним корпоративным Web-

серверам, файловым хранилищам) со стороны внешних сетей;
- Неконтролируемый доступ законных пользователей (удаленных подразделений компании, клиентов) к ресурсам корпоративной сети;
- Неконтролируемые обращения пользователей информационной системы к ресурсам общедоступных сетей (Интернет);
- Нарушение конфиденциальности и целостности информации, передаваемой между объектами корпоративной сети (перехват, несанкционированное ознакомление, распространение, модификация, подделка, разрушение);
- Утечка конфиденциальной информации, хранимой и обрабатываемой в корпоративной сети, через сервисы внешнего обмена (непреднамеренно либо с умыслом);
- Использование неконтролируемых сетевых протоколов для осуществления атак и организации скрытых каналов утечки информации;
- Проникновение потенциально опасных объектов, вирусов и вредоносных кодов; удаленный запуск вредоносных программ;
- Неделовой трафик из-за недисциплинированности пользователей, несанкционированных почтовых рассылок (спам).

При подключении корпоративной информационной системы к открытым сетям необходимо обеспечить:
- Защиту внутренних ресурсов (баз данных, внутренних Web-серверов, файловых хранилищ) от несанкционированного доступа и атак из внешних сетей;
- Контроль использования ресурсов внешних сетей и сервисов информационного обмена;
- Защиту информации, передаваемой по открытым каналам, от перехвата, подмены и искажения;
- Противодействие проникновению вирусов и вредоносных кодов в корпоративную сеть;
- Защиту от утечки конфиденциальной информации, в том числе за счет организации скрытых каналов;
- Мониторинг и контроль защищенности информационной системы;
- Оперативное реагирование на нарушения защиты в реальном времени;
- Регистрацию и анализ событий безопасности;
- Централизованное управление политикой безопасности периметра.

Центр информационной безопасности оказывает следующие услуги:

- Аудит безопасности информационных систем и анализ рисков;
- Разработка организационных документов по информационной безопасности;
- Проектирование и внедрение комплексных систем защиты информации на основе продуктов ведущих производителей и уникальных собственных разработок;
- Аттестация автоматизированных систем и сертификационные испытания средств защиты;
- Техническая поддержка и сервисное обслуживание средств и систем защиты информации;
- Аутсорсинг средств и систем защиты;
- Мониторинг и контроль защищенности корпоративных информационных систем;
- Консультации специалистов по информационной безопасности.

Эти задачи решает система защиты периметра, включающая в свой состав межсетевые экраны, средства создания виртуальных защищенных сетей (VPN), средства контроля содержимого трафика электронной почты, средства обнаружения атак и контроля защищенности периметра, антивирусные системы и другие.

Для создания полнофункциональной системы защиты Центром информационной безопасности компании «Инфосистемы Джет» разработаны уникальные программные продукты, которые в настоящее время используются во многих российских и зарубежных компаниях:
- Система мониторинга и архивирования электронной почты «Дозор-Джет»;
- Система контроля Интернет-ресурсов «Дозор»;
- Межсетевой экран Z-2;
- Средство создания виртуальных защищенных сетей (VPN) «Тропа-Джет».

Все средства защиты имеют сертификаты уполномоченных государственных органов.

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

Контроль над корпоративной электронной почтой предполагает как минимум выполнение трех основных задач:

1. Создание условий для эффективного управления почтовым потоком.
2. Обеспечение безопасности почтовой системы.
3. Обеспечение надежного и долговременного хранения почтовых сообщений с высоким уровнем доступности данных.

Специалистами компании «Инфосистемы Джет» разработана Система мониторинга и архивирования почтовых сообщений «Дозор-Джет» (далее — СМАП «Дозор-Джет»), которая позволяет решить все вышеназванные задачи. Она представляет собой специализированное программное средство, которое обеспечивает мониторинг и контроль входящих, исходящих и внутренних почтовых сообщений.

Управление почтовым потоком

СМАП «Дозор-Джет» позволяет создать условия для гибкого управления почтовым потоком. Это, в первую очередь, подразумевает внедрение политики использования электронной почты и эффективный контроль за исполнением политики всеми пользователями корпоративной почтовой системы.

Такая политика обычно принимается в компаниях на административном уровне. Она устанавливает правила использования электронной почты, то есть определяет следующие параметры:

- **Что контролируется** — прохождение *каких категорий* сообщений электронной почты должно быть разрешено или запрещено;
- **На кого распространяется** — *пользователи/группы пользователей*, которым разрешено или запрещено получать или отправлять сообщения электронной почты определенной категории;
- **Как реагирует система** — *что необходимо делать* с теми или иными сообщениями электронной почты, которые удовлетворяют или не удовлетворяют критериям, определенным правилами использования электронной почты.

Безопасность почтовой системы

С ростом популярности Интернета электронная почта становится важнейшим средством коммуникаций. Электронная почта имеет все необходимые качества для того, чтобы быть самым популярным средством связи: низкая стоимость, простота использования, большое количество пользователей. Однако, наряду с многочисленными преимуществами, существует ряд рисков, связанных с использованием электронной почты. Эти риски могут привести к значительному снижению эффективности работы организации, потере значимой информации.

СМАП «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.

СМАП «Дозор-Джет» осуществляет мониторинг и контроль всех входящих, исходящих и внутренних почтовых сообщений. Мониторинг включает в себя анализ заголовков и структуры сообщений, а также проверку на наличие в тексте сообщения или прикрепленных файлах слов или последовательностей слов, разрешенных или запрещенных к использованию в почтовых сообщениях. Результатом мониторинга может стать, например, задержание подозрительных писем. СМАП «Дозор-Джет» дает возможность 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 файлов 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 отложенная доставка почтового сообщения, когда решение о направлении письма адресату принимается только после его дополнительного анализа Администратором системы. При этом могут применяться и другие системы безопасности помимо СМАП «Дозор-Джет» (антивирусные программы, спам-фильтры и пр.).

Антивирусная защита

Для защиты от вирусов, передаваемых через почтовые сообщения, СМАП «Дозор-Джет» применяет как собственные средства, а именно фильтрацию писем по полям заголовка и по содержанию, так и антивирусные программы третьих производителей.

Проверка на вирус может осуществляться на любом этапе обработки сообщения. В СМАП «Дозор-Джет» реализован унифицированный интерфейс к антивирусным программам Symantec Antivirus (Symantec Corp.), Антивирус Касперского («Лаборатория Касперского») и Dr.Web («ДиалогНаука»). Данные программы обеспечивают антивирусную проверку до начала обработки письма СМАП «Дозор-Джет». После окончания проверки, в зависимости от ее результатов, на письмо ставится соответствующая пометка, которая учитывается при дальнейшей обработке письма. Это позволяет автоматически посылать уведомления о зараженных письмах Администратору системы, адресату и т.д. Затем письмо может быть помещено в архив, где оно хранится в первоначальном виде, то есть с вирусом и пометкой «письмо содержит вирус». Хранение зараженных писем абсолютно безопасно. Кроме того, Администратор системы имеет возможность безопасно ознакомиться с текстом письма без раскрытия вложенных файлов.

Также существует возможность осуществлять проверку на наличие вирусов после проведения декомпозиции письма путем применения действия «вызов внешней программы». В данном случае, по желанию заказчика, помимо указанных программ СМАП «Дозор-Джет» может быть интегрирована с другими антивирусными программами. Это позволяет, например, осуществлять проверку на наличие вируса в отдельных объектах письма.

Борьба со спамом

Фильтрация спама в СМАП «Дозор-Джет» проходит в несколько этапов. Часть спама отсекается уже «на подступах» к системе (30-40%), то есть на этапе получения почты SMTP-прокси:

1. Проверка по RBL-спискам — сервис, обеспечивающий проверку адреса отправителя на принадлежность к одному из следующих списков: списки почтовых адресов известных спамеров; адресов открытых почтовых пересылок (open relay), используемых спамерами эпизодически или регулярно; списки диапазонов адресов тех сетей, которые не борются со спамерами или слишком к ним либеральны.
2. Anti-spoofing — проверка подлинности адресов путем поиска соответствующей записи в DNS (или проверки существования такого домена в DNS).

3. Anti-relay — запрет прохождения писем, адреса отправки и получения которых не принадлежат внутренним доменам.

После завершения первого этапа проверки письмо передается на обработку подсистеме фильтрации. Данная подсистема обеспечивает декомпозицию письма (Модуль разбора) и проверку его на соответствие условиям, заданным Администратором системы (Модуль анализа и Модуль категоризации почтовых сообщений).

С учетом подхода к борьбе со спамом в контексте общей политики информационной безопасности, спам-сообщения относятся СМАП «Дозор-Джет» к одной из категорий, которую необходимо будет фильтровать в соответствии с политикой использования электронной почты. Такую задачу в СМАП «Дозор-Джет» выполняет Модуль категоризации почтовых сообщений.

Архив почтовых сообщений

Подсистема архивирования занимает в структуре СМАП «Дозор-Джет» центральное место. Она участвует во всех процессах, проходящих в системе. К примеру, подсистема фильтрации хранит в архиве базу данных правил, мета-данные, на основе которых осуществляется фильтрация почтовых сообщений. Архив задействован в работе большинства дополнительных модулей. Он используется для создания специальной зоны, так называемого карантина, для временного помещения туда «подозрительных» писем. Накопленная в архиве информация применяется для дальнейшей обработки писем. Конфигурация архива осуществляется с помощью управляющего Web-сервера, который входит в состав подсистемы управления.

Подсистема архивирования СМАП «Дозор-Джет» в настоящее время имеет реализации на двух СУБД:

- Oracle (СМАП «Дозор-Джет», версия Enterprise Edition);
- PostgreSQL (СМАП «Дозор-Джет», версия Lite).

В ближайшем будущем планируется создание версий СМАП «Дозор-Джет», работающих с MS SQL Server.

Архив СМАП «Дозор-Джет» предназначен для хранения и поиска почтовых сообщений. В архиве хранятся оригинал письма и метаданные (служебная информация о письме). В тех случаях, когда архив используется только для создания отчетов по почтовым потокам, вместо оригинала письма в архив можно помещать мета-данные письма.

Архив обеспечивает хранение в режиме on-line большого количества корпоративной электронной почты (до 1 Терабайта) с высоким уровнем доступности данных и долговременное хранение сообщений в течение десяти и более лет. При этом есть возможность экспорта данных на внешние носители, что обеспечивает практически неограниченные возможности по объемам хранения данных. Необходимо отметить, что объем хранимой в архиве информации ограничивается исключительно возможностями аппаратного обеспечения.

Архив СМАП «Дозор-Джет» снабжен как механизмом быстрого поиска писем по любым их атрибутам, так и механизмом индексирования, который позволяет осуществлять полнотекстовый поиск по архиву писем. Формирование критериев поиска осуществляется с помощью Web-интерфейса. СМАП «Дозор-Джет» способна осуществлять следующие виды поиска: контекстный, атрибутивный, морфологический.

Состав системы

СМАП «Дозор-Джет» представляет собой набор программных модулей, которые обеспечивают потоковый анализ SMTP-трафика почтовых сообщений как между локальной сетью компании и внешними открытыми сетями, так и внутри локальной вычислительной сети компании, а также ведение архива почтовых сообщений.

СМАП «Дозор-Джет» состоит из следующих основных подсистем (см. рис. 1):

- Подсистемы мониторинга;
- Подсистемы архивирования;
- Подсистемы управления.

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

СМАП «Дозор-Джет» функционирует под управлением следующих операционных систем:

- **Sun Solaris** (версии 2.6, 2.7 и 2.8);
- **HP-UX** (версии 11.0);
- **Linux** (дистрибутивы RedHat 8.x, 9.0, Fedora Core; RedHat Enterprise Linux 3.0, 2.1; ALTLinux Master 2.0, 2.2, Утес-К; Mandrake 8.x).

Интеграция в почтовую систему

СМАП «Дозор-Джет» легко интегрируется в уже созданную почтовую систему. Она устанавливается на отдельный сервер, как правило, в демилитаризованной зоне корпоративной сети. Система является SMTP-proxy. Доставку электронной почты выполняет почтовый сервер.

Один из вариантов установки СМАП «Дозор-Джет» представлен на рис. 2.

СМАП «Дозор-Джет» функционирует совместно со следующими почтовыми серверами:

- **Sendmail**;
- **Postfix**;
- **Exim**;
- **qmail**;
- **Netscape Messenger**;
- **SunONE Messenger Server**;
- **CommuniGate PRO**;
- **MS Exchange 2000**;
- **MS Exchange 5.5**.

Интеграция с другими системами

СМАП «Дозор-Джет» может интегрироваться с другими системами защиты, используемыми в корпоративных сетях, такими как межсетевые экраны и антивирусные программы. Ниже перечислены продукты, совместимость которых со СМАП «Дозор-Джет» протестирована в ходе эксплуатации системы.

Межсетевые экраны:

- **Z-2**;
- **Cisco PIX**;
- **CheckPoint FW1**.

Антивирусные продукты:

- **Symantec Antivirus**;
- **Антивирус Касперского**;
- **Dr.Web**.

СМАП «Дозор-Джет» имеет много дополнительных функциональных возможностей. В частности, она может взаимодействовать с системой управления **HP OpenView**, которая позволяет контролировать работу компонентов СМАП «Дозор-Джет» и отображать информацию о нарушениях политики использования электронной почты на консоли Администратора системы.

Кроме того, СМАП «Дозор-Джет» может использовать **электронную цифровую подпись (ЭЦП)**. Система позволяет осуществлять централизованную проверку почтовых сообщений и их подпись. Эта функциональность в настоящее время особенно актуальна, поскольку обеспечивает контроль целостности данных, передаваемых по почтовому каналу.

СМАП «Дозор-Джет» позволяет получать и детально анализировать информацию о почтовом потоке организации. Это возможно благодаря архиву почтовых сообщений. Данные из архива могут использоваться для получения статистики и составления отчетов по работе почтовой системы. При этом СМАП «Дозор-Джет» может интегрироваться со следующими системами построения отчетов:

- **Oracle Reports**;
- **Crystal Reports**;
- **MS Query**.

Режимы функционирования системы

Режим функционирования СМАП «Дозор-Джет» выбирается в зависимости от возложенных на нее задач. При необходимости контролировать почтовый поток и влиять на прохождение писем (задерживать, перенаправлять письма и т.д.), СМАП «Дозор-Джет» устанавливается в режиме фильтрации. Задача простого мониторинга почтового потока осуществляется в режиме архивирования.

Режим архивирования

В режиме архивирования СМАП «Дозор-Джет» устанавливается «параллельно» почтовому серверу (рис. 3). Копии всех писем, проходящих через почтовый сервер, направляются в СМАП «Дозор-Джет», а почтовая система обычным образом доставляет их адресатам. Попадая в СМАП «Дозор-Джет», письма анализируются и при необходимости заносятся в архив. Все события, происходящие в системе, регистрируются в системном журнале. Информация, накапливаемая в архиве, может использоваться для составления регулярных отчетов по почтовому трафику, для выявления рисков использования электронной почты, для расследования инцидентов.

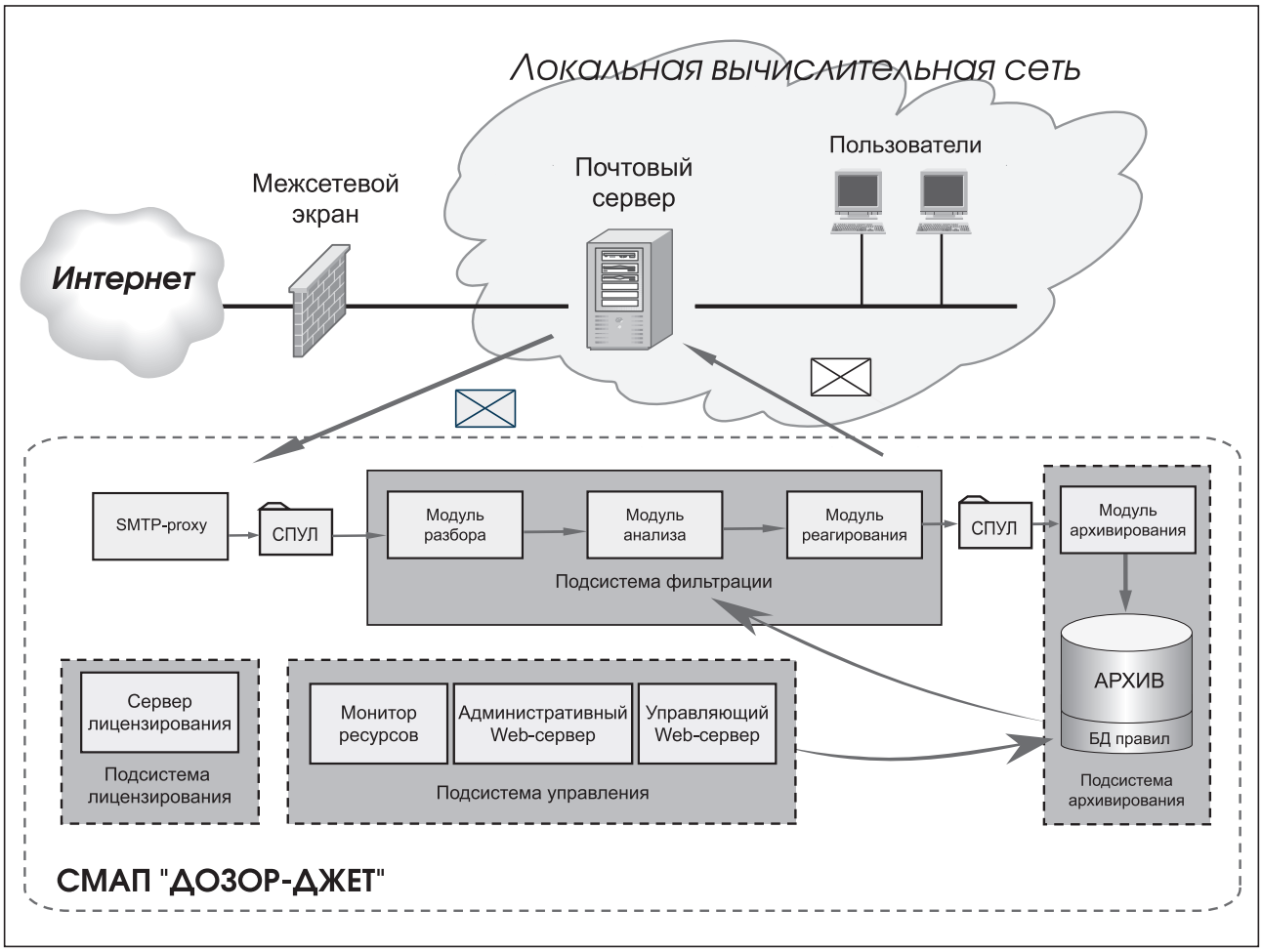

Рис. 1 Архитектура СМАП «Дозор-Джет»

Режим фильтрации

В режиме фильтрации СМАП «Дозор-Джет» устанавливается «в разрыв» (рис. 4). Почтовый поток направляется сначала на сервер, где установлена СМАП «Дозор-Джет». Каждое сообщение проверяется системой на соответствие политике и, в случае несоответствия критериям, оно задерживается, удаляется или перенаправляется Администратору системы. Письма, прошедшие проверку, передаются основной почтовой системе, которая доставляет их адресатам. В этом режиме функционирования одновременно с фильтрацией осуществляется архивирование почтовых сообщений.

Анализ содержимого почтовых сообщений

Все попадающие в СМАП «Дозор-Джет» почтовые сообщения проходят процедуру разбора на составляющие компоненты. При этом происходит разбор как заголовков сообщения (отправитель, получатель, 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 в себя:

- 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.

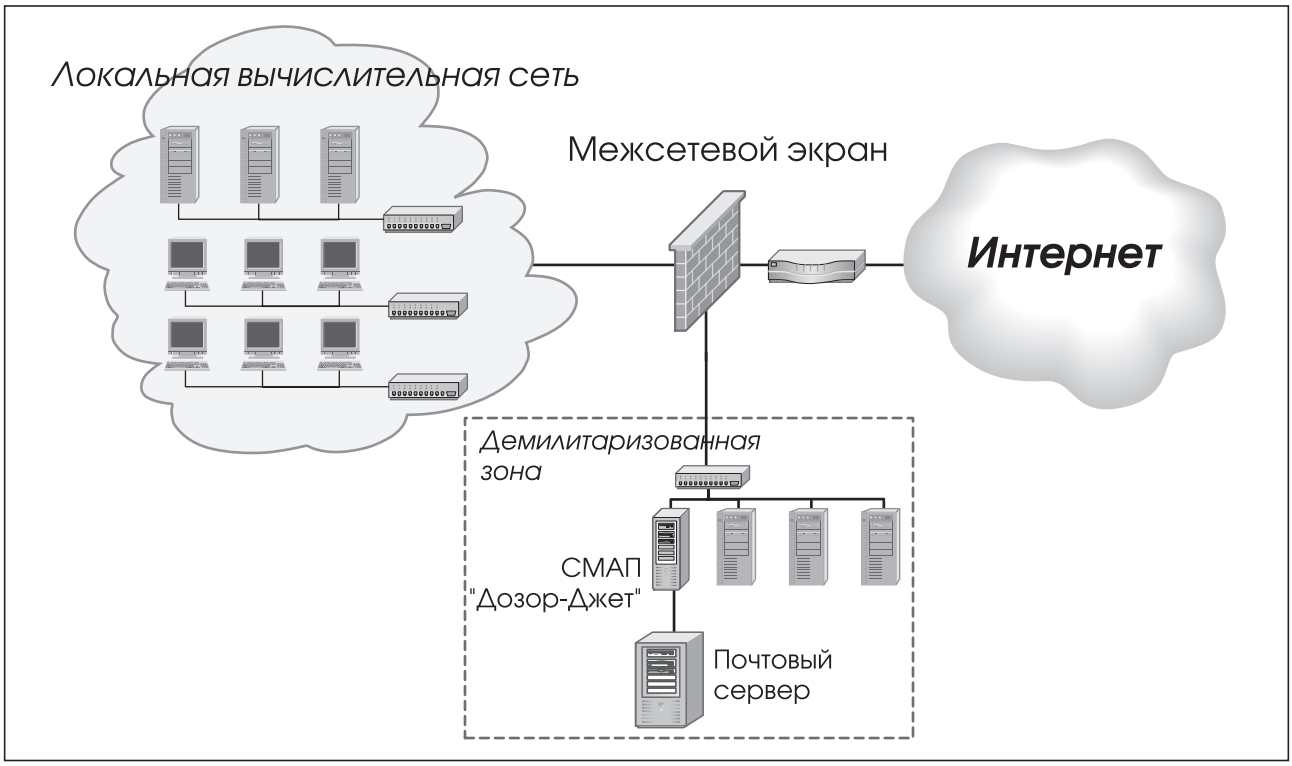

Рис. 2 Вариант установки СМАП «Дозор-Джет»

Варианты реагирования по результатам проверок

При обнаружении писем, отвечающих критериям, заданным Администратором системы, СМАП «Дозор-Джет» 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;
- Отправка письма на дополнительную обработку другой программе;
- Проставление пометок;
- Отправка уведомления (оповещение Администратора системы и др.).

Кроме того, СМАП «Дозор-Джет» может осуществлять реинжиниринг почтовых сообщений, т.е. модификацию сообщений перед доставкой или пересылкой, включая удаление запрещенных вложений и добавление определенного текста (аннотирование письма) в зависимости от результатов анализа сообщения.

Необходимо отметить, что все производимые СМАП «Дозор-Джет» действия обязательно протоколируются.

Получение статистики

Статистическая обработка накопленной в СМАП «Дозор-Джет» информации позволяет проанализировать эффективность 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

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

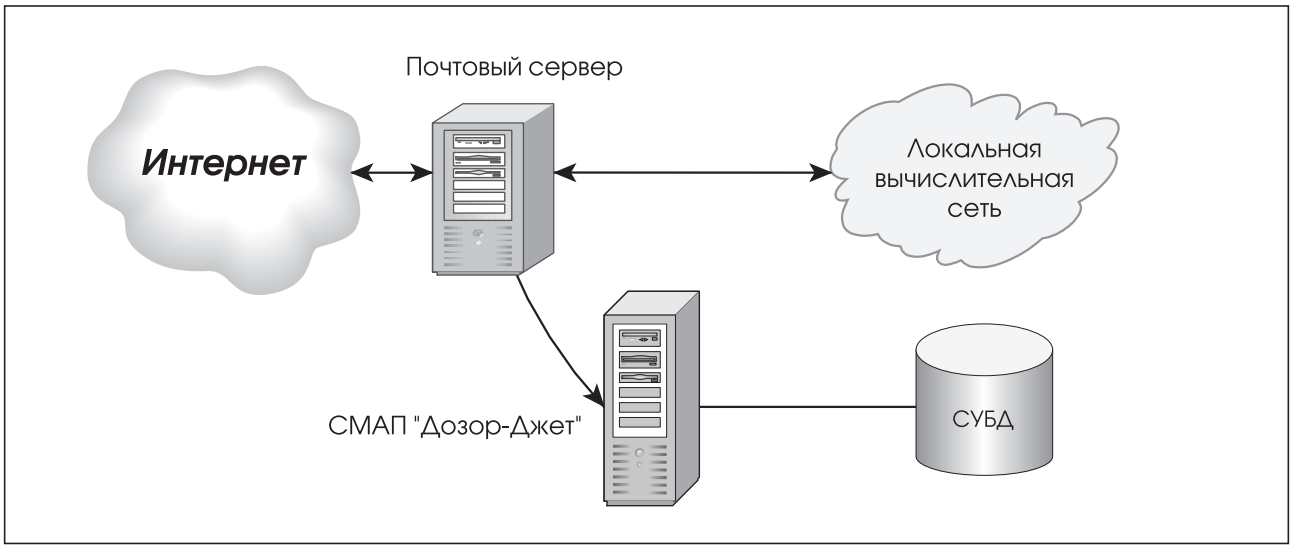

Рис. 3 Схема подключения СМАП «Дозор-Джет» в режиме архивирования

Разграничение доступа к объектам системы

Доступ к объектам СМАП «Дозор-Джет» определяется исходя из списков прав доступа для каждой категории объектов. Например, имеются списки прав для работы с условиями, с поисковыми запросами, с шаблонами уведомлений.

Основными особенностями СМАП «Дозор-Джет» являются:

- Полный разбор сообщений любого уровня вложенности;
- Распознавание форматов присоединенных файлов всех популярных офисных приложений;
- Анализ русскоязычных почтовых сообщений независимо от используемой кодировки кириллицы;
- Мощная подсистема фильтрации сообщений, основанная на механизме правил и позволяющая реализовать политику использования электронной почты любой сложности;
- Гибкие механизмы реагирования на выполнение условий фильтрации;
- Модульная структура, благодаря чему реализуется многофункциональность системы;
- Мощная подсистема архивирования, позволяющая осуществлять полнотекстовый поиск по архиву;
- Внутренние механизмы защиты, обеспечивающие разграничение доступа ко всем объектам системы;
- Высокая степень защиты от спама;
- Интеграция с другими системами (системой HP OpevView, межсетевыми экранами, антивирусными программами и др.).

Существуют также списки прав на выполнение определенных функций администрирования.

Дополнительные возможности

СМАП «Дозор-Джет» представляет собой средство реализации политики использования электронной почты. Однако реализация такой политики является весьма сложной задачей, поскольку кроме некоторого набора «стандартных задач» в политику входят правила, специфичные для каждой конкретной организации. Именно поэтому система управления электронной почтой обязательно должна быть расширяемой.

Как программный комплекс, СМАП «Дозор-Джет» имеет модульную архитектуру. Именно эта архитектура позволяет расширять функциональные возможности системы, интегрируя в нее дополнительные модули, не затрагивая ее ядра, в которое входят модуль разбора писем, модуль применения правил, модуль архивирования и модули, реализующие Web-интерфейсы к основным функциям (см. рис. 1).

Дополнительные модули, расширяющие функциональные возможности СМАП «Дозор-Джет», не входят в стандартный комплект поставки. К ним относятся:

- Модуль подключения ЭЦП;
- Модуль сегментирования архива почтовых сообщений;
- Модуль контекстного поиска в архиве почтовых сообщений;
- Модуль лексического контекстного поиска в архиве почтовых сообщений;
- Модуль статистики и отчетов;

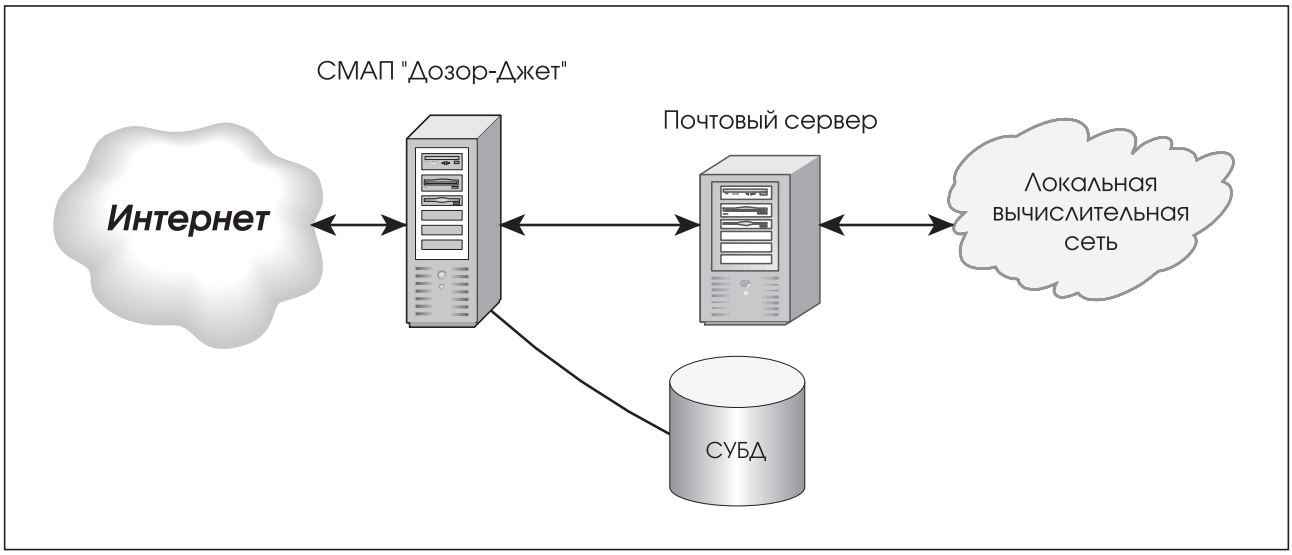

Рис. 4 Схема подключения СМАП «Дозор-Джет» в режиме фильтрации

- Модуль взаимодействия с HP OpenView;
- Модуль категоризации почтовых сообщений (антиспам);
- Модуль доступа к архиву почтовых сообщений по протоколу IMAP4;
- Модуль реконструкции почтовых сообщений;
- Модуль подтверждения отправки почтовых сообщений.

Модуль подключения ЭЦП

Модуль подключения ЭЦП обеспечивает следующие дополнительные функциональные возможности:

- Авторизацию и обеспечение юридической значимости электронных документов при обмене ими между пользователями;
- Обеспечение конфиденциальности и контроля целостности информации, пересылаемой по электронной почте.

Перечисленные функции реализуются посредством использования процедур формирования и проверки электронной цифровой подписи. Постановка ЭЦП и ее проверка осуществляются средствами третьих производителей, для подключения конкретной реализации ЭЦП к СМАП «Дозор-Джет» достаточно, чтобы был обеспечен простой интерфейс, являющийся подмножеством Microsoft CryptoAPI.

Установка Модуля подключения ЭЦП дает СМАП «Дозор-Джет» возможность совершать два новых действия: *подписать письмо* и *проверить подпись*. Оба этих действия возможны только при наличии базы данных, которая связывает авторов писем с соответствующими сертификатами. Такая база данных и средства для ее ведения входят в состав данного модуля.

Модуль сегментирования архива почтовых сообщений

Модуль сегментирования архива почтовых сообщений предназначен для повышения производительности и надежности работы с большими базами данных электронной почты. В модуле используется опция Partitioning СУБД Oracle (Enterprise Edition), которая позволяет строить секционированные таблицы и индексы. Секционированные таблицы и индексы применяются для разделения больших таблиц и индексов на части (секции), управлять которыми можно независимо друг от друга. При секционировании уменьшается время, необходимое для выполнения большинства операций над данными. Объясняется это обработкой меньшего числа «единиц хранения» и увеличением производительности вследствие параллельного выполнения этих операций.

Администраторы баз данных могут определять атрибуты хранения для каждой секции и планировать ее размещение на файловой системе сервера, увеличивая тем самым гибкость управления большой базой данных. Каждая из секций может быть переведена в автономное (off-line) состояние или, наоборот, возвращена в оперативное (on-line) состояние. В автономном состоянии секция может храниться на внешних носителях, что обеспечивает практически неограниченные возможности по объемам хранения данных.

Модуль контекстного поиска в архиве почтовых сообщений

Модуль контекстного поиска позволяет осуществлять в архиве электронной почты поиск по тексту в теле сообщения и прикрепленных файлах. Поиск осуществляется по полному совпадению слова в тексте сообщения вне зависимости от исходной кодировки текста. Если почтовое сообщение содержит архив (zip, rar, tar, arj, gzip), то поиск производится по содержимому архивированных файлов.

Данный модуль поставляется исключительно со СМАП «Дозор-Джет» Enterprise Edition. Интерфейс к функциям этого модуля обеспечивается через систему построения запросов к базе данных писем. Модуль реализован на основе Oracle Intermedia (в настоящее время данная опция СУБД Oracle называется Oracle Text).

Модуль лексического контекстного поиска в архиве почтовых сообщений

Модуль лексического контекстного поиска в архиве почтовых сообщений позволяет осуществлять в архиве электронной почты поиск по тексту в теле сообщения и прикрепленных файлах. В отличие от модуля контекстного поиска, данный модуль позволяет находить в базе письма, содержащие любые грамматические производные от указанного слова.

Данный модуль поставляется исключительно со СМАП «Дозор-Джет» Enterprise Edition. Интерфейс к функциям этого модуля обеспечивается через систему построения запросов к базе данных писем. Модуль реализован на основе Oracle Text и Russian Context Optimizer. Система Russian Context Optimizer (RCO) поставляется третьими производителями, ее стоимость определяется прайс-листами производителя.

Поиск осуществляется вне зависимости от исходной кодировки текста. Если почтовое сообщение содержит архив (zip, rar, tar, arj, gzip), то поиск производится по содержимому архивированных файлов.

Модуль статистики и отчетов

Модуль статистики и отчетов дополняет встроенную в СМАП «Дозор-Джет» систему отчетов. Он позволяет получать детальную информацию о почтовом трафике в формате MS Excel. С помощью этого модуля можно анализировать почтовый трафик организации как за относительно большие периоды времени, так и за сутки, что позволяет оперативно корректировать политику использования электронной почты.

Модуль взаимодействия с HP OpenView

В составе СМАП «Дозор-Джет» поставляется модуль, обеспечивающий взаимодействие с системой HP OpenView. Это позволяет контролировать работу различных компонентов СМАП «Дозор-Джет». Установка этого модуля добавляет в СМАП «Дозор-Джет» дополнительное действие: *сделать запись в журнал*. Это действие аналогично действию *послать уведомление* (за исключением присоединения оригинала письма) и позволяет оперативно выводить на консоль управления HP OpenView информацию об «опасных» письмах.

Кроме того, данный модуль позволяет проводить мониторинг различных параметров СУБД Oracle, которая входит в СМАП «Дозор-Джет», а также контролировать критичные ресурсы системы (мониторинг работы почтовых утилит, http-сервера Apache; контроль размеров каталогов, системных журналов и log-файлов) и передавать полученные результаты Администратору системы. Это значительно повышает надежность работы СМАП «Дозор-Джет».

Модуль категоризации почтовых сообщений

Модуль категоризации почтовых сообщений предназначен для выделения из почтового потока писем определенной категории. Письма автоматически относятся (на основании ранее выполненного анализа) к той или иной категории. Для выбора данной категории Администратор системы подбирает образцы писем. При этом категоризация писем осуществляется на основе теории вероятности с использованием статистических алгоритмов. Данная технология позволяет автоматически корректировать работу категоризатора, что значительно облегчает задачу Администратора системы по ее контролю и настройке и сокращает время на обслуживание СМАП «Дозор-Джет».

Особенностью данного модуля является возможность индивидуальной настройки фильтра в соответствии с требованиями конкретного заказчика. В частности, по желанию заказчика модуль можно настроить на фильтрацию сообщений рекламного характера (спам).

Модуль доступа к архиву электронной почты по протоколу IMAP4

Модуль доступа к архиву электронной почты по протоколу IMAP4 предоставляет Администрато-

ру и пользователям СМАП «Дозор-Джет» возможность доступа к почтовому архиву по стандартному протоколу с помощью пользовательских почтовых клиентов. При этом такими почтовыми клиентами могут быть любые широко используемые в настоящее время программы, например, MS Outlook, Netscape Messenger, The Bat! и т.п.

Модуль предоставляет Администратору и пользователям СМАП «Дозор-Джет» единый интерфейс доступа как к своей электронной почте, так и к почтовому архиву. Они получают возможность экспортировать письма из архива в свой почтовый ящик путем простого «перетаскивания» писем. При этом необходимо отметить, что такую возможность пользователи получают в соответствии с правами доступа, установленными Администратором системы.

Модуль реконструкции почтовых сообщений

Модуль реконструкции почтовых сообщений позволяет вносить изменения в электронное письмо перед отправкой получателю и заменять определенные части письма на текстовые сообщения.

При включении данного модуля в состав СМАП «Дозор-Джет» появляется возможность осуществлять следующие действия над письмом:

- Заменять определенные части письма на заданный текст;
- Удалять, перезаписывать или добавлять заголовки;
- Добавлять дисклеймер (disclaimer — предупреждение об ограничении ответственности).

Решение о замене части письма на заданный текст принимается на основе ее типа (content-type). Для замены части письма Администратором системы задается ряд текстовых шаблонов. Каждому типу соответствует определенный шаблон.

При необходимости оригинал письма (до осуществления реконструкции почтового сообщения) может быть сохранен в архиве электронной почты с пометкой о произведенной модификации.

Модуль подтверждения отправки почтовых сообщений

Данный модуль предназначен для подтверждения автором необходимости отправки почтового сообщения, которое в соответствии с политикой безопасности было задержано СМАП «Дозор-Джет».

Например, если СМАП «Дозор-Джет» определила, что в письме есть текст «запрещенного» содержания, то в соответствии с принятой в компании политикой безопасности данное письмо задерживается. Модуль подтверждения отправки почтовых сообщений добавляет функциональность, при которой «запрещенное» письмо может быть временно помещено в архив, а его автору отправлено уведомление о том, что письмо было задержано. При этом, в случае необходимости, указывается причина задержки. Автору письма передается право решать, подтвердить отправку письма или отменить ее. Для этого существует специальный Web-интерфейс, при обращении к которому пользователю выдается приглашение к авторизации.

В случае успешной авторизации пользователю выдается сообщение о возможности отправить письмо или отменить его отправку. В противном случае пользователь получает сообщение о том, что он не имеет доступа к данному письму.

В зависимости от выбора пользователя на письмо устанавливается соответствующая пометка: «отправка подтверждена» или «отправка отменена». Пользователю выдается сообщение о произведенных действиях: «Ваше сообщение отправлено» или «Отправка сообщения отменена». Все действия пользователя регистрируются в системном журнале. Кроме того, регистрируются попытки неавторизованного доступа к письмам.

Функциональность модуля не зависит от механизма аутентификации пользователя, так как применяется PAM-модуль на Web-сервере, что позволяет подключать различные схемы аутентификации, не модифицируя систему.

Сертификация системы

Гостехкомиссия России провела испытания СМАП «Дозор-Джет» и признала ее соответствие техническим условиям и руководящему документу «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», о чем свидетельствует сертификат № 465 от 14 июня 2001 г.

Срок действия этого сертификата истекает, в настоящее время в соответствии с решением Гостехкомиссии России № 1365 от 24 августа 2004 г. проводится повторная сертификация СМАП «Дозор-Джет», завершение которой планируется в январе 2005 года.

Контроль Интернет-ресурсов: СКВТ «Дозор»

Назначение СКВТ «Дозор»

Неконтролируемое использование Интернета и отсутствие защиты сетевых ресурсов несет в себе множество угроз для бизнеса компании. Это и снижение эффективности работы, и потеря качества услуг информационных систем, и разглашение конфиденциальной информации. Недостаточное внимание к данной проблеме грозит значительными потерями в бизнесе, а в некоторых случаях даже привлечением к юридической ответственности в связи с нарушением законодательства.

Среди основных рисков, возникающих при использовании Интернета, можно выделить:

- Вирусные атаки и вредоносный мобильный код;
- Снижение пропускной способности сети;
- Утечка конфиденциальной информации;
- Снижение производительности труда сотрудников.

Компания «Инфосистемы Джет» предлагает комплексное решение задачи защиты сетевых ресурсов компании на основе Системы контроля Интернет-ресурсов «Дозор» (далее — СКВТ «Дозор»).

СКВТ «Дозор» предназначена для защиты корпоративных локальных вычислительных сетей от рисков, связанных с использованием Интернет-ресурсов. Защита обеспечивается комплексом мер, включая фильтрацию содержимого информационного обмена, осуществляемого по протоколам HTTP и FTP, авторизацию пользователей и протоколирование их действий.

СКВТ «Дозор» представляет собой специализированное программное средство, предназначенное для реализации корпоративной политики использования Интернет-ресурсов в части обеспечения информационной безопасности.

СКВТ «Дозор» позволяет обеспечить:

1. Контроль использования Интернет-ресурсов:
   - Контроль форматов и объемов загружаемых файлов;
   - Контроль содержимого (анализ текста на содержание определенных слов и выражений);
   - Блокировка вредоносного мобильного кода;
   - Ограничение доступа к Web-серверам на основе URL.
2. Разграничение доступа к внешним Интернет-ресурсам по группам пользователей.
3. Разграничение доступа к Интернет-ресурсам в соответствии с временными параметрами (время суток, дни недели и т.п.).
4. Создание отчетов по результатам работы.
5. Сопровождение списков доступных и запрещенных ресурсов.

Политика использования Интернет-ресурсов

Политика СКВТ «Дозор» базируется на четырех понятиях:

- Группы пользователей;
- Направления передачи данных;
- Ресурсы;
- Ограничения по времени.

Взаимосвязь этих понятий приведена на рис. 5.

Группы пользователей

Политика использования Интернет-ресурсов основывается на принадлежности пользователя к определенной группе пользователей. В состав политики, определяемой для группы пользователей, входят проверки запросов к Интернет-ресурсам. Классификация пользователей может производиться разными методами — по данным из файлов, через NSS, используя LDAP. Аутентификация пользователей осуществляется либо с помощью средств прокси-сервера Squid, либо через Identd. К каждой группе пользователей применяется определенный набор правил.

При развертывании системы, по умолчанию определены четыре группы правил: «all», «default», «black» и «white». Правила группы «all» используются для создания политики, которая применяется ко всем группам пользователей. Правила группы «default»

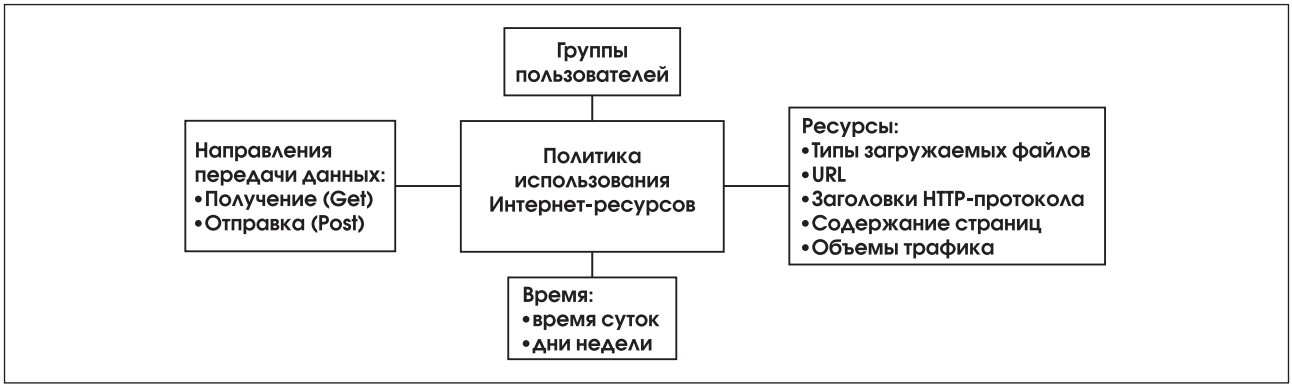

Рис. 5 Политика использования Интернет-ресурсов

применяются к пользователям, которые были авторизованы внешними средствами, но не были найдены ни в одной из групп на LDAP-сервере. Правила групп «black» и «white» используются, соответственно, для выделения пользователей, которым в соответствии с политикой безопасности запрещено использовать Интернет-ресурсы, и пользователей, для которых не установлено никаких ограничений на их использование.

Контроль ресурсов

В соответствии с политикой использования Интернет-ресурсов для каждой группы пользователей устанавливается связь с определенным набором проверок, которые обеспечивают фильтрацию по следующим параметрам:

- Расширение файлов;
- Типы данных;
- Ресурсы и сайты (URL);
- Фразы или словосочетания (контентная фильтрация).

Фильтрация по расширению файлов
Данный тип фильтрации обеспечивает проверку имен передаваемых файлов на наличие запрещенных расширений, что позволяет, например, блокировать передачу мультимедийных файлов в рабочее время. Этот метод обеспечивает быструю проверку, что снижает нагрузку на подсистему фильтрации.

Фильтрация по типам данных
Тип данных идентифицируется не только по расширению файла, но также может явно указываться сервером СКВТ «Дозор». Кроме этого, расширение файла не всегда соответствует формату самого файла. Например, файл с расширением EXE может быть переименован в файл с расширением DOC. Поэтому подсистема фильтрации обеспечивает определение типов передаваемых данных по бинарному следу.

Фильтрация по ресурсам (URL)
Данный метод фильтрации запрещает доступ еще на этапе запроса ресурсов. При осуществлении фильтрации по ресурсам можно запрещать доступ как к целым сайтам, так и к их частям. При этом СКВТ «Дозор» может выполнять обратное вычисление адресов сайтов в тех случаях, когда пользователи вместо имен пытаются использовать числовые адреса.

Контентная фильтрация
Данный метод фильтрации обеспечивает проверку передаваемой информации на наличие в ней определенного текста. При обнаружении заданных фраз передача данных либо блокируется сразу, либо СКВТ «Дозор» продолжает поиск других фраз до тех пор, пока не будет превышен определенный порог, заданный Администратором системы. Этот метод реализуется путем присвоения фразам весовых коэффициентов и их последующего суммирования. При этом фразы могут иметь как положительные, так и отрицательные коэффициенты, что позволяет реализовывать гибкие правила фильтрации. Например, данный метод может быть очень удобен для блокировки передачи данных через Web-почту, серверы которой еще не попали в список запрещенных сайтов.

Действия по результатам проверки
В зависимости от результатов конкретной проверки СКВТ «Дозор» может реагировать различ-ным образом — блокировать передачу данных, разрешать передачу, разрешать передачу с подтверждением. В режиме передачи с подтверждением пользователю требуется подтвердить необходимость получения доступа к указанному ресурсу, и в случае такого под-

тверждения создается временный ключ для доступа к этому ресурсу.

Необходимо отметить, что все производимые СКВТ «Дозор» действия обязательно протоколируются, то есть сохраняются в журнале. Это позволяет Администратору системы анализировать использование Интернет-ресурсов и корректировать политику на основе полученной информации.

Ограничения по времени

СКВТ «Дозор» позволяет разграничить доступ к Интернет-ресурсам в зависимости от времени суток и дней недели. Таким образом, можно связать временные характеристики с параметрами, используемыми для фильтрации (URL, типы данных, контент и т.п.). Например, запретить передачу файлов формата MPEG с 9:00 до 18:00 по рабочим дням.

Фильтрация по направлению передачи данных

Гибкость фильтрации обеспечивается в СКВТ «Дозор» за счет разделения потока по направлению передачи данных. Это позволяет обеспечить гибкий подход к фильтрации входящего и исходящего Web-трафика.

Составление отчетов

СКВТ «Дозор» позволяет создавать следующие виды отчетов:

- По объему трафика для каждого пользователя;
- По ресурсам;
- По инцидентам;
- По типам данных.

Отчет по объему трафика позволяет получить количественную оценку трафика для каждого пользователя за выбранный период. При этом в отчете отражаются все пользователи (в том числе и те, которые ранее были удалены по какой-либо причине из списка пользователей).

Отчет по ресурсам позволяет просмотреть ресурсы, которыми воспользовался кто-либо из существующих пользователей или групп пользователей. При этом имеется возможность сгруппировать ресурсы по названиям сайтов. Этот отчет можно создавать за любой заданный период времени. Данный период можно корректировать динамически. Это означает, что Администратору системы не придется перенастраивать остальные параметры поиска, так как они всегда сохраняются в форме, по которой был создан отчет. Кроме того, существует возможность добавлять указанные в отчете ресурсы в какую-либо из групп ресурсов системы контроля трафика.

Поскольку при работе СКВТ «Дозор» периодически будут возникать блокировки, предупреждения и исключения передачи данных, то возникает необходимость отслеживать возникающие инциденты. Отчет по инцидентам дает возможность подсчитать количество инцидентов того или иного типа в заданный период времени, а также позволяет отражать подробности этих инцидентов в зависимости от типа или все одновременно в хронологическом порядке.

Отчет по типам данных предназначен для быстрой оценки объемов трафика в зависимости от формата данных, что позволяет выявить наиболее часто передаваемые типы файлов.

Состав СКВТ «Дозор»

В состав СКВТ «Дозор» входят:

1. Прокси-серверы Squid.

Они обеспечивают кэширование обработанных запросов и обращение к внешним ресурсам.

2. Модуль контроля содержимого.

Данный модуль позволяет выполнить анализ данных информационного обмена. Модуль анализирует текст на содержание определенных слов и выражений, определяет типы файлов по сигнатурам и т.п. Кроме того, возможно подключение внешних антивирусных программ для проверки содержимого передаваемых файлов.

3. Модуль генерации отчетов.

Данный модуль позволяет получать сводную информацию об использовании сервисов, в том числе информацию об объеме загруженных данных, сгруппированную по адресам внешних источников, группам пользователей или индивидуальным пользователям. Кроме того, модуль позволяет просмотреть журнал запросов пользователями запрещенных ресурсов.

4. Модуль управления.

Данный модуль позволяет управлять СКВТ «Дозор», определять группы пользо-

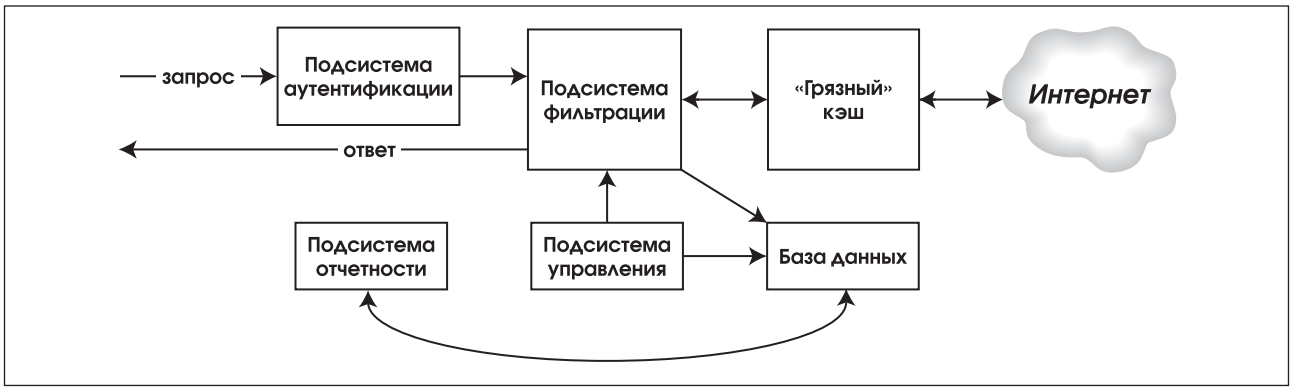

Рис. 6 Архитектура СКВТ «Дозор»

вателей, время доступа, запрещенные ресурсы и другую информацию.

Системные требования и производительность СКВТ «Дозор»

- Аппаратная платформа: Sun SPARC, Intel x86.
- Операционная система: Sun Solaris, Linux.

СКВТ «Дозор» способна обрабатывать десятки мегабайт в час и практически не создает задержек при информационном обмене. Возможность использования многомашинной конфигурации, при которой нагрузка распределяется по отдельным серверам, позволяет при пиковых нагрузках СКВТ «Дозор» обеспечить высокую скорость анализа и предоставления данных информационного обмена. Необходимо иметь ввиду, что производительность СКВТ «Дозор» ограничивается производительностью аппаратного обеспечения.

Структура СКВТ «Дозор»

СКВТ «Дозор» представляет собой набор программных модулей, которые обеспечивают потоковый анализ трафика по протоколам HTTP и FTP.

Архитектура СКВТ «Дозор» представлена на рис. 6. Запросы передаются на модуль аутентификации, который обращается к серверу с «чистым» кэшем. Если в «чистом» кэше есть какие-либо данные, то пользователи эти данные получают. В случае, если данных нет, сервер обращается к модулю контроля содержимого, который через сервер с «грязным» кэшем обращается к внешним ресурсам, анализирует их и принимает решение о разрешении или отказе в доступе к данному ресурсу. Система может использовать не только «грязный» кэш СКВТ «Дозор», но и кэш, который установлен в организации (ISA server, Netscape и т.п.).

Способы размещения СКВТ «Дозор»

Размещение СКВТ «Дозор» в инфраструктуре сети может быть различным и зависит от задач, которые возлагаются на систему. Наиболее эффективным и универсальным, с точки зрения выполняемых системой задач, является размещение СКВТ «Дозор» на двух серверах, установленных последовательно. Первый сервер, как правило, предназначен для реализации связки «модуль разграничения доступа + squid с «чистым» кэшем + модули управления и создания отчетов». На втором сервере может быть развернут контент-фильтр со squid с «грязным» кэшем (см. рис. 7).

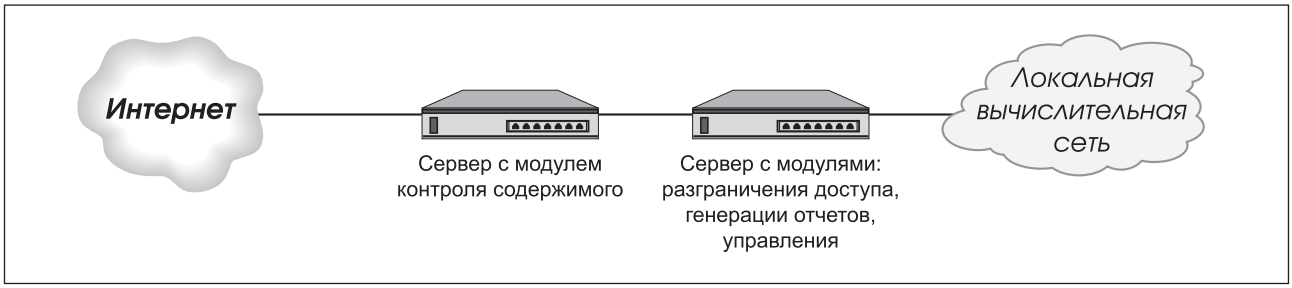

Рис. 7 Схема подключения СКВТ «Дозор»

Z-2 – универсальный межсетевой экран высшего уровня защиты

Для защиты ресурсов компании от несанкционированного доступа при подключении к внешним сетям, разграничения доступа извне и контроля использования ресурсов со стороны внешних сетей применяются специальные программно-аппаратные средства защиты — межсетевые экраны (МЭ).

Межсетевой экран обеспечивает защиту внутренних ресурсов компании в соответствии с установленной политикой безопасности. Для этого он решает следующие задачи:

- Обеспечивает разграничение доступа пользователей к ресурсам на основе заданных правил;
- Проводит идентификацию/аутентификацию пользователей;
- Контролирует входящие/исходящие информационные потоки на нескольких уровнях модели OSI/ISO;
- Осуществляет трансляцию сетевых адресов и сокрытие структуры защищаемой сети;
- Производит регистрацию событий доступа и автоматическое реагирование на нарушения;
- Осуществляет централизованное управление политикой безопасности на нескольких межсетевых экранах.

Для защиты внутренних ресурсов от несанкционированного доступа специалистами компании «Инфосистемы Джет» был разработан Межсетевой экран Z-2 (далее — МЭ Z-2). Он 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 МЭ Z-2 представлена на рис. 8.

Основные функциональные возможности

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

- 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 ОС Solaris компании Sun Microsystems на аппаратной платформе SPARC или Intel, что позволяет подбирать оптимальную конфигурацию оборудования по производительности и цене.

В состав комплекса МЭ Z-2 входят следующие программные компоненты (рис. 9):

- 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.

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 межсетевых экранов;
- Контроль действий Администратора;
- Возможность мониторинга и автоматического реагирования на нарушения политики безопасности;
- Высокая степень собственной защищенности;
- Возможность интеграции с антивирусными решениями и системами блокировки спама;
- Гибкий баланс уровня защиты корпоративной сети и производительности.

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 во (из) всей защищаемой сети или ее сегменте.

Фильтрация информационных потоков производится на основе правил, задаваемых Администратором, в соответствии с принятой в данной компании политикой информационной безопасности.

На сетевом и транспортном уровнях фильтрация соединений выполняется 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 производится 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, NET8 (Oracle) и SNMP.

МЭ Z-2 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, а также протоколирование соединений.

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

Кроме того, МЭ Z-2 может проводить фильтрацию запросов к прикладным сервисам путем создания шлюзов приложений на уровне ядра ОС, для чего в его состав входят шлюзы приложений. Основная их задача — пропустить протокол, который они обслуживают, через межсетевой экран на уровне пакетного фильтра, что позволяет существенно повысить быстродействие МЭ Z-2.

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.

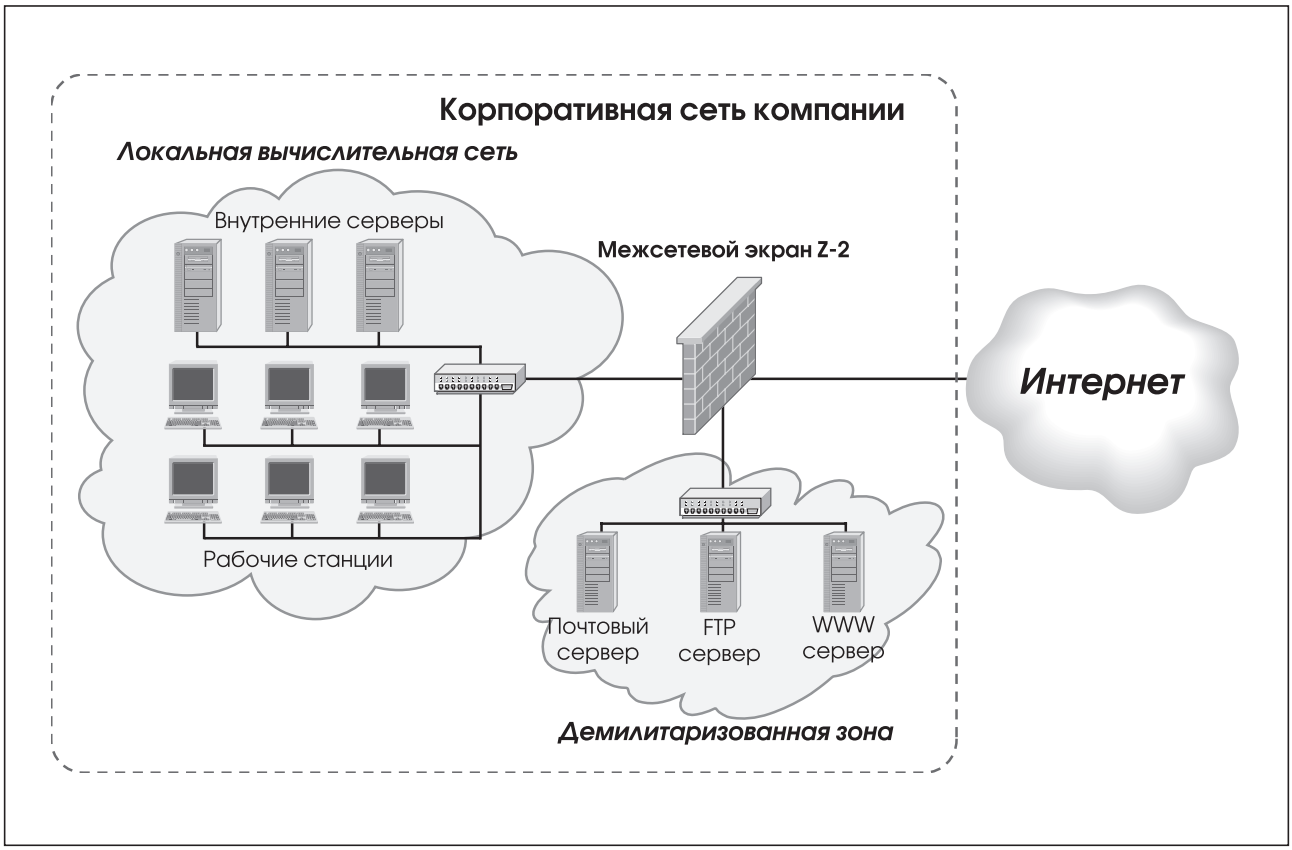

Рис. 8 Схема подключения МЭ Z-2

Верификация правил фильтрации

Для проверки списка правил фильтрации на избыточность и непротиворечивость в состав МЭ Z-2 включены 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 адресов (Network Address Translation, NAT) на основании заданного набора правил. Это дает возможность скрыть структуру внутренней сети от внешних субъектов и расширить возможности 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 реализует 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 при попытках получения несанкционированного доступа, не передается по сети, а используемые для аутентификации пароли не хранятся на определенном 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 хранятся в базе данных пользователей на сервере аутентификации и авторизации МЭ Z-2.

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

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 межсетевым экраном.

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 Z-2

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

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 Z-2

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

МЭ Z-2 поддерживает возможность установки в отказоустойчивой конфигурации, что позволяет защитить систему от остановки в случае выхода из строя аппаратного обеспечения.

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 Z-2 и прочие административные действия, события загрузки и останова МЭ Z-2, 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 может осуществляться только уполномоченным Администратором.

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

Оповещение Администратора МЭ Z-2 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:

- Локальное оповещение Администратора, осуществляющего мониторинг работы межсетевого экрана;
- Удаленное оповещение — отправка Администратору сообщения по электронной почте;
- Другие действия, настраиваемые Администратором.

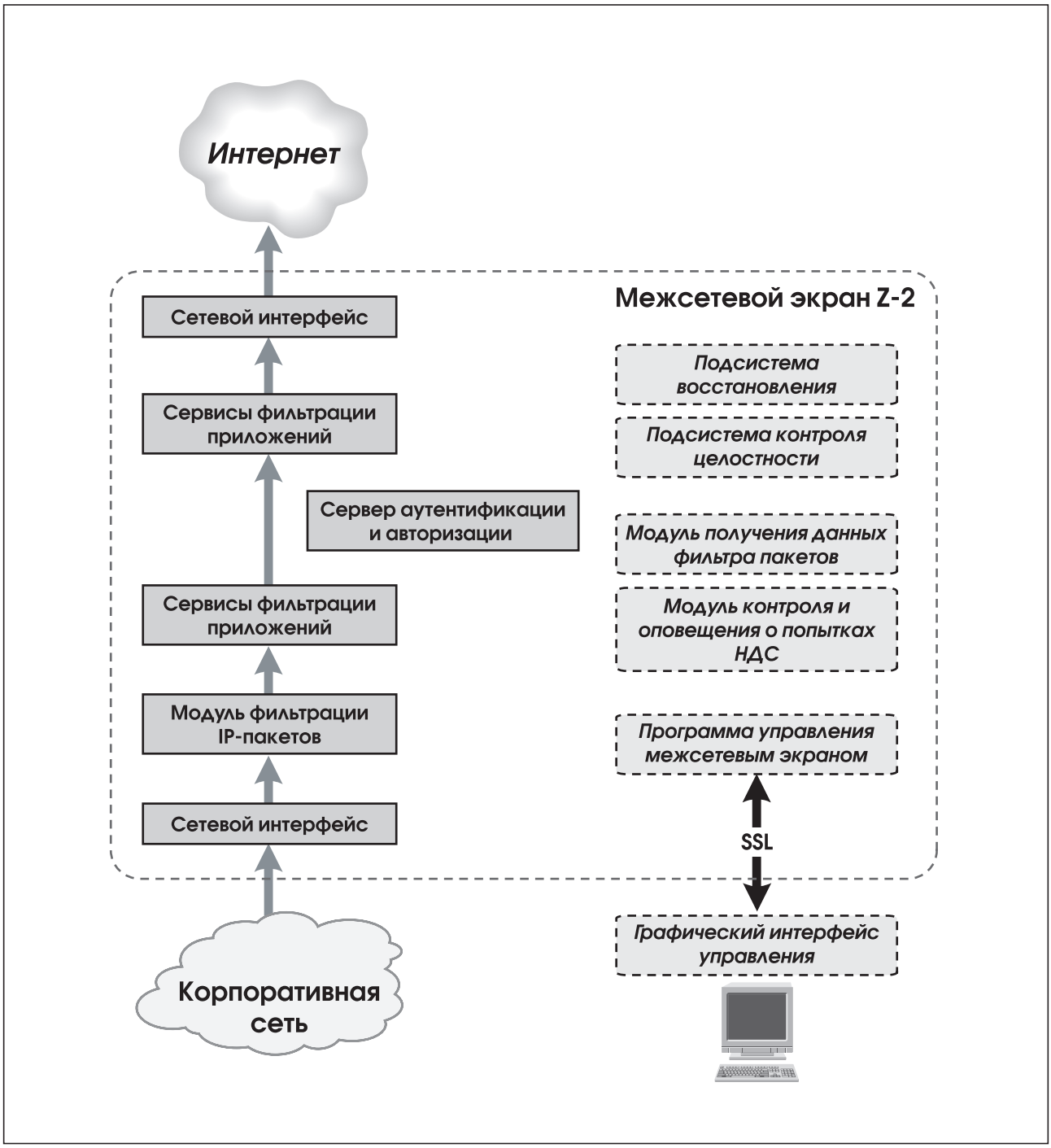

Рис. 9 Архитектура МЭ Z-2

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.

Резервное копирование и восстановление МЭ Z-2

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

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

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

Сертификация МЭ Z-2

МЭ Z-2 имеет следующие сертификаты:

- Сертификат Гостехкомиссии России № 638 на программный комплекс «Межсетевой экран «Z-2» на соответствие 2-му классу защищенности от НСД и 2-му уровню контроля отсутствия НДВ, выданный 27 июня 2002 г.;
- Сертификат Гостехкомиссии России № 806 на программный комплекс «Межсетевой экран «Z-2» на соответствие оценочному уровню доверия ОУД 4 (усиленный), выданный 14 ноября 2003 г.;
- Сертификат Министерства обороны РФ № 266 на программный комплекс «Межсетевой экран «Z-2», выданный 22 июня 2004 г.

Средство создания виртуальных защищенных сетей (VPN) «Тропа-Джет»

Для защиты информации, передаваемой по открытым сетям и каналам связи, необходимо применять средства создания виртуальных защищенных сетей (Virtual Private Networks, VPN).

Виртуальная защищенная сеть позволяет построить единый периметр безопасности, объединяющий все объекты корпоративной сети (центральный офис, подразделения, мобильные пользователи). Весь трафик, передаваемый между абонентами защищенной сети по открытым каналам, кодируется. Для этого в точке подключения локальных сетей объектов к открытым сетям устанавливаются шлюзы VPN, а на рабочие станции, подключаемые по выделенным или коммутируемым линиям, устанавливается программное обеспечение клиентов VPN.

Специалистами компании «Инфосистемы Джет» было разработано Средство создания виртуальных защищенных сетей (VPN) «Тропа-Джет» (далее — VPN «Тропа-Джет»). Оно реализует функции кодирования межсетевых информационных потоков в сетях передачи данных протокола TCP/IP для обеспечения обмена информацией между территориально-распределенными локальными сетями. Это обеспечивается посредством организации виртуальных защищенных сетей.

Основные функциональные возможности

VPN «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, устанавленным 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 периметра безопасности
VPN «Тропа-Джет» позволяет сформировать периметр 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
Периметр безопасности формируется для разделения трафика на кодируемый и некодируемый потоки. Кодирующий модуль VPN «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 VPN «Тропа-Джет» реализована асимметричная ключевая система, когда каждый потенциальный участник обмена данными использует пару долговременных ключей кодирования: секретный и открытый. Кодирование осуществляется на основе сеансовых ключей, автоматичес-

Основными особенностями VPN «Тропа-Джет» являются:

- Полнофункциональная схема управления ключами, позволяющая осуществлять динамическое распределение ключей, 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);
- Возможность выбора платформы — функционирование под управлением 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).

ки формируемых при помощи долговременных ключей и имеющих ограниченное время существования. VPN «Тропа-Джет» осуществляет все необходимые действия по управлению ключами: генерацию и распределение долговременных ключей, выработку сеансовых ключей абонентов, сертификацию открытых ключей, плановую и внештатную смену ключей кодирования.

Регистрация событий, мониторинг и управление межсетевыми потоками

VPN «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 локальной вычислительной сети. 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 VPN «Тропа-Джет»

VPN «Тропа-Джет» состоит из следующих компонентов (см. рис. 10):

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 целостности.

Шлюз с кодирующим/декодирующим модулем

Шлюз является основным модулем VPN «Тропа-Джет», выполняющим функции маршрутизации, фильтрации и кодирования пакетов. Каждый Шлюз предназначен для защиты определенной группы локальных сетей. На компьютере-шлюзе устанавливается модуль с функциями кодирования и декодирования и запускается программа аутентификации. Функциями Шлюза являются:

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

Центр распределения ключей

Центр распределения ключей осуществляет управление периметром 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 защищаемой сети;

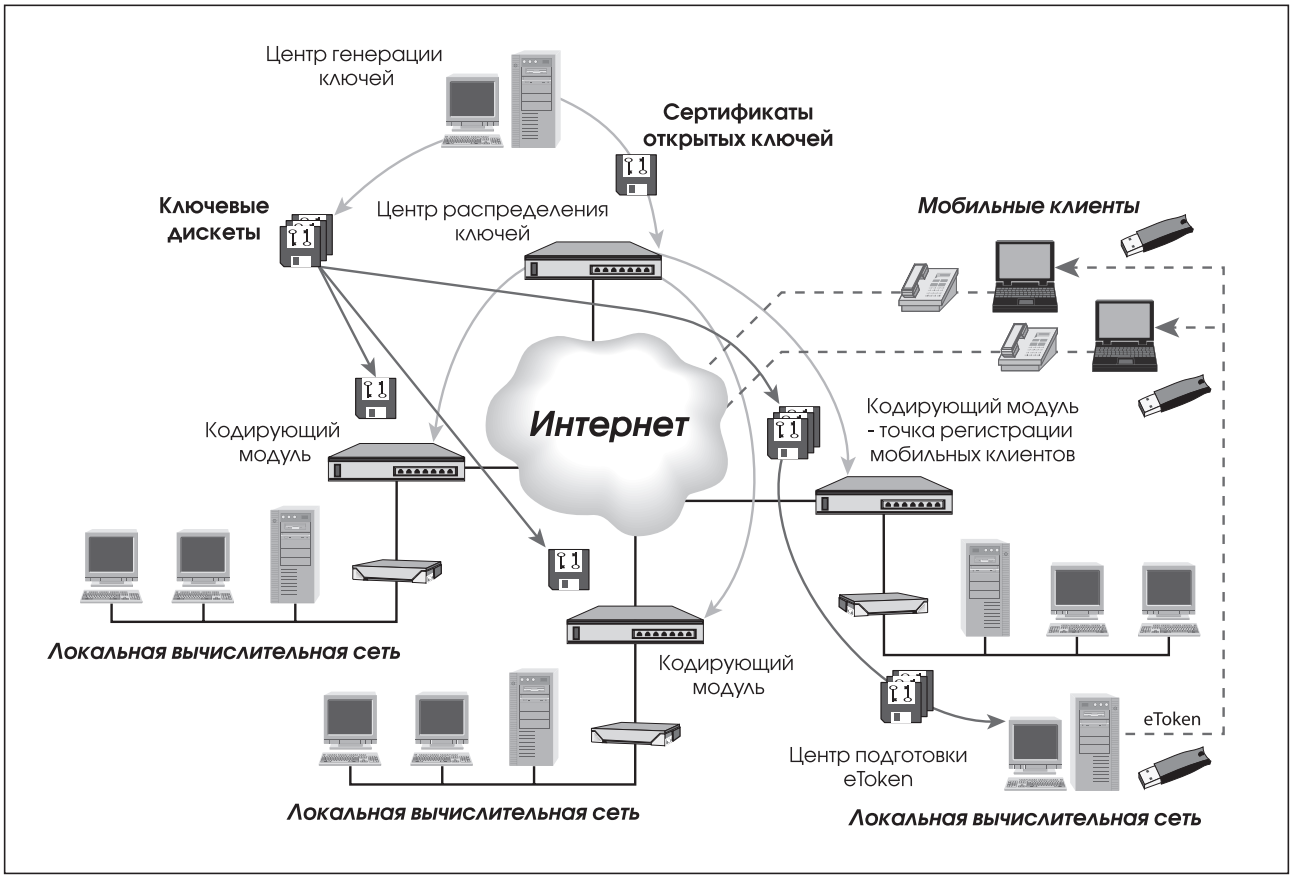

Рис. 10 Архитектура VPN «Тропа-Джет»

- 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 секретного 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 — программа, выполняющаяся на изолированном автоматизированном рабочем месте и предназначенная 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 Мобильный клиент VPN «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/XP 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 VPN «Тропа-Джет».

Обеспечение надежности функционирования

VPN «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 Администратора безопасности об изменении, добавлении и удалении файлов.

VPN «Тропа-Джет» поддерживает возможность установки в отказоустойчивой конфигурации, что позволяет защитить систему от остановки в случае выхода из строя аппаратного обеспечения.

Администрирование VPN «Тропа-Джет»

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

VPN «Тропа-Джет» обеспечивает аутентификацию администраторов и разграничение доступа к функциям администрирования.

Сертификация комплекса

VPN «Тропа-Джет» имеет следующие сертификаты:

- Сертификат Госстандарт РФ № РОСС RU.СП05.Н00059 на программный продукт Комплекс кодирования межсетевых потоков «Тропа-Джет» версия 2.5.0, выданный 15 января 2003 г.;
- Сертификат ФСБ РФ № СФ/114-0563 на программное средство криптографической защиты информации (СКЗИ) «КриптоПро CSP-Solaris» (версия 2.0) — вариант 1 (Sparc) и вариант 2 (Intel), выданный 01 октября 2002 г.

НОВОСТИ ПРОДУКТА

Интеграция с внешними PKI-системами

В последнее время все большее распространение получают системы, реализующие инфраструктуру открытых ключей, или PKI-системы. В связи с этим стали появляться отраслевые стандарты на управление ключевым материалом с помощью PKI-систем.

Учитывая эти обстоятельства, а также стремление соответствовать общепринятым стандартам информационной безопасности, компания «Инфосистемы Джет» провела работы по интеграции собственных продуктов с внешними PKI-системами.

Первым продуктом, интегрирующимся с внешней PKI-системой, стало Средство создания виртуальных защищенных сетей (VPN) «Тропа-Джет», предназначенное для построения VPN-сетей.

Технология работы с открытыми ключами уже давно применяется в VPN «Тропа-Джет». Эта технология существенно повышает безопасность передачи информации по общедоступным каналам, позволяя использовать одноразовые криптографические ключи для каждой сессии обмена данными между криптошлюзами.

В случаях, когда в сети одновременно установлены и PKI-система, и VPN «Тропа-Джет» возникает частичное дублирование таких функций, как выдача, хранение, публикация и отзыв сертификатов. Это приводит к усложнению контроля за работой системы и дополнительным временным затратам на администрирование.

Для интеграции был выбран продукт RSA KEON производства компании RSA Security, специализирующейся на оборудовании и программном обеспечении по информационной безопасности.

Выбор именно RSA KEON для интеграции был не случаен. RSA KEON — один из первых продуктов, поддерживающих российские алгоритмы шифрования, он получил широкое распространение в нашей стране.

Интеграция VPN «Тропа-Джет» и RSA KEON позволила обеспечить централизованную обработку сертификатов открытых ключей на базе единого Управляющего Центра (УЦ) PKI, упростить мониторинг и администрирование, повысить управляемость всей системы информационной безопасности.

Кроме того, единый УЦ PKI позволяет более широко использовать ключевые носители eToken, выдаваемые мобильным пользователям VPN «Тропа-Джет». Теперь мобильные пользователи VPN «Тропа-Джет» могут с помощью одного носителя eToken не только подключаться к VPN, но и воспользоваться дополнительными сервисами безопасности, реализуемыми PKI-системой, а именно: шифровать и подписывать электронную почту, получать авторизованный доступ к рабочим станциям, сетевым серверам и Web-порталам, устанавливать электронно-цифровые подписи на документы и многое другое.

Следует отметить, что при доработке VPN «Тропа-Джет» сохранена возможность полностью автономного функционирования VPN-сети как при наличии внешней PKI-системы, так и без нее.

Интеграция продуктов компании «Инфосистемы Джет» с PKI-системами — это новый шаг к повсеместному внедрению сервисов информационной безопасности и повышению уровня защищенности информационных систем современных предприятий и организаций.

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

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*

Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555