Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 2 (141)/2005

КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-РЕСУРСОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-РЕСУРСОВ

Олег Слепов,
консультант по информационной безопасности

Алексей Отт,
ведущий разработчик программного обеспечения

СОДЕРЖАНИЕ

Сегодня трудно переоценить значение Интернета в жизнедеятельности компаний, организаций или предприятий. С каждым днем этот сервис занимает все более значительное место. Интернет становится основным бизнес-инструментом, реально приносящим прибыль.

Главная задача Интернета осталась той же, что и во времена его зарождения — накопление, хранение, распределение и обмен разнородной информацией. Но инфраструктура, используемая для решения этой задачи, значительно изменилась. Если раньше Интернет был всего лишь объединением некоторого количества локальных сетей, то сегодня это многокомпонентная комплексная структура, охватывающая весь мир. При этом кардинально улучшилось качество обмена информацией: люди, находящиеся в разных концах планеты, без ощутимых задержек связываются друг с другом и обмениваются информацией.

За годы своего существования Интернет стал выполнять множество различных функций. В первую очередь, это средство связи, обладающее важнейшими достоинствами, среди которых оперативность, надежность, способность накапливать информацию, возможность контролировать процесс коммуникации, влиять на его качество и т.п.

Сегодня Интернет — неотъемлемая часть многих бизнес-процессов. Он стал местом и одновременно средством взаимодействия субъектов рыночных отношений — товаропроизводителей, продавцов и покупателей. Наиболее показательными примерами этого являются элек-

тронная коммерция (e-Commerce) и Интернет-банкинг (Internet banking).

Говоря об электронной коммерции, чаще всего имеют в виду розничную торговлю через Интернет. У всех на слуху такие известные Интернет-магазины как dostavka.ru, ozon.ru и т.п. Но не следует забывать о возможностях, предоставляемых Интернетом для ведения более широкой межкорпоративной коммерции. До последнего времени основное внимание в этой области сетевой торговли уделялось корпоративным коммерческим порталам фирм Cisco и Dell Computer, на которых корпоративные клиенты заказывали оборудование, минуя посредников. Но и эти порталы еще мало отличались от розничных Интернет-магазинов. Сегодня же мы говорим о целых электронных торговых площадках (B2B-площадки[1]), которые «посредничают» между покупателями и продавцами, поддерживая между ними информационный обмен.

Интернет-банкинг — это комплекс банковских услуг, предоставляемых в режиме он-лайн: информирование клиента о состоянии его счетов, удаленное управление счетами; внутри- и межбанковские переводы, оплата коммунальных услуг, покупка/продажа безналичной валюты; кредитование, операции с ценными бумагами, управление личными финансами и т.п.

Да и сам Интернет давно уже превратился в своеобразный рынок, на который работают целые отрасли промышленности, создавая потребляемые им товары и услуги.

Таким образом, Интернет стал рабочим инструментом, без которого уже невозможно представить себе повседневную деятельность множества людей. Это и глобальная справочно-информационная система, и способ доступа к технологиям, и транспорт для передачи данных, и, наконец, оперативное и доступное средство коммуникации.

Риски, связанные с использованием Интернет-ресурсов

Одной из особенностей Интернета является то, что на определенном этапе он развивался стихийно. Это, с одной стороны, обеспечило массовый характер его использования, а с другой — породило ряд проблем с серьезными последствиями.

Первое: поскольку Интернет является каналом во внешний мир, он стал основным **источником распространения вредоносного мобильного кода** (вирусов, червей, троянских программ).

Второе: глобальная сеть стала использоваться в качестве **канала, через который осуществляются атаки** на локальные вычислительные сети организаций, отдельные серверы и компьютеры. Многие Интернет-ресурсы включают в себя различный программный код — JavaScript, Flash, ActiveX и другие. Злоумышленники могут эксплуатировать этот код для организации атак на корпоративные сети и пользовательские рабочие места.

Третье: Интернет стал активно применяться в качестве **средства скрытого проникновения** в корпоративные локальные вычислительные сети.

Четвертое: в настоящее время Интернет может рассматриваться как один из основных **каналов утечки конфиденциальной информации**. Например, информационные ресурсы компаний подвергаются серьезным угрозам из-за использования сотрудниками этих компаний бесплатных почтовых ящиков. Согласно статистике, в среднем 80% сотрудников различных компаний помимо внутренних корпоративных почтовых адресов активно используют бесплатные почтовые ящики, предоставляемые различными провайдерами (yandex.ru, hotmail.com, mail.ru, mail.yahoo.com и т.п.). Имея доступ к Интернету со своего рабочего места и зная, что канал не контролируется, любой пользователь может беспрепятственно отправить за пределы организации любую конфиденциальную информацию. Но даже понимая это, только каждая четвертая компания запрещает использовать

1 B2B-площадка (Business to business marketplace) — «место» (сайт), где в режиме он-лайн заключаются сделки между предприятиями-покупателями и предприятиями-продавцами. Системы B2B обеспечивают концентрацию, маршрутизацию и коммутацию информационных потоков между субъектами информационного обмена. Согласно исследованиям, проведенным компанией Brunswick Warburg, рост российского B2B-рынка только в 2004 году составил 245%. В настоящее время, когда около 90% крупнейших российских предприятий имеют доступ к Интернету, количество B2B-площадок уже превышает сотню.

бесплатные почтовые сервисы, а три четверти позволяют своим сотрудникам решать, как и какую информацию отправить за пределы компании.

Пятое: бесконтрольный доступ к Интернету **значительно снижает производительность труда** в коллективе. Простота освоения, легкость поиска необходимой информации и другие полезные качества Интернета — вот причины того, что данный сервис широко применяется, в том числе и для личных целей. Не секрет, что у многих уже давно появилась привычка начинать рабочий день с чтения новостей, просмотра сводок погоды и т.п. По данным компании IDC, около трети своего рабочего времени сотрудники различных организаций и компаний проводят в Интернете в целях, не имеющих прямого отношения к их работе. Это и «походы» в Интернет-магазины, и сетевые игры, и просто поиск информации.

Наконец, еще одно следствие неконтролируемого использования Интернета — это **снижение пропускной способности сети**. Согласно статистике, 44% сотрудников организаций используют корпоративные ресурсы для просмотра видео, прослушивания аудиозаписей (через потоковые аудио- и видеоканалы), играют в сетевые игры, загружают файлы большого объема (например, файлы мультимедиа: графические, музыкальные файлы, фильмы и т.п.), что создает значительную нагрузку на локальные вычислительные сети.

Решение проблемы безопасного использования Интернет-ресурсов

Проблему безопасного и продуктивного использования Интернет-ресурсов можно решить двумя способами. Первый — радикальное запрещение использования Интернета без необходимости. Если принят принцип «запрещено все, что явно не разрешено», пользователям разрешается доступ только к строго определенным сайтам. Второй способ — более гибкий, он позволяет пользователям действовать по принципу «разрешено все, что не запрещено». В этом случае сотрудник может свободно пользоваться ресурсами Интернета, однако его действия находятся под контролем. Это значит, что если пользователь выполнит действия, противоречащие политике безопасности, это будет обнаружено и пресечено.

В настоящее время «радикальный» способ по-прежнему находит применение. Он используется, в первую очередь, организациями, в которых циркулирует информация с грифом «секретно». К таким организациям относятся различные научно-исследовательские институты, военные организации, государственные органы и специальные службы. В таких «секретных» организациях существуют инструкции и документы, которые строго регламентируют поведение пользователей, связанное с получением информации и ее передачей за пределы организации. А это значительно облегчает деятельность контролирующих служб по обеспечению должного уровня защиты.

Другой пример «радикального» способа — применение в компаниях так называемых Интернет-киосков, когда пользователям предоставляется доступ к Интернет-ресурсам через выделенные терминалы. Как правило, в этом случае действия пользователей строго регламентируются, а трафик, проходящий через данный терминал, контролируется специальными средствами.

Большинство же коммерческих организаций и компаний предпочитают более гибкий способ регламентации общения с внешним миром. Далее рассматривается именно этот способ, поскольку именно при его применении возникают существенные проблемы. И состоят они в том, что практически невозможно однозначно определить, к какой информации следует запретить доступ.

Чтобы обеспечить гибкий контроль использования Интернет-ресурсов, необходимо ввести в компании соответствующую политику использования ресурсов. Эта политика может реализовываться как «вручную», так и автоматически. «Ручная» реализация означает, что в организации имеется специальный штат сотрудников, которые в режиме реального времени или по журналам маршрутизаторов, прокси-серверов или межсетевых экранов ведут мониторинг активности пользователей. Естественно, такой мониторинг является проблематичным, поскольку требует больших трудозатрат. Кроме того, он требует не только отслеживания активности пользователя, но и категоризации сайтов, которые посещают пользователи, а провести работу по категоризации сайтов силами сотруд-

ников ИТ-подразделения отдельной компании практически невозможно.

Чтобы избежать описанных выше проблем и обеспечить гибкий контроль использования Интернет-ресурсов, компания должна дать администратору инструмент для реализации политики использования ресурсов компании. Этой цели служит так называемая **контентная фильтрация**[2]. Ее суть заключается в декомпозиции объектов информационного обмена на компоненты, анализе содержимого этих компонентов, определении соответствия их параметров принятой в компании политике использования Интернет-ресурсов и осуществлении определенных действий по результатам такого анализа. В случае фильтрации веб-трафика под объектами информационного обмена подразумеваются веб-запросы, содержимое веб-страниц, передаваемые по запросу пользователя файлы и т.д.

Объективная потребность вызвала к жизни множество программных продуктов, предназначенных для контроля содержимого информационного обмена. Все они в той или иной степени выполняют возложенную на них задачу. Однако необходимо иметь в виду, что никакая автоматическая система не дает 100% гарантии безопасности без деятельного участия человека в процессе фильтрации. Любая технология — только дополнительный инструмент в руках администратора. И от того, насколько система адекватна задачам, которые ставит перед собой администратор, будет зависеть, удастся ли снизить уровень рисков, связанных с использованием Интернета.

Средства контроля использования Интернет-ресурсов

В этом разделе кратко описаны имеющиеся на рынке средства фильтрации веб-трафика. Эти средства можно условно разделить по типам и методам фильтрации. В настоящее время известно три типа средств, способных в той или иной степени обеспечить контроль использования Интернет-ресурсов на корпоративном уровне. К первому типу относятся межсетевые экраны, прокси-серверы, маршрутизаторы и подобные им средства фильтрации. Второй тип — это современные антивирусные программы, обладающие базовыми возможностями контентной фильтрации. К третьему типу относятся специализированные средства, разработанные непосредственно для контроля использования Интернет-ресурсов.

Каждый тип средств контроля использования Интернет-ресурсов предназначен для фильтрации на разных уровнях сетевой иерархии. Средства первого и второго типов напрямую не предназначены для контроля содержимого информационного обмена по каналам Интернета. Так, межсетевые экраны, прокси-серверы и маршрутизаторы осуществляют фильтрацию трафика на сетевом и транспортном уровнях. Специализированные средства контентной фильтрации осуществляют ее на прикладном уровне. Если говорить об антивирусных программах, то со средствами третьего типа их объединяет именно способность осуществлять некоторые базовые функции контентной фильтрации.

В общем, средства первого и второго типов можно считать достаточно эффективными для компаний, в которых контроль содержимого информационного обмена не является первостепенной задачей (например, там, где конфиденциальная информация не циркулирует в корпоративной сети). В организациях же, где активно используется Интернет и при этом актуальны задачи контроля доступа пользователей к Интернет-ресурсам и защиты от утечки конфиденциальной информации, применение таких средств недостаточно. Это обусловлено следующими недостатками средств первого и второго типов:

- ограниченное количество параметров, по которым возможна фильтрация трафика;
- ограниченные возможности по фильтрации текста в запросах пользователей и загружаемых страницах;
- невозможность декомпозиции объектов информационного обмена, следовательно, отсутствие более глубокой фильтрации (например, тип файлов определяется по декларированному, а значит, не обязательно реальному расширению, при этом отсутству-

2 От английского «content filtering». Используются также термины «фильтрация по содержимому» и «технология контроля содержимого информационного обмена». Все эти термины равнозначны и могут заменять друг друга.

ют средства для определения реального типа файла по сигнатуре);
- отсутствие необходимой гибкости при реализации политики использования Интернет-ресурсов;
- отсутствие функциональности, обеспечивающей контентную фильтрацию. Например, не все межсетевые экраны и прокси-серверы поддерживают контроль передаваемых данных на уровне команд протоколов.

Специализированные программные средства контроля использования Интернет-ресурсов предназначены для проверки передаваемых данных на соответствие тем или иным условиям информационного обмена и выполнения соответствующих действий по итогам проверки. Программное обеспечение этого типа можно разделить по месту использования на клиентское и серверное. Клиентское программное обеспечение работает на каждой рабочей станции, где требуется обеспечить контроль использования Интернет-ресурсов.

Применение клиентского программного обеспечения в организациях неэффективно, исключая отдельные специфические случаи. Клиентское программное обеспечение постоянно работает на компьютере пользователя и ненадежно с точки зрения безопасности, поскольку потенциально его конфигурация и настройки могут быть искажены (подделаны) опытным пользователем или специализированным вредоносным кодом. Кроме того, такое программное обеспечение требует больших трудозатрат на настройку и сопровождение, поскольку эти операции осуществляются для каждой рабочей станции в отдельности.

В корпоративной среде наиболее эффективно применение программного обеспечения, функционирующего на выделенном сервере, поскольку оно разработано специально для использования в корпоративных сетях и наиболее полно соответствует требованиям по функциональности и безопасности. К таким требованиям относятся:
- централизованное размещение (обеспечивает удобство установки, настройки и сопровождения);
- размещение на сервере и ограничение доступа к настройкам ПО (обеспечивает безопасность, поскольку исключена возможность изменения настроек пользователями).

Классификация корпоративных средств контроля использования Интернет-ресурсов

Далее рассматриваются **серверные** (а значит, **корпоративные**) **средства фильтрации веб-трафика**. Говоря об их классификации (см. рис. 1), необходимо выделить основные признаки, по которым они различаются:
- используемые методы фильтрации;
- место размещения в инфраструктуре сети и способ воздействия на трафик (технологии pass-by и pass-through);
- возможность выбора режима функционирования — standalone (автономные) и integrated (встраиваемые);
- глубина политики фильтрации;
- подход к оповещению о действиях пользователей;
- возможность генерации различных видов отчетов по данным фильтрации.

Когда говорят о классификации по методам фильтрации, классы определяются набором параметров, по которым производится проверка содержимого информационного обмена. Системы используют различные наборы проверок в зависимости от возложенных на средства фильтрации задач.

Наиболее типичны и распространены системы, в которых основным способом фильтрации веб-трафика является проверка адресов Интернет-ресурсов (URL). Конечно, эти системы применяют и другие способы (фильтрация по командам протоколов, именам пользователей, IP-адресам рабочих станций и типам файлов), однако именно результат проверки адреса сайта служит основанием для решения о блокировании сайта. Такие системы, как правило, фильтруют только запросы пользователей, не проверяя загружаемые сайты на наличие запрещенного политикой безопасности содержимого.

Существуют системы, в которых реализован комплексный подход к фильтрации трафика. В них проверки равноценны по значимости, а состав набора проверок определяется задачами, возлагаемыми на систему контроля. Отличием таких систем является то, что они обладают наиболее широким набором проверок, среди которых одной из важнейших является проверка содержания текста запросов и сайтов.

Существующие системы различаются по месту размещения в корпоративной сети. Их можно разделить на две крупные группы — работающие как прокси-серверы (технология

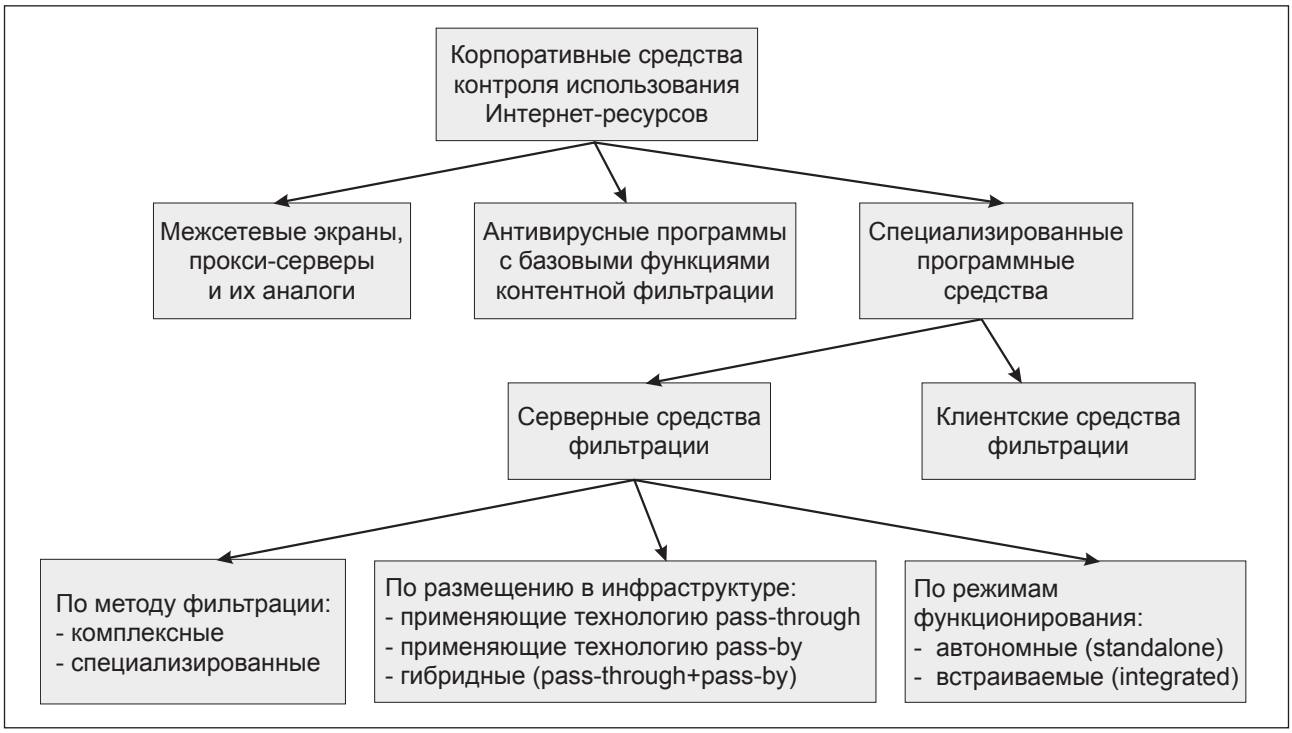

Рис.1. Классификация корпоративных средств контроля использования Интернет-ресурсов

pass-through) и работающие как анализаторы пакетов (packet sniffer), перехватывающие пакеты нужных протоколов и проверяющие их на наличие запрещенного содержимого (технология pass-by).

Системы, использующие технологию pass-through, работают как обычные HTTP-прокси. Как правило, их устанавливают между клиентскими местами и внешним прокси-сервером или межсетевым экраном. Клиентские места должны быть настроены так, чтобы они использовали нужный прокси-сервер.

К достоинствам систем, использующих технологию pass-by, можно отнести их прозрачность для пользователя и возможность установки без перенастройки клиентских мест. Недостатком является то, что они не всегда могут справляться с большим потоком данных, передаваемых по контролируемым протоколам.

Говоря о режимах функционирования системы, различают автономные (standalone) и встраиваемые решения (integrated). Автономные системы, устанавливаемые «в разрыв» и работающие независимо от других подсистем, более надежны с точки зрения качества фильтрации. В них возможность ошибок при фильтрации снижена до минимума за счет полного контроля над передаваемыми данными. Обычно такие решения используются совместно с внешними прокси-серверами в целях увеличения скорости доступа за счет кэширования данных[3].

Некоторые компании поставляют программное обеспечение для контроля использования Интернет-ресурсов в виде встраиваемых модулей к существующим прокси-серверам или межсетевым экранам. Достаточно часто модули фильтрации создаются для широко используемого прокси-сервера Microsoft ISA.

Кроме того, некоторые системы фильтрации поставляются в виде отдельных серверов, а доступ к ним осуществляется по протоколу ICAP, который является стандартом для контроля и модификации запросов и ответов, проходящих через прокси-сервер, поддерживающий данный протокол. Достаточно часто в виде ICAP-серверов реализуются антивирусные комплексы (Symantec Antivirus, Dr.Web, TrendMicro). К достоинствам продуктов, реализованных в виде таких серверов, можно отнести то, что они могут взаимодействовать с разными типами прокси-серверов и межсе-

3 Кэширующий прокси-сервер — это программа, позволяющая ускорить доступ к WWW- и FTP-сайтам за счет кэширования данных, запрошенных различными клиентами на одном и том же ресурсе. Использование кэширующих прокси-серверов в системах контроля Интернет-ресурсов дает некоторые преимущества, поскольку позволяет уменьшить следующие показатели:
- время доступа к сайтам (среднее время доступа при попадании в кэш — 0,04 с; при загрузке из Интернета — 1,7 с);
- нагрузку на канал связи (удешевляет доступ): HTTP-пакеты составляют 70-80% трафика и кэшируются минимум на 20%).

тевых экранов, которые реализуют функцию клиента ICAP, а также то, что серверы могут выполнять проверку только определенных типов данных. Недостатком этого подхода следует считать то, что при использовании протокола ICAP сервер фильтрации может не иметь полного контроля над передаваемыми данными.

Как выбирать систему?

Каков же определяющий фактор при выборе средств фильтрации веб-трафика? Ответ прост — функциональность. Именно этим и различаются представленные на рынке средства контроля использования Интернет-ресурсов. А вот какую именно функциональность выбрать, зависит от задач, стоящих перед организацией.

В идеале специализированные средства фильтрации веб-трафика должны реализовывать следующие функции:

1. проверка адресов Интернет-ресурсов;
2. проверка текстов в передаваемом потоке на наличие запрещенного содержимого (по возможности, с извлечением текста из файлов разных форматов, таких как Microsoft Word/Excel и т.п.);
3. антивирусная проверка;
4. проверка типов передаваемых данных;
5. проверка объема передаваемых данных/предоставление квот на загрузку;
6. проверка присвоенной сайту категории;
7. проверка сайта на соответствие определенному рейтингу;
8. проверка прав доступа пользователей с помощью различных методов аутентификации;
9. проверка времени доступа пользователей к разным категориям ресурсов/предоставление временных квот;
10. поддержка фильтрации HTTPS-трафика;
11. определение разных политик фильтрации для разных направлений передачи данных;
12. определение разных политик фильтрации для разных групп пользователей;
13. модификация или замена передаваемых данных;
14. уведомление администраторов безопасности о нарушении политики безопасности;
15. сохранение всего или части исходящего из организации трафика с возможностью последующего анализа;
16. возможность анализа качества и эффективности политики использования Интернет-ресурсов;
17. возможность масштабирования системы контроля.

Проверка адресов Интернет-ресурсов

Один из основных способов фильтрации веб-трафика — проверка адресов Интернет-ресурсов. Речь идет о фильтрации по URL, «универсальному локатору ресурсов», который представляет собой полный путь к конкретному документу или разделу на сервере или компьютере, подключенном к Интернету. Используя данный способ фильтрации, можно запретить доступ как ко всему сайту или домену, так и к его части или отдельной странице. Рекомендуется выбирать средства фильтрации, которые способны обеспечить блокировку доступа и в том случае, когда пользователь вместо полного URL указывает только IP-адрес сервера или компьютера в сети.

Системы контроля использования Интернет-ресурсов, применяющих данный способ фильтрации, используют специальный сервис по категоризации сайтов. Такой сервис предоставляется по подписке провайдерами Интернет-услуг или компаниями, производящими системы контроля использования Интернет-ресурсов. Основу сервиса составляет база данных URL, которая постоянно обновляется и пополняется. Эта работа производится в специальных лабораториях и позволяет создавать актуальную и относительно полную базу данных адресов Интернет-ресурсов. При выборе системы контроля использования Интернет-ресурсов необходимо учитывать, входит ли в поддержку такой системы предоставление сервиса категоризации. Наиболее ценной при этом является функция категоризации сайтов по запросу. Она включает в себя обязательную организацию обратной связи между клиентом и компанией, занимающейся категоризацией. Это позволяет клиенту в случае появления нового сайта, не указанного в базе данных URL, посылать запрос на категоризацию данного сайта и включать его в базу данных URL.

Для доступа к базам данных URL, как правило, используется специальное программное обеспечение, представляющее собой интерфейс между компьютером клиента с установленной на нем системой контроля использования Интернет-ресурсов и сервером базы данных URL компании-провайдера.

Основной недостаток метода проверки адресов Интернет-ресурсов заключается в том, что базы данных URL заведомо неполны из-за огромной скорости расширения сети Интернет. Ежедневно возникают сотни новых веб-ресурсов, к которым могут получать доступ пользователи. Отследить появление доменов второго уровня

типа www.mysite.ru вполне возможно с помощью баз данных регистраторов. Но как отследить домены третьего, четвертого и прочих уровней? Сайты типа sport.moiportal.ru появляются без всякой регистрации, а содержание поддоменов и каталогов (например, www.moisait.ru/soft) часто не соответствует тематике главной страницы и должно быть отнесено к другой категории.

Многие системы контроля доступа к Интернет-ресурсам используют проверку адреса сайта как основную для принятия решения о его блокировании. Однако необходимо иметь в виду, что Интернет — очень быстро меняющаяся среда. Даже такие гиганты веб-поиска как Google, Altavista или Yahoo зачастую «не знают» и половины всех существующих ресурсов. Сайты часто меняют свое содержание или местоположение, да и новые страницы появляются с поражающей быстротой. Все это обуславливает крайне низкую эффективность фильтрации по адресам Интернет-ресурсов. Выбирая систему фильтрации, необходимо учитывать то, что анализ веб-трафика должен быть комплексным и включать если не все, то большинство из перечисленных выше проверок. В частности, это касается проверки запросов на наличие запрещенного содержимого.

Проверка текстов на наличие запрещенного содержимого

Качество фильтрации значительно повышается за счет контроля веб-трафика на наличие запрещенного содержимого в текстах. Здесь подразумевается проверка на наличие ключевых слов и выражений. Очень важно, чтобы анализировалось содержание не только страниц сайтов, но и запросов пользователей или любой другой передаваемой ими по сети информации. Это, например, необходимо при контроле переписки пользователей, использующих бесплатные почтовые ящики.

Практика показала, что наиболее эффективны системы, использующие так называемый нейро-лингвистический анализ текста. В данном случае речь идет о подходе к реализации ряда функций автоматической обработки, основанном на использовании ассоциативной семантической сети для оценки сверхфразового строения текста.

Кроме того, обычная проверка наличия определенного текста по словарям не должна состоять только из простого сравнения. Качество фильтрации значительно повышается при использовании методики, согласно которой словам и выражениям присваиваются «весовые» категории. Это обеспечивает гибкость при фильтрации по ключевым словам и выражениям.

Одним из основных критериев оценки систем контентной фильтрации для российского рынка является поддержка продуктом различных кодировок кириллицы, что дает возможность анализа русскоязычных текстов. Большинство продуктов иностранного производства не поддерживают кодировки кириллицы, а это значительно снижает пользу от их применения в РФ. Ситуация усложняется еще и тем, что разные части загружаемых сайтов могут иметь различные кодировки. Вдобавок эти кодировки не всегда указаны верно. Большинство систем определяет кодировку по MIME-типу, что приводит к ошибкам. На помощь приходит технология эвристического анализа, то есть специальные алгоритмы анализа последовательности символов, типичных для той или иной кодировки. Такой анализ позволяет практически стопроцентно определить, в какой кодировке написан текст.

Проверка прав доступа пользователей

Выбор системы контроля веб-трафика зависит от того, способна ли система обеспечить проверку прав доступа пользователей. Но обычно такая проверка осуществляется либо внутренними средствами, либо с помощью интегрированной подсистемы аутентификации.

Таким образом, аутентификация пользователей может производиться следующими способами:

- с использованием различных методов аутентификации: RADIUS, TACACS+, NTLM, LDAP;
- с использованием различных баз данных и служб каталогов: Java System Directory Server (Sun Microsystems), Active Directory (Microsoft), eDirectory (Novell);
- с использованием различных внутренних и внешних баз данных.

Антивирусная проверка

Одна из основных задач, возлагаемых на средства контентной фильтрации, — защита от вирусов. Такая защита может осуществляться как встроенными средствами, так и с помощью внешних систем. При выборе систем контроля использования Интернет-ресурсов необходимо учитывать, использует ли данная система результаты антивирусной проверки при дальнейшем анализе трафика. Наличие такой функции позволяет адаптировать политику использования Интернет-ресурсов и избегать, например, за-

грузки данных с тех сайтов, откуда ранее был получен вредоносный мобильный код.

Проверка типов передаваемых данных

Ограничение по типам передаваемых данных может иметь важное значение для многих организаций. Так, можно установить запрет на отправку за пределы организации данных в форматах, отличных от простого текста, например, файлов Microsoft Word и Excel, которые могут содержать важную информацию. При этом тип файла не должен определяться по информации, указанной в запросе или ответе, т.е. по расширению файла или MIME-типу, указанному сервером. Для точной обработки данных система контроля должна определять тип файла по его сигнатуре. Требование определения типа файла по сигнатуре обусловлено еще и тем, что большинство веб-серверов при передаче данных объявляют MIME-тип, ориентируясь на расширение файла, что может быть неправильным из-за неверного указания типа в файле соответствий[4] или переименования файла пользователем.

Проверка размера передаваемых данных/квоты на загрузку файлов

Для обеспечения нормальной работы каналов передачи данных может потребоваться ограничение объемов данных, загружаемых пользователями, поскольку при передаче больших файлов пользователь может занять весь канал, из-за чего доступ других пользователей будет затруднен. Поэтому система контроля должна иметь возможность ограничивать объем передаваемых данных или ограничивать полосу пропускания, выделяемую для отдельного пользователя.

На практике это выглядит следующим образом: устанавливается предельный объем данных, который разрешается ежедневно загружать пользователям (при необходимости пользователи оповещаются об этом). Реализовать данную функциональность помогает квотирование по объему передаваемого трафика. Это дает пользователю возможность самому следить за размером загружаемых файлов.

Проверка присвоенной сайту категории

Производители ПО, как правило, предоставляют услугу категоризации сайтов в качестве одного из элементов технической поддержки продукта. Категоризация осуществляется непосредственно в лингвистических лабораториях производителей и предоставляется по подписке.

Выбирая провайдера данных услуг, важно учитывать полноту и объемы предоставляемых баз данных категорированных сайтов. При этом необходимо, чтобы категоризация осуществлялась с учетом области деятельности заказчика и его представления о том, к какой категории следует относить тот или иной сайт. Ведь один и тот же Интернет-ресурс разными заказчиками может быть отнесен к различным категориям. Например, для банка сайт Интернет-магазина не может представлять информационной ценности, тогда как оптовые компании постоянно используют подобные ресурсы в своей повседневной деятельности.

Серьезным недостатком услуги категоризации является жесткая привязка Интернет-ресурса к его категории. То есть один и тот же ресурс не может принадлежать к нескольким категориям. Но иногда при построении гибкой политики использования Интернет-ресурсов в этом возникает необходимость. В частности, в одной и той же компании в соответствии с политикой безопасности доступ к определенному ресурсу может быть разрешен одним пользователям и запрещен другим.

Проверка времени доступа к ресурсам/ предоставление временных квот

Простой запрет доступа к некоторым ресурсам неудобен в тех случаях, когда требуется предоставить пользователю доступ к ресурсам, но только в определенное время, например, разрешить загружать большие файлы с обновлениями программ только в вечернее время, когда повышенная загрузка каналов из-за большого объема передачи не вызовет затруднений при доступе в Интернет других пользователей. Поэтому в системах контроля доступа к Интернет-ресурсам должны присутствовать средства, обеспечивающие запрещение или разрешение доступа к определенным ресурсам в определенное время, то есть по расписанию.

Кроме того, в некоторых случаях необходимо выделить пользователям квоты на использование определенных Интернет-ресурсов. Например, за день разрешается «провести» на новостных сайтах 30 минут. Пользователь может сделать это сразу, выбрав свою дневную квоту, а может читать новости 6 раз по 5 минут в течение дня. Некоторые средства контроля использования Интернет-ресурсов располагают такой возможностью, что значительно повышает производительность труда сотрудников. При этом со-

4 Так, например, файлы с расширением .rpm одними веб-серверами объявляются как `application/x-rpm`, а другими как `audio/x-pn-realaudio-plugin`.

храняется демократичный подход, который благотворно сказывается на климате в коллективе.

Политика фильтрации для разных направлений передачи данных

Чтобы создаваемая политика доступа к Интернет-ресурсам была эффективной, средства контроля должны обеспечивать возможность задавать разные условия проверки для разных направлений передачи данных и команд протоколов. При наличии такой функциональности можно, например, запретить передачу документов Microsoft Word из организации, при этом разрешая загружать документы этого формата. Эту функциональность можно использовать не только для контроля типов данных, но и для проверки содержимого на наличие запрещенных слов или объема передаваемых данных.

Многие из имеющихся на рынке систем обеспечивают фильтрацию только исходящего трафика, т.е. запросов пользователя, совершенно не уделяя внимания проверке информации, загружаемой на стороне клиента. Это в значительной степени снижает гибкость реализуемой политики использования Интернет-ресурсов, поскольку требует жесткого ограничения доступа пользователей к сайтам. Существуют сайты, на которых часть информации может относиться к категории «запрещенной», а часть — к «разрешенной». Именно на этапе ответа на запрос пользователя возможно разделение на «запрещенное» и «разрешенное» содержание. При этом полезна возможность модификации данных, речь о которой пойдет в следующем разделе.

Модификация или замена передаваемых данных

Иногда полезно предоставить пользователю доступ к данным, например, к странице на вебсервере, но удалить из этих данных какую-либо часть, которая нарушает политику безопасности или может привести к проникновению вредоносного кода в корпоративную сеть. Хороший пример такого подхода — анализ на предмет потенциальной опасности JavaScript, находящегося на странице, и удаление соответствующих частей страницы[5]. Чтобы исключить возможность описанных выше нарушений, системы контроля должны иметь в своем составе средства замены и модификации передаваемых данных.

Политика фильтрации для разных групп пользователей

Средство контроля доступа должно различать пользователей, доступ которых к внешним ресурсам оно контролирует. Если при этом система контроля позволяет «привязать» к пользователю или группе пользователей отдельную политику безопасности, то такой инструмент поможет создать гибкую политику безопасности, что обеспечит эффективную работу с передаваемыми данными. Кроме того, необходима возможность создания правил, которые будут применяться ко всем пользователям, например, правила для проверки передаваемых данных на наличие вредоносного содержимого.

Поддержка фильтрации HTTPS-трафика

Многие сайты для обеспечения безопасности передаваемых данных (таких как пароли, номера кредитных карт и т.п.) предлагают пользователю доступ к сайту по протоколу HTTPS, который шифрует все передаваемые данные.В настоящее время некоторые сайты, предоставляющие бесплатные почтовые ящики, тоже стали предлагать доступ по протоколу HTTPS. Для организации такая услуга может оказаться достаточно серьезной опасностью, поскольку через этот канал может произойти утечка конфиденциальной информации. Поэтому система контроля веб-трафика должна поддерживать обработку зашифрованных данных.

Система уведомлений о нарушении политики безопасности

Оповещение администратора о нарушениях политики безопасности и прочих событиях является достаточно важной частью системы контроля доступа пользователей к Интернет-ресурсам. В различных системах подсистемы оповещения отличаются друг от друга.

В зависимости от настройки системы оповещаться о нарушениях политики может либо администратор, либо пользователь. Обычно пользователю выдается специальным образом оформленная страница с сообщением о том, что ресурс, к которому пользователь обращается, входит в список запрещенных. Такое действие системы называется «уведомление с подтверждением» и является довольно значимой функцией, позволяющей предотвратить ошибочные действия пользователей[6], не прибегая к помощи администратора и не используя дополнительных ресурсов системы. Оповещение админист-

5 Кроме этого, такую функциональность можно использовать для блокирования рекламных объявлений, использующих технологию Flash.

ратора безопасности может производиться различными способами:

- по электронной почте;
- через интерфейсы к внешним подсистемам оповещения (SNMP, SMS, и т.п.);
- путем мониторинга в режиме реального времени.

Мониторинг в режиме реального времени предполагает интерактивный просмотр событий, происходящих в системе. Он реализуется во многих системах контроля веб-трафика и позволяет в режиме реального времени наблюдать за работой пользователей, а также просматривать сетевой трафик в момент его прохождения, выявляя проблемные соединения.

Такой мониторинг требует многоуровневой настройки и включает следующие параметры: страницы, категории, разрешенные/запрещенные страницы, имена пользователей. Цветовая маркировка позволяет быстро определить, к какой категории принадлежит сайт. Кроме прочего, такой мониторинг позволяет в случае необходимости оперативно модифицировать политику безопасности.

Возможность последующего анализа трафика

Для администратора системы контроля трафика может быть полезной возможность анализа переданных данных уже после их передачи. В первую очередь это может касаться данных, переданных из организации во внешний мир. Например, система контроля может сохранять данные, переданные с помощью команды **POST** протокола HTTP в базу данных или в файлы на диске, и предоставлять администратору интерфейс для последующего их анализа. Имея такой инструмент, администратор может корректировать политику безопасности или анализировать передаваемую информацию.

В отношении данных, получаемых из внешних источников, такая функциональность, возможно, неэффективна из-за их большого объема. Однако может быть полезен контроль передаваемых данных для отдельных групп сотрудников. Но анализ большого количества данных может оказаться очень трудоемкой работой и должен производиться только в редких случаях.

Способы представления статистических данных

Применение системы контроля использования Интернет-ресурсов нельзя представить без анализа событий, происходящих в системе. Администраторам необходимо оперативно получать информацию о текущем состоянии системы, а также сводные отчеты об использовании Интернет-ресурсов пользователями или группами пользователей. Такая информация позволяет не только контролировать использование Интернет-ресурсов, но и проверять эффективность политики безопасности и динамически адаптировать ее к изменяющимся условиям и задачам. Поэтому в большинстве существующих средств контроля использования Интернет-ресурсов есть возможность формирования статистических отчетов, а также интерактивного наблюдения за доступом к внешним ресурсам.

Существует несколько способов представления статистических данных о трафике. Первый способ предполагает использование внутренних возможностей продукта, то есть встроенной системы генерации отчетов. Как правило, в состав такой системы входят подсистема генерации отчетов и база данных, в которую в виде журналов записывается вся информация о событиях, а также некоторые запросы пользователей (например, команды **POST**). С помощью внутренних средств производятся SQL-запросы к базе данных, результаты которых дают наглядную картину трафика и действий пользователей. При этом могут создаваться типовые запросы (например, «100 часто загружаемых сайтов», «100 пользователей, переславших наибольшие объемы данных за указанный период», «100 самых активных пользователей» и т.п.) с изменяемыми параметрами (например, по дате и времени).

Другой способ предполагает получение отчетов с помощью стандартных средств, таких как Crystal Reports, Oracle Reports и т.п. Эти средства интегрируются с системой контроля использования Интернет-ресурсов и тоже используют базу данных, которая создается в результате фильтрации трафика. Способность интегрироваться с различными стандартными средствами создания отчетов и должна определять выбор системы контроля веб-трафика.

Имеющиеся на рынке системы контроля также различаются по возможностям представления отчетов в различных форматах. К наиболее популярным форматам можно отнести PDF, HTML, MS Word, MS Excel, MS Access.

Достоинством систем контентной фильтрации является наличие такой функциональностикак возможность удаленного просмотра отчетов через Интернет. При этом важно, чтобы та-

6 Согласно статистике, 65% утечек конфиденциальной информации из корпоративных сетей происходит из-за неумелых или ошибочных действий пользователей.

кой доступ был обеспечен по закрытым каналам, поскольку данная информация во многих случаях является конфиденциальной.

И наконец, достоинством систем контроля использования Интернет-ресурсов, которые имеют возможность накапливать статистическую информацию и обрабатывать ее, является способность вести историю использования Интернет-ресурсов конкретным пользователем или группой пользователей за определенный период с указанием объема передаваемых данных.

Проверка сайта на соответствие определенному рейтингу

Некоторые компании предлагают сервис, который «выставляет» тому или иному сайту определенный рейтинг. Автоматическая система стандартизации (например, PICS — Platform for Internet Content Selection — компании W3C) встраивает в данные, доступные на сайте, специальную метку, которая может учитываться как серверными программами, так и обычными браузерами. На основе данных рейтингов можно обеспечивать управление доступом к различным Интернет-ресурсам.

Возможность масштабирования системы контроля

В связи с ростом пропускной способности Интернет-каналов становится важным вопрос о масштабировании системы контроля веб-трафика. Должна быть предусмотрена возможность расширения пропускной способности системы контроля, ее размещения на нескольких серверах для балансировки нагрузки и обеспечения безотказной работы. При использовании многомашинной конфигурации выход из строя одного из серверов не приведет к отказу всего сервиса, что значительно повышает надежность системы.

Кроме того, масштабирование системы может предусматривать разнесение выполняемых задач на разные серверы. Например, мониторинг содержимого информационного обмена является ресурсоемкой задачей, поэтому выделение специального сервера под выполнение данной задачи значительно снизит нагрузку на систему в целом.

Система контроля веб-трафика «Дозор»

Компания «Инфосистемы Джет» уделяет большое внимание проблеме анализа содержимого информационного обмена. В рамках этой задачи специалистами компании разработан продукт, предназначенный для контроля использования Интернет-ресурсов — система контроля веб-трафика «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.

Архитектура СКВТ «Дозор»

Система контроля веб-трафика состоит из нескольких модулей, обеспечивающих решение конкретных задач.
К этим модулям относятся:

1. **Подсистема аутентификации** — обеспечивает проверку прав доступа пользователя системы и определяет политику безопасности для данного пользователя.
2. **Подсистема фильтрации** — обеспечивает анализ передаваемых данных в обоих направлениях на основании политики безопасности, определенной для данного пользователя.
3. **Кэш-сервер** — используется для кэширования данных, получаемых от внешних серверов.
4. **Подсистема управления** — используется для управления политиками безопасности и пользователями.
5. **Подсистема отчетности** — используется для формирования отчетов об использовании внешних ресурсов и т.п.
6. **Система управления базами данных** — используется для хранения политик безопасности для групп пользователей, а также для хранения журналов доступа пользователей к внешним ресурсам.

Схема взаимодействия основных подсистем СКВТ «Дозор» представлена на рис. 2.

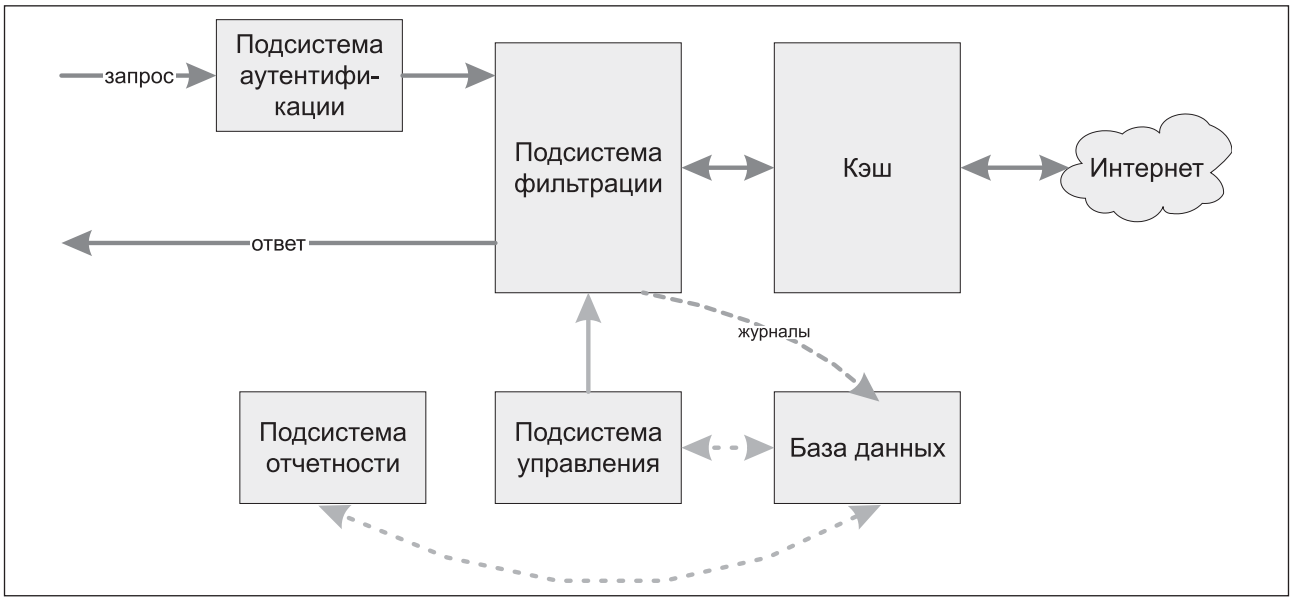

Рис.2. Схема взаимодействия подсистем СКВТ «Дозор»

Подсистема аутентификации

Подсистема аутентификации обеспечивает проверку прав доступа пользователей. Авторизация пользователей производится на основании информации из разных источников данных:

- сервисов каталогов (LDAP);
- данных из доменов Windows NT (используя протокол NTLM);
- баз данных;
- пользовательских данных из обычных файлов.

Проверка прав доступа осуществляется по имени и паролю пользователя. Кроме того, доступ можно разграничить по IP-адресу компьютера. Пользователей можно занести в специальные группы «black» и «white» (см. рис. 3), так что пользователю либо будет полностью закрыт доступ ко всем ресурсам, либо доступ будет полностью открыт и никакие проверки выполняться не будут. Аналогичным образом определен доступ и для IP-адресов, что позволяет не проверять трафик для некоторых компьютеров или наоборот, запрещать доступ с некоторых компьютеров.

Настройки, общие для всех пользователей, можно поместить в специальную группу с именем «all», политика безопасности которой будет учитываться при разработке политики безопасности для конкретной группы пользователей. Кроме того, существует группа «default», политика безопасности которой применяется ко всем пользователям, не включенным явно в какую-либо группу. Эта функциональность может применяться при аутентификации пользователей по данным из внешних источников.

Аутентификация пользователей может осуществляться как прозрачно для пользователей, так и путем проведения ими определенных действий. В первом случае открытие веб-клиентской программы инициирует запрос в службу каталогов. Если пользователь идентифицируется, то запрос проходит незаметно для него. Во втором случае после активизации веб-клиентской программы возникает диалоговое окно, в которое пользователь должен вручную ввести свое имя и пароль. Это бывает необходимо, например, если на одном компьютере работают несколько пользователей, и каждый раз необходимо определять, кто осуществляет вход в Интернет.

Подсистема фильтрации

Проверки, осуществляемые подсистемой фильтрации, можно разделить на несколько категорий:

- адресный контроль (можно ли сюда вообще данному пользователю?);
- контроль форматов и методов (можно ли запрашивать так и это?);
- контроль содержания (что это такое?).

Сложность проверок существенно влияет на производительность системы контроля веб-трафика и, соответственно, на скорость получения данных пользователем.

В СКВТ «Дозор» для каждой группы пользователей можно определить отдельную политику использования Интернет-ресурсов. Комбинируя временные рамки, направления передачи и разные типы проверок, в итоге мы

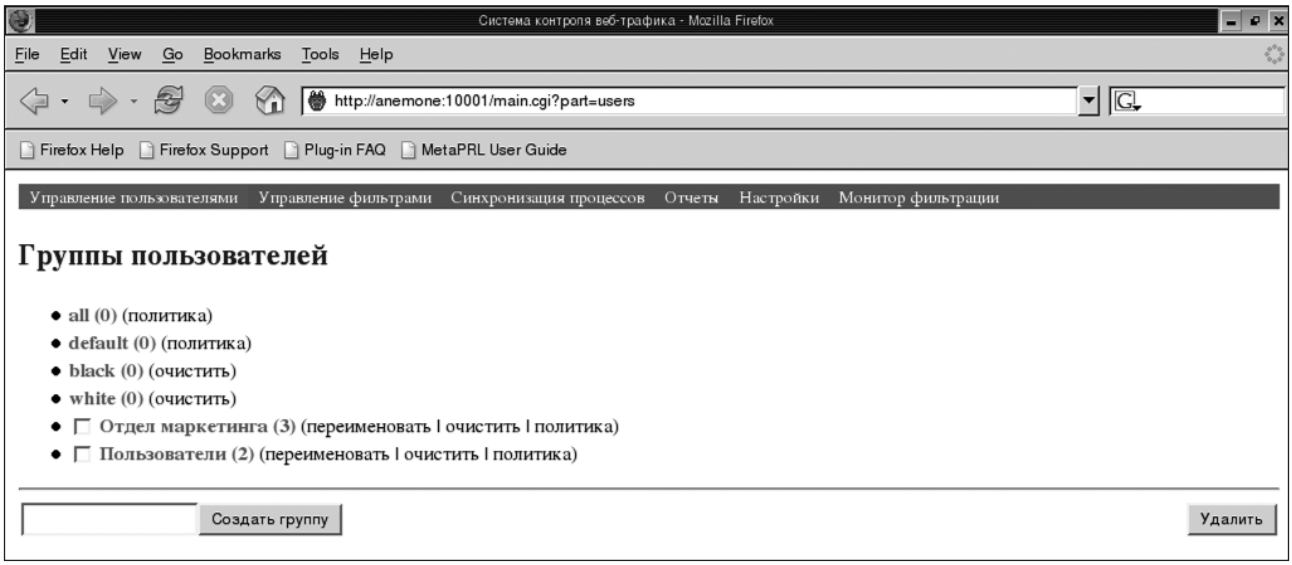

Рис.3. Группы пользователей СКВТ «Дозор»

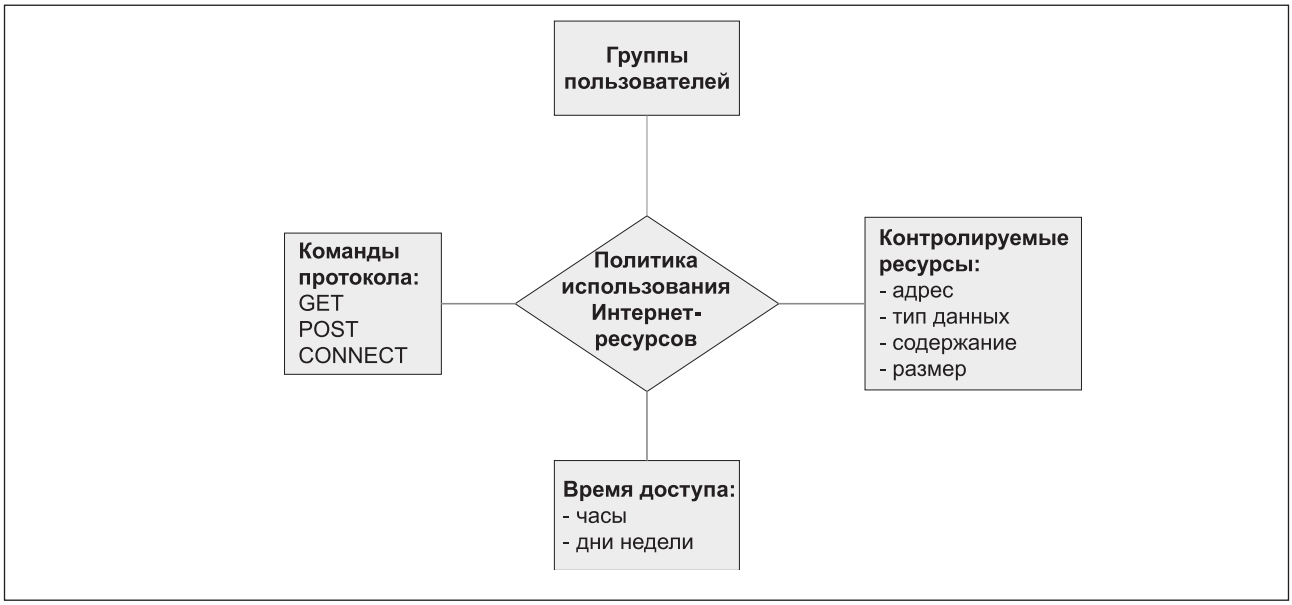

Рис.4. Составные части политики использования Интернет-ресурсов

получаем политику использования Интернет-ресурсов (см. рис. 4).

Порядок выполнения проверок при прохождении данных через подсистему фильтрации показан на рис. 5. В первую очередь выполняются адресные проверки, потом проверки форматов, затем проверки содержимого. Проверки выполняются в порядке возрастания их сложности. Чем сложнее проверка, тем больше ресурсов сервера фильтрации требуется для ее выполнения. Таким образом, указанный порядок проверок позволяет избежать излишней нагрузки на сервер фильтрации.

Адреса для контроля могут браться из различных источников — это и адреса, распространяемые компанией «Инфосистемы Джет» в составе дистрибутива, и адреса, формируемые на основе поиска в Интернете через сравнение передаваемых данных с заранее подготовленным образцом. Адреса проверяются для всех запросов, в том числе и для тех, адреса которых передаются при использовании команды **CONNECT** протокола (правда, в этом случае можно ограничить доступ только ко всему сайту, а не к его части). При работе с серверами, не использующими протокол HTTPS, можно запрещать или разрешать доступ как ко всему сайту, так и к его частям, поскольку существуют порталы, предлагающие разные сервисы, в том числе и бесплатные почтовые ящики, доступ к которым необходимо запретить, оставив при этом доступ к остальным сервисам сайта.

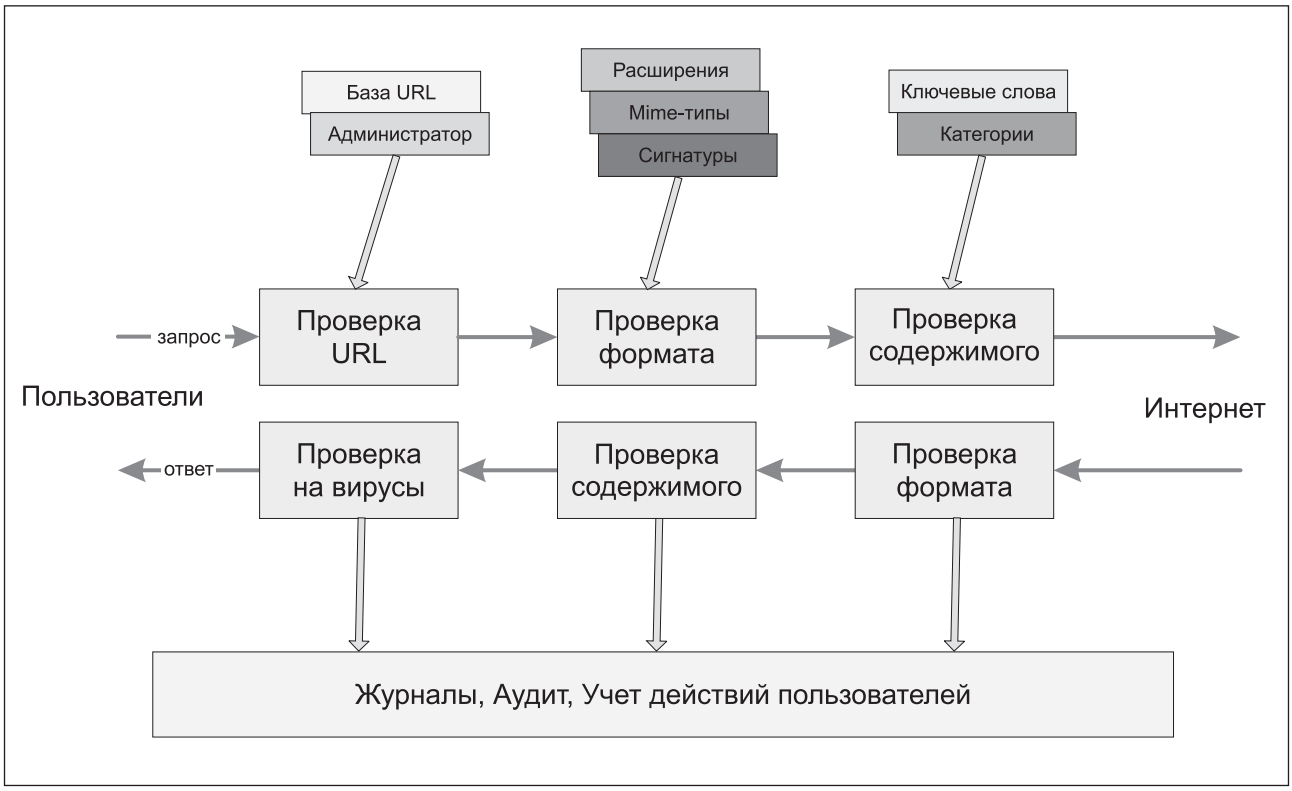

Рис.5. Порядок проверки данных при прохождении через фильтр

Контроль форматов проводится в несколько этапов, а именно:

- контроль расширений файлов;
- контроль MIME-типов передаваемых данных;
- контроль типов по сигнатурам файлов.

Контроль содержания включает в себя следующее:

- поиск по ключевым словам, с учетом весомых коэффициентов для разных слов;
- поиск по шаблонам (регулярные выражения);
- автоматическая категоризация ресурсов (например, бесплатных почтовых ящиков);
- антивирусная проверка.

При анализе текста автоматически определяется кодировка передаваемых данных и, если требуется, производится перекодирование русскоязычного текста в ту кодировку, в которой хранятся списки слов для проверки.

СКВТ «Дозор» позволяет использовать ключевые слова и выражения в следующих ситуациях:

- как признак для запрета передачи данных — «черный» список;
- как признак для разрешения передачи данных — «белый» список.

Следует отметить, что при использовании «черных» списков слова могут обрабатываться двумя способами: либо наличие запрещенного слова сразу запрещает передачу данных, либо передача запрещается при наличии сочетания слов, веса которых складываются друг с другом, и полученный результат служит признаком запрета передачи данных. Именно использование блокировки доступа по результатам подсчета весов слов является наиболее эффективным способом блокировки доступа пользователей к серверам, реализующим функции работы с почтой (сервисами бесплатной почты).

Кроме этого, СКВТ «Дозор» может сравнивать получаемые данные с образцом, который автоматически создан в результате сравнения «плохих» и «хороших» сайтов. При анализе «плохих» сайтов специальная утилита извлекает из страниц ключевые слова и выражения, отсутствующие на «хороших» сайтах, а затем эта информация может использоваться для анализа страниц, проходящих через систему контроля веб-трафика.

Антивирусная проверка производится с использованием внешних антивирусных программ. В настоящее время поддерживаются «Антивирус Касперского» версии 4, Dr.Web, Sophos. Антивирусная поддержка оформлена в виде подгружаемых модулей, так что поддержка

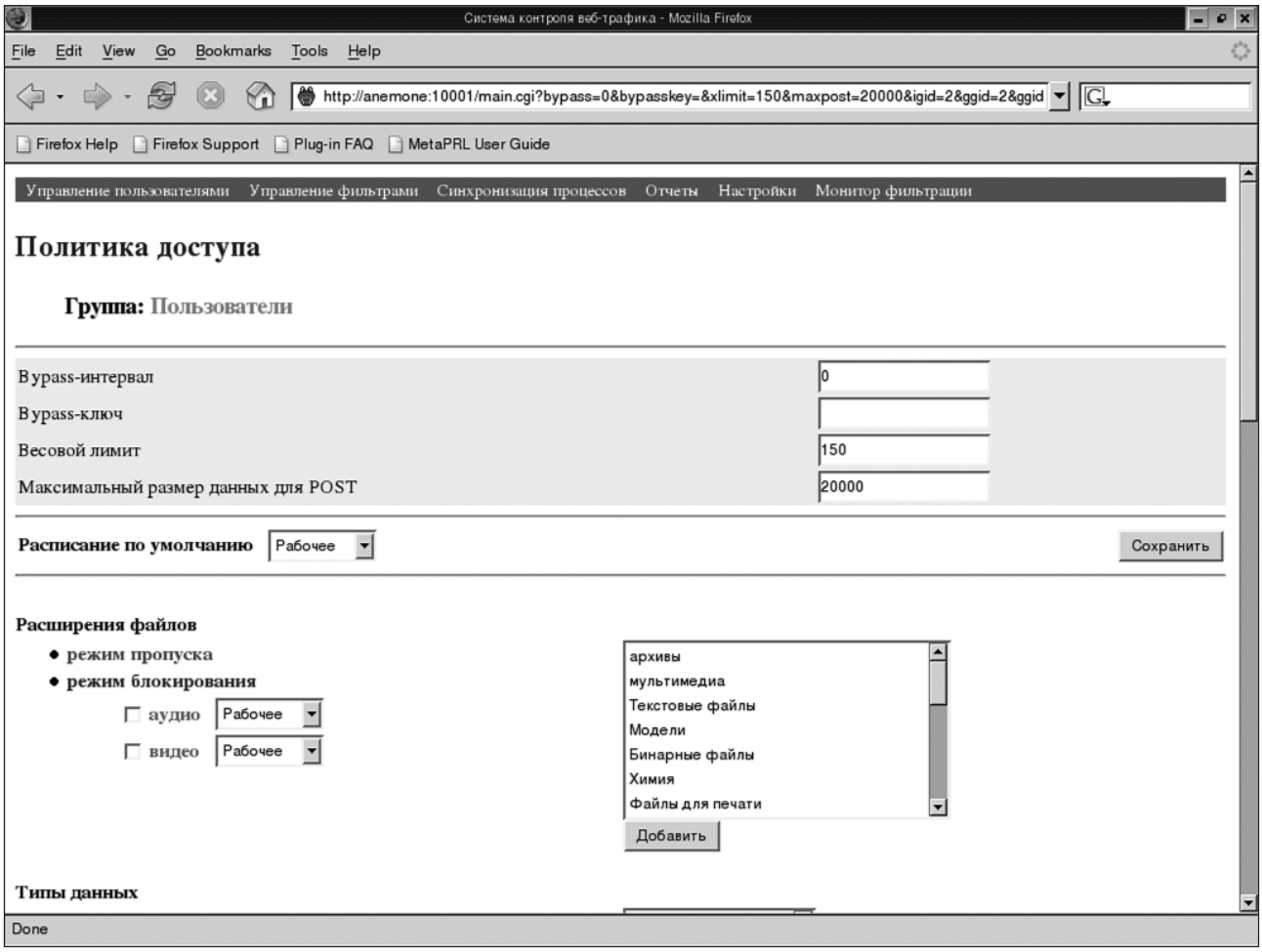

Рис.6. Редактирование политики доступа

новых антивирусов может добавляться без переустановки всей подсистемы фильтрации.

Для группы пользователей можно задать различные ограничения, а также параметры, которые определяют максимальный объем данных, передаваемых с помощью команды **POST**, весовые лимиты для работы в режиме подсчета весовых коэффициентов фраз и т.п.

Пример редактирования политики доступа для группы пользователей приведен на рис. 6.

В зависимости от результатов конкретной проверки СКВТ «Дозор» может реагировать поразному — блокировать передачу данных, разрешать передачу, разрешать передачу с подтверждением. В последнем случае пользователю требуется ответить на запрос системы и подтвердить необходимость доступа к указанному ресурсу. В результате чего 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 СКВТ «Дозор» анализировать использование Интернет-ресурсов и корректировать политику на основе полученной информации.

Кэш-сервер

Данная подсистема предназначена для кэширования передаваемых данных. Это может существенно ускорить процесс доступа к данным, а также уменьшить нагрузку на канал передачи данных. В качестве прокси-сервера по умолчанию в СКВТ «Дозор» используется прокси-сервер Squid 2.5, который часто применяют в операционных системах Linux, FreeBSD и других Unix-подобных системах.

Если в организации уже имеется прокси-сервер, подсистему фильтрации можно настроить на использование этого прокси-сервера, а не входящего в комплект поставки СКВТ «Дозор».

Подсистема управления

Подсистема управления позволяет пользователям СКВТ «Дозор» выполнять следующие задачи:

- управлять СКВТ «Дозор» через веб-браузер;
- разграничивать доступ к подсистеме управления;

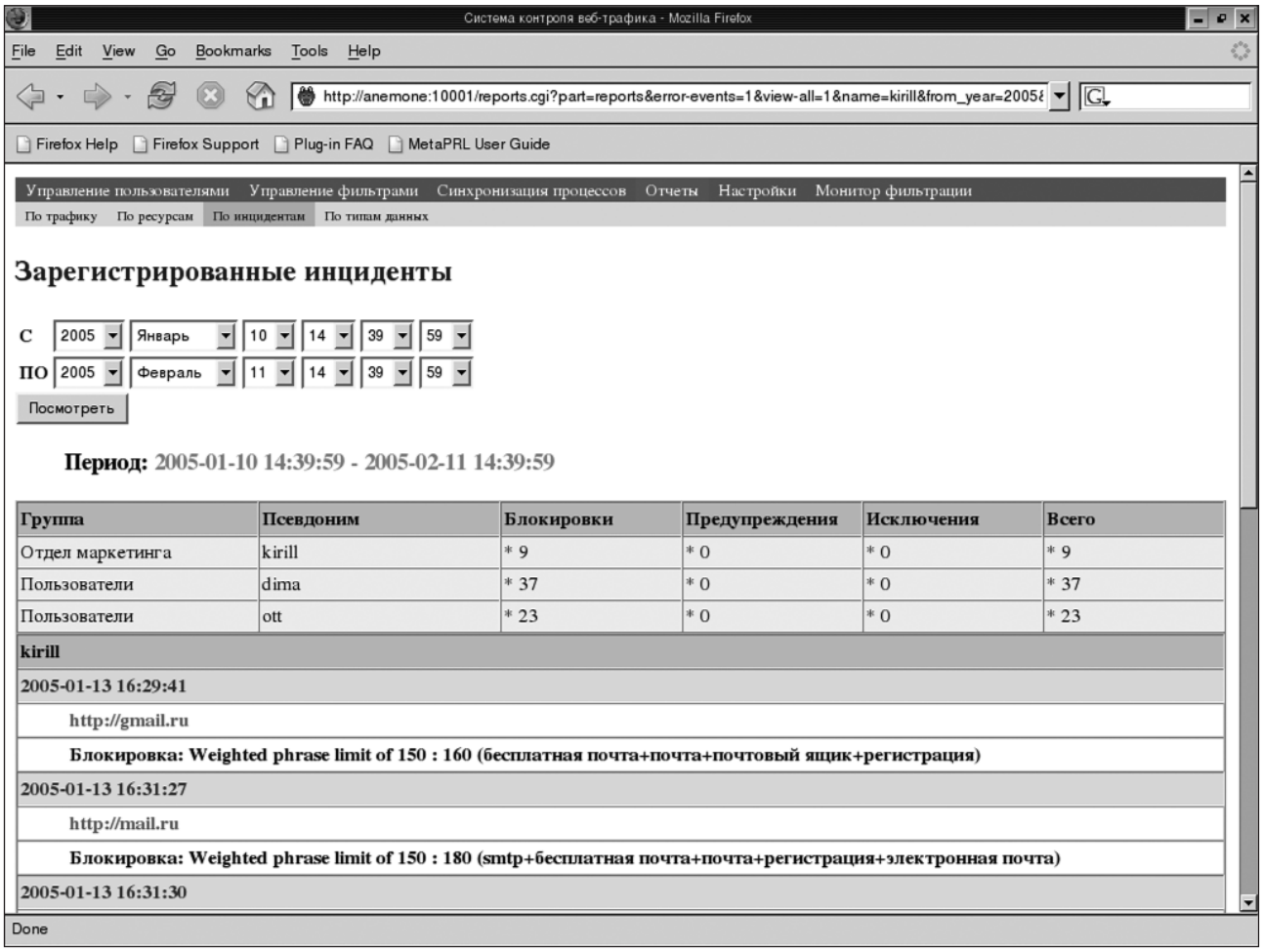

Рис.7. Пример отчета по зарегистрированным инцидентам

- управлять политикой безопасности и настройками СКВТ «Дозор»;
- получать доступ к подсистеме отчетности.

Управление СКВТ «Дозор» с помощью веб-браузера позволяет администратору безопасности практически из любого места контролировать действия пользователей, а также изменять политику безопасности. Доступ к подсистеме управления производится как по протоколу HTTP, так и по протоколу HTTPS.

Разграничение доступа к подсистеме управления позволяет вводить разные роли пользователей — администраторов политик безопасности, операторов, которые анализируют использование Интернет-ресурсов пользователями системы и т.п.

Примеры использования подсистемы управления приведены на рис. 3, 6 и 7.

Подсистема отчетности

Подсистема отчетности обеспечивает сбор статистической информации и формирование отчетов. СКВТ «Дозор» состоит из двух частей. Первая служит для обработки данных, получаемых от подсистемы фильтрации, и загрузки их в базу данных. Вторая — для формирования различных отчетов о доступе к Интернет-ресурсам, о зарегистрированных инцидентах и т.п. В настоящее время в СКВТ «Дозор» реализованы следующие виды отчетов:

- по использованию Интернет-ресурсов пользователями и группами пользователей;
- по типам данных, переданных через СКВТ «Дозор»;
- по объему переданных данных для конкретного пользователя или группы пользователей;
- по инцидентам, зарегистрированным подсистемой фильтрации.

Отчет по объему трафика дает количественную оценку трафика для каждого пользователя за выбранный период. При этом в отчете отражаются все пользователи (в том числе и ранее удаленные 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 можно сгруппировать ресурсы по названиям сайтов. Этот отчет можно создавать за любой заданный период. Период можно корректировать динамически, т.е. администратору СКВТ «Дозор» 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, отказы в передаче данных, а также выдаваться предупреждения, необходимо отслеживать возникающие инциденты. Отчет по инцидентам подсчитывает количество инцидентов того или иного типа в заданный период, а также позволяет вывести подробности об этих инцидентах по типам или все сразу 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.

Пример одного из таких отчетов — отчет по зарегистрированным инцидентам — приведен на рис.7.

Кроме того, дополнительные виды отчетов можно получить с помощью стандартных средств формирования отчетов, таких как Crystal Reports, Oracle Reports и т.п., используя информацию о схеме базы данных, которая поставляется в документации на СКВТ «Дозор».

Системные требования

СКВТ «Дозор» функционирует под управлением Sun Solaris и Linux. Версия под Linux существует для дистрибутивов RedHat Enterprise Linux 3 и RedHat Fedora Core 3. Версия для Sun Solaris функционирует на оборудовании с процессорами Sparc и Intel x86. Она протестирована на Sun Solaris 9. Версии поставляются в виде пакетов для соответствующих операционных систем, что позволяет управлять установкой и обновлением СКВТ «Дозор» с помощью средств операционной системы.

Для функционирования СКВТ «Дозор» необходимо наличие на сервере определенного набора программного обеспечения, а именно:

- прокси-сервер Squid;
- веб-сервер Apache;
- СУБД PostgreSQL;
- интерпретатор языка Perl и набор модулей к нему для доступа к базе данных;
- библиотеки для доступа к серверу каталогов OpenLDAP.

Для установки СКВТ «Дозор» рекомендуется использовать следующее оборудование:

- **На платформе Intel**: процессор Intel Pentium IV 3 GHz[7], 512 Mb RAM, 36 GB SCSI HDD.
- **На платформе Sparc**: Sparc IIIi, 1 GHz, 512 Mb RAM, 36 GB SCSI.

Но конкретная спецификация оборудования составляется в зависимости от объема передаваемых данных, пропускной способности канала доступа в Интернет и количества пользователей.

Выводы

В заключение необходимо сказать о том, что выгодно отличает СКВТ «Дозор» от подобных ей систем, которые представлены на рынке информационной безопасности.

СКВТ «Дозор» обладает мощной и эффективной подсистемой фильтрации трафика, которая обеспечивает:

- распознавание форматов файлов всех популярных приложений;
- анализ русскоязычных текстов независимо от используемой кодировки кириллицы (Win1251, DOS866, ISO8859-5, KOI-8R, MAC и др.), в том числе текстов с неправильно или ошибочно указанной кодировкой;
- гибкую систему создания правил использования Интернет-ресурсов и доступа пользователей к ним;
- фильтрацию по множеству компонентов (URL, заголовки протоколов, содержание текста, типы файлов, объем трафика и размер файлов, направление передачи данных и др.).

СКВТ «Дозор» имеет интуитивно понятный русскоязычный интерфейс управления. Настройка и администрирование производятся централизованно с рабочего места администратора безопасности через веб-интерфейс.

7 Можно также использовать процессоры компании AMD Opteron64.

У СКВТ «Дозор» есть внутренние механизмы защиты: доступ по протоколу HTTPS, разграничение доступа к функциям администратора, доступ только уполномоченных администраторов, контроль действий администратора.

В основу СКВТ «Дозор» положены гибкие механизмы реагирования на выполнение условий фильтрации и возможность автоматического осуществления следующих действий:

- блокировка трафика, параметры которого не соответствуют политике использования Интернет-ресурсов;
- пропуск данных с подтверждением;
- оповещение администратора безопасности о нарушениях политики использования Интернет-ресурсов;
- занесение всей информации о событиях и функционировании СКВТ «Дозор» (в том числе о действиях администратора) в журнал регистрации.

СКВТ «Дозор» обладает высоким уровнем надежности и производительности. Система способна обрабатывать десятки мегабайт трафика в час и практически не создает задержек при информационном обмене. Помимо других факторов, это достигается за счет использования многомашинной конфигурации. Такая конфигурация позволяет разнести выполнение задач, требующих больших ресурсов, на отдельные серверы. В результате можно распределить нагрузку и обеспечить высокую скорость и эффективность анализа данных информационного обмена, а также значительно повысить надежность СКВТ «Дозор».

Структура системы обеспечивает возможность выбора платформы. Функционирование под управлением операционных систем Sun Solaris и Linux на аппаратных платформах Sun SPARC, Intel x86 позволяет подбирать оптимальную конфигурацию по производительности и цене.

СКВТ «Дозор» позволяет получить полную и реальную картину использования Интернет-ресурсов пользователями. Это осуществляется за счет встроенного модуля построения отчетов, который дает возможность получать:

- сводную информацию об использовании Интернета всеми сотрудниками;
- информацию о нарушениях политики безопасности (отчеты практически по любым параметрам веб-трафика);
- информацию об объеме загружаемых данных, сгруппированную по адресам внешних источников, группам пользователей или индивидуальным пользователям.

При этом отчеты можно экспортировать в различные форматы представления данных.

СКВТ «Дозор» является масштабируемой системой. Она масштабируется по производительности и уровню доступности сервиса. Что касается производительности, то модульная структура позволяет разносить выполнение различных задач на несколько отдельных серверов. Высокий уровень доступности сервиса достигается путем построения кластерной конфигурации сервера.

И наконец, компания «Инфосистемы Джет» уделяет большое внимание соответствию своей деятельности в области информационной безопасности российским стандартам и нормативным документам. Все работы по защите информации ведутся на основании лицензий уполномоченных органов, а продукты, поставляемые компанией, проходят соответствующую сертификацию. Поэтому в настоящее время активно ведутся работы по подготовке СКВТ «Дозор» к сертификации в Государственной технической комиссии при Президенте Российской Федерации.

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

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Лапина И.К. *(lapina@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