шаге для этого метод дихотомии. Запишем условия определения ξ_k.:

$$\xi_k = \begin{cases} 1, \Delta F_k > 0 \\ -1, \Delta F_k \le 0 \\ F_h < 0 \end{cases}; \quad \xi_k = \begin{cases} 1, \Delta F_k \le 0 \\ -1, \Delta F_k > 0 \\ F_h > 0 \end{cases}. \qquad (17)$$

Если по завершении итерационного процесса, т.е. k_{max}=n, ни на одном из k шагов не нарушились пары неравенств (16), то ПЛ не пересекает поверхность.

Случай 2. Поверхность F(X′Y′Z′)=0 пересекается ПЛ. Итерационный процесс в этом случае строится следующим образом. Если на нулевом и последующих шагах пары неравенств (16) не нарушаются, то для нахождения ξ_k. используются условия (17). Как только неравенства (16) на каком-либо шаге нарушились, то, начиная со следующего шага, в качестве ПИ выбираются две величины $F_1(t_k)$ и $F_2(t_k)$, позволяющие одновременно с достижением k_{max}=n вычислить две точки пересечения ПЛ с поверхностью: соответственно, ближнюю к h и дальнюю от h. Запишем условия определения ξ_k..

Для первой точки P_1:

$$\xi_k = \begin{cases} 1, F_{1k} > 0 \\ -1, F_{1k} \le 0 \\ F_h > 0 \end{cases}; \quad \xi_k = \begin{cases} 1, F_{1k} \le 0 \\ -1, F_{1k} > 0 \\ F_h < 0 \end{cases}. \qquad (18)$$

Для второй точки P_2:

$$\xi_k = \begin{cases} 1, F_{2k} \le 0 \\ -1, F_{2k} > 0 \\ F_h > 0 \end{cases}; \quad \xi_k = \begin{cases} 1, F_{2k} \le 0 \\ -1, F_{2k} > 0 \\ F_h < 0 \end{cases}. \qquad (19)$$

Из (18) и (19) следует, что для случая F_h<0 координаты точек P_1 и P_2 совпадают. В рассматриваемом итерационном процессе на последнем шаге итераций k_{max}=n будут получены координаты точек пересечения P_1 и P_2 ПЛ с поверхностью. На практике длина поверхности вращения часто ограничивается плоскостями F_1 и F_2.

Пример 3. Поверхность F(X′Y′Z′)=0, длина которой ограничена вдоль оси вращения плоскостями $F_1(X'Y'Z')=0$ и $F_2(X'Y'Z')=0$. Нахождение точек пересечения P_1 и P_2 ПЛ с ГП в рассматриваемом примере выполняется следующим образом. Для плоскостей F_1 и F_2 точки пересечения находим в соответствии с примером 1, а для поверхности вращения – в соответствии с примером 2. Итерационные процессы могут выполняться одновременно. По завершении k_{max}=n шагов необходимо выполнить еще один шаг, на котором устанавливаются истинные точки пересечения. На этом шаге выполняется проверка неравенств. Для координат точек пересечения ПЛ с плоскостями F_1 и F_2 проверяется выполнение неравенств

$$F(X'_1, Y'_1, Z'_1) < 0,\ F(X'_2, Y'_2, Z'_2) < 0, \qquad (20)$$

где X'_1, Y'_1, Z'_1 и X'_2, Y'_2, Z'_2 – координаты точек пересечения ПЛ с плоскостями соответственно F_1 и F_2, подставленные в уравнение, описывающее поверхность вращения. Для координат точек пересечения ПЛ с поверхностью вращения F(X′Y′Z′)=0 проверяется выполнение какой-либо пары неравенств.

Для первой точки:

$$F_1(X'_1, Y'_1, Z'_1) \le 0,\ F_2(X'_1, Y'_1, Z'_1) \ge 0,$$
$$\text{либо } F_1(X'_1, Y'_1, Z'_1) \ge 0,\ F_2(X'_1, Y'_1, Z'_1) \le 0, \qquad (21)$$

где X'_1, Y'_1, Z'_1– координаты первой точки, подставленные в уравнения плоскостей F_1 и F_2.

Для второй точки:

$$F_1(X'_2, Y'_2, Z'_2) \le 0,\ F_2(X'_2, Y'_2, Z'_2) \ge 0,$$
$$\text{либо } F_1(X'_2, Y'_2, Z'_2) \ge 0,\ F_2(X'_2, Y'_2, Z'_2) \le 0, \qquad (22)$$

где X'_2, Y'_2, Z'_2 – координаты второй точки, подставленные в уравнения плоскостей F_1 и F_2.

Совместный логический анализ неравенств (20), (21), (22) позволяет установить, на каких поверхностях оказались истинные точки пересечения.

В заключение отметим, что итерационный алгоритм хорошо реализуется однородной параллельно-конвейерной структурой, число тактов которой определяется требуемой точностью вычислений.

Литература. 1. *Иванов В.П., Батраков А.С.* Трехмерная компьютерная графика. М.: Радио и связь, 1995. 224 с. 2. *Гусятин В.М.* Математическая модель геометрических преобразований для спецпроцессоров растровой графики // Радиоэлектроника и информатика. 1997. №1. С. 86-87. 3. *Башков Е.А., Зори С.А.* Устройство синтеза реалистических изображений устилающей поверхности Земли для систем визуализации тренажеров. Донецк: Сб. трудов ДонГТУ. 1996. С. 148-152.

Поступила в редколлегию 14.09.98

Рецензент: д-р техн. наук Алипов Н.В.

Гусятин Владимир Михайлович, канд. техн. наук, доцент кафедры электронных вычислительных машин ХТУРЭ. Научные интересы: теория и практика построения спецпроцессоров растровых графических систем реального времени. Адрес: Украина, 310726, Харьков, пр. Ленина, 14, тел. 40-93-54, 66-61-22.

УДК 681.326

БЕЗОПАСНОСТЬ В INTERNET. ВОЗМОЖНОСТИ НОВОГО ПРОТОКОЛА IPv6

ФРАДКОВ С.А.

Описываются новые возможноси Internet-протокола IPv6, способствующие усилению безопасного обмена конфиденциальной информацией во всемирной Сети.

В августе 1990 г. на конференции IETF (Internet Engineering Task Force) в Ванкувере впервые обсуждалась проблема неспособности Internet справляться с экспоненциальным ростом числа подключенного к сети оборудования. Изначально, в 1973 г., Internet должен был соединять около сотни компьютеров. Однако с каждым годом все более многочисленные категории пользователей начали подключаться к созданной сети. Вначале это были научные центры и университеты, потом, в 1992 г., Internet был открыт для коммерческой деятельности, расцвет которой мы можем сейчас наблюдать. Так как размер адреса Internet составляет 32 бита, то количество возможных адресов в нем теоретически равно 2^{32}=4294967296. Но так как адреса выделяются не последовательно, а в пределах подсетей класса A (16777214 адресов), B (65534 адреса) и C (254 адреса), и так как количество подключенного оборудования удваивается ежегодно, то специалисты предсказывали полный крах всей сети в 1994 г. Опасения оказались преждевременными, но начиная с 1993 г. были предприняты срочные

меры по предотвращению кризиса, что отдалило «час X» на несколько лет. В настоящее время ожидается, что нехватка адресов IP наступит в 2008 (+/- 3) г. Инженеры и исследователи, работающие в организациях по стандартизации Internet, воспользовались этой отсрочкой для разработки новой версии протокола. Текущая версия именуется IPv4 и, так как номер 5 был уже присвоен экспериментальному протоколу, то результат усилий IETF получил название Internet Protocol версия 6 (IPv6).

Протокол IPv6 имеет много принципиальных отличий от своего предшественника и много новшеств. В списке последних можно отметить мобильность и безопасность. Был изменен формат заголовка IP и введена возможность внедрения дополнительных заголовков (или расширений) к основному. Цель данной статьи – рассмотрение идеологии безопасности, применяемой в реализации IPv6. Так как все новые возможности реализованы именно в виде расширений, рассмотрим это.

1. Расширения IPv6

Все расширения (кроме расширения «шаг-за-шагом») обрабатываются оборудованием-получателем пакета. Расширение имеет переменную длину, кратную 8 байтам. Оно начинается однобайтовым полем «следующий заголовок», которое определяет тип данных, следующих за расширением: другое расширение или протокол версии 4 (табл. 1). Для расширений с переменной длиной следующий байт содержит длину расширения в 8-байтных словах, не считая первого слова (расширение длиной 16 байтов имеет в поле длины единицу).

RFC 1883 рекомендует следующий порядок расширений:

— «шаг-за-шагом» (всегда должен быть первым);

— назначение (обрабатывается маршрутизаторами, перечисленными станцией-отправителем в расширении маршрутизации);

— маршрутизация;

— фрагментация;

— аутентификация;

— конфиденциальность;

— назначение (обрабатывается только принимающей станцией).

В данной статье нас интересуют только проблемы безопасности, поэтому все прочие расширения мы не будем рассматривать.

2. Безопасность

Безопасность является одной из основных целей проработки IAB (Internet Architecture Board), так как изначально требования к протоколу IPng (Internet Protocol next generation), названному теперь IPv6, содержали секцию безопасности.

Элементы безопасности:

— конфиденциальность — позволяет благодаря механизмам шифрования передавать данные в виде, распознаваемом только авторизованными сетями/станциями. Обычно используют алгоритмы симметричного шифрования, где для шифрования и дешифрования применяется один и тот же ключ. Чем интенсивнее используется ключ, тем более он уязвим. Его обновление реализуется с помощью алгоритмов асимметричного шифрования;

— аутентификация — гарантирует, что полученные данные отправлены указанной станцией/пользователем. Используются алгоритмы цифровой подписи;

— целостность — гарантирует, что полученные данные не подверглись модификации во время прохождения по сети. Используются функции хеширования;

— предотвращение повторного использования - гарантирует, что полученные данные не были уже ранее приняты.

Наилучший уровень (по модели OSI) для реализации безопасности — «сетевой», так как все вышестоящие уровни и приложения могут пользоваться этими механизмами. IAB рассматривает систему безопасности IPv6 (IPsec) как обязательную в финальной реализации IPv6. IPsec также предложен для IPv4, но не поставляется, как стандарт, на большинство действующих систем. Функции аутентификации/конфиденциальности определены одновременно для IPv4 и IPv6, их общая архитектура описана в RFC 1825.

3. Анализ угроз

В сети IP могут быть реализованы две классические атаки:

1) IP sniffing — состоит в прослушивании трафика сети злоумышленником. Он может знать содержимое электронных сообщений или пароли, циркулирующие в сети. Атака может быть реализована двумя способами:

— злоумышленник располагается в сети, реально распространяющей данные (Ethernet или Token Ring). После этого он может восстановить и проанализировать трафик сети на своей рабочей станции;

— злоумышленник использует анализатор сетевого протокола без ведома сетевого администратора. Этот анализ ограничен сегментом сети, к которому подключился злоумышленник.

2) IP spoofing – мистификация/подмена. Состоит в узурпации персонального идентификатора. Цель атаки – установление соединения с рабочей станцией- под видом другого лица или подмена данных в существующем трафике. Возможны варианты:

— модификация аппаратного адреса рабочей станции злоумышленника;

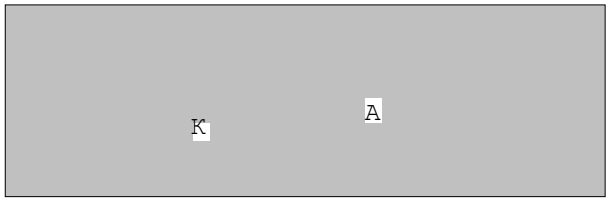
— создание сообщений протокола ICMP в целях переадресации пакетов IP по направлению к станции злоумышленника;

— компрометация сервера DNS может служить для перенаправления запроса DNS к станции, контролируемой злоумышленником, которая вернет ложный адрес IP на станцию, пославшую запрос DNS;

— введение пакетов TCP с некорректными номерами последовательности в процессе соединения может его нарушить.

4. Направления исследований, выбранные IETF

Как показывает табл. 2, для предотвращения атак «IP sniffing» и «IP spoofing» необходимо ввести следующие компоненты безопасности:



— конфиденциальность;
— целостность;
— аутентификация.

Для введения этих компонент безопасности и обеспечения защиты обмены пакетами IP IETF определил два новых заголовка безопасности IP (описанные в RFC 1752):

— Authentication Header (AH) — заголовок аутентификации, выполняющий функции аутентификации и целостности и, в зависимости от алгоритма, – функцию предотвращения повторного использования;

— Encapsulating Security Payload (ESP) — заголовок безопасности. Выполняет функцию конфиденциальности и, в зависимости от алгоритма, –функции целостности и аутентификации.

Определение двух заголовков вместо одного разумно потому, что законодательство, применяемое для функций конфиденциальности, более строгое, чем для функций аутентификации/целостности. Каждая страна по-своему регламентирует правила импорта, экспорта и использования алгоритмов безопасности. Например, во Франции с 27 июля 1996г. криптография может свободно использоваться для аутентификации автора или доказательства целостности сообщения. Зато для шифрования сообщений необходимо прибегнуть к третьему лицу, обладающему доверием (признаваемому премьер-министром и подчиненному профессиональной тайне), которое должно знать используемый ключ шифрования. Благодаря наличию двух заголовков для функций конфиденциальности и целостности/аутентификации, два пользователя, которые не могут обеспечить конфиденциальность их сообщений из-за законодательства их стран (ы), могут воспользоваться функциями обеспечения целостности/аутентификации.

Эти заголовки полезны для защиты соединения (рис. 1). Защита может выполняться:

— "от края до края", между двумя соединяющимися станциями;

— в сегменте сети, между двумя объектами сети IP (например, маршрутизаторами);

— между станцией и одним/многими объектами сети.

При подключении локальной "надежной" сети к внешней имеет смысл сконцентрировать механизмы обеспечения безопасности в оборудовании, размещенном на границе этих сетей (рис. 2).

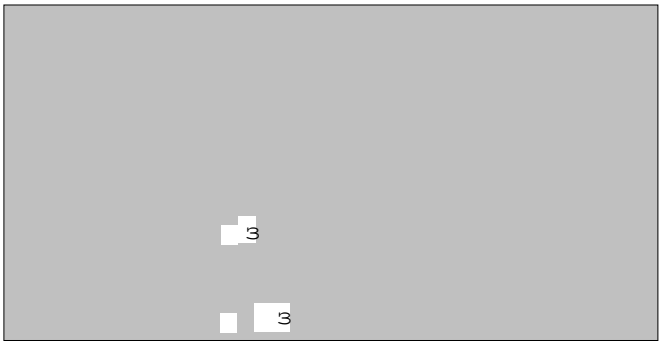


Рис. 1. Защита соединения

Безопасность данных, передаваемых между рабочими станциями локальной и внешней сети, контролируется, таким образом, не станцией, а промежуточным компьютером, который играет роль «firewall» (защитного шлюза) для этой станции. Этот компьютер часто называется «прокси-сервером безопасности». Его задача заключается в модификации датаграмм, отправляемых станцией локальной сети, таким образом, чтобы поддержать нужный уровень безопасности для защиты данных локальной станции. Затем он должен выбрать, как функцию от указанного уровня безопасности, список адекватных параметров безопасности (алгоритмы шифрования, хеширования и т.д.). Совокупность выбранных параметров и механизмов безопасности формирует ассоциацию безопасности для соединения. Прокси-сервер должен затем создать заголовки безопасности и добавить их к датаграмме перед отправкой ее получателю (рис. 3).

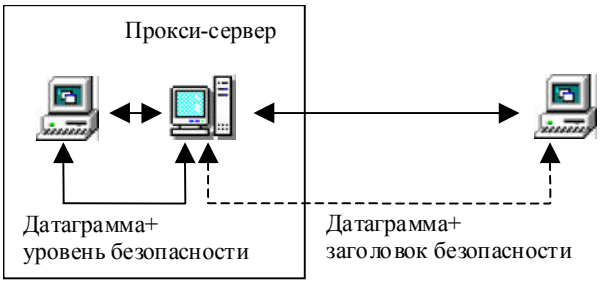


Рис. 2. Прокси-сервер безопасности для локальной сети

5. Ассоциации безопасности

Ассоциация безопасности (АБ) IPv6 включает список функций безопасности для введения в строй коммуникаций и различных параметров безопасности (алгоритмы и ключи шифрования, параметры синхронизации и т.д.) для защиты выполняемого обмена данными. Она должна быть известна оборудованию (т.е. рабочим станциям, серверам и прокси-серверам), ответственному за защиту обмена информацией.

АБ однозначно идентифицируется индексом параметров безопасности SPI (Security Parameter Index), иногда называемым SAID (Security Association IDentifier), и адресом получателя пакета IP. Оборудование безопасности IPv6 может участвовать во многих ассоциациях безопасности.

АБ однонаправленна. Двунаправленный обмен данными между двумя рабочими станциями А и В обязывает использовать две ассоциации безопасно-

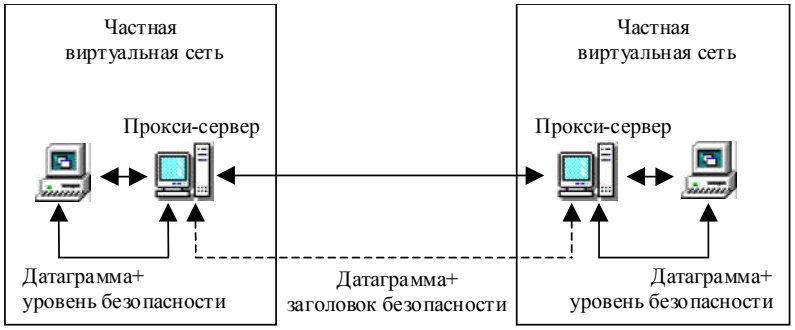


Рис. 3. Прокси-сервер для частной виртуальной сети

сти: для А, чтобы защищать датаграммы от А к В, и для В, чтобы защищать датаграммы от В к А.

АБ содержит среди прочих следующие параметры:

— алгоритм шифрования для построения заголовка аутентификации;

— ключ, используемый алгоритмом шифрования для построения заголовка аутентификации;

– алгоритм шифрования для построения заголовка конфиденциальности (ESP);

— ключ, используемый алгоритмом шифрования для построения заголовка конфиденциальности;

— время жизни ключей или период их обновления;

— время жизни ассоциации безопасности;

— уровень секретности защищаемых данных.

Для того чтобы аппаратура безопасности могла корректно интерпретировать полученные заголовки безопасности, ассоциация безопасности (т.е. SPI), использованная при их создании, должна быть упомянута в каждом из заголовков безопасности.

Выбор АБ на уровне станции-отправителя может зависеть:

— исключительно от станции. В этом случае одна и та же ассоциация безопасности используется многими пользователями на одной и той же станции при отсылке пакетов к одному и тому же получателю. Этот подход имеет большой недостаток – злоумышленник может вычислить ключ, используемый между двумя станциями, подключившись к этой станции и выполнив атаку «выбранный открытый текст» (Chosen Plaintext Attack), которая состоит в передаче специального открытого текста этой станции и анализа соответствующего шифротекста (передаваемого по сети) для нахождения используемого ключа шифрования. Знание этого ключа позволит затем дешифровать весь трафик обмена между двумя станциями (но только в одну сторону);

— от идентификатора пользователя (user id) или даже от используемого приложения (используемые номера портов/сокетов). Этот подход является гораздо более надежным, чем предыдущий.

6. Аутентификация (RFC 1826)

Заголовок аутентификации (AH-Authentication Header) (рис.4) позволяет доказать факт, что отправитель сообщения именно тот, кто претендует им быть. Он служит также для контроля целостности, гарантирующего получателю, что никто не изменил содержимого сообщения в процессе передачи его по сети.

Принцип относительно прост. Отправитель вычисляет цифровую подпись с помощью алгоритма, базирующегося на симметричных ключах, и посылает ее вместе с сообщением, для которого эта подпись вычислялась. Получатель извлекает подпись из переданного сообщения, дешифрует ее с помощью того же секретного ключа и сравнивает с подписью, вычисленной им самим. Если подписи разные, то либо отправитель не располагает правильным ключом, либо сообщение подверглось модификации в пути. Заметим, что само сообщение не шифруется — таким образом, злоумышленник всегда может прослушивать трафик между двумя корреспондентами. Зато секретный ключ никогда не циркулирует в сети. Злоумышленник не может получить этот ключ простым прослушиванием канала.

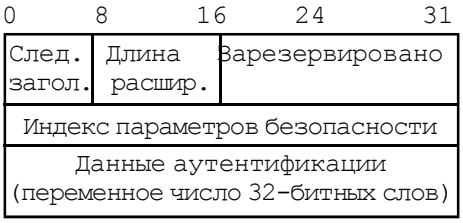


Рис. 4. Формат заголовка аутентификации

Обычно заголовок аутентификации используется «от края до края», но шлюз безопасности, обрабатывающий пакеты, может использовать его для аутентификации крайних точек туннеля.

Источник сообщения вычисляет цифровую подпись на построенный пакет в той форме, в которой он должен появиться на принимающей стороне (заголовок маршрутизации будет иметь адреса в соответствующем порядке), со всеми полями, могущими измениться в пути, установленными в ноль. Поле данных аутентификации установлено в ноль. Цифровая подпись размещается на месте данных аутентификации. Верификация производится по тому же алгоритму — вычисляется подпись и сравнивается с полученной в пакете.

Предложена опциональная защита против повторного использования. Она состоит в счетчике последовательности, увеличивающемся при отсылке каждого пакета. Получатель может проверять это строгое возрастание, отбрасывая все пакеты с уже полученным номером последовательности. При достижении максимального номера последовательности счетчик должен быть переустановлен.

Были определены два алгоритма хеширования для вычисления цифровой подписи — MD5 (Message Digest 5 [RFC 1321]) и SHA-1 (Secure Hash Algorithm [FIPS-180-1]). В настоящее время алгоритмом генерации цифровой подписи по умолчанию является Keyed MD5 (Ключевой MD5), состоящий в добавлении к отправляемому сообщению секретного ключа и конденсата сообщения, вычисленного с помощью MD5. Алгоритм должен быть заменен более проработанным алгоритмом HMAC (Hash Message Authentication Code [RFC 2085]).

7. Конфиденциальность (RFC 1827)

Заголовок конфиденциальности (ESP-Encapsulating Security Payload) (рис.5) позволяет шифровать совокупность пакетов или их транспортные части. Так же как и аутентификация, конфиденциальность предполагает наличие ассоциации безопасности, включающей среди прочего ключ шифрования и индекс параметров безопасности.

Конфиденциальность имеет два режима:

— транспортный «от края до края», где информация протокола верхнего уровня (в основном транспортного протокола), включая его заголовок, шифруется;

— туннельный между двумя шлюзами безопасности, где пакеты шифруются целиком.

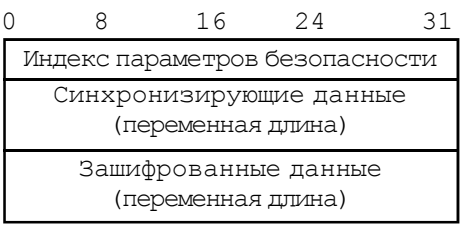


Рис. 5. Формат заголовка конфиденциальности

Перед шифрованием к сообщению добавляется необходимое количество битов выравнивания, число которых зависит от алгоритма шифрования. Опциональный номер последовательности может быть размещен в незашифрованной части заголовка.

Стандартным алгоритмом для шифрования является DES (Data Encryption Standard) [FIPS-46] и тройной DES в режиме CBC (Cipher Block Chaining) [FIPS-81]. Также предлагаются другие алгоритмы, такие как IDEA, RC5 или CAST-128.

Последние предложения описывают смешанный режим аутентификация/конфиденциальность, который обеспечивает аутентификацию, целостность, защиту от повторного использования и конфиденциальность – и все это используя единую АБ.

8. Управление ассоциациями безопасности и ключами

Существует два подхода к управлению ключами шифрования в сети. Наиболее простой – ручное управление ключами, состоящее в том, чтобы позволить каждому пользователю конфигурировать вручную систему ключей на каждом компьютере системы безопасности. Этот подход оказывается довольно практичным в статической среде малых размеров. В случае локальной сети ручная конфигурация ключей каждого маршрутизатора позволит шифровать маршрутизируемые данные и снижать риск вторжения на маршрутизатор. Однако ввиду быстрого разрастания сетей этот подход не годится надолго.

Другой подход – это автоматическое управление ключами, которое состоит в обмене ключами шифрования путем посылки соответствующих сетевых сообщений. В настоящее время разработано множествопротоколов управления ключами для АБ:

— ISAKMP (Internet Security Association and Key Management Protocol) — доминирующее предложение на сегодняшний день. Оно определяет протокол для АБ, обеспечивающий создание, модификацию и распространение ключей. Обеспечивает также аутентификацию партнеров;

— Oakley — протокол аутентификации партнеров и управления ключами шифрования. Oakley базируется на алгоритме обмена ключей Диффи-Хеллмана;

— SKIP (Simple Key-Management for Internet Protocols) — позволяет аутентифицировать ключи. Не управляет базами данных АБ, но систематически отправляет необходимые криптографические данные в заголовке, предшествующем заголовкам AH и ESP;

— Photoris — протокол, реализующий аутентификацию и обмен публичными ключами.

Среди всех протоколов управления ключами и/или АБ только для ISAKMP, Oakley и Photoris компрометация долговременного ключа не компрометирует предварительно обменяные ключи и, следовательно, конфиденциальность проведенного сеанса связи.

Литература: 1. *Scott O. Bradner, Allison Mankin*. IPng. Internet Protocol Next Generation. Addison-Wesley, Reading, Massachusetts. 1995. 307 p. 2. *Huitema C.* IPv6: The New Internet Protocol. Prentice Hall, Englewood Cliffs, New Jersey. 1996. 188 p. 3. *Stephen A. Thomas*. IPv6 and the TCP/IP Protocols. Wiley Computer Publishing. 1996. 481 p. 4. *Gisèle Cizault*. IPv6: Théorie et pratique. O'Reilly, Paris. 1998. 285 p.

Поступила в редколлегию 09.10.98

Рецензент: д-р техн. наук Долгов В.И.

Фрадков Сергей Александрович, аспирант кафедры АПВТ ХТУРЭ. Научные интересы: сетевые технологии, защита информации, техническая диагностика. Увлечения: программирование, путешествия, иностранные языки. Адрес: Украина, 310726, Харьков, пр.Ленина, 14, тел. +38 (0572) 40-93-26.

УДК 681.325

АЛГОРИТМЫ УСЛОВНОГО ДИАГНОСТИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ

ХАХАНОВ В.И., СЫСЕНКО И.Ю., ПОБЕЖЕНКО В.В., МОНЖАРЕНКО И.В.

Предлагаются алгоритмы условного диагностирования введенного класса макродефектов вычислительных устройств с использованием методов обратного прослеживания и половинного деления на основе выполнения безусловных процедур структурного анализа и моделирования результатов диагноза. Для выбора точки контроля используется граф функциональных связей эквипотенциальных линий, задаваемый в виде матрицы достижимостей.

1. Алгоритм обратного прослеживания

Представленный ниже алгоритм условного диагностирования, не дифференцируемый строго на процедуры контроля и поиска дефектов, описывается обобщенным уравнением диагноза:

$$F^*(F,T,D)\,|_{F,T,g^*} = \cup_i \left(g(T,F) \cap g^*(T,F,D_i)\right) = \varnothing,$$

где g, g^* – эталонная и экспериментальная реакции наблюдаемых линий цифрового устройства (ЦУ); F,