УДК 621.391.28

Мошак Н.Н., д.т.н., профессор СПбГУТ им. проф. М.А. Бонч-Бруевича

ФОРМАЛИЗАЦИЯ И ОЦЕНКА ПРОЦЕССОВ ПРЕДОСТАВЛЕНИЯ МЕХАНИЗМОВ ЗАЩИТЫ В МУЛЬТИСЕРВИСНОЙ СЕТИ. ОБЩИЙ ПОДХОД

Ключевые слова. Мультисервисная сеть, инфотелекоммуникационная транспортная система, услуги безопасности, механизмы защиты.

Реферат. Предложены математическое описание процессов задействования механизмов защиты и метод оценки их влияния на информационное окружение мультисервисной сети связи на технологии IP-QoS. Метод базируется на оптимизации комплексного функционального критерия эффективности сети с учетом выполнения заданных требований к сквозному качеству передачи мультимедийного трафика.

Moshak N.N. FORMALIZATION AND EVALUATION OF SECURITY SERVICES GRANT PROCESSES IN MULTISERVICE NETWORK. GENERAL APPROACH

Keywords. Multiservice network, Infotelecommunication Transport System, Security services.

Abstract. Mathematical formulation of security services enabling processes and evaluation method of theirs influence on informational environment of multiservice IP-QoS telecommunication network are proposed. The method is based on optimization of network efficiency complex functional criterion when meet given requirements to the "end-to-end" quality of multimedia traffic transfer.

Введение. Создание национальной защищенной мультисервисной сети связи (МСС) и, в частности, ее коммуникационного ядра - инфотелекоммуникационной транспортной системы (ИТС) - является задачей ближайшей перспективы. Выделяют специальные механизмы защиты (обеспечение целостности данных, шифрование, цифровая подпись, контроль доступа, аутентификация, нотаризация (заверение), заполнение трафика, управление маршрутизацией), которые используются для реализации конкретных услуг безопасности или их сервисов и общие (доверительная функциональность, метки безопасности, «аудиторская» проверка), не относящиеся к конкретным услугам [1]. Указанные механизмы реализуют связи базовые услуги безопасности (конфиденциальность, аутентификация, целостность, контроль доступа, причастность), также определенных [1].

Известно [2], что любые механизмы защиты вносят временную, протокольную и потоковую избыточность в информационное окружение сети и приводят к ухудшению ее характеристик. Эти виды избыточности при проектировании защищенной сети должны быть учтены в критериях эффективности и ограничениях задач анализа МСС [3]. Однако модели процессов предоставления механизмов защиты в рамках единых критериев эффективности на сегодня исследованы недостаточно полно**.** Прикладные аспекты указанной проблемы связаны с повышением качества проектирования защищенных МСС, что в конечном итоге приводит к повышению эффективности использования сетевых ресурсов и сокращению затрат на их создание.

Данная работа посвящена построению моделей процессов задействования специальных механизмов защиты и является дальнейшим развитием идей работ [4-6]. Метод оценки их влияния на информационное окружение ИТС, реализованной на технологии IP-QoS, базируется на общих принципах, разработанных и сформулированных в [6].

Задача анализа МСС

Пусть входная мультимедийная нагрузка по вызовам дается выражением $Y^{malty} = \left\| a_{ij}^{malty} \right\| = Y^B + Y^C = \left\| a_{ij}^B \right\| + \left\| a_{ij}^C \right\|$, где Y^B и Y^C - матрицы тяготений мультимедийной нагрузки (цифровая речь класса B и данные класса C в терминах ATM Fotum). Задача анализа МСС в общем виде формулируется следующим образом [3]. При заданной топологии МСС, структуре двухкомпонентных мультимедийных потоков Y^B и Y^C, заданной системе маршрутов $M_{st}^{B(C)}$ найти оптимальные значения длины речевых пакетов L_{opt}^B и значения коэффициентов загрузки ρ_{ij}^B, доставляющих максимум функционалу

$$\arg\max\ K^B(L^B, \rho_{ij}^B) \qquad (2)$$

при ограничениях

$$\sum_{m=1}^{M_{st}^B} p_{st,m}^B\ (1 - F_{st,m}^B(\theta_{st}^B)) \le d^B\ ,$$

$$L^B \lhd \theta_{st}^B \upsilon^B - H_{IP}\,,$$

$$0 \le \rho_{ij}^B \lhd 1,\ \forall\ st \in S^B : a_{st}^B \ne 0\,. \qquad (2)$$

По полученным значениям $\rho_{ij}^{B\max}$ и L_{opt}^B найти значения $\rho_{ij}^{C\max}$ и L_{opt}^C, доставляющих максимум функционалу

$$\arg\max\ K^C(L^B, \rho_{ij}^B, L^C, \rho_{ij}^C) \qquad (3)$$

при ограничениях

$$T_{st}^C = \sum_{m=1}^{M_{st}^C} p_{st,m}^C\ (\sum_{ij \in l_{st,m}^{Cp}} T_{ij}^C + \sum_{\forall j: ij \in l_{st,m}^{Cp}} T_j^C) - \frac{L^C - H_{IP}}{\omega^C} \le T^C \text{ или}$$

$$\sum_{m=1}^{M_{st}^C} p_{st,m}^C\ (1 - F_{st,m}^C(T^C)) \le d^C,\ \forall\ st \in S^C : a_{st}^C \ne 0 \qquad (4)$$

и все параметры первой задачи найдены и фиксированы.

Здесь $p_{st,m}^{B(C)}$ - вероятность выбора m-го маршрута $l_{st,v}^{B(C)}$ из множества $M_{st}^{B(C)}$; $F_{st,m}^{B(C)}$ - функция распределения сквозного времени пребывания θ_{st}^B (T^C) речевого пакета (пакета данных) в тракте $st \in S^{B(C)}$. $d^{B(C)}$ - вероятность превышения задержки θ_{st}^B (T^C) пребывания пакетов в тракте передачи $st \in S^{B(C)}$. T_j^C - задержка пакетов в коммутационном поле маршрутизатора, с; $T_{ij}^C -$ время обслуживанием пакетов в маршрутизаторе, с; $(L^C - H_{IP})/\omega^C$ - время накопления информационной части пакета у отправителя, с (H_{IP} - длина заголовка IP-пакета, бит; ω^C - скорость работы установки данных в мультимедийной оконечной установке, бит/с); υ^B - скорость работы речепреобразующего устройстве в мультимедийной оконечной установке, бит/с.

Формализация процессов предоставления механизмов защиты

Предоставление механизмов защиты осуществляется по принципам предоставления сервиса базовой эталонной модели взаимодействия открытых систем [4]. *Будем различать 1) протокольные механизмы защиты, применение которых преобразует структуру и/или формат уровневого примитива архитектуры МСС и вносит временную и/или протокольную избыточность в информационное окружение сети* (например, механизмы симметричного шифрования с и механизмы обеспечения целостности с применением симметричных ЭЦП без центра сертификации (Authentication Center, *CA*); коды обнаружения целостности и/или имитозащитных вставок (ИЗВ)). При этом могут быть востребованы один или одновременно несколько механизмов защиты соответствующего

логического уровня при формировании защищенного протокольного блока для каждого типа информации многокомпонентной потоковой структуры мультимедийного соединения в режиме сессии.

2) потоковые механизмы защиты, применение которых порождают дополнительный трафик безопасности и вносит потоковую избыточность в информационное окружение сети (например, механизмы защиты с применением простой аутентификации без защиты, «Заполнение трафика», «Нотаризация»). Кроме того, трафик безопасности порождается при обмене сертификатами центра сертификации *CA* между центром и корреспондентом в процессе аутентификации открытых ключей и формировании сеансовых ключей в двухключевых криптосистемах; при восстановлении целостности сообщений. Эти процессы включают в себя как фазу передачи сервисных примитивов трафика безопасности, так и процесс их обработки в оконечных системах [6].

3) *гибридные механизмы защиты, применение которых как преобразует структуру и/или формат уровневого примитива, так и порождают дополнительный трафик безопасности (например, механизмы обеспечения целостности с применением ассиметричной ЭЦП, механизмы простой аутентификации с защитой, механизмы строгой аутентификации и др.)* Определим, что в первом случае процессы предоставления услуг безопасности моделируется системами массового обслуживания с протокольной услугой безопасности (СМОПб), во втором – отдельными однофазными или многофазнми СМО с потоковой услугой безопасности (СМОУб), в третьем – сочетаниями указанных СМО.

Моделирование процессов предоставления протокольных механизмов защиты Рассмотрим типовые модели процессов предоставления механизмов защиты, вносящих временную и протокольную избыточность в информационное окружение сети, на примерах механизмов «Шифрование» (предоставление криптографических процедур в одноключевой криптосистеме) и «Контроль целостности» (применение имитозащитных вставок).

Механизмы шифрования. Механизмы шифрования или криптографические механизмы представляют собой совокупность криптографических алгоритмов и криптопеременных секретных величин. Различают симметричные и ассиметричные системы шифрования или одноключевые и двух ключевые шифры. Симметричные системы применяются в основном для предоставления криптографических процедур, в то время как применение асимметричных шифров можно свести к двум основным аспектам применения [7]: 1) цифровая подпись $S^i(M)$**,** когда отправитель i «подписывает» сообщение M с помощью своего личного ключа S_i; 2) обмен ключами, при котором происходит обмен сеансовым ключом с применением личных ключей одной и/или обеих сторон.

Симметричное шифрование E (дешифрование D) базируется на централизованном изготовлении и распространении секретных ключей K_e центром доверия. Симметричные шифры разделяют на ***поточные***, которые преобразуют каждый символ в потоке исходных данных, и ***блочные***, осуществляющие последовательное преобразование блоков данных. В основном применяется блочное шифрование. Оно осуществляется как многократное выполнение типовой процедуры преобразования, называемой раундом шифрования или раундовой функцией шифрования R . Для осуществления блочного шифрования данные представляются в виде последовательности m_i-битовых блоков сообщения $M = \{m_i\}$, $i = \overline{1,n}$. В наиболее широко применяемых шифрах размер выходных блоков равен размеру входных блоков. Минимальной безопасной длиной блока принято считать значение m_i=64 бит. Базовыми криптографическими примитивами во многих современных шифрах

являются операция подстановки и операция перестановки, которая органически ее дополняет. Блочный шифр, как правило, представляет собой множество подстановок большого размера, заданных на множестве возможных входных блоков, выбираемых от секретного ключа. Временная избыточность, вносимая процессом симметричного шифрования/расшифрования в информационного окружения сети может быть формализована аддитивной формой

$$t_{убш} = t_{ш} + t_{рш} = n\ R(m_i / V_{ш} + m_i / V_{рш}), \qquad (5)$$

где каждая составляющая моделируется СМОПб вида $t_{ш} = m_i / V_{ш}$,с и $t_{рш} = m_i / V_{рш}$, с. Здесь m_i-длина i-го блока, бит ($i = \overline{1,n}$, $n = M / m$); $V_{ш}$, $V_{рш}$, бит/с – соответственно скорость шифрования/расшифрования; R – число раундов шифрования одного m_i-битового блока. В качестве примеров блочных симметричных шифров на основе управляемых операций преобразования можно указать шифры ASE, DES, Triple DES, RC2, RC5, RC6, CAST-128, Blowfish, ARCFour, Rijndael, DDP-64, CIKS-1, SPECTR-H64 и другие [8].

Для задания неопределенности хода шифрования информации могут применяться вероятностные шифры [7], в которых в преобразуемое сообщение вводятся случайные данные. Если функция шифрования E_K имеет исходное значение скорости преобразования $V_{ш0}$, то при использовании шифров с простым вероятностным механизмом скорость шифрования $V_{ш}^{*} = V_{ш0}(M^{*} - r) / M^{*}$, где $M^{*} = r + M$ – шифруемое сообщение, M –битовый блок открытого сообщения, r-битовый случайный блок. Таким образом, скорость уменьшается в r/M раз, а блоки шифротекста увеличиваются в M^{*}/M раз (здесь и далее * - будем обозначать защищенный параметр). При вероятностном объединении случайных и информационных битов в зависимости от секретного ключа требует существенного увеличения доли случайных битов (80% и более), что значительно увеличивает время шифрования.

Временная избыточность $t_{убш}$ должна быть учтена в ограничениях первой и второй задачи анализа на задержку пакетов данных в тракте передачи

$$\theta_{st}^{*B} = \theta_{st}^{B} - t_{убш} \text{ и } T_{st}^{*C} = T_{st}^{C} - t_{убш} \qquad (6)$$

Механизмы контроля целостности данных. Контроль целостности данных – это обнаружение их несанкционированных изменений в процессе передачи. Механизмы «Контроль целостности» вносят как временную, так и протокольную избыточность, связанную с вычислением защитных контрольных сумм (ЗКС) или кодов обнаружения модификаций (КОМ). Существует два типа механизмов обеспечения целостности данных: 1) для защиты целостности отдельного блока данных и 2) для защиты, как целостности отдельного блока данных, так и последовательности потока блоков данных в сеансе связи. Значение криптографических КОМ может быть получено за один или несколько шагов и является математической функцией криптопеременных и данных.

В мультисервисных сетях связи формирование/проверка КОМ осуществляется в сеансе связи для каждого пакета данных только в оконечных мультимедийных установках. При этом функции формирования/проверки КОМ, как правило, реализуются в виде соответствующих программ на транспортном или сеансовом уровнях логической структуры сети в оконечных мультимедйных системах (Maltimedia End System, MES). Для обеспечения целостности последовательности блоков данных в протоколах с установлением связи одновременно с КОМ отдельных пакетов используются

возможности протоколов с установлением связи: *нумерация* пакетов, *повторная передача*, а также дополнительные средства – *временные или синхронизирующие метки*, обычно используемые для цифровых видео или аудио приложений. Указанный механизм не задействуется при передаче изохронного трафика класса B, ввиду его значительной информационной избыточности. При передаче данных могут быть использованы *отметки времени* в целях обеспечения ограниченной формы защиты против воспроизведения отдельных блоков данных. Этот механизм сам по себе не может защитить от воспроизведения отдельного блока данных. На соответствующих уровнях архитектуры обнаружение манипуляции может привести к задействованию процедуры восстановления как отдельного блока данных, так и последовательности потока блоков данных.

Укажем основные таксоны КОМ – 1) Электронная цифровая подпись (ЭЦП) и ее разновидности (контрольные суммы CRC и коды аутентификации сообщений (message authentication code, MAC), известные также как коды проверки подлинности данных (data authentication code, DAC)); 2) имитозащитные вставки (ИВЗ). Построим модели процессов контроля целостности отдельных блоков данных на примере ИЗВ.

Имитозащитная вставка представляет собой k-битовый блок, который вырабатывается по определенному правилу из открытых данных с использованием симметричного секретного ключа, который и гарантирует невозможность (трудность) подделки. Для вычисления имитовставки используется алгоритм, задающий зависимость ИЗВ от каждого бита сообщения. В качестве алгоритма для вычисления имитовставки используется хэш-функция - односторонняя функция $\mathrm{h}(M)$, преобразующая сообщение M произвольной длины в выходной хэшкод постоянной длины H с применением или без применения секретных параметров и не позволяющее осуществить обратное преобразование. Могут быть использованы следующие два варианта: 1) *вычисление ИЗВ по открытому тексту* M и 2) *вычисление ИЗВ по шифротексту* M^***.** В первом случае отправитель формирует $H_{ИВЗ1i} = \mathrm{h}(M)$ за время $t_i^{H\,ИВЗ1}$. На приеме получатель извлекает M за время $t_j^{M\,ИВЗ1}$, сам формирует $H_{ИВЗ1j} = \mathrm{h}(M)$ за время $t_j^{H\,ИВЗ1}$ и сравнивает их за время $t_j^{сравнН\,ИВЗ2}$ Во втором случае отправитель формирует $H^*_{ИВЗ2} = \mathrm{h}(M^*) = \mathrm{h}(\mathrm{E}_{K_i^{ИВЗ2}}(M))$, а время его вычисления $t_{ИВЗ1i}$ включает в себя время $t_i^{M*ИВЗ2}$, затрачиваемое на шифрование пакета (сообщения) M, и время $t_i^{H*ИВЗ2}$, затрачиваемое на вычисление собственно ИВЗ. Максимальная длина ИЗВ определяется схемой или режимом простой замены и составляет k=64 бит. Значение параметра k (число двоичных разрядов в имитовставке) определяется криптографическими требованиями с учетом того, что вероятность навязывания ложных данных $p = 1/2^k$. На практике, как правило, используют ИЗВ длиной 32 бит (один блок), предоставляющую достаточный ($p = 10^{-9}$) уровень защищенности. На приеме получатель извлекает шифрованное M^* за время $t_j^{M*ИВЗ2}$ расшифровывает его на секретном ключе отправителя $K_i^{ИВЗ2}$ за время $t_j^{M\,ИВЗ2}$.

Процесс формирования/проверки ИВЗ может быть представлен соответственно двумя аддитивными формами.

$$t_{ИВЗ1}^{цел} = t_i^{H\,ИВЗ1} + t_j^{M\,ИВЗ1} + t_j^{H\,ИВЗ1} + t_j^{сравнН\,ИВЗ2} \tag{6}$$

$$t_{ИВЗ2}^{цел} = t_i^{M*ИВЗ2} + + t_i^{H*ИВЗ2} + t_j^{M*ИВЗ2} + t_j^{M\,ИВЗ2} \tag{7}$$

Операция конкатенации КОМ к пакету данных, вносящая протокольную избыточность, может быть формализована аддитивной формой

$$L^{*C} = L^C + S^i \qquad (8)$$

Процессы создания/проверки КОМ моделируются СМОПб и должны быть учтены во второй задаче анализа по аналогии с применением процессов симметричного шифрования.

Моделирование процессов предоставления потоковых механизмов защиты

Построим типовые модели процессов предоставления потоковых механизмов защиты, вносящих потоковую избыточность в информационное окружение сети на примере процесса предоставления механизмов простой аутентификации без защиты и процессов восстановления целостности.

Различают услугу аутентификации или подтверждение подлинности равноправных логических объектов (пользователей, инфоприложений), которая реализуется на фазе установления мультимедийного соединения потоковыми механизмами простой и/или строгой аутентификации, и услугу аутентификации отправителя данных в сессии, которая реализуется протокольными механизмами защиты [1]. Протоколы аутентификации можно классифицировать в соответствии со следующими параметрами [7]: тип аутентификации, тип используемой криптосистемы, вид реализации криптосистемы, количеству обменов служебными сообщениями между субъектами. Дополнительно они могут различаться наличием диалога и доверия между субъектами, а также использованием в протоколах отметок времени. При использовании криптографических процедур они должны сочетаться с протоколами квитирования установления связи, что обеспечивает защиту от воспроизведения. Различают простую и строгую аутентификацию. Простая аутентификация может быть осуществлена без защиты и с защитой.

Простая аутентификация без защиты с центром CA. В случае применения простой аутентификации без защиты с центром CA транзакция аутентификации равноправных логических объектов включает в себя следующие фазы: 1) отправитель i передает получателю в открытом (незащищенном) виде свой идентификатор (*имя*) ID_i и (необязательно) *пароль* Pi за время $t_{i,j}^{прдIDi,Pi}$; 2) получатель j передает ID_i и Pi за время $t_{j,CA}^{прдIDi,Pi}$ центру CA для сопоставления за время $t_{CA}^{обрPi}$ с Pi, который хранится у него в качестве атрибута; 3) центр CA подтверждает или отрицает получателю j действительность удостоверений за время $t_{CA,j}^{прдPi}$; 4) успешность или неуспешность аутентификации может быть сообщена отправителю i за время $t_{j,i}^{прдPi}$.

Процесс простой аутентификации с центром CA можно формализовать аддитивной формой вида

$$t_{б/з}^{аут} = t_{i,j}^{прдIDi,Pi} + t_{j,CA}^{прдIDi,Pi} + t_{CA}^{обрPi} + t_{CA,j}^{прдPi} + t_{j,i}^{прдPi} \qquad (9)$$

Процессы применения механизмов простой аутентификации без защиты с центром CA, порождающие дополнительный трафик безопасности, формализуются в соответствии с их вербальным описанием следующей аддитивной формой

$$\rho_{б/з}^{аут} = \rho_{i,j}^{прдIDi,Pi} + \rho_{j,CA}^{прдIDi,Pi} + \rho_{CA,j}^{прдPi} + \rho_{j,i}^{прдPi}. \qquad (10)$$

Здесь $\rho_{i,j}^{прдIDi,Pi}$; $\rho_{j,CA}^{прдIDi,Pi}$; $\rho_{CA,j}^{прдPi}$; $\rho_{j,i}^{прдPi}$ - соответственно коэффициенты загрузки линейно-цифрового тракта (ЛЦТ) при передаче пароля P_i отправителя i к получателю j; от получателя j к центру СА; от центра СА к получателю j; от получателя j к

отправителю i. Каждая фаза передачи трафика безопасности в (9) моделируется СМОУб. Потоковые модели типа (10) должны быть учтены во второй задаче анализа при расчете коэффициента загрузки сети трафиком класса C при условии, что приоритеты обслуживания служебных сообщений безопасности и трафика данных совпадают.

Потоковые модели процессов восстановления целостности передаваемых данных могут быть построены, например, на базе моделей механизмов обратной связи в виде функциональной зависимости $S^{цел\,k} = f(L^{*k}, p_{ij}^{KOM})$ [6], где L^{*C} - длина защищенного пакета (бит), а p_{ij}^{KOM} - вероятность нарушения его целостности, которая в свою очередь зависит от модели нарушителя в сети. Для речевых пакетов будем считать $S^{цел\,B}$=1, так как для них недопустимы переспросы, но могут допускаться их определенные потери. Величина $S^{цел\,C}$ зависит от модели нарушителя и является отдельной научной проблемой, исследование которой выходит за рамки данной работы. Предположим, что вероятность $p_{ij}^{KOM} \approx p^{KOM}$ для всей ИТС одинакова. Если обозначить p_0^{KOM} вероятность отсутствия нарушения целостности в кадре длины L^{*C} и предположить, что число переспрашиваемых кадров подчинено геометрическому распределению, то для модели тракта передачи с решающей обратной связью

$$S^{цел\,C} = -\frac{p_0^{KOM}}{1-p_0^{KOM}} \ln p_0^{KOM}. \qquad (11)$$

Эта потоковая модель процесса восстановления целостности данных должна быть учтена в защищенных моделях логических соединений транспортного уровня ИТС-IP-QoS (так как восстановление сообщений осуществляется на транспортном уровне) при введении механизмов восстановления целостности передаваемых блоков данных класса C в мультимедийном соединении [6].

Формализовать процесс восстановления целостности блоков данных класса C можно также следующим способом. Пусть пользователь производит повторную попытку передачи пакета при обнаружении нарушения целостности на i-ом транзитном маршрутизаторе с вероятностью p^{KOM}. Вероятность успешной передачи пакета с n-й попытки равна $(p^{KOM})^{n-1}(1-p^{KOM})$, а среднее число повторных попыток на одно соединение для абсолютно настойчивого пользователя

$$M^{KOM} = \sum_{n=1}^{\infty} n\,(p^{KOM})^{n-1}(1-p^{KOM}). \qquad (12)$$

В этом случае интенсивность $\lambda_{st}^{*C,KOM}$ поступления пакетов данных класса C в тракт передачи дается выражением:

$$\lambda_{st}^{*C,KOM} = \lambda_{st}^{C} \sum_{n=1}^{\infty} n\,(p^{KOM})^{n-1}(1-p^{KOM}) = \frac{\lambda_{st}^{C}}{1-p^{KOM}}, \qquad (13)$$

где λ_{st}^{C} –интенсивность поступления пакетов данных класса C в тракт передачи в сессии от отправителя s к получателю t без учета нарушения их целостности.

Таким образом, при необходимости учета процессов восстановления целостности передаваемых сообщений необходимо в моделях логических соединений уровня межсетевого доступа параметр λ_{st}^{C} в выражении для коэффициентов загрузки тракта передачи ρ_{st}^{C} [6] заменить на $\lambda_{st}^{*C,KOM}$.

Моделирование процессов предоставления гибридных механизмов защиты

Применение гибридных механизмов защиты вносит как временную и протокольную, так и потоковую избыточность в информационное окружение сети. Построим типовую модель предоставления гибридных механизмов защиты на примере механизма строгой аутентификации на основе *асимметричных ЭЦП* с центром CA.

Строгая аутентификация — опирается на использование криптографической техники для защиты обмена удостоверяющей информации и заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом. В соответствии с рекомендациями стандарта **X.509** различают процедуры одно-, двух- и трехсторонней строгой аутентификации.

Односторонняя аутентификация предусматривает передачу мандата только в одном направлении. Данный тип аутентификации позволяет *подтвердить подлинность* отправителя и гарантировать, что мандат (информация, формируемая и передаваемая пользователем в процессе обмена строгой аутентификацией) был фактически сгенерирован отправителем, а также *подтвердить подлинность* получателя, которому был предназначен мандат отправителя Дополнительно односторонняя аутентификация позволяет *обнаружить нарушение целостности*, передаваемой информации и проведение атаки типа «повтор передачи».

Двусторонняя аутентификация устанавливает дополнительно тот факт, что ответный мандат был фактически выработан получателем и предназначен отправителю, а также, что метка времени является «текущей».

Трехсторонняя аутентификация содержит дополнительную передачу дополнительного мандата отправителя и, в отличие от двухсторонней аутентификации, не требует проверки метки времени.

Проведение строгой аутентификации требует обязательного согласования сторонами используемых криптографических алгоритмов и ряда дополнительных параметров. В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы:

1) протоколы на основе *симметричных алгоритмов шифрования*,
2) протоколы на основе *однонаправленных ключевых хеш-функций*,
3) протоколы на основе *асимметричных алгоритмов шифрования*,
4) протоколы на основе алгоритмов *электронной цифровой подписи*.

Строгая аутентификация на основе асимметричных ЭЦП. ЭЦП S^i – это зашифрованное каким-либо личным (секретным) ключом отправителя Si (не обязательно совпадающего с ключом, использованным для шифрования сообщения) значение хэш-функции $H = \mathrm{h}(M)$. Процесс шифрования хэшкода сообщения и называется подписью S^i. Электронная цифровая подпись S^i добавляется к мандату M ($M^* = M + S^i$) при аутентификации равноправных логических объектов или к пакету L^C ($L^{*C} = L^C + S^i$) при аутентификации отправителя данных и может шифроваться вместе с ним при необходимости сохранения данных в тайне. Для проверки ЭЦП S^i используется открытый ключ отправителя Pi. Двухключевые криптоалгоритмы позволяют обеспечить строгую доказательность факта составления того или иного сообщения конкретными пользователями криптосистемы. Использование однонаправленных функций в асимметричных системах ЭЦП не позволяет злоумышленнику вычислить личный ключ отправителя Si, применяемый к хэшкоду. Например, в ЭЦП S^{RSA} RSA – это задача факторизации, а в ЭЦП S^{EGSA} Эль Гамаля – это задача дискретного логарифмирования. Таким образом, строгая аутентификация здесь основывается на наличии у пользователей аутентифицирующих их личных ключей. Открытые ключи могут быть получены а) по запросу из центра CA или б) переданы непосредственно отправителями в процессе аутентификации Процедура аутентификации в этом случае выглядит следующим образом (временем, затраченным на формированием открытого и секретного ключей пользователем будем пренебрегать).

Рассмотрим обобщенную схему формирования и проверки ассиметричной ЭЦП на примере ЭЦП RSA. Перед отправкой сообщения M вычисляется его хэш-функция $H_i = \mathrm{h}(M)$ за время t_i^{Hi}. Затем вычисляется ЭЦП RSA $S^{iRSA} = \mathrm{E}_{\mathrm{Si}}(H_i)$ с применением личного ключа отправителя Si за время t_i^{SiRSA} и мандат ($M^*_{iRSA} = M \,||\, S^{iRSA}$) отправляется получателю за время $t_{i,j}^{прдMiRSA}$. При получении пары ($M \,||\, S^{iRSA}$) получатель j вычисляет хэш-значение M двумя разными способами. Во-первых, он восстанавливает хэшкод $\tilde{H}_i = \mathrm{D}_{P_i}(E_{S_i}(H_i))$, применяя криптографическое преобразование ЭЦП с использованием открытого ключа отравителя P_i за время $t_j^{\tilde{H}i}$. Во-вторых, получатель рассчитывает хэш-значение сообщения $H_j = \mathrm{h}(M)$ с помощью аналогичной хэш-функции h(*) за время t_j^{Hj} и сравнивает эти значения за время $t_j^{сравнH}$. Если эти два значения совпали, получатель считает, что мандат подлинный. Невозможность подделки ЭЦП гарантируется сохранением в тайне личного ключа отправителя S_i, т. е. ответственность возлагается на пользователя.

Любая транзакция аутентификации открытых ключей пользователей в двухключевой криптосистеме, получаемых по запросу из центра сертификации CA включает в себя следующие фазы. Получатель j при получении мандата M^*_{iRSA} 1) запрашивает в CA цифровой сертификат отправителя (содержит открытый ключ P_i и время действия сертификата) за время $t_{j,CA}^{запрPi}$. Ответ CA 2) шифруется на личном ключе центра за время $t_{CA}^{обрPi}$ и 3) направляется отправителю за время $t_{CA,j}^{отвPi}$. Получатель j, используя открытый ключ центра, который известен каждому, 4) расшифровывает шифрограмму за время $t_j^{аутCA}$ и получает заверенную версию открытого ключа получателя P_j.

Если центр сертификации CA не участвует, то в этом случае отправитель пересылает свой открытый ключ самостоятельно при передаче мандата M^*_{iRSA}.

Процесс строгой аутентификации с центром CA в этом случае можно формализовать следующей аддитивной формой

$$t_{строг,ассим\ ЭЦП}^{аутCA} = t_i^{Hi} + t_i^{SiRSA} + t_{i,j}^{прдM*iRSA} + t_{j,CA}^{запрPi} + t_{CA}^{обрPi} + t_{CA,j}^{отвPi} + t_j^{аутCA} + t_j^{\tilde{H}i} + t_j^{Hj} + t_j^{сравнH} \quad (14)$$

Трафик безопасности $\rho_{строг,асимЭЦП}^{аутCA}$ здесь порождается при передаче мандатов и в процессе аутентификации открытых ключей пользователей при обмене с центром CA, а процесс его передачи моделируется трехфазной СМОУб и может быть формализован аддитивной формой вида

$$\rho_{строг,асимЭЦП}^{аутCA} = \rho_{i,j}^{прдMi*RSA} + \rho_{j,CA}^{запрPi} + \rho_{CA,j}^{отвPi} \quad (15)$$

В этой транзакции процессы вычисления хэшкода, ЭЦП, их проверки и сравнения моделируются соответствующими СМОПб. Подходы к реализации указанных моделей приведены в [5]. Необходимо отметить, что 1) в зависимости от применяемых процедур одно-, двух- и трехсторонней строгой аутентификации транзакция аутентификации требует обмена от двух до семи служебных сообщений [1]; 2) объем трафика аутентификации, порождаемого при аутентификации равноправных логических объектов, напрямую зависит от величины интенсивности λ^{multy} (вызов/час) мультимедийных вызовов, которые создают пропущенную нагрузку (среднее число занятых приборов обслуживания в момент t)

$$\widehat{a}_{ij}^{multy} = (a_{ij}^{B} + a_{ij}^{C})\,(1 - b^{malty}) = N_{ij}^{multy} Mark_{ij}^{multy}\,\lambda_{ij}^{multy} \cdot t^{multy}\,\,(1 - b^{malty})\,(\text{Эрл}), \qquad (16)$$

где $Mark_{ij}^{multy} = \sum_{k} \left\lceil \frac{\upsilon^{k}}{\Theta^{\min}} \right\rceil = \left\lceil \frac{\upsilon^{B}}{\Theta^{\min}} \right\rceil + \left\lceil \frac{\upsilon^{B}}{\Theta^{\min}} \right\rceil$ - суммарная марка трафика (обслуживающий прибор), требуемого для обслуживания всех потоковых компонент $k-$го класса мультимедийного соединения в линейно-цифровом тракте (ЛЦТ) ij [8]; $\Theta^{\min}$ - базовая минимальная ширина полосы пропускания, бит/с; t^{multy} – средняя длительность мультимедийного соединения, час; b^{multy} - величина допустимых потерь мультимедийного вызова в сети; N_{ij}^{multy} - количество мультимедийных оконечных устройств, включенных в машрутизатор i, создающих суммарную нагрузку в направлении маршрутизатора j.

В сессии каждая их потоковых компонент мультимедийного соединения обслуживается на транзитных маршрутизаторах с заданным качеством QoS, которое обеспечивается, с одной стороны, зарезервированными на фазе установления соединения требуемыми сетевыми ресурсами (в частности, пропускной способностью) и соответствующей дисциплиной обслуживания - с другой. Текущая загрузка ЛЦТ базовыми потоками ρ_{ij}^{B} и ρ_{ij}^{C} в МСС на технологии IP-QoS с учетом абсолютного приоритета обслуживания речевых пакетов (с дообслуживанием) по отношению к пакетам данных дается выражениями [3]

$$\rho_{ij}^{B} = \frac{L^{B} + H_{NA}}{L^{B} - H_{IP}}\,\frac{Mark_{ij}^{B}\Theta^{\min}}{V_{ij}}\,\widehat{a}_{ij}^{B}\,\eta^{B} z^{B}, \qquad (17)$$

$$\rho_{ij}^{C} = 1 - \rho_{ij}^{B} - \frac{L^{C} + H_{NA}}{T_{ij}^{C} V_{ij}} - \frac{\rho_{ij}^{B}}{1 - \rho_{ij}^{B}}\,\frac{L^{B} + H_{NA}}{T_{ij}^{C} V_{ij}}. \qquad (18)$$

Здесь H_{NA} - заголовок уровневого примитива уровня сетевого доступа, бит; η^{B}, z^{B} - соответственно коэффициенты уплотнения пауз в речевом потоке и коэффициент сжатия речевого потока; T_{ij}^{C} - заданное среднее время пребывания пакета данных в ЛЦТ, с; V_{ij} - скорость передачи в ЛЦТ, с.

Служебные пакеты трафика аутентификации, могут обрабатываться на маршрутизаторах с более низким или равным приоритетом по отношению к пакетам основных потоковых компонент. В предположении, что они обслуживаются в сети с одинаковым приоритетом для пакетов данных, то коэффициент загрузки ЛЦТ трафиком аутентификации в общем виде можно представить как

$$\rho_{ij}^{*} = \frac{L^{*} + H_{NA}}{L^{*} - H_{IP}}\,\frac{Mark_{ij}^{C}\Theta^{\min}}{V_{ij}}\,a_{ij}^{*}, \qquad (19)$$

где для фазы установления мультимедийного соединения

$$a_{ij}^{*} = N_{ij}^{multy} Mark_{ij}^{multy}\,\lambda_{ij}^{multy}\,\,(1 - b^{malty})\,\theta_{ij}^{*}\,Mn^{*}. \qquad (20)$$

Здесь θ_{ij}^{*} - непроизводительное время занятия ЛЦТ трафиком безопасности на фазе установления мультимедийного соединения, час; Mn^{*} - математическое ожидание числа служебных сообщений трафика безопасности, приходящихся на один мультимедийный

вызов, при формализации процессов аутентификации равноправных логических объектов, будем обозначать

Для фазы сессии

$$a_{ij}^{*} = N_{ij}^{multy} Mark_{ij}^{C} \lambda_{ij}^{C} \theta_{ij}^{ses*} Mn^{*}, \quad (21)$$

где λ_{ij}^{C} - интенсивность поступления в ЛЦТ пакетов данных, пакет/час; θ_{ij}^{ses*} - непроизводительное время занятия ЛЦТ трафиком безопасности в сессии, час.

При сделанных выше предположениях суммарный коэффициент загрузки ЛЦТ трафиком данных и трафиком безопасности будет иметь следующий вид

$$\rho_{ij}^{*C} = \rho_{ij}^{C} + \sum_{l} \rho_{ij}^{*l}, \quad (22)$$

где ρ_{ij}^{*l} - величина коэффициента загрузки l-ой потоковой компоненты трафика безопасности (например, аутентификации, восстановления целостности, заполнения трафика).

Выводы

1. Процессы предоставления механизмов защиты в мультисервисной сети могут моделироваться как отдельными системами массового обслуживания с протокольной услугой безопасности СМОПб или системами массового обслуживания с потоковыми услугами безопасности СМОУб, так и совокупностью указанных СМО.
2. Модели процессов предоставления механизмов защиты, вносящих временную и протокольную избыточность в информационное окружение сети, в виде СМОПб должны учитываться в ограничениях и критериях эффективности задач анализа МСС.
3. Модели процессов предоставления механизмов защиты, вносящих потоковую избыточность в информационное окружение сети, в виде СМОУб должны учитываться в коэффициентах загрузки базового трафика при одинаковом приоритете обслуживания или отдельно при обслуживании с более низким приоритетом в задачах анализа МСС и/или ее сигнальной системы.
4. Метод оценки влияния процессов предоставления механизмов защиты на характеристики и ресурсы сети должен базироваться на построении и сравнительном анализе критериев эффективности защищенных и не защищенных ИТС на технологии IP-QoS с учетом ее архитектуры и общих принципах, разработанных и сформулированных в [6].

Литература

1. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть.2. Архитектура защиты. – М.: ИПК Издательство стандартов, 1999.

2. *А.М. Александров*. Безопасность сетей связи и некоторые задачи теории телетрафика // Электросвязь. - 2003.- №12.-с.20-21.

3.*Мошак, Н.Н.* Теория проектирования транспортной системы инфокоммуникационной сети: учеб. пособие для вузов / Н.Н. Мошак. СПб.: Энергомашиностроение, 2006. 159 с.

4.*Мошак, Н.Н.* Особенности архитектуры мультисервисных сетей с услугами безопасности / Н.Н. Мошак // Электросвязь. 2007. № 5. с. 34 – 40.

5.*Мошак, Н.Н.* Модели услуг аутентификации в задаче анализа инфокоммуникационной сети / Н.Н. Мошак // Известие вузов России, Радиоэлектроника. 2007. №5. с.18-25.

6.*Мошак, Н.Н.* Модели, методы и алгоритмы анализа процессов функционирования инфотелекоммуникационных транспортных систем: дис. 05.13.13 докт. тех. наук: защищена 16.12.2009. утв. 09.04.2010 / Мошак Николай Николаевич. Л., 2009. 345 с.

7.*Молдавян, А.А*. Криптография: от примитивов к синтезу алгоритмов / А.А. Молдовян, Н.А. Молдовян, М.А. Еремеев. СПб.: БХВ-Петербург, 2004. 448 с.: ил.

8. *Фергюстен Н., Шнайер Б.* Практическая криптография / Н. Фергюстен, Б. Шнайер; пер. с англ. Н.Н. Селиной. М.: Издательский дом «Вильямс». 2005. 424 с.:ил.

9. *Ершов, В.А.* Метод расчета пропускной способности узла мультисервисной АТМ-сети с обходами / В.А.Ершов, Э.Б.Ершова // Электросвязь. 2002. № 12. С. 10–12.