УДК 621.391.28

Н. Н. Мошак
Государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Модели услуг аутентификации в задаче анализа инфокоммуникационной сети

Приведены модели механизмов простой (пароль, хэш-функция, одноразовые параметры) и строгой (одно- и двухключевое шифрование, ключевая хэш-функция, электронная цифровая подпись) аутентификации равноправного логического объекта и отправителя данных. Сформулирована задача анализа инфокоммуникационной сети на базе общих функционалов оценки эффективности использования ее ресурсов с учетом указанных моделей.

Инфокоммуникационная сеть, модели механизмов аутентификации, информационная безопасность

В основе защиты инфокоммуникационной сети (ИКС) лежит ее политика информационной безопасности (в дальнейшем "Политика"), которая формулирует требования к подсистеме защиты и контролю ее состояния [1]. Указанные требования разрабатываются с учетом моделей угроз и нарушителя (в том числе легальных пользователей), а также приоритетов услуг безопасности в ИКС. Стандарт ГОСТ Р ИСО 7498-2-99 [2] определяет пять базовых услуг для обеспечения защиты компьютерных систем, входящих в архитектуру защиты эталонной модели взаимодействия открытых систем взаимодействия открытых систем (ВОС): конфиденциальность, аутентификацию, целостность, контроль доступа, причастность. Факультативно может быть задействована дополнительная услуга безопасности – доступность, которая может частично определяться услугой контроля доступа или быть характеристикой качества данного ресурса или услуги.

Для реализации базовых услуг безопасности в сети применяются специальные механизмы защиты (шифрование, заполнение трафика, управление маршрутизацией, цифровая подпись, контроль доступа, обеспечение целостности, аутентификация, нотаризация) и общие механизмы защиты (доверительная функциональность, метки безопасности, "аудиторская" проверка), которые которые могут быть задействованы для усиления последних [2]. Любая система защиты вносит избыточность в информационное окружение сети и приводит к ухудшению ее временных характеристик (ВХ) и вероятносто-временных характеристик (ВВХ). Поэтому крайне важно исследовать и выявить влияние конкретных механизмов защиты, используемых для реализации различных базовых услуг безопасности, на эффективность использования сетевых ресурсов ИКС и, в частности, ее транспортной системы (ТС), рассматриваемой в аспекте канального, сетевого и транспортного уровней [3]. Для оценки влияния механизмов защиты на характеристики ТС ИКС необходимо проведение на их моделях комплексного сравнительного анализа указанных характеристик без услуг безопасности и с их включением на всех фазах организации, поддержания и разрушения сеанса связи.

Известно [4], что спецификации каждого логического уровня всегда включают в себя спецификацию протокола и спецификацию сервиса, который обеспечивается соответствующей службой и поддерживается этим протоколом для вышерасположенного уровня. При этом услуга защиты может включаться в процесс обслуживания протокольного блока уровня для каждого типа информации и/или представлять собой отдельную услугу уровня. В первом случае процесс предоставления механизмов защиты моделируется как система массового обслуживания (СМО) с протокольной услугой безопасности, во втором – моделируется отдельной однофазной или многофазной СМО с услугой безопасности (СМО УБ) и включает в себя как фазу передачи сервисных примитивов уровня, так и процесс их обработки в конечных и/или промежуточных

системах. В любом случае реализация механизмов защиты осуществляется по принципам предоставления сервиса ВОС [4]. Уровни, которые не содержат отдельных служб безопасности, могут запросить их на низших уровнях в процессе установления сеанса связи.

Механизм аутентификации реализует в сети одноименную базовую услугу безопасности аутентификации разноуровневых элементов. Различают простую аутентификацию и строгую аутентификацию. Простая аутентификация может быть осуществлена различными способами с использованием учетных записей пользователей (идентификаторы, пароли) или цифровых сертификатов с одновременным согласованием средств их использования и обработки. Такими средствами могут служить одноразовые параметры (nonce): случайные числа r_i, временные метки t_i, номера последовательностей N_i, формируемые выработкой одноразового значения из монотонно возрастающей последовательности (например, меток времени) или случайных чисел соответствующей длины. Одноразовые параметры обеспечивают однозначность, уникальность и своевременность или временную гарантию передаваемых сообщений. В рекомендациях X.509 процедура простой аутентификации с защитой предусматривает передачу пароля (совместно со случайным числом r_i, временной меткой t_i и идентификатором ID_i) с применением односторонней хэш-функции h. Хэш-функция является наиболее общим представителем алгоритмов вычисления защитных контрольных сумм. В качестве односторонней простой аутентификации отправителя i, который посылает (знак направления передачи «$\rightarrow$») сообщение получателю j можно привести следующий пример: $i \rightarrow j: t_{i1}, r_{i1}, ID_i, h_1(t_{i1}, r_{i1}, P_i)$. В передаваемом сообщении случайное число r_i, гарантирует его уникальность и однозначность, а временная метка t_i - его временную гарантию. Процедура может быть усилена повторным раундом хэширования с введением новых значений дополнительных параметров, используемых в первом раунде $i \rightarrow j: t_{i1}, r_{i1}, t_{i2}, r_{i2}, ID_i, h_2(t_{i2}, r_{i2}, h_1(t_{i1}, r_{i1}, P_i))$. Получатель может подтвердить подлинность отправителя $i \leftarrow j: ID_j$. Проверка подлинности i-го пользователя основана на сравнении его пароля P_i с исходным значением P_i^*, **хранящимся на сервере аутентификации**, а также на гарантии уникальности и своевременности. Таким образом, общее время $T_{уб}^k$, затрачиваемое на задействование услуги простой аутентификации на сетевом уровне модели ВОС, реализуемой механизмами блочного симметричного шифрования, хэш-функции и одноразовых параметров, можно представить аддитивной формой вида

$$T_{\text{уб}}^k = T_i^k + T_{ij,n}^k + T_{\text{аут}}^k.$$

Здесь T_i^k, время, затрачиваемое на процесс формирования дайджеста протокольного блока уровня (пакета); $T_{ij,n}^k$ - время задержки протокольного блока уровня в n-ом пути ($n = \overline{1, M_{ij}^k}$) сквозного тракта передачи $ij \in S^k$ от источника i до получателя j, который принадлежит множеству путей S^k; $T_{аут}^k$ - время, затрачиваемое на аутентификацию протокольного блока (пакета) на стороне получателя.

В общем случае, время T_i^k включает в себя время шифрования $t_{шбл}^k$ и хеширования $t_{хэш}^k$ блоков пакета, а также время, затрачиваемое на предвычисления $t_{првыч}^k$ и генерацию одноразовых параметров $t_{t_i}^k$ и $t_{r_i}^k$

$$T_i^k = t_{ш}^k + t_{хэш}^k + t_{t_i}^k + t_{r_i}^k.$$

Здесь $t_{ш}^{k}$ время шифрования уровневого примитива (для недетерминированных шифров $t_{ш}^{k} = N_R \frac{M^k}{m} t_{шбл}^{k} + t_{предвыч}^{k}$, с, где $t_{шбл}^{k} = m / V_{ш}$, $V_{ш}$ - скорость шифрования, бит/с ; для шифров на базе управляемых операций преобразования $t_{ш}^{k} = N_R \frac{M^k}{m} t_{шбл}^{k}$, с, а для вероятностных шифров $t_{ш}^{k} = N_R \frac{M^{*k}}{m^k} t_{шбл}^{k}$, с; m – типовой 64-битовый блок; $t_{хэш}^{k} = (m_n + H_2) / \upsilon_{хэш}$ – время хеширования (64-битовый блок шифруется совместно со значением хэш-функции H_2 бит, т. е. блок $m \| H_2$, где "‖" – обозначает операцию конкатенации),с; $\upsilon_{\text{хэш}}$ – скорость хеширования, бит/с.

Время, затрачиваемое на аутентификацию сообщения на стороне получателя дается выражением

$T_{аут}^{k} = t_{рш}^{k} + t_{хэш}^{k} + t_{nonce}^{k}$, где $t_{рш}^{k}$, с - время расшифрования протокольного блока на приеме (для недетерминированных шифров и шифров на базе управляемых операций преобразования $t_{рш}^{k} = N_R \frac{M^k}{m} t_{ршбл}^{k}$, где $t_{ршбл}^{k} = m / V_{рш}$, $V_{рш}$ - скорость расшифрования, бит/с; для вероятностных шифров $t_{рш}^{k} = N_R \frac{M^{*k}}{m} t_{ршбл}^{k}$. Здесь $V_{рш}^{*} = V_{рш}(M^{*} - r) / M^{*}$, бит/с); t_{nonce}^{k},с – время проверки одноразовых параметров у получателя.

Плотность вероятностей распределения времени задержки речевого пакета $T_{ij,n}^{B}$ дается выражением

$$f_{ij,n}^{B}(t) = L^{-1}(\bullet)\left[\prod_{ab \in \hat{l}_{ij,n}^{B}} \frac{\mu_{ab}^{B}(1-\rho_{ab}^{B})}{s + \mu_{ab}^{B}(1-\rho_{ab}^{B})}\right]$$

(с учетом, что каждый канал пути, вместе с соответствующей памятью маршрутизатора, моделируется системой массового обслуживания (СМО) $M/M/1$; суммарные потоки от всех источников таковы, что агрегированные потоки на входе каждого канала независимы и являются простейшими. Время обработки пакета на транзитных маршрутизаторах не учитывается [7]. Здесь $L^{-1}(\bullet)$ - обратное преобразование Лапласа-Стильтьеса, ρ_{ab}^{B} - загрузка канала $ab \in \hat{l}_{ij,n}^{k}$, $\mu_{ab}^{k} = V_{ab} / L^{B}$ - величина, обратная средней длительности обслуживания речевого пакета в каждой отдельной СМО типа $M/M/1$ пути $\hat{l}_{ij,n}^{k}$. Для расчета времени $T_{ij,n}^{C}$ можно воспользоваться подходом, изложенным в [7], при условии что речевые пакеты обслуживаются с абсолютным приоритетом (с дообслуживанием) по отношению к пакетам данных. Как правило, процедура простой аутентификации является односторонней. При осуществлении также аутентификации получателя j на стороне отправителя i время $T_{уб}^{k}$ удваивается.

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 обмен информациёй только в одном направлении. Данный тип аутентификации позволяет подтвердить подлинность только одной стороны информационного обмена и гарантировать, что передаваемыми аутентификационными данными может воспользоваться только проверяющая сторона. Дополнительно односторонняя аутентификация позволяет обнаружить нарушение целостности, передаваемой информации и проведение атаки типа «повтор передачи». *Двусторонняя аутентификация* подтверждает, что связь устанавливается именно с тем партнером, которому были предназначены аутентификационные данные, и что метка времени является «текущей». *Трехсторонняя аутентификация* содержит дополнительную передачу данных от доказывающей стороны проверяющей и, в отличии от двухсторонней аутентификации, не требует проверки метки времени. Протоколы многократной аутентификации в условиях недоверия между абонентами, в большинстве случаев, базируются на задачах дискретного логарифмирования. 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:

- протоколы на основе симметричных алгоритмов шифрования;
- протоколы на основе однонаправленных ключевых хеш-функций;
- протоколы на основе асимметричных алгоритмов шифрования;
- протоколы на основе алгоритмов электронной цифровой подписи (ЭЦП).

В протоколах строгой аутентификации на основе асимметричных алгоритмов процесс аутентификации может быть основан на расшифровании сообщения, зашифрованного на открытом ключе P_i, или ЭЦП отправителя, формируемой им с использованием закрытого ключа S_i.

Симметричное шифрование E_i осуществляется на секретном ключе K_i отправителя, который известен всем участникам информационного обмена. При этом количество циклов шифрования (хэширования) входного блока определяется количеством применения к нему типовой процедуры шифрования, называемой «рауновой функцией R». Допустимое число циклов шифрования N_R должно быть не менее трех. [5]. Необходимо отметить, что для недетерминированных шифров запуск криптосистемы предполагает также использование этапа настройки шифра, выполняемой при введении секретного ключа. Для многих приложений время $t^k_{предвыч}$, затрачиваемое на выполнение алгоритма предвычислений или этап настройки шифра составляет 0.5…1.0 с [6]. Индексом k здесь и далее обозначен тип шифруемого трафика (B - речевого трафика, C - трафика данных в терминах ATM Forum). При использовании шифров с простым вероятностным механизмом скорость шифрования составит $V^*_ш = V_ш(M^* - r)/M^*$, где $V_ш$ – исходное значение скорости преобразования; $M^{*k} = r + M^k$ – шифруемое сообщение (M^k – битовый блок открытого сообщения; r – битовый случайный блок). Таким образом, скорость уменьшается в r/M^k раз, а блоки шифротекста увеличиваются в M^{*k}/M^k раз. При вероятностном объединении случайных и информационных битов в зависимости от секретного ключа требуется существенное увеличение доли случайных бит (80 % и более) [5].

Задействование механизмов шифрования осуществляется на фазе установленного соединения (N-соединения). При этом процесс шифрования включается в процесс обслуживания протокольного блока уровня для каждого типа информации. Протоколы аутентификации с использованием симметричного шифрования E_i на ключе K_i

предполагают, что проверяемый i-й субъект доказывает свою подлинность, демонстрируя знание секретного ключа K_i при расшифровании полученного сообщения.

Существует два варианта использования однонаправленных ключевых хэш-функций. В первом случае хэш-функция применяется к сообщению M, дополненному секретным ключом K_i. При этом отправитель вычисляет дайджест $H_1 = h(M, K_i)$ зависящий одновременно от сообщения и ключа K_i. На приеме, извлекая сообщение M, получатель дополняет его известным ключом отправителя K_i, вычисляет, применяя ту же хэш-функцию, дайджест и сравнивает его с полученным дайджестом. Во втором случае осуществляется шифрование сообщения с помощью функции h на секретном ключе K_i. В этом случае вид хэш-функции зависит от ключа, а значение этой функции – от содержания сообщения. Дайджест $H_2 = h_{K_i}(M)$ присоединяется к исходному сообщению M и передается получателю, который, зная вид функции h, вычисляет дайджест и сравнивает его с расшифрованным на ключе K_i. Чаще всего используются блочные хэш-функции, использующие алгоритмы блочного шифрования. При использовании блочного шифрования, например, в режиме обратной связи по шифротексту, дайджест $H_2 = h_{K_i}(m_n, H_{n-1})$ представляет собой последний блок битов m_n передаваемого сообщения $M = \{m_i\}$, $i = \overline{1,n}$. Так как результат шифрования зависит от всех битов входного сообщения M и секретного ключа K_i, последний зашифрованный блок m_n будет отличен для различных входных сообщений M или для различных ключей K_i. Получатель, расшифровав дайджест H_2 на ключе K_i, получает значение хэш-функции. Подлинность отправителя устанавливается получателем при совпадении принятого и вычисленного им дайджеста от сообщения M по известной всем односторонней хэш-функции. На практике в основном используются скоростные программные хэш-функции, основанные на типовых процедурах шифрования, базирующихся на операциях подстановок, зависящих от преобразуемых данных [5], [6]. ЭЦП – это зашифрованное секретным ключом S_i значение хэш-функции H, которое добавляется к сообщению M. Разновидностью ЭЦП являются коды аутентификации сообщений MAC) (message authentication code) и имитозащитная вставка (ИЗВ). Принципиально различаются симметричная и асимметричная системы ЭЦП. В случае симметричной системы ЭЦП пользователи сети засекреченной связи образуют (назначают) центр доверия. Ключи симметричного шифрования вырабатываются и распределяются центром доверия. При этом у каждого из пользователей есть собственный ключ, копия которого хранится в центре доверия. Процедура проверки ЭЦП состоит в том, что получатель, получив от отправителя файл и шифрованное значение хэш-функции (ЭЦП), направляет ЭЦП в центр доверия. Центр перешифровывает значение хэш-функции с использованием ключей отправителя и получателя, возвращает ЭЦП получателю. Последний, расшифровав ЭЦП на собственном ключе, получает значение хэш-функции. Вычислив значение хэш-функции принятого сообщения и сравнив его с полученным от центра, получатель принимает решение об истинности либо ложности полученного сообщения.

Ассиметричная ЭЦП, базируется на двухключевых криптографических алгоритмах, в которых предусматривается использование двух ключей – открытого и секретного. На приеме ЭЦП проверяется с помощью открытого ключа отравителя P_i. Протокол односторонней аутентификации с ЭЦП и применением временных меток и случайных чисел можно формализовать в виде $i \to j : ID_i, S_i(t_i, r_i, ID_j)$. Согласно вербальным описаниям процессов формирования ЭЦП (MAC, ИВЗ) [5], [6], задержка на создание, передачу и проверку подлинности ЭЦП (ИВЗ, MAC) представляется соответственно аддитивными формами: для ЭЦП ($T^k_{убЭЦП} = t^k_{i\,ЭЦП} + T^k_{ij,n} + t^k_{jЭЭП}$, где

$t^k_{i\,ЭЦП} = t^k_{хэш} + t^k_{ЭЦП} + t^k_{t_i} + t^k_{r_i}$, с; $t^k_{j\,ЭЦП} = t^k_{ЭЦП} + t^k_{nonce}$, с, $t^k_{ЭЦП} = H/v_{ЭЦП}$, с. Здесь $\upsilon_{ЭЦП}$ - скорость создания ЭЦП, бит/с); в качестве алгоритма для вычисления имитовставки используется хеш-функция $h(*)$. Могут быть использованы следующие два варианта: 1) вычисление ИЗВ по открытому тексту M и 2) вычисление ИЗВ по шифртексту M^*. В первом случае $ИВЗ_1 = h(M)$, а время его вычисления $t_{iИИВ_1} = M/V_{хэш}$. Во втором случае: $ИВЗ_2 = h(M^*) = h(E(M))$ и $t_{iИИВ_2} = t_{iш} + t_{i\,хэш} = M/V_{ш} + ИВЗ_2/\upsilon_{хэш}$. Таким образом, $T^k_{уб\,ИВЗ} = t^k_{i\,ИВЗ1,2} + T^k_{ij,n} + t^k_{j\,ИВЗ}$. Здесь $t^k_{j\,ИВЗ} = M/V_{рш} + ИВЗ_2/\upsilon_{хэш}$; простая форма МАС добавляет сообщение к ключу отправителя (секретному паролю отправителя P_i), а затем генерирует дайджест сообщения $MAC_1 = h(M, P_i)$ за время $t_{MAC_1} = \dfrac{M + P_i}{V_{хэш}}$. Ключ является частью ввода и изменяет дайджест сообщения. Таким образом, здесь мы получаем зависящий от пароля МАС. Вторая форма МАС использует некоторую форму метода шифрования потока (например, RC4 или DES) в режиме обратной связи по шифротексту CFB (Clphertext Feedback). Ключ в данном случае - это пароль шифрования P_i, а МАС - $MAC_2 = E_{P_i}(m_n)$ - это последний блок битов сообщения $M = \{m_i\}$, $i = \overline{1,n}$. Время вычисления MAC_2 определяется выражением $t_{MAC_2} = \dfrac{nm}{V_{хэш}}$. Так как результат шифрования зависит от всех битов ввода и секретного пароля P_i, последний блок m_n будет отличен для различных M или для различных паролей P_i. Общее время задержки в этом случае дается выражением $T^k_{уб\,MAC} = t^k_{i\,MAC1,2} + T^k_{ij,n} + t^k_{j\,MAC}$, составляющие которой вычисляются аналогичным образом. Строгую аутентификацию в двух направлениях можно представить на примере; $i \to j : ID_i, S_i(t_i, r_i, ID_j)$; $i \leftarrow j : ID_i, S_j(r_j, r_i, ID_i)$.

Процесс формирования и проверки ЭЦП и ее разновидностей формализуется СМО УБ и учитывается в общем балансе времени передачи пакетов классов B и/или C.
Аналитические модели пакетных ТС ИКС и метод расчета их характеристик в режиме установленного соединения основаны на построении и оптимизации общих функционалов K^k_{ab} использования пропускной способности межузловых трактов передачи $ab \in \widehat{l}^k_{ij,n}$ интегральным трафиком классов B и C [7]. Указанный метод интегрирован в рамках единых моделей и базируется на принципе декомпозиции (разложения) сети по парам "источник–получатель" с учетом архитектуры ТС и требуемых QoS-норм на передачу разнородного трафика, а также топологии сети и системы матриц распределения нагрузки $Y^k = \left\| a^k_{ij} \right\|$. В рамках предложенной концепции эффективность использования ТС ИКС предлагается оценивать с помощью набора уровневых функционалов $K^k_{h,ab}$ (здесь h - номер логического уровня модели ВОС) использования пропускной способности каждого тракта трафиком различных классов, которые зависят не только от необходимой для их работы служебной информации соответствующих объемов, но и от протоколов функционирования отдельных уровней архитектуры ТС ИКС, поддерживающих соответствующие службы, в том числе и протоколов аутентификации. Важно, что общий функционал использования составных путей $\widehat{l}^k_{ij,n}$ пакетами данных K^C_{ab} зависит от параметров общего функционала их использования речевым трафиком K^B_{ab}, т. е. носит ярко выраженный условный характер. В силу того, что транспортное виртуальное соединение может быть организовано между парой ij по нескольким виртуальным путям $\widehat{l}^k_{ij,n}$ ($n = \overline{1, L^k_{ij}}$), – выражение для общих функционалов использования всех транспортных

соединений ТС K_{ij}^k можно представить в виде среднегеометрического составляющих уровневых функционалов использования пропускной способности пути n-го выбора $K_{ij,n}^k$ для пары $ij \in S^k$. Например, для ТС ИКС на технологии IP-QoS

$K_{ij}^k = \sum_{n=1}^{L_{ij}^k} p_{ij,n}^k K_{TCP}^k \sqrt[l_{ij,n}^k]{\prod_{ab \in l_{ij,n}^k} K_{ab}^k}$, где K_{TCP}^k – функционал логического уровня TCP, $p_{ij,n}^k$ – глобальная вероятность распределения информации в дереве путей между узлами $ij \in S^k$. Для всей сети средневзвешенные по потокам общие функционалы использования пропускной способности ТС разнородным трафиком имеют вид:

$K^k = \sqrt[q^k]{\sum_{ij \in S^k} \frac{a_{ij}^k}{Y^k} (K_{ij}^k)^{q^k}}$, где $q^k = |S^k|$.

Для пакетной ТС инфокоммуникационной сети с учетом выше введенных предположений задачу анализа в общем виде можно записать как последовательность двух задач оптимизации.

1. Найти $\arg\max K^B$ при условиях: $b_{ij}^B \le b^B$, $\Pr_{ij,n}(t \ge \theta^B) \le d^B \; \forall ij \in S^B : a_{ij}^B \ne 0$, где $\Pr_{ij,n}(t \ge \theta^B)$ – вероятность превышения *B*-пакетами заданной сквозной задержки θ^B в пути n-го выбора для пары $ij \in S^B$, d^B – допустимая вероятность превышения θ^B, b_{ij}^B – вероятность потери вызова для пары $ij \in S^B$.

2. Найти $\arg\max K^C$ при условиях: $b_{ij}^C \le b^C, T_{ij,n}^C \le T^{*C} \forall ij \in S^C : a_{ij}^C \ne 0$ и все параметры первой задачи найдены и фиксированы. Здесь $T_{ij,n}^C$ – среднее время передачи пакетов класса C в пути n-го выбора для пары $ij \in S^C$; T^{*C} – заданное время передачи пакетов класса C в сети.

В физическом смысле вероятность d^B есть доля *B*-пакетов, превысивших время θ^B. Эта величина характеризует качество передачи изохронного трафика в сети. Выбор указанного ограничения на передачу определяется тем, что, например, для качественного воспроизведения речи важно не среднее время пребывания речевого пакета в сети, а доля речевых пакетов, не доставленных получателю за заданное время d^B, т. е. при анализе необходима фиксация заданного квантиля распределения времени пребывания пакета $F_{ij,n}^B(\theta^B)$.Фиксация среднего времени $T_{ij,n}^C$ пребывания пакета данных в тракте передачи связано с тем, что для пользователей сети представляет интерес не просто минимальное время пребывания пакета в сети (которое само по себе может оказаться достаточно большим и не приемлемым, например, для интерактивного обмена), а заданное среднее время.

Модели механизмов аутентификации должны быть учтены при построении общих функционалов K^k использования пропускной способности ТС ИКС, а также в ограничениях задачи анализа ТС ИКС. При этом, достаточно параметры θ^B и $T_{ij,n}^C$, фигурирующие в первой и второй задаче анализа, заменить на величины $\theta^{*B} = \theta^B - T_{уб}^k$ и $T^{*C} = T_{ij,n}^C - T_{уб}^C$. Кроме того, в указанных моделях ТС ИКС должна быть учтена протокольная избыточность механизмов шифрования, вносимая в сервисные примитивы логических уровней служебной информацией и/или значением хэш-функции, а в вероятностных шифрах без предварительного сжатия исходного сообщения –

дополнительными случайными данными. В моделях ТС ИКС в общем случае также должен быть учтен дополнительный трафик, создаваемый процессами управления ключами и аутентификации. Например, процесс двухфазовой аутентификации сеансовых ключей, можно рассматривать как дополнительный сетевой фоновый трафик и учитывать в модели ТС с более низким относительным приоритетом обслуживания по отношению к базовым трафикам классов B и/или C.

Библиографический список

1. Мошак Н. Н., Тимофеев Е. А. Особенности построения политики информационной безопасности в инфокоммуникационной сети // Электросвязь. 2005. № 9. С. 23–28.

2. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 2. Архитектура защиты. М.: Изд-во стандартов, 1999. ? с.

3. Мошак Н. Н. Модели оценки влияния механизмов аутентификации на параметры пакетной транспортной системы инфокоммуникационной сети // Междунар. конф. "Региональная информатика-2006" (РИ-2006). Санкт-Петербург, ?–? ? 2007 г. Мат-лы конф. СПб.: ?, 2006. С. ?–?.

4. Зайцев С. С., Кравцунов М. И., Ротанов С. В. Сервис открытых информационно-вычислительных сетей: Справ. Радио и связь, 1990. 240 с.

5. Молдовян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом. СПб: БХВ-Петербург, 2005. 288 с.

6. Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004. 448 с.

7. Мошак Н. Н. Теоретические основы проектирования транспортной системы инфокоммуникационной сети: Учеб. пос. для вузов. СПб.: Энергомашиностроение, 2006.159 с. ?ИА?

N. N. Moshak