УДК 004.056

С. В. Запечников

ОБЕСПЕЧЕНИЕ СТОЙКОСТИ И КОРРЕКТНОСТИ ФУНКЦИОНИРОВАНИЯ КРИПТОСИСТЕМ В УСЛОВИЯХ УТРАТЫ АУТЕНТИЧНОСТИ ЧАСТИ КЛЮЧЕВОГО МАТЕРИАЛА

Введено понятие аутентичности как одного из аспектов безопасности ключевого материала криптосистем. Изложены теоретические положения, задающие систему показателей и критериев обеспечения аутентичности ключей. Приведены доказанные утверждения и теоремы о структуре ключевой системы, обеспечивающей выполнение требований аутентичности. Даны примеры анализа показателей аутентичности для некоторых типовых элементов ключевых систем.

E-mail: SVZapechnikov@mephi.ru

Ключевые слова: *защита информации, криптография, управление ключами, информационные ресурсы.*

Решение проблемы обеспечения стойкости средств криптографической защиты информации (СКЗИ) в условиях частичного разрушения ключевой системы (КС) требует создания соответствующего научно-методического аппарата. Математическая модель КС СКЗИ предложена в работах [1, 2]. В терминах этой модели под ключевым материалом СКЗИ понимается совокупность всех криптографических ключей участников криптосистемы и информация, сопровождающая их применение в СКЗИ. Модель оперирует понятиями: объект ключевой системы (ОКС) — минимальная совокупность взаимосвязанного ключевого материала — и компонент ОКС — минимальная логически неделимая единица ключевого материала в составе ОКС. В качестве наиболее существенного структурного свойства КС выделяется вычислимость значений одних компонентов ОКС из значений других компонентов. На основе этого свойства определяются понятия функциональной зависимости и временно́й функциональной зависимости между компонентами ОКС; строятся графы зависимости для ОКС, для любых элементов и подсистем КС, а также, КС в целом.

Методическая база количественных оценок безопасности ключевого материала СКЗИ предложена в работе [3]. Безопасность ключевого материала характеризуется показателями его доступности, аутентичности и секретности, построенными на основе единых предположе-

ний о противнике, и интегральным показателем безопасности. Система показателей естественным образом расширяется для ОКС и для подсистем КС. Понятия доступности и секретности в применении к ключевому материалу криптосистем по сути не отличаются от аналогичных понятий, применяемых к любой другой циркулирующей в компьютерных системах информации. Однако традиционное понятие целостности как одного из аспектов безопасности информации (наряду с доступностью и секретностью) требует расширения, когда речь идет о ключевом материале СКЗИ. В связи с этим предлагается использовать понятие аутентичности ключевого материала [3, 4].

Развернутое обсуждение показателей доступности и секретности проводится в работах [5 и 6] соответственно. В настоящей работе подробно рассмотрены показатели, характеризующие аутентичность ключевого материала.

Аутентичность ключевого материала как составляющая безопасности криптосистем. Показатели аутентичности ключевого материала. Аутентичность компонента ОКС $Com_j \in Obj_i$ на непрерывном временно́м интервале λ определяем как свойство компонента Com_j, заключающееся в том, что значение компонента, считанное либо записанное в некоторый экземпляр ОКС в произвольный момент времени τ в интервале λ, совпадает с его истинным значением.

Свойство аутентичности компонента ОКС подразумевает неизменность его значения в момент τ по сравнению с истинным значением, которое он принял в момент создания либо последнего выполнения операции записи. Аутентичность проявляется в двух аспектах: целостности и подлинности. Вообще говоря, ни один из них не имеет смысла, если не обеспечен другой. Но в конкретных ситуациях существенное значение может иметь только один из них: так, при долговременном хранении экземпляра ОКС ставится задача обеспечения целостности, при передаче экземпляра ОКС по каналу связи важна подлинность.

Аутентичность в момент τ означает возможность санкционированного совершения с компонентом ОКС в этот момент любой из операций (чтение, запись, удаление), причем при выполнении операции чтения из экземпляра ОКС будет считано значение $Com_j \in Obj_i$, совпадающее со значением, помещенным в него при выполнении последней по времени операции записи; при выполнении операции записи в экземпляр ОКС будет записано значение $Com_j \in Obj_i$, совпадающее с его истинным значением.

Придерживаясь предположения о том, что утрата безопасности ключевого материала всегда происходит по причинам, связанным с деятельностью противника, введем предположения о противнике. Допустим, что противнику известна структура КС, включая минимальные

множества вычислимости (ММВ) и минимальные последовательности вычислимости (МПВ) всех ее элементов [2]. Противник может нарушать аутентичность отдельных компонентов ОКС, что может быть обнаружено системными средствами СКЗИ, а может и не быть обнаружено. Противник самостоятельно выбирает стратегию нарушения аутентичности экземпляров ОКС. Пусть Φ_1 — подмножество ОКС, заблокированных противником, Φ_2 — подмножество ОКС, аутентичность которых нарушена противником, и нарушение аутентичности обнаружено системными средствами СКЗИ. Обозначим $\Phi = \Phi_1 \cup \Phi_2$. Противник способен выполнять любые полиномиально ограниченные алгоритмы и, кроме того, имеет доступ к оракулам, реализующим применяемые в СКЗИ алгоритмы генерации кодов аутентификации сообщений и алгоритмы генерации электронной цифровой подписи (ЭЦП). Его преимущество над симметричными схемами аутентификации выражается величинами $Adv_A^{MAC}(t, q, \mu)$, над схемами ЭЦП — величинами $Adv_A^{DS}(t, q, \mu)$, где t и μ — доступные противнику временны́е и емкостные ресурсы соответственно, q — число запросов к оракулу, которое он может сделать. В этом смысле принятая модель противника является расширением моделей доказательной криптографии [7].

Вероятность успеха противника, т.е. вероятность того, что в произвольный момент времени τ, приходящийся на интервал λ, компонент $Com_j \notin \Phi$ будет признан СКЗИ аутентичным, хотя на самом деле таковым не является, обозначим $\beta(Com_j, \lambda)$, считая ее постоянной на данном интервале. Если она зависит от времени, то в качестве $\beta(Com_j, \lambda)$ примем ее максимальное значение на интервале λ.

Выведем формулы для оценки значений $\beta(Com_j, \lambda)$.

Если в КС имеется n экземпляров ОКС Obj_i, содержащего компонент Com_j, а для получения значения Com_j достаточно любого одного экземпляра ОКС, то $\beta(Com_j) = \beta^{(i)}(Com_j)$, где $\beta^{(i)}$ – вероятность нарушения аутентичности i-го экземпляра ОКС. Если используется мажоритарный метод контроля, то

$$\beta(Com_j) = \beta\left(Com_j^{(n)}\right) = \\ = 1 - \sum_{u \in U}\left[\prod_{i \in u}\beta^{(i)}(Com_j)\prod_{j \in W \setminus u}\left(1 - \beta^{(j)}(Com_j)\right)\right], \quad (1)$$

где W — множество всех экземпляров ОКС, $|W| = n$, U — множество всех подмножеств $u \in W$, таких, что $|u| < n/2$.

Для оценки вероятности нарушения аутентичности компонента Com_j в каждом из экземпляров ОКС необходимо провести анализ методов обеспечения их аутентичности. Основным методом контроля

является введение избыточности в данные. Решение об аутентичности может быть принято либо при действительном совпадении проверочных разрядов с контрольным значением, либо при фальсификации противником информационных и проверочных разрядов блока данных, не обнаруживаемой системными средствами контроля. Учитывая тот факт, что всего насчитывается четыре типовых способа обеспечения аутентичности, можно указать следующие формулы для расчета этой вероятности.

1. Для идеальной бесключевой хэш-функции (вследствие свойства трудности обнаружения коллизий)

$$\beta^{(i)}\left(Com_j\right) = 2^{-|h|/2}\beta\left(h\right), \tag{2}$$

где $|h|$ — длина хэш-кода; $\beta\left(h\right)$ — вероятность нарушения аутентичности хэш-кода.

2. Для кодов, исправляющих ошибки (КИО) (зависит от кода, но ограничена сверху),

$$\beta^{(i)}\left(Com_j\right) \leqslant \max\left(2^{-|d|};\ 2^{-|Com_j|}\right)\beta\left(d\right), \tag{3}$$

где $|d|$ — длина проверочных разрядов КИО; $\beta\left(d\right)$ — вероятность нарушения аутентичности проверочных разрядов КИО.

3. Для симметричной схемы аутентификации сообщений (зависит от применяемой криптосхемы)

$$\begin{aligned}&\beta^{(i)}\left(Com_j\right) = \\ &= 1 - \left(1 - InSec^{mac-frg}_{MA,A}\left(t,q,\mu\right)\right)\left(1-\beta\left(Com_k\right)\right)\left(1-\gamma\left(Com_k\right)\right),\end{aligned} \tag{4}$$

где $InSec^{mac-frg}_{MA,A}\left(t,q,\mu\right)$ — значение функции небезопасности симметричной схемы аутентификации сообщений при атаках полиномиально ограниченного противника, способного делать q запросов к криптосхеме, обладающего временными ресурсами t и емкостными ресурсами μ [7, с. 129]; $\beta\left(Com_k\right)$; $\gamma\left(Com_k\right)$ – соответственно вероятности нарушения аутентичности и секретности ключа k симметричной схемы аутентификации сообщений.

4. Для схемы ЭЦП (зависит от применяемой криптосхемы)

$$\begin{aligned}\beta^{(i)}\left(Com_j\right) = 1 - \left(1 - InSec^{ds-frg}_{DS,A}\left(t,q,\mu\right)\right) \times \\ \times \left(1-\beta\left(Com_{sk}\right)\right)\left(1-\gamma\left(Com_{sk}\right)\right)\left(1-\beta\left(Com_{pk}\right)\right),\end{aligned} \tag{5}$$

где $InSec^{ds-frg}_{DS,A}\left(t,q,\mu\right)$ — значение функции небезопасности схемы ЭЦП при атаках полиномиально ограниченного противника, способного делать q запросов к схеме, обладающего временными ресурсами t и емкостными ресурсами μ [7, с. 166]; $\beta\left(Com_{sk}\right)$, $\beta\left(Com_{pk}\right)$ — соответственно вероятности нарушения аутентичности секретного sk и

открытого pk ключей схемы ЭЦП; $\gamma\left(Com_{sk}\right)$ — вероятность нарушения секретности ключа sk схемы ЭЦП.

Формулы (2)–(5) демонстрируют взаимосвязь между криптографическими и некриптографическими механизмами обеспечения аутентичности данных. Так, из соотношений (2) и (3) следует, что только бесключевые механизмы могут рассматриваться в качестве первичных, обеспечивающих заданные показатели аутентичности: если дополнительных мер для обеспечения аутентичности хэш-кодов и проверочных разрядов КИО не принимается, то эти формулы принимают вид $\beta^{(i)}\left(Com_j\right) = 2^{-|h|/2}$ и $\beta\left(Com_j\right) \leqslant \max\left(2^{-|d|}; 2^{-|Com_j|}\right)$ соответственно. Ключевые механизмы вторичные, так как для них имеют место лишь рекуррентные соотношения (4) и (5), а достигаемые с их помощью показатели аутентичности зависят не только от показателей аутентичности ключевого материала криптосхемы, но и от показателей его секретности.

Если ни один из экземпляров Obj_i не аутентичен, то аутентичное значение Com_j может быть восстановлено из любого ММВ $\omega\left(Com_j\right)$ при условии, что все элементы этого множества аутентичны. Таким образом,

$$\beta\left(\omega\left(Com_j\right)\right) = 1 - \prod_{Com_l \in \omega(Com_j)} \left(1 - \beta\left(Com_l\right)\right), \tag{6}$$

где $\beta\left(Com_l\right)$ отыскиваются по формуле (1).

Если ни один из экземпляров Obj_i не аутентичен и не существует $\omega\left(Com_j\right)$, из которого могло бы быть восстановлено аутентичное значение Com_j, его можно восстановить из любой МПВ $\theta\left(Com_j\right)$ при условии, что все элементы этой последовательности аутентичны. Таким образом,

$$\beta\left(\theta\left(Com_j\right)\right) = 1 - \prod_{Com_m \in \theta(Com_j)} \left(1 - \beta\left(Com_m\right)\right), \tag{7}$$

где $K_{\text{Д}}\left(Com_m\right)$ отыскиваются по формуле (1).

Пусть $\bar{\Omega}\left[Com_j, \lambda_\tau\right] \subseteq \Omega\left[Com_j\right]$ – подмножество множества всех ММВ компонента Com_j, состоящее из таких ММВ, для которых жизненный цикл (ЖЦ) всех элементов ММВ включает интервал λ_τ. Минимальные множества вычислимости $\bar{\omega}\left(Com_j, \lambda_\tau\right) \in \bar{\Omega}\left[Com_j, \lambda_\tau\right]$ будем называть ММВ, действующим на интервале λ_τ.

Пусть $\Lambda = \langle \lambda_1, \lambda_2, \ldots, \lambda_m \rangle$ — непрерывная последовательность временны́х интервалов. Пусть $\bar{\Theta}\left[Com_j, \Lambda\right] \subseteq \Theta\left[Com_j\right]$ – подмножество множества всех МПВ компонента Com_j, состоящее из таких МПВ, все элементы которых присутствуют в КС в течение хотя бы одного временного интервала $\lambda_\tau \in \Lambda$. Любую МПВ $\bar{\theta}\left(Com_j\right) \in \in \bar{\Theta}\left[Com_j, \Lambda\right]$ будем называть МПВ, действующей на последовательности интервалов Λ.

Лемма. Вероятность того, что компонент ОКС $Com_j \in Obj_i$ неаутентичен в произвольный момент времени τ временного интервала λ, составляет

$$\beta\left(Com_j, \lambda_\tau\right) = \beta\left(Com_j\right) \times \\ \times \prod_{\omega(Com_j)\in\bar{\Omega}[Com_j,\lambda_\tau]} \beta\left(\omega\left(Com_j\right)\right) \prod_{\theta(Com_j)\in\bar{\Theta}[Com_j,\lambda_\tau]} \beta\left(\theta\left(Com_j\right)\right), \quad (8)$$

где $\beta\left(Com_j\right)$ определяется уравнением (1), $\beta\left(\omega\left(Com_j\right)\right)$ — уравнением (6); $\beta\left(\theta\left(Com_j\right)\right)$ — уравнением (7).

Следствие. Пусть на непрерывной последовательности интервалов $\Lambda = \langle\lambda_1, \lambda_2, \ldots, \lambda_m\rangle$ задано множество моментов времени $(\tau_1, \tau_2, \ldots, \tau_m)$, таких, что $\tau_1 \in \lambda_1$, $\tau_2 \in \lambda_2, \ldots, \tau_m \in \lambda_m$. Тогда вероятность того, что $Com_j \in Obj_i$ неаутентичен хотя бы в один из этих моментов времени, равна

$$\beta\left(Com_j, \Lambda\right) = 1 - \prod_{s=1}^{m}\left(1 - \beta\left(Com_j, \lambda_s\right)\right). \quad (9)$$

Критерии аутентичности ключевого материала. В терминах введенных выше определений, используя лемму и ее следствие, доказывается справедливость следующих двух теорем (приводятся здесь без доказательства).

Теорема 1. (Критерий аутентичности ключевого материала на одном временном интервале.) Пусть Φ — подмножество компонентов ОКС Obj_i, аутентичность которых нарушена противником в некоторый момент времени τ, приходящийся на временной интервал λ_τ. Если для компонента $Com_j \in Obj_i$ существует хотя бы одно действующее ММВ или хотя бы одна действующая МПВ, ни один компонент которых не принадлежит множеству Φ, то из них можно получить истинное значение $Com_j \in Obj_i$ с вероятностью $P = 1 - P^*$, где

$$P^* = P(Com_j^* \neq Com_j \Big| \Phi : (Com_j(\lambda_\tau) \notin \Phi) \vee \\ \vee \left(\exists\bar{\omega}(Com_j(\lambda_\tau)) : \forall Com_{\bar{\omega}} \notin \Phi\right) \vee \\ \vee \left(\exists\bar{\theta}(Com_j(\lambda_\tau)) : \forall Com_{\bar{\theta}} \notin \Phi)\right) \leqslant \beta(Com_j, \lambda_\tau). \quad (10)$$

Теорема 2. (Критерий аутентичности ключевого материала на непрерывной последовательности временных интервалов.) Пусть $\{\Phi_1, \Phi_2, \ldots, \Phi_m\}$ — подмножества компонентов ОКС Obj_i, аутентичность которых нарушена противником в некоторые моменты времени, приходящиеся на временные интервалы, образующие непрерывную последовательность $\Lambda = \langle\lambda_i, \lambda_{i+1}, \ldots, \lambda_\tau, \ldots, \lambda_{i+m}\rangle$. Если для компонента $Com_j \in Obj_i$ существует хотя бы одно ММВ или хотя бы одна

МПВ, действующие на Λ, ни один компонент которых не принадлежит множеству Φ, то из них можно получить истинное значение $Com_j \in Obj_i$ с вероятностью $P = 1 - P^*$, где

$$P^* = P\left(Com_j^*(\lambda_\tau) \neq Com_j(\lambda_\tau) \,|\, \{\Phi_1, \Phi_2, \ldots, \Phi_m\} : (Com_j(\lambda_\tau) \notin \Phi) \vee \right.$$
$$\vee \left(\forall k = \overline{1,m}\,(\exists \bar{\omega}\,(Com_j(\lambda_k)) : \forall Com_{\bar{\omega}} \notin \Phi_k)\right) \vee$$
$$\left. \vee \left(\forall k = \overline{1,m}\,\left(\exists \bar{\theta}\,(Com_j(\lambda_k)) : \forall Com_{\bar{\theta}} \notin \Phi_k\right)\right)\right) \leqslant$$
$$\leqslant 1 - \prod_m (1 - \beta(Com_j, \lambda_m)). \quad (11)$$

Критерии аутентичности носят вероятностный характер. Вероятность выполнения условий, сформулированных в теоремах 1 и 2, не превышает коэффициента доступности компонента Com_j, но если необходимые условия выполнены, то вероятность обеспечения аутентичности определяется по формулам (10) и (11).

Структура КС, обеспечивающая аутентичность ключевого материала. Аутентичность ОКС Obj_i на непрерывном временном интервале λ определим как свойство ОКС, состоящее в том, что $\forall Com_j \in Obj_i$, для которого требуется обеспечение аутентичности, аутентичен в любой момент времени τ, приходящийся на интервал λ.

Согласно модели [2] все компоненты ОКС, требующие обеспечения аутентичности, сосредоточены в его полях B, C, D, E. Обозначим $\beta(Obj_i, \lambda)$ — вероятность того, что хотя бы один компонент Com_j, содержащийся в полях B, C, D, E объекта Obj_i неаутентичен в фиксированный момент времени τ, приходящийся на временной интервал λ. Если определены $\beta(Com_j, \lambda)$ для $\forall Com_j \in B \cup C \cup D \cup E$, то

$$\beta(Obj_i, \lambda) = 1 - \prod_{Com_j \in B \cup C \cup D \cup E} (1 - \beta(Com_j, \lambda)). \quad (12)$$

Вероятность того, что хотя бы один компонент Com_j, содержащийся в полях B, C, D, E объекта Obj_i, неаутентичен по крайней мере в один из фиксированных моментов времени $(\tau_1, \tau_2, \ldots, \tau_m)$, приходящихся на непрерывную последовательность временных интервалов $\Lambda = \langle \lambda_1, \lambda_2, ..., \lambda_m \rangle$, таких, что $\tau_1 \in \lambda_1$, $\tau_2 \in \lambda_2, \ldots, \tau_m \in \lambda_m$, равна

$$\beta(Obj_i, \Lambda) = 1 - \prod_{Com_j \in Obj_i.B \cup C \cup D \cup E} (1 - \beta(Com_j, \Lambda)). \quad (13)$$

Вследствие малости абсолютных величин β для качественных механизмов обеспечения аутентичности экспериментальное определение β затруднено, поэтому при расчетах по формулам (1)–(9), (12)–(13) следует пользоваться аналитическими выражениями.

Проведем теперь анализ показателей аутентичности более крупных элементов КС. Прежде всего укажем очевидное условие аутентичности ОКС.

Утверждение. Если в орграфе G_{Obj_i} существует путь, начинающийся из компонента Com_{j_1}, принадлежащего полю F, и заканчивающийся в компоненте Com_{j_2}, принадлежащем полю B либо C, то аутентичность компонента Com_{j_2} не может быть нарушена противником, пока для $\forall\omega\,(Com_{j_2})$: $Com_{j_1} \in \omega\,(Com_{j_2})$ противником не нарушена аутентичность всех элементов этого ММВ.

Следствие. Чем меньше для некоторого Obj_i или $Com_j \in Obj_i$ мощность подмножества таких ММВ (МПВ), в которых противник может получить несанкционированный доступ хотя бы к одному элементу, тем ниже вероятность нарушения аутентичности Obj_i или Com_j соответственно.

События, заключающиеся в нарушении аутентичности каждого отдельно взятого компонента или ОКС, как правило, можно считать независимыми. Поэтому $\beta\,(KS, \lambda) = 1 - \prod\limits_{Obj_i \in KS} (1 - \beta\,(Obj_i, \lambda))$ и $\beta\,(KS, \Lambda) = 1 - \prod\limits_{Obj_i \in KS} (1 - \beta\,(Obj_i, \Lambda))$, где $\beta\,(Obj_i, \lambda)$ определяется последовательно по уравнениям (12) и (8), $\beta\,(Obj_i, \Lambda)$ — по уравнениям (13) и (9).

Оценка показателей аутентичности некоторых схем управления ключевым материалом. В работе [8] введено понятие схемы управления ключевым материалом (СУКМ). Под СУКМ понимается совокупность однородных в функциональном отношении криптографических протоколов и функций, предназначенных для организованного управления ОКС (компонентом ОКС) на протяжении его ЖЦ. Формально СУКМ — это совокупность четырех алгоритмов (протоколов), выполнимых за полиномиальное время:

$$KMMS = \\ = \{Par\_Gen, KM\_Gen\_Distr, KM\_Regen\_Redistr, KM\_Del\}.$$

В нее входят следующие алгоритмы и (или) протоколы.

1. Алгоритм генерации начальных параметров схемы *Par_Gen* — детерминированный или вероятностный алгоритм, исходными данными для которого служат политика управления ключами и (или) политика безопасности КС. Алгоритм возвращает выбранные им значения параметров криптосистемы, необходимые для применения СУКМ.

2. Алгоритм (протокол) генерации и распределения ключевого материала *KM_Gen_Distr* — вероятностный алгоритм, на вход которого подаются выработанные алгоритмом *Par_Gen* параметры криптосистемы. Он возвращает выбранные в соответствии с этими параметрами значения множества компонентов ОКС, задействованных в СУКМ.

3. Алгоритм (протокол) регенерации и перераспределения ключевого материала *KM_Regen_Redistr* — детерминированный либо веро-

ятностный алгоритм, на вход которого подаются параметры криптосистемы, выработанные алгоритмом *Par_Gen*, значения компонентов ОКС, выработанные при вызове алгоритма *KM_Gen_Distr* либо при предыдущих вызовах алгоритма *KM_Regen_Redistr*. Алгоритм возвращает выбранные им новые значения множества компонентов ОКС, задействованных в СУКМ.

4. Алгоритм уничтожения ключевого материала *KM_Del* — детерминированный алгоритм, на вход которого подаются параметры, выработанные алгоритмом *Par_Gen*. Алгоритм присваивает всем компонентам ОКС, задействованным в СУКМ, пустые значения.

Пусть $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ — последовательность временны́х интервалов, составляющих ЖЦ СКЗИ, на каждом из которых ключевой материал неизменен. Алгоритм *Par_Gen* выполняется однажды перед началом работы СУКМ, *KM_Gen_Distr* выполняется перед началом интервала λ_1, *KM_Regen_Redistr* выполняется каждый раз перед началом интервалов $\lambda_2, \ldots, \lambda_m$, *KM_Del* выполняется после окончания интервала λ_m.

С помощью понятия СУКМ удобно формализуются широко распространенные на практике приемы повышения стойкости криптосистем к разрушению ключевого материала. На основе обобщения многочисленных примеров криптосхем, взятых из зарубежной литературы, выделяется несколько СУКМ, в частности: простое резервирование ключевого материала; пороговая схема разделения секрета (СРС); СРС с произвольной структурой доступа; СРС, функционирующая в модели "активной безопасности"; схема дистанционного управления ключами; схема эволюции ключей, обеспечивающая совершенную опережающую безопасность (perfect forward security); схема эволюции ключей с изоляцией ключа (key-insulated cryptosystem); схема эволюции ключей с базой, устойчивая к вторжению (intrusion-resilient cryptosystem).

Показатели аутентичности являются объективно фиксируемыми величинами. Анализ показателей аутентичности элементов КС имеет целью получение для СУКМ выражений, позволяющих рассчитать $\beta\left(SKS^{\text{СУКМ}}, \lambda_\tau\right)$ или $\beta\left(SKS^{\text{СУКМ}}, \Lambda\right)$, и сопоставление их с величинами, характеризующими аутентичность ключевого материала без применения СУКМ. Изменение показателей аутентичности элементов КС при применении СУКМ характеризуется коэффициентом, выражающим отношение вероятностей того, что один и тот же ключевой материал утратит аутентичность за одинаковое время в условиях применения к нему СУКМ и без таковой: $A^{\text{СУКМ}} = \dfrac{\beta\left(SKS^{\text{СУКМ}}, \lambda_\tau\right)}{\beta\left(SKS, \lambda_\tau\right)}$ или $A^{\text{СУКМ}} = \dfrac{\beta\left(SKS^{\text{СУКМ}}, \Lambda\right)}{\beta\left(SKS, \Lambda\right)}$.

Анализ проводился при следующих исходных предположениях:

• границами интервалов являются моменты смены (перезаписи) значений компонентов ОКС;

• утрата аутентичности ключевого материала происходит в некоторый момент времени, приходящийся на рассматриваемый интервал, вследствие деятельности противника, при этом фаза ЖЦ компонента ОКС, в которой происходит это событие, и способ совершения атаки не принимаются во внимание;

• показатели аутентичности всех задействованных в СУКМ компонентов ОКС определяются по формулам (1)–(5) в зависимости от используемых методов контроля целостности и подлинности;

• для СУКМ с изменяющимся ключевым материалом нарушения аутентичности компонентов ОКС, не обнаруженные на одном временном интервале, приводят к нарушению аутентичности компонентов ОКС на всех последующих интервалах, поэтому показатели аутентичности считается зависящими от показателей на предыдущих интервалах.

Приведем примеры полученных результатов.

Пример 1. *Резервирование ключевого материала*. Особенность данной СУКМ состоит в том, что анализ ее показателей аутентичности в сильной степени зависит от принятого способа доступа к компонентам ОКС и контроля их достоверности.

1. Если значение Com_j считывается каждый раз из некоторого одного, i-го экземпляра ОКС, то $\beta\left(Com_j^{Backup}, \lambda\right) = \beta\left(Com_j^{(i)}, \lambda\right)$, где $\beta\left(Com_j^{(i)}, \lambda\right)$ — его показатель аутентичности. Чаще всего на практике все экземпляры ОКС характеризуются равными показателями аутентичности. Если при этом каждый из них подвержен атакам противника, приводящим к нарушению аутентичности, с равными и постоянными интенсивностями μ, то, считая, что суммарная их интенсивность до и после применения СУКМ не изменяется, получаем $A^{Backup} = \left(1 - e^{-\mu|\lambda|}\right) \Big/ \left(1 - e^{-\mu n|\lambda|}\right)$.

2. Если значение Com_j считывается всякий раз из одного, но случайно выбранного экземпляра ОКС, то $\beta\left(Com_j^{Backup}, \lambda\right) = \max\limits_{i=\overline{1,n}} \beta\left(Com_j^{(i)}, \lambda\right)$, а A^{Backup} вычисляется так же.

3. Если при чтении значения Com_j используется мажоритарный контроль, то

$$\beta\left(Com_j^{Backup}, \lambda\right) = 1 - \sum_{u \in U} \left[\prod_{l \in u} \beta\left(Com_j^{(l)}, \lambda\right) \prod_{m \in W \setminus u} \left(1 - \beta\left(Com_j^{(m)}\right)\right) \right],$$

где W — множество всех экземпляров ОКС; $|W| = n$; U — множество всех подмножеств $u \in W$, таких, что $|u| < n/2$. При равных вероятностях нарушения аутентичности всех экземпляров имеем $\beta\left(Com_j^{Backup}, \lambda\right) = 1 - \sum\limits_{l=0}^{\lfloor n/2 \rfloor} C_n^l \left(\beta\left(Com_j^{(i)}, \lambda\right)\right)^l \left(1 - \beta\left(Com_j^{(i)}\right)\right)^{n-l}$, где $i = \overline{1, n}$.

Когда все экземпляры ОКС, кроме того, характеризуются равными и постоянными интенсивностями μ атак противника, приводящих к нарушению аутентичности, имеем

$$A^{Backup} = \left(1 - \sum_{l=0}^{\lfloor n/2 \rfloor} C_n^l \left(1 - e^{-\mu|\lambda|}\right)^l e^{-\mu(n-l)|\lambda|}\right) \Big/ \left(1 - e^{-\mu n|\lambda|}\right).$$

Пример 2. *Пороговые СРС*. В (m, n)-пороговой СРС значение компонента Com_j восстанавливается при условии доступа к любому подмножеству из m долей секрета. Обозначим через B_m m-элементные подмножества долей секрета $\{Com_{l_1}, \ldots, Com_{l_m}\}$. В каждом случае восстановление значения Com_j может осуществляться из различных m-элементных подмножеств долей секрета в соответствии с используемым алгоритмом доступа к Com_j. За показатель аутентичности следует принять наибольшую величину, т.е.

$$\beta\left(Com_j^{TSS}, \lambda\right) = \max_{B_m} \left\{1 - \prod_{j \in B_m} \left(1 - \beta\left(Com_{l_j}, \lambda\right)\right)\right\}.$$

Если показатели аутентичности для всех долей секрета СРС одинаковы, то $\beta\left(Com_j^{TSS}, \lambda\right) = 1 - \left(1 - \beta\left(Com_l, \lambda\right)\right)^m$. При тех же предположениях относительно интенсивностей атак противника, что и для предыдущей СУКМ, $A^{TSS} = \left(1 - e^{-\mu m|\lambda|}\right) \big/ \left(1 - e^{-\mu n|\lambda|}\right)$.

Пример 3. *СРС с произвольной структурой доступа*. В этой СУКМ восстановление значения компонента Com_j осуществляется при условии доступа к любому из минимальных авторизованных подмножеств B^* долей секрета, каждое из которых совпадает с одним из ММВ компонента Com_j. Нарушение аутентичности минимального авторизованного подмножества происходит, если нарушена аутентичность хотя бы одного его элемента. Итак, за показатель аутентичности следует принять

$$\beta\left(Com_j^{GSS}, \lambda\right) = \max_{B^*} \left\{1 - \prod_{j \in B^*} \left(1 - \beta\left(Com_{l_j}, \lambda\right)\right)\right\}.$$

При тех же предположениях, что и ранее, имеем

$$A^{GSS} = \max_{B^*} \left\{1 - e^{-\mu|B^*||\lambda|}\right\} \Big/ \left(1 - e^{-\mu n|\lambda|}\right).$$

Пример 4. *СРС, функционирующие в модели "активной безопасности"* [9]. На каждом отдельно взятом временном интервале λ_s данная СУКМ характеризуется теми же показателями аутентичности, что и СРС с произвольной структурой доступа:

$$\beta\left(Com_j^{SSPS}, \lambda_s\right) = \max_{B^*}\left\{1 - \prod_{j\in B^*}\left(1 - \beta\left(Com_{l_j}, \lambda_s\right)\right)\right\},$$

где B^* — минимальные авторизованные подмножества долей секрета. Значения $\beta\left(Com_l, \lambda_s\right)$ не зависят от показателей аутентичности долей секрета на предыдущих временных интервалах, так как перед началом каждого нового интервала происходит регенерация долей секрета. На последовательности интервалов $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ в соответствии с (9) показатель аутентичности принимает вид

$$\beta\left(Com_j^{SSPS}, \Lambda\right) = 1 - \prod_{s=1}^{m}\left(1 - \beta\left(Com_j^{SSPS}, \lambda_s\right)\right) =$$

$$= 1 - \prod_{s=1}^{m}\left(1 - \max_{B^*}\left\{1 - \prod_{j\in B^*}\left(1 - \beta\left(Com_{l_j}, \lambda_s\right)\right)\right\}\right).$$

Пример 5. *Схема эволюции ключей, обеспечивающая совершенную опережающую безопасность*. Очевидно, что применение к компоненту ОКС Com_j этой СУКМ не изменяет его показателей аутентичности на каждом отдельно взятом временном интервале. Учитывая, что СУКМ функционирует на последовательности интервалов $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$, заметим, что показатель аутентичности Com_j на каждом очередном интервале определяется всей совокупностью показателей на предыдущих интервалах. Отсюда получаем

$$\beta\left(Com_j^{PFS}, \Lambda\right) = 1 - \prod_{s=1}^{m}\left(1 - \beta\left(Com_j, \lambda_s \,|\lambda_1, ..., \lambda_{s-1}\right)\right) =$$

$$= 1 - \prod_{s=1}^{m}\left(1 - \prod_{u=1}^{s}\beta\left(Com_j, \lambda_u\right)\right).$$

Задачи, возникающие в связи с обеспечением аутентичности ключевого материала. Задача обеспечения аутентичности определяется особенностями этого понятия применительно к ключевому материалу криптосистем — в широком смысле она включает в себя контроль информационных ресурсов СКЗИ, т.е. контроль элементов информационного наполнения КС и взаимосвязей между ними, и контроль функциональных ресурсов СКЗИ, т.е. в контексте решаемой задачи контроль целостности программного обеспечения. Контроль информационных ресурсов подразумевает обеспечение неизменности

значений ключевого материала на всех этапах его жизненного цикла (целостность), привязку к субъектам-владельцам и информации, определяющей порядок его применения в криптосистеме (подлинность), а также невозможность отказа от факта обладания ключом и совершения посредством него криптографических операций (неотказуемость).

Введенный в работе [1] подход к описанию структуры КС на основе выделения функциональных зависимостей между ОКС и их компонентами позволяет дать удобную классификацию задач, решение которых необходимо для обеспечения аутентичности информационных ресурсов СКЗИ.

Пусть $G_{Obj_i} = (V_{Obj_i}, E_{Obj_i})$ — граф зависимости между компонентами ОКС Obj_i. Если в графе G_{Obj_i} существуют такие множества вершин $V_1, V_2, \ldots, V_m$, где $V_s = \{Com_{k_1}, \ldots, Com_{k_s}\}$, $s = \overline{1,m}$, что для $\forall p \in \{1, \ldots, m\}$ существует $r \neq p$, такое, что $A_p = \omega(A_r)$, $A_r = \omega(A_p)$ и $\exists\varphi$, такое, что $A_p = \varphi(A_r)$, $A_r = \varphi^{-1}(A_p)$, где φ — биективное отображение, то будем называть подмножество вершин $A = A_1 \cup A_2 \cup \ldots \cup A_m$ областью эквивалентности ключевого материала ОКС Obj_i. Область эквивалентности — это такое подмножество компонентов ОКС, которое представляет изоморфные компоненты ОКС, причем переход из одной формы их представления в другую всегда возможен с помощью некоторой последовательности биективных отображений.

Пример 6. Для компонента Com_j, к которому применена (t,n)-пороговая СРС и используется шифрование для защиты пересылаемых по каналам связи долей секрета, область эквивалентности есть множество $V = \{Com_j\} \cup B_1^* \cup \ldots \cup B_{C_n^t}^* \cup D_1^* \cup \ldots \cup D_{C_n^t}^* = \{Com_j\} \cup \{Com_{s_1}\} \cup \ldots$ $\ldots \cup \{Com_{s_n}\} \cup \{Com_{e_1}\} \cup \ldots \cup \{Com_{e_n}\}$, где B_i^*, $i = \overline{1, C_n^t}$ — минимальные авторизованные подмножества долей секрета, D_i^*, $i = \overline{1, C_n^t}$ — подмножества шифротекстов долей секрета, составляющих минимальные авторизованные подмножества B_i^*, а значения каждой пары компонентов связаны соотношениями $Com_{e_q} = E_k\left(Com_{s_q}\right)$, $q = \overline{1,n}$, где E — некоторое преобразование зашифрования, k — ключ шифрования.

Используя введенное понятие, можно выделить три самостоятельных задачи контроля информационных ресурсов СКЗИ.

1. *Обеспечение целостности компонентов ОКС* — это обеспечение достоверности компонентов ОКС, входящих в каждую из областей эквивалентности ключевого материала ОКС, т.е. обеспечение биективности всех преобразований компонентов ОКС в пределах области эквивалентности и в том числе тождественного преобразования, в условиях отсутствия абсолютно надежных средств преобразования и хранения данных.

2. *Обеспечение подлинности ОКС* — это фиксация существования функциональных зависимостей первого либо второго рода между компонентами ОКС, что соответствует регистрации факта существования дуг в графе, описывающем ОКС.

3. *Обеспечение невозможности отказа от ключевого материала и совершенных с помощью него операций* — это фиксация факта существования на определенном временном интервале (или в определенный момент времени) какого-либо компонента ОКС, что соответствует регистрации факта существования вершин в графе, описывающем ОКС.

Решение всех трех задач основано на введении информационной и структурной избыточности в СКЗИ путем создания и сохранения избыточных компонентов ОКС, функционально зависимых от контролируемых компонентов ОКС.

Задача обеспечения целостности ключевого материала есть задача контроля биективности тождественного преобразования данных, интерпретируемых как информационные разряды кодового слова. Для реализации процедур контроля необходимо добавление проверочных разрядов: они могут рассматриваться как дополнительные компоненты ОКС, функционально зависимые от контролируемых компонентов. При транспортировке и хранении ключей на ключевых носителях СКЗИ она решается традиционными средствами — при помощи КИО и криптографических хэш-функций.

Задача обеспечения подлинности ключевого материала в отличие от предыдущей может быть сформулирована только применительно к совокупности компонентов ОКС, находящихся в отношении функциональной зависимости (как предельный случай — применительно к ОКС в целом). Средствами обеспечения подлинности являются симметричные схемы аутентификации сообщений и схемы ЭЦП.

Задача обеспечения невозможности отказа от ключевого материала и совершенных посредством него криптографических операций решается посредством применения схем ЭЦП для подписания сообщения, содержащего удостоверяемый ключевой материал и метку времени, фиксирующую момент его существования. Невозможность отказа может быть обеспечена только асимметричными криптосхемами, т.е. в данном случае — схемами ЭЦП, так как секретные ключи подписи всегда имеют единственного владельца. Следовательно, при возникновении спора о факте создания какого-либо документа, заверенного цифровой подписью, его автор устанавливается однозначно.

Среди перечисленных задач новой является задача обеспечения целостности данных при нетождественных биективных преобразованиях ключевого материала. Автором разработан метод решения этой задачи и реализующие его алгоритмы контроля целостности ключевого

материала при его преобразованиях в СКЗИ, использующих пороговые СРС и пространственное распределение ключевого материала по принципу систем с дробной кратностью резервирования [10].

Заключение. В работе обобщены результаты исследования, направленного на разработку теоретических основ создания СКЗИ, корректно функционирующих и сохраняющих криптографическую стойкость при разрушении части ключевого материала, и на поиск путей их реализации. Так, на основе разработанного автором подхода к модельному представлению КС предложена и обоснована система показателей аутентичности единиц ключевого материала, сформулированы и доказаны критерии его аутентичности. Выяснены требования к структуре КС, обеспечивающие гарантии аутентичности ключевого материала по введенной системе показателей. Поисковая часть исследования позволила выявить и формализовать типовые элементы конструкции КС, названные схемами управления ключевым материалом. Для некоторых из них даны аналитические оценки величин, показывающих их способность влиять на безопасность ключевого материала СКЗИ в части показателей аутентичности. Систематизированы технические задачи, возникающие в связи с необходимостью обеспечить аутентичность ключевого материала, и намечены пути их решения.

СПИСОК ЛИТЕРАТУРЫ

1. З а п е ч н и к о в С. В. Модель ключевой системы многопользовательских средств защиты информации // Управление защитой информации: Материалы X Междунар. науч.-практ. конф.: сб. науч. тр. – Минск, “Амалфея”, 2006. – С. 199–201.
2. З а п е ч н и к о в С. В. Модельное представление ключевых систем средств криптографической защиты информации // Безопасность информационных технологий. – 2008. – № 4. – С. 84–92.
3. З а п е ч н и к о в С. В. Принципы обеспечения стойкости криптосистем к компрометации ключей // Безопасность информационных технологий. – 2008. – № 1. – С. 80–87.
4. З а п е ч н и к о в С. В. Методы и алгоритмы, обеспечивающие аутентичность ключевого материала криптосистем в условиях воздействия дестабилизирующих факторов // Материалы X Междунар. науч.-практич. конф. Информационная безопасность. Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2008. – С. 146–149.
5. З а п е ч н и к о в С. В. Обеспечение высокой доступности ключевого материала криптосистем в условиях воздействия дестабилизирующих факторов // Актуальные проблемы безопасности информационных технологий: Материалы II Междунар. науч.-практич. конф. (Сиб. гос. аэрокосмич. ун-т, 9–12 сент. 2008 г.) – Красноярск, 2008. – С. 17–21.
6. З а п е ч н и к о в С. В. Обеспечение криптографической стойкости при компрометации части ключей // Безопасность информационных технологий. – 2008. – № 4. – С. 93–102.
7. G o l d w a s s e r S., B e l l a r e M. Lecture notes on cryptography [электронный ресурс]. – University of California at San Diego, 1997 – 2000. – Режим доступа: http://www-cse.ucsd.edu/users/mihir.

8. З а п е ч н и к о в С. В. Повышение стойкости средств криптографической защиты информации на основе применения схем управления ключевым материалом // Материалы XII Международной конференции "Комплексная защита информации", Ярославль, 2008 г. – М.: РФК-Имидж Лаб, 2008. – С. 85–87.
9. З а п е ч н и к о в С. В. Модель "активной безопасности" и возможности ее реализации в системах криптографической защиты информации // Безопасность информационных технологий. – 1998. – № 4. – С. 52–54.
10. З а п е ч н и к о в С. В. Контроль целостности информационных ресурсов при распределенном хранении данных // Безопасность информационных технологий. – 2008. – № 2. – С. 86–91.

Статья поступила в редакцию 20.11.2008

Сергей Владимирович Запечников родился в 1974 г., окончил в 1997 г. Московский государственный инженерно-физический институт (технический университет). Канд. техн. наук, доцент кафедры "Информационная безопасность банковских систем" национального исследовательского ядерного университета "МИФИ". Автор 88 научных работ в области информационной безопасности и защиты информации.

S.V. Zapechnikov (b. 1974) graduated from the Moscow Engineering and Physics Institute (technical university) in 1997. Ph. D. (Eng.), assoc. professor of "Data Security of Banking Systems" department of the National Research Nuclear University "MIFI". Author of 88 publications in the field of data security and data protection.

УДК 004.78:025.4.036

В. М. В и ш н е в с к и й, Р. В. Ж е л е з о в

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННО-СПРАВОЧНАЯ СИСТЕМА ПОИСКА ОПТИМАЛЬНЫХ ПУТЕЙ ПРОЕЗДА НА ПАССАЖИРСКОМ ТРАНСПОРТЕ

Рассмотрены принципы построения и реализации информационно-справочной системы поиска оптимальных путей проезда на пассажирском транспорте. Описан оригинальный алгоритм поиска кратчайших путей с учетом расписаний пассажирского транспорта. Приведена архитектура программно-аппаратной реализации системы и интернет-сайта для доступа к справочной информации.
E-mail: vishn@iitp.ru

Ключевые слова: *информационная система, расписание, пассажирский транспорт, оптимизация, Интернет.*

Предоставление справочной информации об оптимальных путях проезда на пассажирском транспорте является необходимым условием для качественного обслуживания пассажиров. Полнота предоставленной информации не только помогает пассажиру, но и повышает эффективность пассажирских перевозок, уменьшает нагрузку на транспортные сети вследствие оптимизации пассажиропотока.

Первые электронные справочные системы расписаний транспорта появились в 80-х годах прошлого века. На постсоветском пространстве