13. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
14. Основные направления фундаментальных исследований Российской Федерации: Распоряжение Президиума РАН от 22 января 2007 г. № 10103-30.
15. *Фалеев М. И.* О базовых и приоритетных направлениях научно-технической политики МЧС России на 2008–2010 г. Доклад на коллегии МЧС России. 2007 год.
16. Заключительный отчет о НИР «Создание научно-методических основ информирования и оповещения населения с использованием современных технических средств массовой информации в местах массового пребывания людей». П. 4.3.1 ЕТП НИОКР МЧС России на 2007 год. М., 2007. – 362 с.

С. В. Запечников (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ СТОЙКОСТИ КРИПТОСИСТЕМ К КОМПРОМЕТАЦИИ КЛЮЧЕЙ

Приводится обзор результатов исследования, целью которого являлась разработка теоретических основ обеспечения стойкости ключевых систем (КС) средств криптографической защиты информации (СКЗИ) к частичному разрушению ключевого материала. Основные элементы излагаемого подхода: модель ключевых систем СКЗИ, система показателей и критериев безопасности ключевого материала, а также доказанные утверждения и теоремы о свойствах КС, определяющих стойкость СКЗИ.

Современные СКЗИ характеризуются очень высокой стойкостью применяемых в них криптографических алгоритмов, в связи с чем нарушение их безопасности посредством криптоаналитических атак маловероятно. Основным источником уязвимостей является слабость методов управления ключами, идентификаторами и другой информацией, определяющей политику безопасности систем защиты информации (ЗИ), а также методов и протоколов аутентификации. Стойкость существующих СКЗИ целиком основывается на предположении о безопасности используемых в них криптографических ключей. Криптоанализ требует от противника значительных вычислительных, временных и финансовых затрат. Похищение ключевого материала криптосистем или преднамеренное воздействие на него может быть значительно проще, а по эффективности сравнимо с криптоанализом.

1. Проблемы обеспечения стойкости СКЗИ

Криптографическая стойкость – фундаментальное понятие криптографии – свойство криптосистемы, характеризующее ее способность противостоять атакам противника, как правило, имеющим целью получить секретный ключ или открытое сообщение [1].

Проблема анализа и оценки стойкости СКЗИ относится к числу самых сложных проблем теории и практики ЗИ. Выделяется шесть принципиально различных подходов к анализу стойкости криптосистем: эвристический, теоретико-информационный, теоретико-системный, теоретико-сложностной, формально-логический и доказательный (редукционистский). Ни один из них нельзя считать бесспорным – каждый находит применение для решения определенного, чаще всего широкого, круга задач.

Основными задачами управления ключами являются:

– обеспечение требуемого качества ключевого материала;

– обеспечение безопасности ключевого материала, а именно: обеспечение доступности, аутентичности и секретности для секретных ключей; обеспечение доступности и аутентичности для открытых ключей и параметров криптосистемы.

Задачу обеспечения безопасности ключевого материала криптосистемы можно сформулировать как задачу защиты информации, обеспечивающей выполнение криптосистемой своих основных функций, т. е. как задачу *обеспечения собственной безопасности*, или как задачу *самозащиты* СКЗИ. Подавляющее большинство СКЗИ являются многофункциональными и многопользовательскими, поэтому задача управления ключами решается в них не для отдельных ключей, а для КС в целом. В связи с этим возникает проблема организации ключевых систем в сложных криптосистемах.

Важнейшей характеристикой КС является ее стойкость к компрометациям ключей. Пусть T — допустимая граница трудоемкости нарушения безопасности ключа. Говорят, что КС, работоспособность которой обеспечивается с помощью N ключей, *выдерживает r компрометаций*, $r<N$, если при компрометации r ключей нарушение безопасности остальных N-r ключей требует по-прежнему не менее T элементарных операций (если количество операций и уменьшается, то требуемая граница не преодолевается) [2].

Первым этапом решения проблемы обеспечения стойкости криптосистем в условиях компрометации части ключевого материала должна стать выработка инструментальной и методической базы. С этой целью строится математическая модель изучаемого объекта — ключевой системы СКЗИ, позволяющая описывать ее статическую структуру и динамику поведения. Для построения модели выделяются такие элементы КС и связи между ними, которые имеют наиболее существенное значение для обеспечения стойкости СКЗИ.

2. Модель ключевых систем СКЗИ

Рассмотрим вкратце основные элементы статической модели КС.

Объектом ключевой системы Obj будем называть минимальную совокупность взаимосвязанного ключевого материала криптосистемы. Критерием выделения ОКС является невозможность построения такой криптосистемы, в которой использовался бы ключевой материал в объеме, меньшем, чем содержащийся в одном ОКС.

Компонент ОКС Com — это минимальная логически неделимая единица ключевого материала в составе ОКС, применение которой еще возможно для выполнения криптографических операций либо для решения задач, связанных с управлением ключами. Область допустимых значений компонента станем обозначать $D(Com)$.

Если $\exists\, Com_0 \in Obj_i$, $\exists\, Com_1 \in Obj_i$, ... , $\exists\, Com_j \in Obj_i$, $\exists\, Com_q \in Obj_i$ и существует функция $f: D(Com_1)\text{x}...\text{x}\, D(Com_j)\text{x}...\text{x}\, D(Com_q) \to D(Com_0)$, такая, что для любого значения Com_j существует алгоритм A_1 вычисления значения Com_0 при фиксированных значениях других аргументов функции f, выполнимый за время $t_{A_1} \le \rho_{A_1}(|Com_1| + ... + |Com_j| + ... + |Com_q|)$, где $\rho_{A_1}(\cdot)$ — некоторый полином, то будем говорить, что *компонент* Com_0 *находится в отношении функциональной зависимости первого рода от компонента* Com_j, и обозначим этот факт как $Com_j \rhd_f Com_0$.

Если $\exists\, Com_{j_1} \in Obj_{i_1}$, $\exists\, Com_{j_2} \in Obj_{i_1}$, $\exists\, Com_k \in Obj_{i_2}$ и существует семейство функций F : $D(Com_{j_1})\,\text{x}\,D(Com_k) \to D(Com_{j_2})$, такое, что для любого фиксированного значения Com_k существует алгоритм A_1 вычисления значения по заданному значению Com_{j_2}, выполнимый за время $t_{A_2} \le \rho_{A_2}(|Com_{j_1}| + |Com_k|)$, где $\rho_{A_2}(\cdot)$ — некоторый полином, то будем говорить, что *компонент* Com_{j_2} *находится в отношении функциональной зависимости второго рода от компонента* Com_{j_1}, и обозначим этот факт как $Com_{j_2} \rhd_F Com_{j_1}$.

Любое подмножество $\omega \subseteq \{Com_{j_1},...,Com_{j_\rho},Com_{j_{\rho+1}},...,Com_{j_{\rho+q}}\}$ компонентов ОКС, такое, что для любых фиксированных значений компонентов $Com_{j_1} \in Obj_i$, ... , $Com_{j_\rho} \in Obj_i$, $Com_{j_{\rho+1}} \in Obj_{r_1}$, ... , $Com_{j_{\rho+q}} \in Obj_{r_q}$, где , $r_1 \ne i$... , $r_q \ne i$, существует алгоритм A_3 вычисления значения $Com_0 \in Obj_i$, выполнимый за время $t_{A_3} \le \rho_{A_3}(|Com_{j_1}| + ... + |Com_{j_\rho}| + |Com_{j_{\rho+1}}| + ... + |Com_{j_{\rho+q}}|)$, где $\rho_{A_3}(\cdot)$ — некоторый полином, но при неизвестном значении хотя бы одного из компонентов множества ω значение Com_0 не определено, будем называть *минимальным множеством вычислимости (ММВ) компонента* Com_0

и обозначать его $\omega(Com_0)$. Множество всех ММВ компонента обозначим через $\Omega[Com_0]$.

Если $\exists Com_{j_1} \in Obj_i$ и $\exists Com_{j_2} \in Obj_i$, такие, что область допустимых значений $D(Com_{j_2}) \subseteq \{0,1\}^{|Com_{j_2}|}$ существенно зависит от значения, принимаемого Com_{j_1}, то будем говорить, что *компонент* Com_{j_2} *находится в отношении параметрической зависимости от компонента* Com_{j_1}, и обозначим этот факт как $Com_{j_1} \rhd_\rho Com_{j_2}$.

Определим, что *компонент* Com_{j_2} *зависим от* Com_{j_1}, и обозначим этот факт $Com_{j_1} \rhd Com_{j_2}$, если $Com_{j_1} \rhd_f Com_{j_2}$, либо $Com_{j_1} \rhd_F Com_{j_2}$, либо $Com_{j_1} \rhd_\rho Com_{j_2}$. Введенные отношения отображают самые существенные с точки зрения стойкости свойства компонентов ОКС — вычислимость одних ключей криптосистемы из совокупности других.

Отношения между компонентами ОКС удобно задавать, руководствуясь теоретико-графовым подходом. Пусть $G^f_{Obj_i} = (V^f_{Obj_i}, E^f_{Obj_i})$ — ориентированный граф, описывающий отношения функциональной зависимости первого рода между компонентами ОКС Obj_i: $V^f_{Obj_i}$ — множество его вершин, $E^f_{Obj_i}$ — множество дуг. Множество вершин этого графа образуют все компоненты $Com_j \in Obj_i$, связанные отношением функциональной зависимости первого рода. Дуга $e \in E^f_{Obj_i}$ направлена от Com_ρ к Com_q, если $Com_\rho \rhd_f Com_q$. По аналогии можно определить орграф $G^F_{Obj_i} = (V^F_{Obj_i}, E^F_{Obj_i})$, описывающий отношение функциональной зависимости второго рода между компонентами ОКС Obj_i, и орграф $G^\rho_{Obj_i} = (V^\rho_{Obj_i}, E^\rho_{Obj_i})$, описывающий отношения параметрической зависимости между компонентами ОКС Obj_i. Орграф $G_{Obj_i} = (V_{Obj_i}, E_{Obj_i})$, полученный объединением орграфов $G^f_{Obj_i}$, $G^F_{Obj_i}$ и $G^\rho_{Obj_i}$, т. е. $V_{Obj_i} = V^f_{Obj_i} \cup V^F_{Obj_i} \cup V^\rho_{Obj_i}$ и $E_{Obj_i} = E^f_{Obj_i} \cup E^F_{Obj_i} \cup E^\rho_{Obj_i}$, будем называть *графом зависимости между компонентами ОКС* Obj_i.

В модели выделяются понятия владельца ОКС, обладателя экземпляра ОКС, участника КС и противника. Противник — это лицо, которое в соответствии с регламентом функционирования криптосистемы не имеет права санкционированного доступа к содержанию одного или нескольких компонентов по крайней мере одного ОКС, но фактически получило или стремится получить несанкционированный доступ к нему.

На основе статической строится динамическая модель КС, учитывающая взаимосвязи не только между ключами, одновременно присутствующими в криптосистеме, но и между изменяющимися во времени значениями одного ключа. Так, любое подмножество значений компонента $\theta \subseteq \{Com_j(\lambda_1), ..., Com_j(\lambda_{\tau-1}), Com_j(\lambda_{\tau+1}), ..., Com_j(\lambda_q)\}$ на непересекающихся временных интервалах, такое, что для любых фиксированных значений этого компонента $Com_j(\lambda_1)$, ... , $Com_j(\lambda_{\tau-1})$, $Com_j(\lambda_{\tau+1})$, ... , $Com_j(\lambda_q)$ существует алгоритм C_4 вычисления значения $Com_j(\lambda_\tau)$, выполнимый за время $t_{C_4} \le \rho_{C_4}(q \cdot |Com_j|)$, где $\rho_{C_4}(\cdot)$ — некоторый полином, но хотя бы при одном неизвестном значении компонента Com_j, принадлежащем множеству θ, значение $Com_j(\lambda_\tau)$ не определено, будем называть *минимальной последовательностью вычислимости (МПВ)* компонента Com_j и обозначим ее $\theta(Com_j(\lambda_\tau))$.

Модель расширяема и в другом направлении: аналогичные отношения выделяются между ОКС и, таким образом, описываются существенные свойства КС в целом. КС также описывается теоретико-графовой моделью. Так может быть описано абсолютное большинство КС современных СКЗИ на основе симметричных криптосистем, криптосистем с инфраструктурой открытых ключей, идентификационных и бессертификатных криптосистем.

3. Показатели и критерии безопасности ключевого материала

Для исследования стойкости СКЗИ к компрометации необходимо ввести меру безопасности ключевого материала и уметь получать количественные оценки безопасности. С этой целью автором разработаны способы формирования таких оценок, а с их помощью доказаны утверждения о необходимых условиях безопасности ОКС. Все три аспекта безопасности ключевого материала — доступность, аутентичность и подлинность — характеризуются количественными показателями, построенными на

основе единой модели противника, которая учитывает большинство возможностей нарушения безопасности ключевого материала.

Доступность компонента ОКС $Com_j \in Obj_i$ *на непрерывном временном интервале* λ определим как свойство компонента Com_j, заключающееся в возможности совершения с ним любой санкционированной операции в произвольный момент времени τ, приходящийся на временной интервал λ.

Коэффициентом доступности компонента ОКС Com_j *на временном интервале* λ будем называть вероятность того, что компонент будет доступен в произвольный момент времени τ, приходящийся на временной интервал λ. В стационарном режиме он равен отношению той части временного интервала, в течение которого компонент ОКС сохраняет свойство доступности, к общей длине временного интервала: $K_д(Com_j, \lambda) = T_д/(T_д + \tilde{T}_{пр})$, где $T_д$ — время, в течение которого компонент ОКС доступен в СКЗИ, $\tilde{T}_{пр}$ — время, в течение которого компонент считается заблокированным в результате деятельности противника, причем $\tilde{T}_{пр} = T_{пр} + T_{тех}$, где $T_{пр}$ — время, в течение которого компонент заблокирован противником, $T_{тех}$ — время, в течение которого компонент недоступен из-за технических отказов.

Вероятность успеха противника, т. е. вероятность того, что Com_j не будет доступен в произвольный момент времени τ в течение временного интервала λ, обозначим $\alpha(Com_j, \lambda)$, считая, что она постоянна на данном интервале. Если эта вероятность зависит от времени, то в качестве $\alpha(Com_j, \lambda)$ примем ее максимальное значение на интервале λ.

Лемма 1. Вероятность того, что компонент ОКС $Com_j \in Obj_i$ недоступен в произвольный момент времени τ в течение временного интервала λ, равна

$$\alpha(Com_j, \lambda_\tau) = 1 - K_Д(Com_j, \lambda_\tau) \cdot \prod_{\omega \in \bar{\Omega}[Com_j, \lambda_\tau]} K_Д(\omega, \lambda_\tau) \cdot \prod_{\theta \in \bar{\Theta}[Com_j, \lambda_\tau]} K_Д(\theta, \lambda_\tau).$$

Пусть $\bar{\Omega}[Com_j, \lambda_\tau] \subseteq \Omega[Com_j]$ — подмножество множества всех ММВ компонента Com_j, состоящее из таких ММВ, для которых ЖЦ всех элементов ММВ включает интервал λ_τ. ММВ $\bar{\omega}(Com_j, \lambda_\tau) \in \bar{\Omega}[Com_j, \lambda_\tau]$ будем назвать *ММВ, действующим на интервале* λ_τ.

Пусть $\bar{\Theta}[Com_j, \lambda_\tau] \subseteq \Theta[Com_j]$ — подмножество множества всех МПВ компонента Com_j, состоящее из таких МПВ, все элементы которых присутствуют в КС одновременно в течение временного интервала λ_τ. МПВ $\bar{\theta}(Com_j, \lambda_\tau) \in \bar{\Theta}[Com_j, \lambda_\tau]$ будем назвать *МПВ, действующей на интервале* λ_τ.

Теорема 1. *(Критерий доступности ключевого материала на одном временном интервале)* Если в произвольный момент времени τ, приходящийся на временной интервал λ_τ, противник заблокировал доступ к некоторому подмножеству Ф компонентов ОКС, то до тех пор, пока остается незаблокированным доступ к компоненту $Com_j \in Obj_i$, или хотя бы к одному его действующему ММВ, или хотя бы к одной его действующей МПВ, значение этого компонента однозначно определено следующим образом:

$$H(Com_j(\lambda_\tau) | \Phi : (Com_j(\lambda_\tau) \notin \Phi) \vee (\exists \bar{\omega}(Com_j(\lambda_\tau)) \not\subset \Phi) \vee (\exists \bar{\theta}(Com_j(\lambda_\tau)) \not\subset \Phi)) = 0,$$

где $H(Com_j)$ — энтропия компонента Com_j. Если компонент $Com_j \in Obj_i$ заблокирован противником и не найдется ни одного действующего ММВ и ни одной действующей МПВ, то значение этого компонента не может быть определено однозначно:

$$0 < H(Com_j(\lambda_\tau) | \Phi : (Com_j(\lambda_\tau) \in \Phi) \wedge (\forall \bar{\omega}(Com_j(\lambda_\tau)) \subseteq \Phi) \wedge (\forall \bar{\theta}(Com_j(\lambda_\tau)) \subseteq \Phi)) \leq H(Com_j).$$

Аутентичность компонента ОКС $Com_j \in Obj_i$ *на непрерывном временном интервале* λ определим как свойство компонента Com_j, заключающееся в том, что значение компонента, считанное либо записанное в некоторый экземпляр ОКС в произвольный момент времени τ в течение временного интервала λ, совпадает с его истинным значением.

Вероятность успеха противника, т. е. вероятность того, что в произвольный момент времени τ в течение временного интервала λ компонент $Com_j \notin \Phi$ будет признан СКЗИ аутентичным, хотя на

самом деле таковым не является, обозначим $\beta(Com_j, \lambda)$, считая, что она постоянна на данном временном интервале. Если эта вероятность зависит от времени, то в качестве $\beta(Com_j, \lambda)$ примем ее максимальное значение на интервале λ.

Лемма 2. Вероятность того, что компонент ОКС $Com_j \in Obj_i$ неаутентичен в произвольный момент времени τ в течение временного интервала λ, равна

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

Теорема 2. *(Критерий аутентичности ключевого материала на одном временном интервале)* Пусть Ф — 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 Ф, то из них можно получить истинное значение $Com_j \in Obj_i$ с вероятностью $P = 1 - P^*$, где

$$P^* = P\left(Com_j^* \neq Com_j \middle| \Phi : \left(Com_j(\lambda_\tau) \notin \Phi\right) \vee \left(\exists \overline{\omega}\left(Com_j(\lambda_\tau)\right) : \forall Com_{\overline{\omega}} \notin \Phi\right) \vee \right.$$
$$\left. \vee \left(\exists \overline{\theta}\left(Com_j(\lambda_\tau)\right) : \forall Com_{\overline{\theta}} \notin \Phi\right)\right) \leq \beta\left(Com_j, \lambda_\tau\right)$$

Похожим образом определяется критерий аутентичности ключевого материала на непрерывной последовательности временных интервалов.

Секретность компонента ОКС $Com_j \in Obj_i$ на непрерывном временном интервале λ определим как свойство компонента Com_j, заключающееся в том, что его значение в произвольный момент времени τ в течение временного интервала λ известно только владельцам ОКС $Own\ (Obj_i)$ и неизвестно никому более.

Вероятность того, что противнику в некоторый момент времени τ в течение временного интервала λ станет известно значение $Com_j \notin \Phi \backslash X$, обозначим через $\gamma(Com_j, \lambda)$, считая, что она постоянна на данном временном интервале. Если эта вероятность зависит от времени, то в качестве $\gamma(Com_j, \lambda)$ примем ее максимальное значение на интервале λ. Формулы для оценки значений $\gamma(Com_j, \lambda)$ задаются следующими доказанными утверждениями.

Если в КС имеется n экземпляров ОКС Obj_i, то для нарушения секретности достаточно, чтобы противник получил доступ хотя бы к одному экземпляру ОКС, т. е.

$$p_{ПДК}\left(Com_j\right) = p_{ПДК}\left(Com_j^{(n)}\right) = 1 - \prod_{(i)} \left(1 - p_{ПДК}^{(i)}\left(Com_j\right) \cdot p_{обх}^{(i)}\left(Com_j\right)\right) \quad (1)$$

где $p_{ПДК}^{(i)}$ — вероятность прямого доступа к i-му экземпляру ОКС, $p_{обх}^{(i)}$ — вероятность «обхода» противником механизма аутентификации.

Вероятность успеха противника при осуществлении одного из видов атак на КС определяется видом атаки.

Вероятность случайного угадывания можно оценить следующим соотношением:

$$\frac{1}{\left|E\left(Com_j\right)\right|} \geq p_1\left(Com_j\right) \geq \frac{1}{\left|D\left(Com_j\right)\right|} \geq \frac{1}{2^x} \quad (2)$$

где $E\ (Com_j)$ — множество значений, образующих составленный противником словарь.

Вероятность восстановления компонента ОКС из функционально зависимых компонентов ОКС составит величину

$$p_2\left(Com_j, \lambda_\tau\right) = 1 - \prod_{i=1}^{\left|\Omega\left[Com_j(\lambda_\tau)\right]\right|} \left(1 - \prod_{s=1}^{\left|\omega_i\left(Com_j(\lambda_\tau)\right)\right|} \gamma\left(Com_s(\lambda_\tau)\right)\right) \quad (3)$$

Вероятность восстановления компонента ОКС из последовательности изменяющихся во времени значений компонента ОКС будет

$$p_3\left(Com_j,\lambda_\tau\right)=1-\prod_{i=1}^{\left|\Theta\left[Com_j(\lambda_\tau)\right]\right|}\left(1-\prod_{s=1}^{\left|\theta_i\left(Com_j(\lambda_\tau)\right)\right|}\gamma\left(Com_s(\lambda_\tau)\right)\right) \quad (4)$$

Вероятность восстановления компонента ОКС из последовательности изменяющихся во времени значений функционально зависимых компонентов ОКС:

$$p_4\left(Com_j,\lambda_\tau\right)=1-\prod_{r=1}^{\left|\Omega\left[Com_j(\lambda_\tau)\right]\right|}\left(1-\prod_{\substack{u=1\\u\neq\tau}}^{\left|\Theta\left[Com_r(\lambda_\tau)\right]\right|}\gamma\left(Com_r(\lambda_u)\right)\right)\cdot\prod_{s=1}^{\left|\Theta\left[Com_j(\lambda_\tau)\right]\right|}\left(1-\prod_{\substack{v=1\\v\neq\tau}}^{\left|\Omega\left[Com_j(\lambda_\tau)\right]\right|}\gamma\left(Com_s(\lambda_v)\right)\right) \quad (5)$$

Лемма 3. Вероятность того, что компонент ОКС $Com_j \in Obj_i$ утратил секретность в произвольный момент времени τ в течение временного интервала λ, равна

$$\gamma\left(Com_j,\lambda_\tau\right)=1-\left(1-p_{ПДК}\left(Com_j\right)\right)\cdot\prod_{i}\left(1-p_i\left(Com_j,\lambda_\tau\right)\cdot p_{НСП}\left(Com_j\right)\right),$$

где $p_{ПДК}$ определяется уравнением (1), p_i, $i=\overline{1,4}$ — уравнениями (2) — (4) соответственно.

Теорема 3. *(Критерий секретности ключевого материала на одном временном интервале)* Пусть $Com_j \in Obj_i$ и пусть $\{\Psi_1, \Psi_2,..., \Psi_t,..., \Psi_m\}$ — множества компонентов ОКС, значения которых на временных интервалах $\lambda_1, \lambda_2,..., \lambda_t,..., \lambda_m$, образующих непрерывную последовательность $\Lambda=<\lambda_1, \lambda_2,..., \lambda_t,..., \lambda_m>$, известны противнику. Если из множества известных противнику компонентов ОКС никаким способом невозможно сформировать ни одного ММВ и ни одной МПВ, т. е.

$$\left(\nexists\omega\left(Com_j(\lambda_\tau)\right)\subseteq\Psi_\tau\right)\vee\left(\nexists\theta\left(Com_j(\lambda_\tau)\right)\subseteq\Psi_1\times\Psi_2\times...\times\Psi_m\right)\vee$$
$$\vee\left(\nexists\omega\left(Com_r(\lambda_i)\right)\subseteq\Psi_i, i=i_1,i_2,...,i_m : \left\{Com_r\left(\lambda_{i_1}\right),...,Com_r\left(\lambda_{i_m}\right)\right\}=\theta\left(Com_j(\lambda_\tau)\right), r\neq j\right)\vee$$
$$\vee\left(\nexists\theta\left(Com_s(\lambda_\tau)\right)\subseteq\Psi_{i_1}\times...\times\Psi_{i_m}, s=s_1,,,s_k : \left\{Com_{s_1}(\lambda_\tau),...,Com_{s_k}(\lambda_\tau)\right\}=\omega\left(Com_j(\lambda_\tau)\right) s_1\neq...\neq s_k\neq j\right),$$

то вероятность утраты секретности Com_j на произвольно выделенном из последовательности Λ интервале λ_τ не превосходит величины $P(Com_j(\lambda_\tau)|\{\Psi_1, \Psi_2,..., \Psi_m\}) \le \gamma(Com_j, \lambda_\tau)$.

Если же хотя бы одно из этих условий не выполнено, то $P(Com_j(\lambda_\tau)|\{\Psi_1, \Psi_2,..., \Psi_m\})=1$ и $Com_j(\lambda_\tau)\in\Psi_\tau$.

В качестве интегрального показателя безопасности (ИПБ) компонента на интервале λ предлагается брать величину $S\left(Com_j,\lambda\right)=1-\left[\alpha\left(Com_j,\lambda\right)+\left(1-\alpha\left(Com_j,\lambda\right)\right)\cdot\beta\left(Com_j,\lambda\right)+\right.$
$\left.+\left(1-\alpha\left(Com_j,\lambda\right)\right)\cdot\left(1-\beta\left(Com_j,\lambda\right)\cdot\gamma\left(Com_j,\lambda\right)\right)\right]$.

Обоснование выбора величины S в качестве ИПБ таково: это вероятность того, что в течение выбранного временного интервала или последовательности интервалов будет обеспечена безопасность компонента Com_j в смысле того, что не наступит ни одно из трех событий: 1) утрата доступности компонента Com_j, вероятность чего равна $\alpha(Com_j, \lambda)$; 2) утрата аутентичности компонента Com_j, вероятность чего равна $\beta(Com_j, \lambda)$, при условии его доступности; 3) утрата секретности компонента Com_j, вероятность чего равна $\gamma(Com_j, \lambda)$, при условии его доступности и аутентичности. Очевидно, что наступление хотя бы одного из этих событий делает компонент ОКС непригодным для применения в СКЗИ.

Система показателей безопасности естественным образом расширяется для ОКС и для подсистем КС. Обладая методами количественной оценки безопасности более крупных единиц ключевого материала, уже возможно исследовать свойства КС в целом, необходимые для обеспечения стойкости СКЗИ к частичному разрушению ключевого материала.

Выводы

1. Разработана математическая модель, позволяющая описывать широкий класс ключевых систем СКЗИ, которая используется в качестве инструмента исследования стойкости КС. Модель позволяет проводить анализ безопасности КС с заданной структурой ключевого материала.

2. Предложена система количественных показателей безопасности ключевого материала. Она построена по модульному принципу, включает частные и интегральный показатели. Научная новизна предложенного подхода состоит в том, что впервые анализ всех аспектов безопасности ведется на основе единой модели активного противника, управляющего воздействием дестабилизирующих факторов. Предложенный набор критериев не является «закрытым» — он может пополняться, а способы формирования количественных показателей безопасности — совершенствоваться.

3. Исследованы свойства объектов КС, определяющие стойкость содержащегося в нем ключевого материала. Доказаны теоремы, задающие критерии обеспечения доступности, аутентичности и секретности компонентов ОКС на непрерывных временных интервалах, в течение которых ключевой материал остается неизменным, а также на непрерывных последовательностях таких интервалов. Получены уравнения для расчета вероятностей утраты доступности, нарушения аутентичности и секретности компонентов ОКС.

СПИСОК ЛИТЕРАТУРЫ

1. Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. М., 2006. — 94 с.
2. *Фомичев В. М.* Симметричные криптосистемы. Краткий обзор основ криптологии для шифрсистем с секретным ключом: Учебное пособие. М., 1995. — 44 с.