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

МОДЕЛЬНОЕ ПРЕДСТАВЛЕНИЕ КЛЮЧЕВЫХ СИСТЕМ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Представлен подход к построению моделей ключевых систем средств криптографической защиты информации (СКЗИ), позволяющий описывать их статическую структуру и динамику поведения. Для построения моделей выделяются такие элементы ключевых систем и связи между ними, которые имеют наиболее существенное значение для обеспечения стойкости СКЗИ. Рассматриваются примеры описания ключевых систем с помощью предложенных моделей.

Введение

Ключевые системы (КС) современных СКЗИ характеризуются сложностью и разнообразием устройства. Предполагается, что в будущем, с расширением функциональности и масштабов использования СКЗИ, их КС будут только усложняться. Исследование проблем обеспечения стойкости СКЗИ и проектирование сложных криптосистем требуют средств формального описания возможно более широкого класса КС. В связи с этим становится необходимым построение моделей КС, которые позволяют адекватно описывать КС и могут являться инструментом дальнейшего их исследования.

1. Объекты ключевой системы и их компоненты

Объектом ключевой системы (ОКС) 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. ОКС будем обозначать символами *Obj* с соответствующими индексами.

Компонент ОКС — 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 криптосистемы. Компоненты ОКС будем обозначать символами *Com* с соответствующими индексами. Область допустимых значений компонента *Com* станем обозначать *D(Com)*.

Жизненный цикл (ЖЦ) ОКС — это последовательность состояний и переходов между ними, которые проходит ОКС за время своего существования в криптосистеме. ЖЦ ОКС есть совокупность ЖЦ всех его компонентов, каждый из которых может быть определен в соответствии с ISO/IEC 11770.

Формат ОКС — это условное описание структуры ОКС. В самом общем виде формат любого ОКС может быть представлен как упорядоченная совокупность шести множеств $Obj = (A,B,C,D,E,F)$, где: $A = \{a_1, a_2,..., a_{|A|}\}$ — множество компонентов ОКС, содержащих открытые общедоступные параметры криптосистемы, управляющую и служебную информацию, обеспечивающую ЖЦ криптосистемы; $B = \{b\}$ — компонент ОКС, содержащий секретный ключ; $C = \{c_1, c_2,..., c_{|C|}\}$ — множество компонентов ОКС, содержащих ключевой материал, который может зависеть от значений компонентов множеств A и B, требующий обеспечения секретности и аутентичности; $D = \{d_1, d_2,..., d_{|D|}\}$ — множество компонентов ОКС, содержащих открытые ключи; $E = \{e_1, e_2,..., e_{|E|}\}$ — множество компонентов ОКС, содержащих ключевой материал, который может зависеть от значений компонентов множеств A, B и D, требующий обеспечения аутентичности; $F = \{f_1, f_2,..., f_{|F|}\}$ — множество компонентов ОКС, содержащих значения, зависимые от значений компонентов множеств A, B, C, D и E. Подмножество $M = \{B, C, D, E\}$ компонентов ОКС будем называть *ключевой частью* ОКС, подмножество $N = \{A, F\}$ — *неключевой частью* ОКС.

ОКС может содержать не более одного компонента, принадлежащего множеству B — это критерий объединения совокупности взаимосвязанного ключевого материала в ОКС.

Все компоненты ОКС для применения в криптосистеме требуют обеспечения доступности. Ключевая часть ОКС есть подмножество компонентов ОКС, требующих дополнительно обеспечения аутентичности. Поля $\{B,C\}$ ключевой части есть подмножество компонентов ОКС, требующих дополнительно обеспечения секретности.

Приведем примеры наполнения полей ОКС: A — описания алгебраических структур, необходимых для криптографических алгоритмов и протоколов, общеизвестных идентификаторов участников, параметров криптосистемы и длин ключей; B — общие секретные ключи участников симметричных криптосистем, персональные секретные ключи участников асимметричных криптосистем; C — доли разделенного посредством СРС секретного ключа, производные ключи в схемах с базой, проверочные разряды для контроля целостности секретных ключей; D — открытые ключи, цепочки открытых ключей участников асимметричных криптосистем; E — владельцы ОКС, проверочные разряды для секретных и открытых ключей (MDC — manipulation detection codes), зашифрованные секретные ключи; F — сертификаты открытых ключей, коды аутентификации для секретных и открытых ключей (MAC — message authentication codes), зашифрованные и подписанные секретные ключи, подписанные открытые ключи, метки времени, порядковые номера ключей, адресная информация.

Для описания взаимосвязей компонентов введем определения отношений между ними.

Пусть Obj_i — некоторый ОКС. 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 $f: D(Com_1)\times\ldots\times D(Com_j)\times\ldots\times D(Com_q)\to D(Com_0)$, 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 $t_{A_1} \le \rho_{A_1}(|Com_1|+\ldots+|Com_j|+\ldots+|Com_q|)$, где $p_{A_1}(.)$ — некоторый полином, то будем говорить, что *компонент* Com_0 *находится в отношении функциональной зависимости первого рода от компонента* Com_j, и обозначать этот факт $Com_j \rhd_f Com_0$.

Если $\exists Com_{i_1} \in Obj_{i_1}$, $\exists Com_{i_2} \in Obj_{i_1}$, $\exists Com_k \in Obj_{i_2}$ и существует семейство функций F : $D(Com_{j1})\times D(Com_k)\to D(Com_{i_2})$, такое, что для любого фиксированного значения Com_k существует алгоритм A_2 вычисления значения Com_{i2} по заданному значению Com_{j1}, выполнимый за время $t_{A_2} \le \rho_{A_2}(|Com_j|+|Com_k|)$, где $\rho_{A_2}(.)$ — некоторый полином, то будем говорить, что *компонент* Com_{i2} *находится в отношении функциональной зависимости второго рода от компонента* Com_{j1}, и обозначать этот факт $Com_{i_2} \rhd_F Com_{i_1}$. Если $i_2 \ne i_1$, то такую зависимость будем называть *внешней*, в противном случае — *внутренней*.

В случае если компонент ОКС функционально зависим от нескольких компонентов различных ОКС, отнесение его к тому или иному ОКС является предметом соглашения. Для удобства такие компоненты могут быть выделены в новый ОКС.

Любое подмножество компонентов ОКС $\omega \subseteq \{Com_{i_1},\ldots, Com_{i_\rho}, Com_{i_{\rho+1}},\ldots, Com_{i_{\rho+q}}\}$, такое, что для любых фиксированных значений компонентов $Com_{j1} \in Obj_i$, ..., $Com_{i_\rho} \in Obj_i$, $Com_{i_{\rho+1}} \in Obj_{r1}$, ..., $Com_{i_{\rho+q}} \in Obj_{r_q}$, где $r_1 \ne i$, ... , $r_q \ne i$, существует алгоритм A_3 вычисления значения $Com_0 \in Obj_i$, выполнимый за время $t_{A_3} \le \rho_{A_3}(|Com_{i_1}|+\ldots+|Com_{i_\rho}|+|Com_{i_{\rho+1}}|+\ldots+|Com_{i_{\rho+q}}|)$, где $\rho_{A_3}(.)$ — 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 $\omega(Com_0)$. Обозначим подмножества множества ω_{Com_0} следующим образом: $\{Com_{j1},\ldots, Com_{i_\rho}\}=\omega'(Com_0)$, $\{Com_{i_{\rho+1}},\ldots, Com_{i_{\rho+q}}\}=\omega''(Com_0)$. Очевидно, $\omega(Com_0)=\omega'(Com_0)\cup\omega''(Com_0)$. Если множество $\omega''(Com_0)$ непусто, то будем называть ММВ *внешним*, если же $\omega''(Com_0)=\varnothing$, то *внутренним*. Множество всех ММВ компонента Com_0 обозначим $\Omega[Com_0]$.

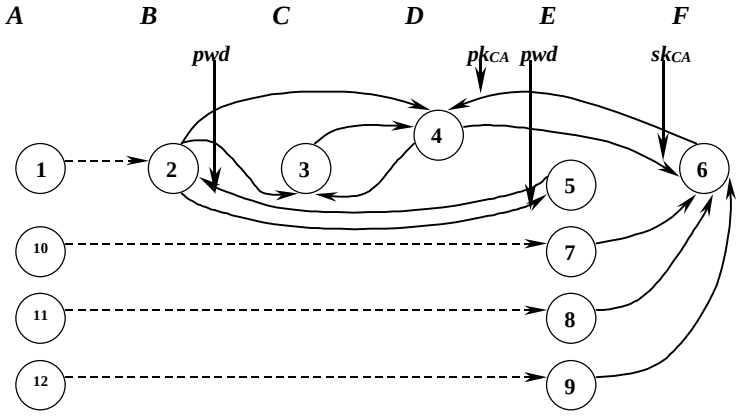
Если $\exists Com_{i_1} \in Obj_i$ и $\exists Com_{i_2} \in Obj_i$, такие, что область допустимых значений $D(Com_{i_2}) \subseteq \{0,1\}^{|Com_{i_2}|}$ существенно зависит от значения, принимаемого Com_{i_1}, то будем говорить, что *компонент* Com_{i_2} *находится в отношении параметрической зависимости от компонента* Com_{i_1}, и обозначать этот факт $Com_{i_1} \rhd_{\rho} Com_{i_2}$.

Будем говорить, что *компонент* Com_{i_2} *зависим от компонента* Com_{i_1}, и обозначать этот факт $Com_{i_1} \rhd Com_{i_2}$, если $Com_{i_1} \rhd_f Com_{i_2}$ либо $Com_{i_1} \rhd_F Com_{i_2}$ либо $Com_{i_1} \rhd_{\rho} Com_{i_2}$.

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 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 Obj_i, и орграф $G^{\rho}_{Obj_i}=(V^{\rho}_{Obj_i}, E^{\rho}_{Obj_i})$, описывающий отношения параметрической зависимости между компонентами 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* Obj_i.

Приведем один пример. На рис. 1 показан граф, описывающий ОКС «Ключи участника криптосистемы с инфраструктурой открытых ключей (ИОК) для схемы ЭЦП RSA», в предположении, что секретный ключ шифруется на личном пароле владельца ключа. Дуги, не имеющие исходящих вершин, показывают функциональную зависимость компонентов ОКС от компонентов других ОКС. Тонкими стрелками показана функциональная зависимость первого рода, жирными стрелками — функциональная зависимость второго рода, пунктирными стрелками — параметрическая зависимость.

Экземпляр ОКС — это единичная копия ОКС или любого непустого подмножества его компонентов. Количество экземпляров ОКС может изменяться в течение ЖЦ ОКС. Из предыдущих рассуждений следует, что формат каждого экземпляра ОКС есть подмножество упорядоченного множества. В каждом конкретном ОКС любое из этих множеств компонентов может отсутствовать. Таким образом, в пределе все экземпляры ОКС могут различаться, а некоторые компоненты, номинально описанные в формате ОКС, не присутствовать ни в одном экземпляре ОКС.



1 – длина модуля n схемы RSA;
2 – секретный ключ схемы RSA $sk=(p,q)$;
3 – секретный ключ генерации подписи / расшифрования RSA $d: ed \equiv 1(\mathrm{mod}(p-1)(q-1))$;
4 – открытый ключ схемы RSA $pk=(n,e): n=pq$;
5 – зашифрованный на пароле pwd секретный ключ;
6 – сертификат открытого ключа, подписанный секретным ключом УЦ sk_{CA}, проверяемый открытым ключом pk_{CA};
7–идентификатор (атрибут) владельца ключевой пары RSA;
8 – метка времени момента генерации ключевой пары RSA;
9 – адрес владельца ключевой пары RSA;
10 – допустимое множество идентификаторов (атрибутов);
11 – допустимое множество меток времени;
12 – допустимое множество адресов.

Рис. 1. ОКС «Ключи схемы цифровой подписи RSA участника криптосистемы с ИОК»

Владелец ОКС Obj_i — это участник криптосистемы, который в соответствии с регламентом функционирования криптосистемы имеет право санкционированного доступа к содержанию компонента $b \in B$ ОКС Obj_i. Будем обозначать владельца $Own(Obj_i)$. Владельцами одного ОКС могут быть один, два и более участников криптосистемы. Каждый ОКС ассоциирован со своим множеством владельцев, которое остается неизменным в течение всего ЖЦ ОКС. Если компонент $b \in B$ отсутствует в ОКС, т. е. $b=\varnothing$, считаем его владельцами всех участников криптосистемы.

Обладатель компонента Com_j *ОКС* Obj_i — это участник криптосистемы, который фактически имеет возможность доступа к компоненту ОКС, содержащемуся в доступных ему экземплярах ОКС. Будем обозначать обладателя компонента $Pos(Obj_i.Com_j)$. Количество обладателей ОКС может превышать количество владельцев ОКС. Очевидно, что любой владелец ОКС Obj_i одновременно является обладателем компонента $b \in B$ этого ОКС.

Участник КС — это любой владелец ОКС либо обладатель по крайней мере одного компонента ОКС. *Коалиция участников КС* — это подмножество множества участников КС, таких, что вся информация о КС, ОКС и СКС, известная одному из участников коалиции, немедленно становится известна всем остальным участникам коалиции. *Субъектом ключевой системы (СКС)* будем называть участника КС либо коалицию участников КС, который(-ая) является легальным владельцем одного либо нескольких ОКС либо обладателем по крайней мере одного компонента ОКС. СКС будем в дальнейшем обозначать символами *Sub* с соответствующими индексами.

Противник — это участник либо коалиция участников КС, не являющиеся СКС. Таким образом, противник — это лицо, которое 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. В частности, всякий обладатель компонента из поля B, не являющийся владельцем ОКС, является противником.

Операция СКС над ОКС — это логически неделимая совокупность действий СКС над ОКС или отдельными его компонентами, приводящая к изменению содержания компонентов ОКС либо количества экземпляров ОКС. Выделим следующие три операции СКС над ОКС:

- запись в компонент Com_j ОКС Obj_i непустого значения — $W(Obj_i.Com_j;Sub_k)$;
- чтение из компонента Com_j ОКС Obj_i — $R(Obj_i.Com_j;Sub_k)$;
- уничтожение компонента Com_j ОКС Obj_i — $D(Obj_i.Com_j;Sub_k)$.

Для простоты операции порождения и удаления ОКС не рассматриваются, а структура КС считается «предопределенной» и фиксированной в течение всего ЖЦ КС.

Введенных терминов достаточно для построения статической модели КС.

2. Статическая модель ключевой системы

Ключевая система KS — это совокупность трех элементов: множества всех ОКС $KObj=\{Obj_1,...,Obj_N\}$, множества всех СКС $KSub=\{Sub_1,...,Sub_L\}$, которые являются владельцами или обладателями этих ОКС:

$$KSub = \left(\bigcup_{Obj_i \in KObj} Own(Obj_i) \right) \bigcup \left(\bigcup_{Com_j \in Obj_i} Pos(Obj_i.Com_j) \right),$$

и множества всех операций СКС над ОКС:

$$KOp = \left\{ \bigcup_{i,j,k} W(Obj_i.Com_j;Sub_k); \bigcup_{i,j,k} R(Obj_i.Com_j;Sub_k); \bigcup_{i,j,k} D(Obj_i.Com_j;Sub_k) \right\},$$

где $Obj_i \in KObj$, $Com_j \in Obj_i$, $Sub_k \in KSub$.

Для описания временного аспекта функционирования КС введем ряд определений и обозначений.

Такт КС — промежуток времени между любыми двумя последовательными операциями R, W, D над ОКС.

Пусть $T=\{\tau_1, \tau_2,..., \tau_n\}$ — множество точек на оси времени, обозначающих моменты выполнения последовательных операций R, W, D над ОКС, $\tau_i \in R^+ \cup \{0\}$, где R^+ — множество положительных

действительных чисел, причем $\tau_1 < \tau_2 < \ldots < \tau_n$. Вероятность того, что две операции будут завершены в точности в один и тот же момент времени, принимается равной нулю. Будем обозначать $T_i = [\tau_i;\ \tau_{i+1})$ — интервал на оси времени, составляющих такт КС t_i. Пусть $T=(t_1,t_2,\ldots,t_n)$ — последовательность тактов КС. Обозначим через $t_i \in T$ факт принадлежности такта t_i последовательности T. Будем обозначать символом λ с соответствующими индексами подпоследовательности последовательности T, состоящие из одного, двух или более подряд идущих тактов: $\lambda = <t_{i_1}, t_{i_2}, \ldots, t_{i_j}>$, и называть λ *временными интервалами*.

Обозначим символом Λ с соответствующими индексами последовательности из одного, двух или более подряд идущих временных интервалов: $\Lambda = <\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_k}>$. Введем обозначение $\lambda_j \in \Lambda$ для того, чтобы показывать факт принадлежности временного интервала λ_j последовательности Λ. Обозначим $\Rho$ — множество всех непрерывных подпоследовательностей последовательности T. Символом $\lambda \in \Rho$ будем обозначать факт принадлежности последовательности λ множеству $\Rho$. Каждому непрерывному временному интервалу соответствует некоторое множество подряд идущих интервалов на оси времени:

$$\{T_j, T_{j+1}, \ldots, T_{j+l}\} = [\tau_j;\tau_{j+1}) \cup [\tau_{j+1};\tau_{j+2}) \cup \ldots \cup [\tau_{j+k};\tau_{j+k+1}) = [\tau_j;\tau_{j+k+1}).$$

На длительность каждого отдельно взятого такта никаких ограничений не накладывается. ЖЦ КС состоит не менее чем из одного такта.

Рассмотрим теперь структуру КС в произвольно взятый фиксированный момент времени. Каждый ОКС имеет формат в соответствии с введенным ранее определением. Для описания взаимосвязей ОКС введем определения отношений между ними.

Пусть $\tau_0^{(j)}$ — момент начала ЖЦ компонента Com_j объекта Obj_i, т. е. точка на оси времени, когда этому компоненту впервые было присвоено непустое значение.

Если $\exists Com_{j_{i_1}}^{(i_1)} \in Obj_{i_1}, \ldots, \exists Com_{j_{i_q}}^{(i_q)} \in Obj_{i_q}, \ldots, \exists Com_{j_{i_r}}^{(i_r)} \in Obj_{i_r}, \exists Com_{m_1}^{(m)} \in Obj_m, \ldots, \exists Com_{m_s}^{(m)} \in Obj_m, \exists Com_0^{(m)} \in Obj_m$, причем $\tau_0^{(m)} \geq \tau_{j_{i_1}}^{(i_1)}, \ldots, \tau_0^{(m)} \geq \tau_{j_{i_q}}^{(i_q)}, \ldots, \tau_0^{(m)} \geq \tau_{j_{i_r}}^{(i_r)}, \tau_0^{(m)} \geq \tau_{m_1}^{(m)}, \ldots, \tau_0^{(m)} \geq \tau_{m_s}^{(m)}$, и $\exists f : D(Com_{j_{i_1}}) \times \ldots \times D(Com_{j_{i_q}}) \times \ldots \times D(Com_{j_{i_r}}) \times \ldots \times D(Com_{m_1}) \times \ldots \times D(Com_{m_s}) \to D(Com_0)$, такая, что для любого значения $Com_{j_{i_q}}^{(i_q)}$ существует алгоритм B_1 вычисления значения $Com_0^{(m)}$ при фиксированных значениях других аргументов функции f, выполнимый за время $t_{B_1} \leq p_{B_1}\left(\left|Com_{j_{i_1}}\right| + \ldots + \left|Com_{j_{i_q}}\right| + \ldots + \left|Com_{j_{i_r}}\right| + \left|Com_{m_1}\right| + \ldots + \left|Com_{m_s}\right|\right)$, где $\rho_{B1}(.)$ — некоторый полином, то будем говорить, что *ОКС* Obj_m *находится в отношении функциональной зависимости первого рода от* Obj_{i_q}, и обозначать этот факт $Obj_{i_q} \succ_f Obj_m$.

Если $\exists Com_{j_1}^{(i_1)} \in Obj_{i_1}$, $\exists Com_{j_2}^{(i_1)} \in Obj_{i_1}$ и $\exists Com_k^{(i_2)} \in Obj_{i_2}$, причем $\tau_{j_2}^{(i_1)} \geq \tau_{j_1}^{(i_1)}$, и существует семейство функций $F : D(Com_{j_1}) \times D(Com_k) \to D(Com_{j_2})$, такое, что для любого фиксированного значения $Com_{j_1}^{(i_1)}$ существует алгоритм B_2 вычисления значения $Com_{j_2}^{(i_1)}$ по заданному значению $Com_k^{(i_2)}$, выполнимый за время $t_{B_2} \leq \rho_{B_2}(|Com_{j_1}| + |Com_k|)$, где $\rho_{B_2}(.)$ — некоторый полином, то будем говорить, что *ОКС* Obj_{i_1} *находится в отношении функциональной зависимости второго рода от* Obj_{i_2}, и обозначать этот факт $Obj_{i_2} \succ_F Obj_{i_1}$.

Выделение двух форм функциональной зависимости связано с тем, что криптографические алгоритмы, как правило, задают не единственную функцию, а семейство функций, которые при известном значении ключа легко вычислимы на всей области определения, а при неизвестном являются однонаправленной функцией (ОНФ). Таким образом, криптографический алгоритм $F_k(z)$ нельзя представить в виде двухаргументной ОНФ $F(k,z)$. Допускаются вырожденные случаи функциональной зависимости между ключами: $f \equiv 1$ или $F_k \equiv 1$.

Если $\exists Com_{j_1} \in Obj_{i_1}$ и $\exists Com_{j_2} \in Obj_{i_2}$, 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 *ОКС* Obj_{i_2} *находится в отношении параметрической зависимости от* Obj_{i_1}, и обозначать этот факт следующим образом: $Obj_{i_1} \succ_p Obj_{i_2}$.

Будем говорить, что Obj_{i2} *зависим от* Obj_{i1}, и обозначать этот факт $Obj_{i_1} \succ Obj_{i_2}$, если $Obj_{i_1} \succ_f Obj_{i_2}$ либо $Obj_{i_1} \succ_F Obj_{i_2}$ либо $Obj_{i_1} \succ_p Obj_{i_2}$.

Бинарные отношения между ОКС могут быть удобно описаны в терминах ориентированных графов. Пусть $G^f=(V^f, E^f)$ — орграф, описывающий отношения функциональной зависимости первого рода между ОКС ключевой системы KS. Множество его вершин V^f соответствует множеству ОКС, связанных отношением функциональной зависимости первого рода, E^f — множество дуг, причем дуга направлена от Obj_r к Obj_s, если $Obj_r \succ_f Obj_s$. По аналогии можно определить орграф $G^F=(V^F, E^F)$, описывающий отношения функциональной зависимости второго рода, и орграф $G^p=(V^p, E^p)$, описывающий отношения параметрической зависимости. Дуги в них направлены соответственно от Obj_t к Obj_u, если $Obj_t \succ_F Obj_u$, и от Obj_v к Obj_w, если $Obj_v \succ_p Obj_w$. Орграф $G = (V, E)$, полученный объединением орграфов G^f, G^F и G^p, т. е. со множеством вершин $V = V^f \cup V^F \cup V^p$ и со множеством ребер $E = E^f \cup E^F \cup E^p$, будем называть *графом зависимости между объектами ключевой системы* KS.

Выделим некоторый ОКС $v \in V$. Будем рассматривать связный подграф $G^*=(V^*, E^*)$ орграфа $G=(V, E)$, полученный следующим образом. Пусть V' — множество всех вершин v' орграфа G, таких, что существуют пути из v в v'. Тогда обозначим $V^*=\{v\} \cup V'$, а E^* — множество всех дуг, исходящих из v_i и входящих в v_j, таких, что $v_i \in V^*$ и $v_j \in V^*$. Таким образом, любой ОКС формирует подсистему КС, состоящую из него самого и всех зависимых от него ключей. *Подсистемой* KS^* ключевой системы KS будем называть совокупность трех элементов: множества ОКС $KObj^* \subseteq KObj$, являющихся вершинами орграфа G^*, множества всех СКС $KSub^* \subseteq KSub$, которые являются владельцами либо обладателями этих ОКС:

$$KSub^* = \left(\bigcup_{Obj_i \in KObj^*} Own\left(Obj_i\right) \right) \bigcup \left(\bigcup_{Com_j \in Obj_i} Pos\left(Obj_i.Com_j\right) \right),$$

и множества всех операций СКС над ОКС:

$$KOp^* = \left\{ \bigcup_{i,j,k} W\left(Obj_i.Com_j; Sub_k\right); \bigcup_{i,j,k} R\left(Obj_i.Com_j; Sub_k\right); \bigcup_{i,j,k} D\left(Obj_i.Com_j; Sub_k\right) \right\},$$

где $Obj \in KObj^*$, $Com_j \in Obj_i$, $Sub_k \in KSub^*$.

Введенные до сих пор определения не зависели от конкретного наполнения компонентов ОКС. Между тем по этому признаку, а именно, по содержанию ключевой части M, ОКС удобно классифицируются на три типа. Если поля B и D ОКС Obj не содержат ни одного компонента, будем называть такой ОКС *бесключевым*, или *параметрическим* ОКС. Если поле B содержит один компонент, а поле D не содержит компонентов, будем называть такой Obj *одноключевым*, или *симметричным* ОКС. Если поле B содержит один компонент, и поле D содержит один или более компонентов, производных от компонента из поля B, то такой Obj будем называть *многоключевым*, или *асимметричным* ОКС. В частности, если поле D содержит точно один компонент, то Obj будем называть *двухключевым*.

Тогда будем считать, что *чисто симметричная КС* — это КС, состоящая только из одноключевых и бесключевых ОКС. *Чисто асимметричная КС* — КС, состоящая только из многоключевых и бесключевых ОКС. *Комбинированная КС* — КС, подсистемами которой являются как чисто симметричные, так и чисто асимметричные КС.

Приведем простые примеры — все криптосистемы взяты из учебного пособия [1]. КС сети защищенной связи, построенная по принципу полной ключевой матрицы, является чисто симметричной, причем общее количество ОКС равно $n(n-1)$ или $n(n-1)/2$, если матрица симметрическая. КС сети защищенной связи с центром трансляции ключей и центром распределения ключей также являются

чисто симметричными. КС простой системы защищенного электронного документооборота на базе ИОК включает два вида ОКС: ОКС «Ключи УЦ криптосистемы для схемы ЭЦП» и ОКС «Ключи участника криптосистемы для схемы ЭЦП», следовательно, она будет чисто асимметричной. Если в последнем примере полагать, что каждый участник криптосистемы является владельцем двух ОКС: «Ключи участника криптосистемы для схемы ЭЦП» и «Ключи участника криптосистемы для схемы открытого шифрования», причем последние используются для генерации по протоколы Диффи — Хеллмана общих секретных ключей для шифрования трафика, то такая КС становится комбинированной (Рис. 2). Идентификационные [2] и бессертификатные [3] криптосистемы имеют комбинированную КС.

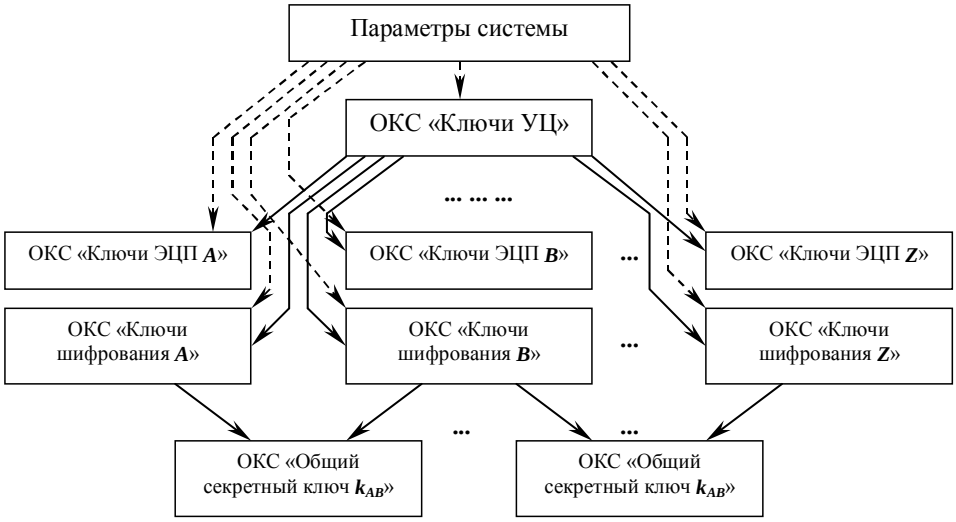


Рис. 2. Граф зависимостей между ОКС для комбинированной криптосистемы с ИОК

3. Динамическая модель ключевой системы

Введенной теоретико-графовой модели достаточно, чтобы описать статическую структуру КС. Для описания динамики поведения КС на произвольных временных интервалах $\lambda \in P$ модель необходимо расширить, введя в рассмотрение зависимость ОКС от времени.

Рассмотрим некоторый ОКС Obj_i. Выделим в нем компоненты Com_0, Com_1,…, Com_j,…, Com_q. Пусть интервал времени $T=[\tau_1;\tau_n)$ задает время ЖЦ ОКС Obj_i. Пусть $T^{(j)}=\{\tau_1^{(j)}, \tau_2^{(j)},\ldots, \tau_{n_j}^{(j)}\}$ — множество точек на оси времени, обозначающих моменты выполнения последовательных операций, приводящих к изменению значения компонента $Com_j \in Obj_i$, $j=\overline{1,q}$, причем $\tau_1^{(j)} \geq \tau_1$, $\tau_{n_j}^{(j)} < \tau_n$. Обозначим $\lambda_i^{(j)}=[\tau_i^{(j)};\ \tau_{i+1}^{(j)})$, $i=\overline{1,n_j-1}$. Очевидно, что момент $\tau_1^{(j)}$ соответствует первой операции $W(Obj_i.Com_j;Own(Obj_i))$, приводящей к записи в Com_j непустого значения. Моменты $\tau_2^{(j)},\ldots,\ \tau_{n_j-1}^{(j)}$ соответствуют всем последующим операциям $W(Obj_i.Com_j;Own(Obj_i))$. Момент $\tau_{n_j}^{(j)}$ соответствует операции $D(Obj_i.Com_j;Own(Obj_i))$.

Пусть $T^{(0)} = \bigcup_{j=\overline{1,q}} T^{(j)}$.

Обозначим $\lambda_i^{(0)}=[\tau_i^{(0)};\tau_{i+1}^{(0)})$, $i=\overline{1,n_0-1}$. Очевидно, что $\tau_1^{(0)}=\min_j \tau_1^{(j)}$, а $\tau_{n_0}^{(0)}=\max_j \tau_{n_j}^{(j)}$.

Зададим некоторый момент времени $\tau:\ \tau_1 \leq \tau < \tau_n$. Обозначим $\lambda_\tau^{(j)}$, $j=\overline{0,q}$ — непрерывные временные интервалы $\lambda_i^{(j)}=[\tau_i^{(j)};\tau_{i+1}^{(j)})$, такие, что $\tau_i^{(j)} \leq \tau < \tau_{i+1}^{(j)}$, для всех $j=\overline{0,q}$ (Рис. 3).

Пусть $\Lambda^{(j)} = \left\langle \lambda_1^{(j)}, \lambda_2^{(j)},\ldots, \lambda_{|\Lambda^{(j)}|}^{(j)} \right\rangle$ — множество непрерывных временных интервалов между последовательными операциями, приводящими к изменению значения Com_j. Очевидно, $\Lambda^{(j)} \subset P$, $\lambda_i^{(j)} \in P$ для $\forall i=\overline{1,|\Lambda^{(j)}|}$. На каждом из интервалов $\lambda_i^{(j)}$ компонент Com_j принимает некоторое значение $Com_j(\lambda_i^{(j)}) \in D(Com_j) \subseteq \{0,1\}^{|Com_j|}$, которое можно рассматривать как случайную величину.

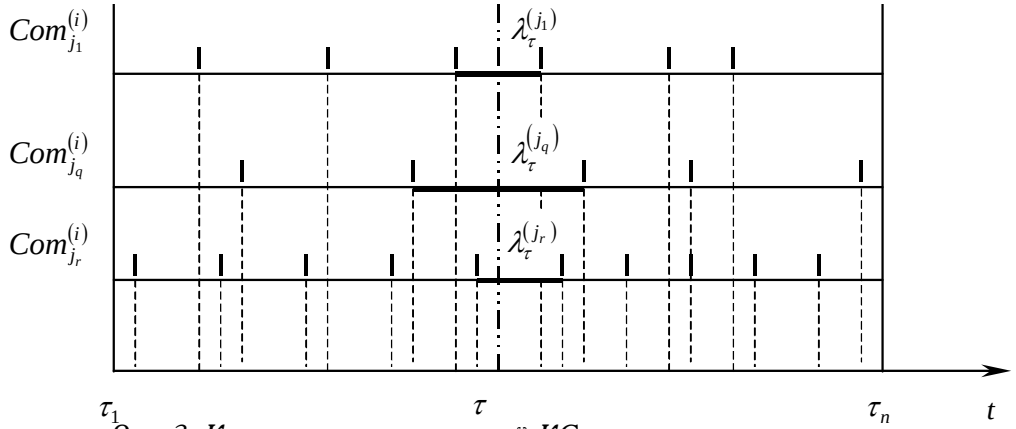


Рис. 3. К определению состояний КС на временных интервалах

Таким образом, последовательность случайных величин $Com_j(\lambda_1(^i)), Com_j(\lambda_2(^i)), \ldots, Com_j\left(\lambda^{(j)}_{|\Lambda^{(i)}|}\right)$ есть случайный процесс с дискретным временем и дискретными состояниями, где каждое состояние процесса есть одно из возможных значений компонента, а моменты переходов между состояниями совпадают с началами некоторых тактов КС.

Если $\exists Com_0 \in Obj_i, \exists Com_1 \in Obj_i, \ldots, \exists Com_j \in Obj_i, \ldots, \exists Com_q \in Obj_i$ и существует функция $f: D(Com_1)\times\ldots\times D(Com_j)\times\ldots\times D(Com_q)\to D(Com_0)$, такая, что для любого фиксированного момента времени $\tau: \tau_1 \le \tau < \tau_n$ и для любого фиксированного значения $Com_j(\lambda_\tau^{(i)})$ существует некоторый алгоритм C_1 вычисления значения $Com_0(\lambda_\tau^{(0)})$ при фиксированных значениях $Com_1(\lambda_\tau^{(1)})$, ..., $Com_{j-1}(\lambda_\tau^{(j-1)})$, $Com_{j+1}(\lambda_\tau^{(j+1)})$, ..., $Com_q(\lambda_\tau^{(q)})$, выполнимый за время $t_{C_1} \le \rho_{C_1}(|Com_1|+\ldots+|Com_j|+\ldots+|Com_q|)$, где $\rho_{C_1}(.)$ — некоторый полином, то будем говорить, что *компонент* Com_0 *находится в отношении временной функциональной зависимости первого рода от компонента* Com_j, и обозначать этот факт $Com_j(\lambda) \triangleright_f Com_0(\lambda)$.

Если $Com_{j_1} \in Obj_{i_1}, \exists Com_{j_2} \in Obj_{i_1}, \ldots, \exists Com_k \in Obj_{i_2}$, и существует семейство функций $F: D(Com_{j_1})\times D(Com_k)\to D(Com_{j_2})$, такое, что для любого фиксированного момента времени $\tau: \tau_1 \le \tau < \tau_n$ и для любого фиксированного значения $Com_k(\lambda_\tau^{(k)})$ существует некоторый алгоритм C_2 вычисления значения $Com_{j_2}(\lambda_\tau^{(j_2)})$ по заданному значению $Com_{j_1}(\lambda_\tau^{(j_1)})$, выполнимый за время $t_{C_2} \le \rho_{C_2}(|Com_{j_1}|+|Com_k|)$, где $\rho_{C_2}(.)$ — некоторый полином, то будем говорить, что *компонент* Com_{j_2} *находится в отношении временной функциональной зависимости второго рода от компонента* Com_{j_1}, и обозначать этот факт $Com_{j_1}(\lambda) \triangleright_F Com_{j_2}(\lambda)$.

Любое подмножество $\omega \subseteq \{Com_{j_1}, \ldots, Com_{j_\rho}\}$ компонентов Obj_i, такое, что для любых фиксированных значений компонентов $Com_{j_1}(\lambda_\tau^{(j_1)})$, ..., $Com_{j_\rho}(\lambda_\tau^{(j_\rho)})$, $Com_{j_{\rho+1}}(\lambda_\tau^{(j_{\rho+1})})$, ..., $Com_{j_{\rho+q}}(\lambda_\tau^{(j_{\rho+q})})$, где $Com_{j_{\rho+1}} \in Obj_{r_1}$, ..., $Com_{j_{\rho+q}} \in Obj_{r_q}$, $r_1 \ne i$, ..., $r_q \ne i$, существует алгоритм C_3 вычисления значения $Com_0(\lambda_\tau^{(0)})$, выполнимый за время $t_{C_3} \le \rho_{C_3}(|Com_{j_1}|+\ldots+|Com_{j_\rho}|+|Com_{j_{\rho+1}}|+\ldots+|Com_{j_{\rho+q}}|)$, где $\rho_{C_3}(.)$ — некоторый полином, но при неизвестном значении хотя бы одного из компонентов множества ω значение $Com_0(\lambda_\tau^{(0)})$ не определено, будем называть *минимальным множеством вычислимости (ММВ)* компонента Com_0, и обозначать его $\omega(Com_0(\lambda))$. Множество всех ММВ компонента Com_0 обозначим $\Omega[Com_0(\lambda)]$.

Любое подмножество $\theta \subseteq \{Com_j(\lambda_1), \ldots, Com_j(\lambda_{\tau-1}), Com_j(\lambda_{\tau+1}), \ldots, Com_j(\lambda_q)\}$ значений компонента $Com_j \in Obj_i$ на непересекающихся временных интервалах, такое, что для любых фиксированных значений $Com_j(\lambda_1)$, ..., $Com_j(\lambda_{\tau-1})$, $Com_j(\lambda_{\tau+1})$, ..., $Com_j(\lambda_q)$ 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 $\rho_{C_4}(.)$ — 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 обозначать ее $\theta(Com_j(\lambda))$. Множество всех МПВ компонента Com_j обозначим $\Theta(Com_j(\lambda))$.

Будем говорить, что Com_{j_2} *зависим во времени от* Com_{j_1}, и обозначать этот факт $Com_{j_1}(\lambda) \triangleright Com_{j_2}(\lambda)$, если $Com_{j_1}(\lambda) \triangleright_f Com_{j_2}(\lambda)$ либо $Com_{j_1}(\lambda) \triangleright_F Com_{j_2}(\lambda)$ либо $Com_{j_1} \triangleright_p Com_{j_2}$.

По аналогии с тем, как это было сделано применительно к описанию статической структуры ОКС, динамику поведения ОКС можно описывать с помощью орграфов, отображающих временную зависимость между компонентами ОКС: $G^f_{Obj_i(\lambda)}$, $G^F_{Obj_i(\lambda)}$ и $G^\rho_{Obj_i(\lambda)}$.

Для описания временных зависимостей между ОКС используем следующие определения.

Если $\exists Com^{(i_1)}_{j_1} \in Obj_{l_1}, ..., \exists Com^{(i_1)}_{j_q} \in Obj_{l_1}, ..., \exists Com^{(i_1)}_{j_r} \in Obj_{l_1}, \exists Com^{(l_2)}_{m_1} \in Obj_{l_2}, ..., \exists Com^{(l_2)}_{m_s} \in Obj_{l_2}$, $\exists Com^{(l_2)}_0 \in Obj_{l_2}$, причем $\tau^{(0)}_0 \geq \tau^{(i_1)}_0, ..., \tau^{(0)}_0 \geq \tau^{(i_q)}_0$, $..., \tau^{(0)}_0 \geq \tau^{(i_r)}_0, \tau^{(0)}_0 \geq \tau^{(m_1)}_0, ..., \tau^{(0)}_0 \geq \tau^{(m_s)}_0$, и $\exists f : D\left(Com^{(l_1)}_{j_1}\right) \times ... \times D\left(Com^{(l_1)}_{j_q}\right) \times ... \times D\left(Com^{(l_1)}_{j_r}\right) \times D\left(Com^{(l_2)}_{m_1}\right) \times ... \times D\left(Com^{(l_2)}_{m_s}\right) \to D\left(Com^{(l_2)}_0\right)$, такая, что для любого фиксированного момента времени $\tau : \tau^{(0)}_0 \leq \tau < \tau^*$, где $\tau^* = \min\left\{ \min\limits_{j=j_1,...,j_r} \tau^{(j)}_n ; \min\limits_{m=m_1,...,m_s} \tau^{(m)}_n ; \tau^{(0)}_n \right\}$, и для любого фиксированного значения $Com^{(l_1)}_{j_q}\left(\lambda^{(j_q)}_\tau\right)$ существует некоторый алгоритм D_1 вычисления значения $Com^{(l_2)}_0(\lambda^{(0)}_\tau)$ при фиксированных значениях других аргументов функции f, выполнимый за время

$$t_{D_1} \leq p_{D_1}\left(\left|Com^{(l_1)}_{j_1}\right| + ... + \left|Com^{(l_1)}_{j_q}\right| + ... + \left|Com^{(l_1)}_{j_r}\right| + \left|Com^{(l_2)}_{m_1}\right| + ... + \left|Com^{(l_2)}_{m_s}\right| + \left|Com^{(l_2)}_0\right|\right),$$

где $\rho_{D_1}(.)$ — некоторый полином, то будем говорить, что Obj_{i_2} *находится в отношении временно́й функциональной зависимости первого рода от* Obj_{i_1}, и обозначать этот факт $Obj_{l_1}(\lambda) \succ_f Obj_{l_2}(\lambda)$.

Если $\exists Com^{(l_2)}_{j_1} \in Obj_{l_2}$, $\exists Com^{(l_2)}_{j_2} \in Obj_{l_2}$ и $\exists Com^{(l_1)}_k \in Obj_{l_1}$, причем $\tau^{(k)}_0 \geq \tau^{(i_1)}_0$, и существует семейство функций $F : D\left(Com^{(l_2)}_{j_1}\right) \times D\left(Com^{(l_1)}_k\right) \to D\left(Com^{(l_2)}_{j_2}\right)$, такое, что для любого фиксированного момента времени $\tau : \tau_1 \leq \tau < \tau^*$, где $\tau^* = \min\left\{\tau^{(j_1)}_n, \tau^{(j_2)}_n, \tau^{(k)}_n\right\}$, и для любого фиксированного значения $Com^{(l_2)}_{j_1}(\lambda^{(i_1)}_\tau)$ существует алгоритм D_2 вычисления значения $Com^{(l_2)}_{j_2}(\lambda^{(i_2)}_\tau)$ по заданному значению $Com^{(l_1)}_k(\lambda^{(k)}_\tau)$, выполнимый за время $t_{D_2} \leq \rho_{D_2}(|Com^{(l_2)}_{j_1}| + |Com^{(l_1)}_k|)$, где $\rho_{D_2}(.)$ — некоторый полином, то будем говорить, что Obj_{i_2} *находится в отношении временно́й функциональной зависимости второго рода от* Obj_{i_1}, и обозначать этот факт $Obj_{l_1}(\lambda) \succ_F Obj_{l_2}(\lambda)$.

Будем говорить, что Obj_{i_2} *зависим во времени от* Obj_{i_1}, и обозначать этот факт $Obj_{l_1}(\lambda) \succ Obj_{l_2}(\lambda)$, если $Obj_{l_1}(\lambda) \succ_f Obj_{l_2}(\lambda)$, либо $Obj_{l_1}(\lambda) \succ_F Obj_{l_2}(\lambda)$, либо $Obj_{l_1} \succ_p Obj_{l_2}$.

Определенные таким образом бинарные отношения между ОКС могут быть описаны орграфами G^f_λ, G^F_λ, G^ρ_λ и G_λ по аналогии со статической моделью.

4. Заключение

Предложен подход к построению математических моделей ключевых систем СКЗИ, позволяющий описывать широкий класс КС. Основной единицей ключевого материала в предложенной модели являются объекты ключевой системы — ОКС. Каждый ОКС представляется как система компонентов. Введены понятия функциональной и параметрической зависимости между ОКС и компонентами одного ОКС. Предполагается возможность построения двух типов моделей: статических и динамических. Первая позволяет описывать состав и структуру ключевого материала, вторая — процессы, протекающие в КС. В терминах предложенных моделей структура каждого ОКС описывается графом, показывающим внутренние отношения зависимости между компонентами ОКС. Структура КС также описывается графом, показывающим внешние отношения зависимости между ОКС. Приведены примеры модельного представления различных КС. Модели предназначены для анализа безопасности КС с известной структурой ключевого материала и синтеза новых КС.

СПИСОК ЛИТЕРАТУРЫ:

1. *Запечников С. В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учеб. пособие для вузов. М., 2007. — 320 с.

2. *Shamir A.* Identity-based cryptosystems and signature schemes // Advances in Cryptology. Proc. of CRYPTO'84, LNCS. Springer-Verlag, 1985. Vol. 196. P. 47–53.

3. *Al-Riyami S., Paterson K.* Certificateless public key cryptography // Advances in Cryptology. Proc. of Asiacrypt'2003, LNCS. Springer-Verlag, 2003. Vol. 2894. P. 452–473.