На правах рукописи

Аристархов
Иван Владимирович

ПЛАНИРОВАНИЕ СМЕНЫ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ОБЩЕДОСТУПНЫХ СИСТЕМАХ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидат технических наук

Санкт – Петербург

2011

Работа выполнена в в/ч 43753

Научный руководитель:	доктор технических наук, профессор Гаценко Олег Юрьевич
Официальные оппоненты:	доктор технических наук, Скиба Владимир Юрьевич
	кандидат технических наук, доцент Гончаренко Владимир Анатольевич
Ведущая организация:	ФГУП ЦНИИ ЭИСУ

Защита состоится «___» _____ 2011 года в 16 час. на заседании диссертационного совета ДС 212.229.27 Санкт-Петербургского государственного политехнического университета, 195251, Санкт-Петербург, ул. Политехническая, д. 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского государственного политехнического университета

Автореферат разослан «___» _____ 2011 года.

Ученый секретарь
диссертационного совета Платонов В.В.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Современные технологии обработки информации предоставляют возможность всё более эффективно управлять информационными ресурсами. Одной из востребованных и актуальных задач в этом направлении является внедрение систем электронного документооборота.

В настоящее время широкое распространение получают специализированные информационные системы (ИСС), базирующиеся на сетях общего доступа и обрабатывающие открытую информацию. Для ряда подобных систем является актуальной проблема обеспечения целостности и достоверности обрабатываемой информации, обеспечения ее юридической значимости, а также аутентификации её поставщиков и потребителей. В качестве примеров ИСС можно привести Портал государственных и муниципальных услуг, а также электронные площадки, обеспечивающие проведение мероприятий Гособоронзаказа (в соответствии с Федеральным законом № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд»).

На основании информации, поступающей в ИСС по электронным общедоступным каналам связи от удаленных источников, могут приниматься решения, имеющие правовые последствия, вследствие чего вопрос правого статуса электронных документов (ЭД) приобретает первостепенное значение. При этом важнейшим условием обеспечивающим эффективность функционирования систем подтверждения подлинности электронного документооборота (СППЭД) является решение проблемы управления ключами ЭЦП на всех этапах их использования**.**

Основное внимание в работах отечественных и зарубежных исследователей по тематике управления ключами ЭЦП сводится, в основном, к описанию требований по криптографической безопасности. В настоящее время эксплуатационной документацией устанавливается постоянный период действия ключей на средства ЭЦП. При этом отсутствует обоснование такого порядка смены ключей в условиях наличия угроз безопасности информации и оценки влияния данных угроз на коэффициент готовности информационной системы (требование введено Приказом Минкомсвязи России от 25.08.2009 г. № 104).

Однако, в условиях активных информационных воздействий на ИСС целесообразно рассмотреть задачу выбора срока действия ключей ЭЦП (периода действия КИ) с точки зрения минимизации затрат на обеспечение доверия к электронным документам, обрабатываемым в СППЭД ИСС. Сокращение периода действия КИ в СППЭД ИСС позволяет ограничить объем информации, доступной нарушителю и ограничить объем данных, подписанных ЭЦП с использованием ключа, который впоследствии может быть скомпрометирован. С другой стороны, необоснованное сокращение периода действия КИ может стать причиной повышенной нагрузки на компоненты инфраструктуры открытых ключей (ИОК), в частности, на Центр сертификации при массовой смене ключей абонентами СППЭД.

Данное обстоятельство обуславливает актуальность задачи разработки рациональных организационных решений по планированию смены ключей подписи.

В соответствии с этим **целью исследования** является минимизация суммарных временных затрат на восстановление доверия к электронным документам и смену ключевой информации в СППЭД ИСС на основе разработки метода планирования

смены ключей ЭЦП.

Объект исследования: система подтверждения подлинности электронного документооборота информационных специализированных систем.

Предмет исследования: модели, методы и алгоритмы управления ключевой информацией (ключами подписи) в СППЭД ИСС.

Научная задача заключается в разработке метода планирования смены ключей ЭЦП, минимизирующего математическое ожидание суммарных временных затрат на смену ключевой информации и восстановление доверия к электронным документам.

Положения, выносимые на защиту.

1. Модель планирования смены ключевой информации с учетом объекта воздействия.
2. Модели планирования смены ключевой информации в условиях неопределенности исходных данных о деструктивных воздействиях нарушителя.
3. Методика оценивания временных затрат на переход к новой ключевой информации в СППЭД ИСС с учетом изменения интенсивности обслуживания заявок на получение сертификатов открытого ключа.
4. Алгоритм имитационного моделирования процесса смены и компрометации ключей в СППЭД ИСС.

В качестве основных **методов исследования** использованы методы теории принятия решений, теории надежности, теории массового обслуживания, основные положения теории информации, методы теории вероятностей и математической статистики, методы компьютерного моделирования.

Научная новизна результатов работы состоит в разработке моделей, методики и алгоритма, позволяющих в отличие от известных подходов планировать смену ключевой информации в ИСС с учетом различной информированности о возможностях нарушителя по реализации воздействий, способных привести к компрометации закрытых ключей, а также с учетом возможностей Центра регистрации по обслуживанию заявок на получение сертификатов открытого ключа.

Практическая значимость диссертационной работы определяется созданием готовых к непосредственному применению оригинальных моделей и алгоритмов, позволяющих выработать рекомендации по планированию смены ключей ЭЦП, впервые учитывающие комплекс характеристик СППЭД ИСС:

- количество абонентов СППЭД;
- архитектурные и функциональные возможности подсистем используемого УЦ;
- интенсивность деструктивных информационных воздействий, потенциально приводящих к компрометации закрытых ключей.

Реализация: результаты работы реализованы в в/ч 43753, НИИЦ ФСО России, НИЦ «Курчатовский институт».

Апробация работы: основные результаты диссертационных исследований обсуждались и получили одобрение научной общественности на XIV Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации», XII Международной конференции «Информатизация и информационная безопасность правоохранительных органов», III научно-практической конференции «Инновационные технологии и технические средства специального назначения БГТУ «Военмех», общероссийской конференции «Математика и безопасность

информационных технологий» (МАБИТ-2010).

Публикации: по теме диссертации опубликовано 10 печатных работ, в том числе, 2 статьи в изданиях, включенных в Перечень ведущих рецензируемых научных журналов, 8 тезисов докладов и ряд отчетов о НИР Академии криптографии Российской Федерации.

Структура и объём диссертации: диссертационная работа включает введение, четыре раздела, заключение и список литературы.

2. СОДЕРЖАНИЕ РАБОТЫ

Во введении диссертации обоснована актуальность решаемой научной задачи, кратко изложены результаты анализа работ в области организации защиты информации, в общем виде сформулированы цель и задача исследования, определены положения, выносимые на защиту, научная новизна и практическая значимость работы, представлена краткая аннотация диссертации.

Первый раздел содержит анализ особенностей обеспечения защиты электронных документов в ИСС, в частности, угрозы и способы злоумышленных действий в системе обмена электронными документами, а также защитные меры для противодействия.

Применительно к СППЭД можно утверждать, что **необходимым условием обеспечивающим эффективность ее функционирования** на заданном уровне **является решение задачи оптимальной смены ключей ЭЦП, чему и посвящена настоящая работа.**

Решаемая задача может быть сформулирована следующим образом: при заданных временных затратах на восстановление доверия к ЭД после компрометации закрытого ключа, заданном периоде планирования, характеристиках возможностей нарушителя по компрометации закрытых ключей и временных характеристиках Центра регистрации, найти временную последовательность смены ключевой информации, минимизирующую математическое ожидание суммарных временных затрат на смену ключевой информации и восстановление доверия к электронным документам. Формальная постановка задачи. Дано:

t_r - время на восстановление доверия к ЭД, подписанным в период между началом действия закрытого ключа субъекта СППЭД и его компрометацией; t_s - время на восстановление доверия к ЭД, подписанным в период между началом действия закрытого ключа УЦ и его компрометацией; T - период, на который осуществляется планирование смены ключевой информации;

p, q - вероятности компрометации закрытых ключей субъекта и УЦ соответственно; n - количество причин, по любой из которых возможна компрометация закрытого ключа; $F_{x_i}(t)$ - функции распределения времени между последовательными компрометациями закрытого ключа по i-й причине, $i = 1,2,...,n$;

N - количество абонентов СППЭД;

μ_i - интенсивность обработки заявки на получение сертификата открытого ключа на i-м этапе ее обработки в ЦР.

Найти:

временную последовательность смены ключевой информации $\tau = \{\tau_1, \tau_2, ..., \tau_m\}$, где m - количество переходов на новую ключевую информацию за время T, минимизирующую математическое ожидание суммарных временных затрат на

смену ключевой информации ($\bar{t}_{см}$) и восстановление доверия к электронным документам ($\bar{t}_{в}$), подписанным с использованием скомпрометированной ключевой информации:

$$\tau^{*} = \underset{m,\tau_1,\ldots,\tau_n}{Arg\,\min}(\bar{t}_{в} + \bar{t}_{см}) .$$

При ограничениях: компрометация закрытого ключа в результате внешнего воздействия обнаруживается внутри интервала действия ключевой информации τ_i, $i = \overline{0,m}$; количество абонентов СППЭД N на планируемом периоде остается неизменным; каждый абонент имеет один комплект ключевой информации.

Для решения этой задачи **во втором разделе** рассмотрены различные модели планирования смены ключевой информации.

Предполагается, что неизвестное число m пар ключей будет использоваться на планируемом периоде функционирования СППЭД. Переход i-ю пару ключей осуществляется, когда СППЭД функционировала в условиях доверия к подписанным документам до времени $t_{н_i}$, $1 \le i \le m$. Определим i-й интервал между сменой ключей τ_i, $0 \le i \le m$, как время работы системы между переходом с i-ой на $(i+1)$-ю пару ключей, т.е. $\tau_i = t_{н_i+1} - t_{н_i} - t_c, 0 \le i \le m$, $(t_{н_0} = 0; t_{н_{m+1}} = t_н)$, где t_c - время необходимое для получения сертификата открытого ключа.

Предположим, что компрометация закрытого ключа в результате внешнего воздействия осуществляется с интенсивностью λ и обнаруживается внутри интервала τ_i, $i = \overline{0,m}$. Процесс восстановления доверия к электронным документам, подписанным скомпрометированными закрытыми ключами, представлен на рис. 1.

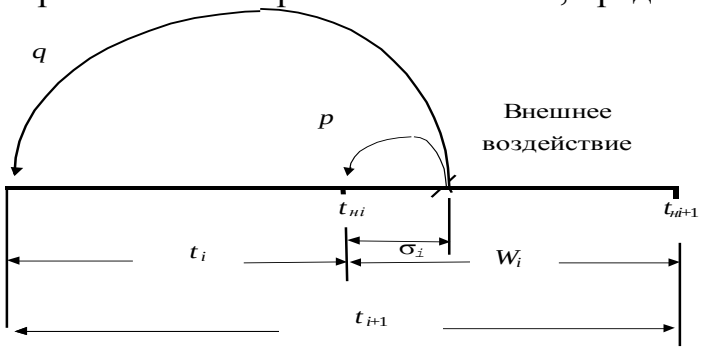

Рис. 1 Процесс восстановления доверия к электронным документам, подписанным скомпрометированными закрытыми ключами

Пусть σ_i - случайное время функционирования СППЭД в пределах интервала τ_i до того как будет обнаружено внешнее воздействие, а $\tau_в$ - представляет собой случайный интервал времени между двумя последовательными компрометациями закрытых ключей с плотностью распределения

$$f_{\tau_в}(\tau_в) = \lambda e^{-\lambda\tau_в},\ \tau_в \ge 0 .$$

Решением поставленной задачи являются временные интервалы между сменой ключевой информации τ_i, обеспечивающие минимум целевой функции (средние временные затраты необходимые на восстановление доверия к ЭД, подписанным ключами которые впоследствии были скомпрометированы нарушителем, и на смену ключевой информации) $\bar{t} = f(m,\tau_0,\ldots,\tau_m)$ при известных $t_r, t_s, t_c, p, \lambda$.

В результате решения задачи было получено рекуррентное выражение, определяющее $\bar{t}$ через $\bar{t}$i, где t_i, $i = \overline{1,m+1}$ является случайным временем,

прошедшим от начала регистрации субъекта СППЭД до первого перехода на i-ю пару ключей.

Плотность распределения случайного времени σ_i до обнаружения внешнего воздействия на интервале τi:

$$f_\sigma(\eta) = \frac{f_{\tau_в}(\eta)}{F_{\tau_в}(\tau_i)} = \frac{\lambda e^{-\lambda\eta}}{1-e^{-\lambda\tau_i}} \ ; \ 0 \le \eta \le \tau_i ,$$

где $\tau_в$- случайный интервал времени между двумя последовательными компрометациями закрытых ключей.

Математическое ожидание случайной величины σ_i определяется выражением:

$$\bar{\sigma}_i = \frac{\tau_i e^{-\lambda\tau_i}}{1-e^{-\lambda\tau_i}} .$$

Различным реализациям случайной величины t1 соответствуют различные вероятности их появления.
Поэтому,

$$t_1 = \begin{cases} \tau_0, 1-F_{\tau_в}(\tau_0); \\ \bar{\sigma}_0 + t_S + \bar{t}_1, F_{\tau_в}(\tau_0) \end{cases} .$$

Откуда среднее время функционирования до первого перехода на новую пару ключей

$$\bar{t}_1 = \tau_0 + \frac{F_{\tau_в}(\tau_0)}{1-F_\tau(\tau_0)}(\bar{\sigma}_0 + t_S) . \qquad (1)$$

Случайное время t_{i+1} до перехода на $i+1$-ю пару ключей также определяется наступлением различных событий. Процесс может осуществляться путем смены ключевой информации субъектом СППЭД или УЦ. Следовательно, $t_{i+1} = t_i + w_i$, $i = \overline{1,m}$, где

$$w_i = \begin{cases} \tau_i, \quad 1-F_{\tau_в}(\tau_i); \\ \bar{\sigma}_i + t_r + \bar{w}_i, \quad F_{\tau_в}(\tau_i)p; \\ \bar{\sigma}_i + t_s + \bar{t}_{i+1}, \quad F_{\tau_в}(\tau_i)q; \end{cases}$$

и среднее время функционирования до i-й смены ключевой информации определяется выражением

$$\bar{t}_{i+1} = \bar{t}_i \frac{1-F_{\tau_в}(\tau_i)p}{1-F_{\tau_в}(\tau_i))} + \tau_i + (\bar{\sigma}_i + t_r p + t_s q)\frac{F_{\tau_в}(\tau_i)}{1-F_{\tau_в}(\tau_i)}. \qquad (2)$$

Подставляя выражения для $F_{\tau_в}(\tau_i)$ и $\bar{\sigma}_i$ в (1) и (2), имеем

$$\begin{aligned} \bar{t}_1 &= (\frac{1}{\lambda} + t_s)(e^{\lambda\tau_0} - 1); \\ \bar{t}_{i+1} &= (e^{\lambda\tau_i} q + p)\bar{t}_i + (e^{\lambda\tau_i} - 1)(\frac{1}{\lambda} + t_r p + t_s q). \end{aligned} \qquad (3)$$

Из формул (3) следует выражение для среднего времени функционирования

$$\bar{t} = \bar{t}_{m+1} = hz_0 \prod_{j=1}^{m} u_j + kz_1 \prod_{j=2}^{m} u_j + ... + kz_{m-1}u_m + kz_m , \qquad (4)$$

где

$$h = \frac{1}{\lambda} + t_s ; \quad k = \frac{1}{\lambda} + t_r p + t_s q ; \quad u_i = qe^{\lambda\tau_i} + p ; \quad z_i = e^{\lambda\tau_i} - 1.$$

Минимизация целевой функции (4) по отношению к количеству m смен ключевой информации и интервалам $\tau_i, i=\overline{0,m}$ между ними осуществляется с использованием теоремы Лагранжа для условных экстремумов.

В результате получаем,

$$\begin{cases} \tau_0 = \tau_1 + \dfrac{1}{\lambda}\ln\dfrac{k-hq}{hp}; \\ \tau_i = \tau_{i+1}, \quad i=\overline{1,m-1}. \end{cases} \tag{5}$$

Выражения (5) показывают, что оптимальные интервалы между сменой ключевой информации должны быть равными за исключением первого, который больше остальных на

$$\frac{1}{\lambda}\ln\frac{k-hq}{hp}.$$

Стратегия смены ключевой информации должна учитывать характер априорной информации о возможностях нарушителя по компрометации закрытых ключей, характеризуемой законами распределения времени между последовательными деструктивными воздействиями. Различие в характере имеющейся информации о возможностях нарушителя потребовало разработки нескольких **моделей планирования смены ключевой информации**.

Моменты смены ключевой информации $\{\tau_1, \tau_2, ..., \tau_k, ..., T\}$ составляют определенную последовательность, подлежащую отысканию. Для большинства практических случаев можно положить $T<\infty$.

Допустимой временной последовательностью на промежутке $[0,T]$ назовем совокупность

$$S_n = \{\tau_1, \tau_2, ..., \tau_n, \tau_{n+1} : 0 \le \tau_1 \le \tau_2 \le ... \le \tau_n \le \tau_{n+1} \le T\}.$$

Множество всех допустимых на промежутке $[0,T]$ временных последовательностей смены ключевой информации обозначим S.

Модель планирования смены ключевой информации в условиях одного типа воздействия нарушителя при известном законе распределения позволяет найти оптимальную временную последовательностью смены ключевой информации, удовлетворяющую условию:

$$S_n^* = \underset{S_n \in S}{\text{Argmin}}\, R(S_n, \varphi_t),$$

где R - математическое ожидание временных затрат на восстановление доверия к ЭД, подписанными скомпрометированными ключами, и на смену ключевой информации, а φ_t - известная плотность распределения времени t до нарушения защищенности информации в ИСС, способного привести к компрометации закрытого ключа.

При известном распределении времени до момента компрометации закрытого ключа в виде функции распределения F_t, математическое ожидание временных затрат на интервале $[\tau_{k-1}; \tau_k]$ можно записать с помощью интеграла Стилтьеса:

$$\int_{\tau_{k-1}}^{\tau_k} [t_n k + (\tau_k - t)]\, dF_t(t).$$

Для получения полных ожидаемых потерь времени просуммируем математическое ожидание временных затрат на восстановление доверия к ЭД, подписанными скомпрометированными ключами, и на смену ключевой информации по всем возможным количествам переходов на новую ключевую информацию k:

$$R(F_t)=\sum_{k=0}^{n}\int_{\tau_{k-1}}^{\tau_k}\left[t_n k+(\tau_k-t)\right]dF_t(t)+t_n(k+1)F_t(T).$$

Последовательность неотрицательных чисел

$$\left\{\tau_1^*,\tau_2^*,...,\tau_k^*,...,\tau_n^*,\tau_{n+1}^*\right\}=T,$$

минимизирующую полные ожидаемые потери времени R, найдем из условия

$$\frac{\partial R(S_n,\varphi_t)}{\partial\tau_k}=0,\quad k=\overline{1,...,n}.$$

Для дифференцирования выражения, содержащего переменную в пределах интегрирования, воспользуемся формулой Лейбница. В результате получим рекуррентную последовательность, позволяющую определить момент начала очередной смены, если известен момент начала предшествующей смены ключевой информации:

$$\tau_{k-1}-\tau_k=\frac{F_t(\tau_k)-F_t(\tau_{k-1})}{\varphi_t(\tau_k)}-t_n.$$

Таким образом, последовательность величин τ_k определяется однозначно, как только выбран момент τ_1.

Аналогично в условиях двух конкурирующих воздействий нарушителя при известных законах распределения получена оптимальная временная последовательность смены ключевой информации в виде рекуррентного соотношения, однозначно связывающего моменты смены ключевой информации τ_k при заданном моменте первой смены τ_1:

$$\tau_{k+1}=\tau_k+\Delta_{k+1}\Leftrightarrow\tau_k=\tau_k(\tau_1),$$

причем

$$\Delta_{k+1}=\frac{\int_{\tau_{k+1}}^{\tau_k}\overline{F}_z(t)dF_y(t)}{\overline{F}_z(\tau_k)\varphi_y(\tau_k)}-t_n(1+\frac{\lambda_z(\tau_k)}{\lambda_y(\tau_k)}),$$

где $\lambda_z=\frac{\varphi_z}{\overline{F}_z}$ и $\lambda_y=\frac{\varphi_y}{\overline{F}_y}$ - интенсивности компрометации закрытого ключа по двум различным причинам.

В общем случае компрометация закрытого ключа абонента СППЭД возможна в результате различных воздействий нарушителя. Оптимальную временную последовательность смены ключевой информации для данных условий можно получить, обобщив описанную выше модель для случая n конкурирующих воздействий нарушителя.

Пусть случайные величины $x_1,...,x_n$ соответствуют временам до наступления моментов компрометации из-за n различных воздействий нарушителя, $F_{x_i}(t)$ - функции распределения x_i, T - планируемый период смены ключевой информации.

Смена ключевой информации производится в некоторые моменты времени τ_k и имеет среднюю длительность t_m.

Средние затраты времени на проведение смены ключей за период T:

$$t_m\{\sum_{k=1}^{m+1} k[\sum_{i=1}^{n} \int_{\tau_{k-1}}^{\tau_k} \left(\prod_{j=1}^{n} \overline{F}_{x_j}(t) / \overline{F}_{x_i}(t) \right) dF_{x_i}(t)] + (m+1) \prod_{j=1}^{n} \overline{F}_{x_j}(T)\}.$$

Средние временные потери на восстановление доверия к ЭД, подписанным с использованием скомпрометированного ключа, путем переподписывания их с использованием новой ключевой информацией из-за любого из m возможных воздействий нарушителя, способных привести к компрометации, определяются следующим выражением

$$\sum_{k=1}^{m+1} \left\{ \sum_{i=1}^{n} \int_{\tau_{k-1}}^{\tau_k} \frac{(\tau_k - t) \prod_{j=1}^{n} \overline{F}_{x_j}(t)}{\overline{F}_{x_i}(t)} dF_{x_i}(t) \right\}, \quad \tau_0 = 0.$$

Сумма данных выражений является целевой функцией R и представляет собой общее среднее время потерь абонента СППЭД (на смену ключей и на восстановление доверия).

Далее порядок расчета оптимальной временной последовательности смены ключевой информации аналогичен.

Разработанные модели в качестве априорной информации требуют не только законы распределения между воздействиями, способными привести к компрометации закрытых ключей, но и оценки временных затрат, необходимых для перехода на новую ключевую информацию. Способы получения таких оценок рассматриваются в следующем разделе.

В третьем разделе проведен анализ особенностей функционирования Центра регистрации который показал, что временные затраты на получение сертификата нового открытого ключа существенным образом зависят от того является ли переход на новую ключевую информацию плановым или же осуществляется после компрометации закрытого ключа.

Предложена методика оценивания временных затрат на переход к новой ключевой информации в СППЭД ИСС с учетом изменения интенсивности обслуживания заявок на получение сертификатов открытого ключа. Методика основана на формализации процесса функционирования Центра регистрации (ЦР) с использованием математического аппарата замкнутых сетей массового обслуживания (СеМО).

Такая СеМО включает в себя $M = \{1,2,...,8\}$ узлов (рис. 2), в которых функционируют K одних и тех же заявок. Каждый узел i сети представляет собой многоканальную СМО с n_i обслуживающими каналами и очередью емкости k_i, функция распределения времен обслуживания заявок в любом канале узла i является экспоненциальной с параметром μ_i, порядок выбора заявок из очередей определяется дисциплиной FCFS.

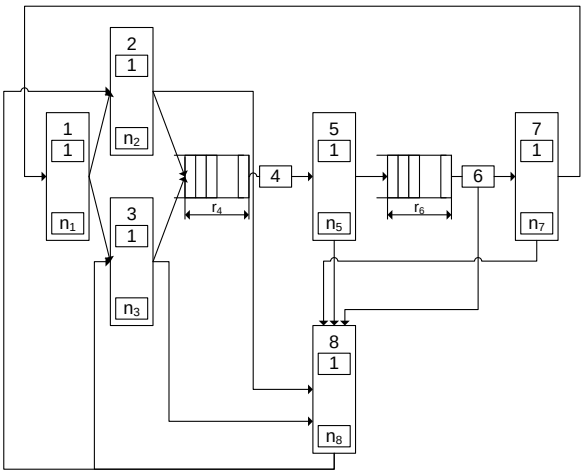

Рис.2. СеМО, формализующая процесс функционирования ЦР

Чтобы учесть различное время обработки заявок на получение сертификата открытого ключа в случае первичной регистрации (или после компрометации ключевой информации) и при плановой смене ключей в СеМО введен узел 1, вероятности перехода заявок из которого в узлы 2 и 3 определяются вероятностью компрометации ключевой информации p на периоде τ_i, где $i = 1,2,...,n$.

Узлы 2 и 3 формализуют работу Центра регистрации на этапе приемки заявки на обновление ключевой информации (в случае первичной регистрации и после компрометации ключевой информации соответственно).

Узел 4 формализует функционирование приложения, обеспечивающего проверку уникальности регистрационных данных. Максимальная длина очереди r_4 задается в серверном приложении.

Одноканальный узел 6 и длиной очереди r_6, формализует процесс формирования сертификата, выработка ЭЦП издателем.

Последний этап прохождения заявки осуществляется в многоканальном узле 7 формализующем процесс формирования Центром регистрации СМР сообщения для пользователя, выработку ЭЦП.

В случае, если на каких-либо этапах заявка не может быть обработана, то она теряется, после чего узел 8 моделирует повторное формирование заявки в ЦР.

Маршрутизация заявок будет определяться вероятностями перехода θ_{ij}, где $i, j = \overline{1, M}$. При этом, учитывая, что заявки не покидают сеть, имеем

$$\sum_{j=1}^{M} \theta_{ij} = 1, \; i = \overline{1, M}.$$

Блуждание заявок для любого узла i^* может быть описано однородной поглощающей цепью Маркова с множеством состояний M и поглощающим состоянием i^*.

Среднее число посещений h_j заявкой узла j, $j \in M^*$, на интервале времени между соседними посещениями узла i^* удовлетворяет следующей системе уравнений

$$h_j = \sum_{i=1}^{M} h_i \theta_{ij}, \; j = \overline{1, M}$$

По теореме Гордона-Ньюелла, если в замкнутой однородной экспоненциальной сети матрица переходов Θ неразложима, то стационарное распределение $p(\vec{h}) > 0$,

$\vec{k} \in \mathrm{X}(M,K)$ представляется в мультипликативном виде

$$p(\vec{h}) = G^{-1}(M,K)\prod_{i=1}^{M}\frac{d_i^{h_i}}{\beta_i(h_i)},\ \vec{k} \in \mathrm{X}(M,K), \qquad (6)$$

где $d_i = h_i/\mu_i$, h_i, $i=\overline{1,M}$, $\beta_i(h)=\prod_{j=1}^{h}\gamma_j(k)$, $\gamma_i(h_i)=\min(k_i,h_i)$, $h\geq 1$ и $\beta_i(0)=1$,

а нормирующая константа определяется из условия

$$G(M,K) = \sum_{\vec{k}\in \mathrm{X}(M,K)}\prod_{i=1}^{M}\frac{d_i^{k_i}}{\beta_i(h_i)}. \qquad (7)$$

Уравнения (6) и (7) предполагают решение системы линейных алгебраических уравнений. В нашем случае ввиду небольшого количества узлов СеМО и достаточно простой структуры матрицы Θ решение не представляет больших вычислительных трудностей.

Выражение (7) справедливо для СеМО с одноканальными узлами. С учетом того, что узлы СеМО 1-3,5,7,8 (рис. 2) являются многоканальными, рассмотрим общий случай, т.е. $n_i \geq 1$, $i=\overline{1,M}$. Введем дополнительно функции

$$f_i(k) = \frac{d_i^k}{\beta_i(k)},\ i=\overline{1,M},\ k\geq 0.$$

По аналогии со случаем одноканальных узлов рассмотрим функции

$$g(M,K) = \sum_{\vec{k}\in \mathrm{X}(M,K)}\prod_{i=1}^{m} f_i(k_i),\ m=\overline{1,M},\ k=\overline{1,K}$$

При этом граничные условия задаются формулами

$$g(m,0)=1,\ m=\overline{1,M} \qquad (8)$$

и

$$g(0,k)=0,\ k=\overline{0,K}. \qquad (9)$$

С учетом этого окончательно получаем

$$g(m,k) = \sum_{l=0}^{h} f_m(l)\,g(m-1,k-1),\ m=\overline{1,M},\ h=\overline{0,K} \qquad (10)$$

Так как $g(M,K)=G(M,K)$, то формула (10) вместе с начальными условиями (8) и (9) определяет рекуррентный алгоритм расчета нормирующего множителя $G(M,K)$ в сети с многоканальными узлами.

Интенсивность λ_i выходящего из узла i потока заявок равна интенсивности μ_i обслуживания в узле i, умноженной на долю времени, в течение которого канал узла i был занят обслуживанием равную $1-p_i(0)$. Таким образом,

$$\lambda_i = \mu_i\left[1-p_i(0)\right],\ i=\overline{1,M},$$

откуда, принимая во внимание равенство $d_i = h_i/\mu_i$, окончательно получаем

$$\lambda_i = h_i\frac{g(M,K-1)}{G(M,K)},\ i=\overline{1,M}$$

Таким образом, используя математический аппарат СеМО, найдены расчетные формулы для определения интенсивности обслуживания заявок на получение сертификатов открытого ключа.

В четвёртом разделе проведено исследование функционирования УЦ с использованием нагрузочных испытаний, которое позволило получить оценку изменения среднего времени обработки запроса при увеличении множественности

запросов, оценку изменения пропускной способности программно-технического комплекса УЦ в части обработки множественных запросов и оценку изменения среднего времени обработки запроса при увеличении количества изданных сертификатов.

Тестирование временных характеристик ЦР показало, что множественность запросов увеличивает среднее время обработки запроса (примерно в k раз, где k – коэффициент множественности), и существует некоторый предел количества запросов, обрабатываемых в режиме on-line (в тесте – 20), после которого остальные запросы ставятся в очередь. Обработка отложенных запросов осуществляется в режиме off-line и практически эквивалентна событию отклонения запроса, поскольку нарушает концепцию клиент-серверного взаимодействия и требует интерактивного протокола, реализуемого Администратором ЦС. Полученные в ходе тестирования временные характеристики обработки запросов согласуются с оценками интенсивности обработки запросов, рассчитанными по методике, разработанной в третьем разделе.

Для преодоления ограничений моделей планирования смены ключевой информации, связанных с допущениями об экспоненциальных законах распределения времени между последовательными компрометациями ключевой информации, о марковском потоке заявок на получение сертификатов открытого ключа, экспоненциальном законе распределения времени обслуживания этих заявок на различных этапах их прохождения в ЦР разработан **алгоритм имитационного моделирования процесса смены и компрометации ключей в СППЭД ИСС**, который сводится к следующим действиям:

1) вводятся исходные данные (функции распределения времени между нарушениями способными привести к компрометации ключевой информации, зависимость математического ожидания времени обслуживания заявки на получение КИ от интенсивности поступления заявок);

2) генерируется время до компрометации КИ;

3) определяется событие с минимальным временем – наиболее раннее событие (плановая смена КИ или компрометация КИ);

4) в зависимости от типа события предпринимаются различные действия. В случае если компрометация закрытого ключа произошла в процессе перехода на новую КИ осуществляется переход к п.2, при компрометации в период действия КИ – переход к п. 5

5) суммируется время, затраченное на восстановление доверия к ЭД, подписанных с использованием скомпрометированной КИ.

6) перечисленные действия повторяются до истечения времени моделирования

7) обрабатываются полученные статистические данные (вычисляется математическое ожидание выборочного коэффициента готовности и его доверительный интервал).

Моделирование процесса смены КИ при функционировании СППЭД ИСС позволило получить ряд численных зависимостей.

На рис. 3 показана зависимость коэффициента готовности СППЭД ИСС от математического ожидания времени между последовательными компрометациями закрытого ключа. Кривая отражает зависимость, полученную с использованием аналитических моделей, а точками показаны результаты имитационного моделирования процесса функционирования.

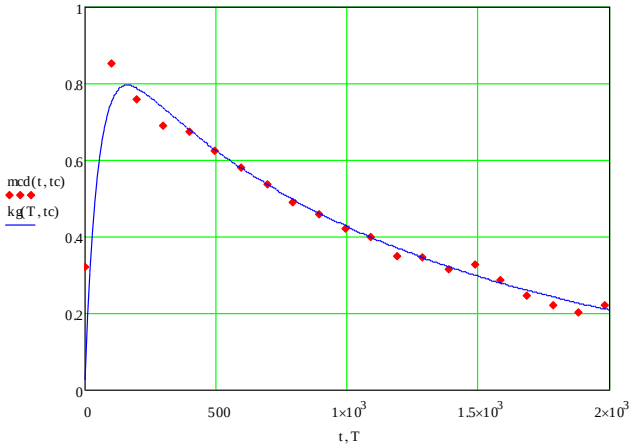

Рис. 3. Зависимость коэффициента готовности СППЭД от периода действия КИ

Оптимальный период смены КИ (для заданных исходных данных составил 157 суток. Оценка коэффициента готовности 0,86.

Для вычисления дисперсии оценки коэффициента готовности было проведено имитационное моделирование функционирования СППЭД при оптимальном периоде смены КИ.

Объем испытаний 300. При проведении интервального оценивания коэффициента готовности на уровне значимости 0,9 получен доверительный интервал:

$$\mathrm{IMx}(\gamma, n) = \begin{pmatrix} 0.852 \\ 0.871 \end{pmatrix}$$

Для оптимального периода смены КИ с использованием аналитических моделей и имитационного моделирования была получена зависимость коэффициента готовности от математического ожидания времени между компрометациями ключевой информации.

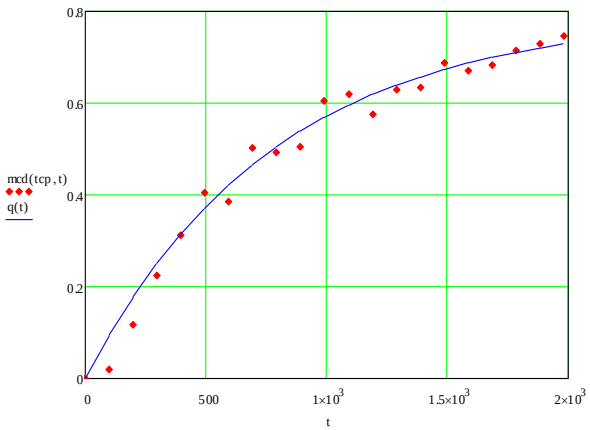

Рис. 4, Зависимость коэффициента готовности от математического ожидания времени между компрометациями ключей ЭЦП

Представленные на рис. 4 и 5 зависимости получены применительно к случаю одинаковых интервалов времени между сменами ключевой информации.

Таблица 1 - Оптимальные продолжительности использования ключевой информации (сутки).

τ_0	τ_1	τ_2	τ_3	τ_4	τ_5
87	103	126	162	228	390

Оптимизация размеров интервалов по предложенным выше моделям позволяет повысить коэффициент готовности СППЭД. Применительно к случаю одного типа воздействия с известным законом распределения до компрометации закрытого ключа, используя соответствующую модель планирования, были получены оптимальные продолжительности использования КИ (табл. 1).

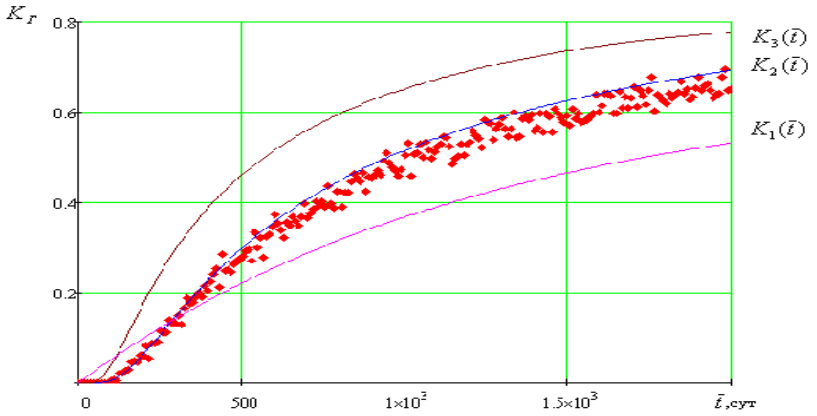

Рис. 5. Зависимость коэффициента готовности от среднего времени между воздействиями для различных стратегий смены ключей ЭЦП

Результаты моделирования временных затрат на восстановление функционирования СППЭД для различных стратегий смены ключевой информации (рис. 5):

К1 -существующая политика смены ключей (ежегодная смена);

К2 -политика смены ключей с оптимизацией количества интервалов (m=7, интервалы одинаковой продолжительности);

К3 -политика смены ключей с оптимизацией количества интервалов и продолжительности каждого интервала.

В целом, полученные зависимости могут быть использованы для обоснования планов смены ключевой информации для различных значений исходных данных.

Моделирование процесса функционирования СППЭД ИСС показало, что планирование смены ключевой информации с использованием предложенных моделей по сравнению с существующей на сегодняшний день политикой ежегодной смены ключевой информации позволяет повысить коэффициент готовности СППЭД ИСС на 12%.

В заключении сформулированы основные результаты работы, кратко охарактеризована их новизна и практическая ценность. Сделан вывод о степени выполнения поставленных задач и достижения цели исследования.

3. ЗАКЛЮЧЕНИЕ ПО РАБОТЕ

В результате решения поставленной в работе научной задачи, получены следующие новые научные и практические результаты:

1) Разработаны математические модели планирования смены ключевой информации, позволяющие выполнить обоснованный выбор времени перехода на новую ключевую информацию с учетом характера информированности о возможных способах действий нарушителей, приводящих к компрометации закрытых ключей.

2) Разработана методика оценивания временных затрат на переход к новой ключевой информации в СППЭД ИСС которая позволяет учесть интенсивность обслуживания заявок на сертификаты открытого ключа и возможность внеплановой смены ключевой информации. При расчете интенсивности обработки запросов на сертификаты открытых ключей учитывается вероятность компрометации закрытого ключа в течении периода действия КИ.

3) Предложен алгоритм, позволяющий осуществлять имитационное моделирование процесса функционирования СППЭД ИСС и получать математическое ожидание выборочного коэффициента готовности и его доверительный интервал.

4) Применительно к функционированию ИСС при организации электронного документооборота получены численные оценки коэффициента готовности СППЭД в условиях моделирования воздействий, которые могут привести к компрометации закрытых ключей.

Таким образом, цель диссертационных исследований достигнута, поставленная научно-техническая задача решена полностью.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Аристархов И.В. Планирование смены ключевой информации в системах подтверждения подлинности электронного документооборота // Проблемы информационной безопасности, Компьютерные системы №1, 2011. СПб.: СПГТУ, с. 34-39. (перечень ВАК)**

2. **Аристархов И.В.**, Логачев А.С., Прокопьев С.Е. Использование изоляционного подхода в реализации сервисов инфраструктуры открытых ключей. Общероссийская конференция «Математика и безопасность информационных технологий» (МАБИТ-2010), МГУ, М., с. 5, 2010г.

3. **Аристархов И.В.**, Камышев С.Н., Логачев А.С. О некоторых проблемах безопасного применения ЭЦП в системах документооборота специального назначения. III научно-практическая конференция «Инновационные технологии и технические средства специального назначения. БГТУ «Военмех», СПб, с. 3, 2010 г.

4. **Аристархов И.В., Гаценко О.Ю., Максимов С.В. Оценивание временных затрат Центра регистрации при обслуживании заявок абонентов СППЭД на сертификаты открытых ключей // Проблемы информационной безопасности, Компьютерные системы №3, 2010. СПб.: СПГТУ, с. 45-51. (перечень ВАК)**

5. Абрамкин М.А., **Аристархов И.В.** О некоторых проблемах определения уникальности имен в сертификатах ключей подписи для УЦ, встроенного в Microsoft Windows Server 2003 // 5-ая Всероссийская научная конференция «Проблемы развития системы специальной связи и специального информационного обеспечения государственного управления России», Академия ФСО, Орёл, с. 2, 2007 г.

6. **Аристархов И.В.**, Камышев С.Н. О некоторых тенденциях развития в области функционирования инфраструктуры открытых ключей // VI Межведомственная конференция «Научно-техническое и информационное обеспечение деятельности спецслужб», ИКСИ Академии ФСБ России, с. 3, 2006 г.

7. Алимов Р.Е., **Аристархов И.В.**, Логачев А.С. О некоторых тенденциях развития в области функционирования инфраструктуры открытых ключей // XIV общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», СПб., с. 4, 2005 г.

8. **Аристархов И.В.**, Логачев А.С. О требованиях к информационной безопасности удостоверяющих центров // XII Международная конференция «Информатизация и информационная безопасность правоохранительных органов», М, с 4, 2004 г.

9. Алимов Р.Е., **Аристархов И.В.** О внедрении технологии электронной цифровой подписи в систему информационно-правового обеспечения // V межведомственная конференция «Научно-техническое и информационное обеспечение деятельности спецслужб», ИКСИ Академии ФСБ России, с.3, 2004 г.

10. **Аристархов И.В.**, Логачев А.С. О концепции создания инфраструктуры удостоверяющих центров органов государственной власти РФ // IV межведомственная конференция «Научно-техническое и информационное обеспечение деятельности спецслужб», ИКСИ Академии ФСБ России, с. 4, 2002 г.