*На правах рукописи*

**Аристархов Иван Владимирович**

# УПРАВЛЕНИЕ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

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

**АВТОРЕФЕРАТ**
диссертации на соискание ученой степени
кандидат технических наук

Санкт – Петербург - 2012

Работа выполнена в в/ч 43753

| | |
|---|---|
| Научный руководитель: | доктор физико-математических наук, профессор<br>Баранов Александр Павлович |
| Официальные оппоненты: | доктор технических наук,<br>Скиба Владимир Юрьевич |
| | кандидат технических наук,<br>доцент<br>Самонов Александр Валерьянович |
| Ведущая организация: | ФГУП ЦНИИ ЭИСУ, г. Москва |

Защита состоится «___» _____ 2012 года в 16 часов на заседании диссертационного совета 212.229.27 ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет», 195251, Санкт-Петербург, ул. Политехническая, д. 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет»

Автореферат разослан «___» _____ 2012 года.

Ученый секретарь
диссертационного совета Платонов В.В.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность.** Современные технологии обработки информации предоставляют возможность всё более эффективно управлять различными 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 данных 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 размещению заказов (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, принимаются 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 сертификатами ключей проверки электронной подписи (ЭП) на всех этапах их использования**.**

Основными функциями управления сертификатами ключей проверки ЭП являются – издание сертификата и его отзыв (прекращение действительности), и связаны они с управлением периодом действия ключа ЭП.

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

В тоже время в условиях активных информационных воздействий на ИСС целесообразно рассмотреть задачу выбора периода действия сертификата ключа ЭП, который с одной стороны снижал бы вероятность компрометации ключа, а с другой стороны обеспечивал бы приемлемые временные затраты на обеспечение готовности СППЭД ИСС. Сокращение периода действия сертификата ключа проверки ЭП в СППЭД ИСС позволяет ограничить объем информации, доступной нарушителю и ограничить объем данных, подписанных ЭП с использованием ключа, который впоследствии может быть скомпрометирован. Но необоснованное сокращение срока действия может стать причиной повышенной нагрузки на компоненты инфраструктуры PKI, в частности, на Центр сертификации при массовой смене ключей и издании новых сертификатов для абонентов СППЭД.

Данное обстоятельство обуславливает актуальность задачи разработки рациональных организационных решений по управлению сертификатами ключей проверки ЭП.

В соответствии с этим **целью исследования** является описание процесса смены и компрометации ключей ЭП и построение метода планирования смены сертификатов ключей проверки ЭП, минимизирующего суммарные временные затраты на восстановление доверия к электронным документам в СППЭД ИСС.

**Объект исследования:** система управления сертификатами ключей проверки ЭП в условиях наличия угроз информационной безопасности.

**Предмет исследования:** модели, методы и алгоритмы управления сертификатами ключей проверки ЭП в СППЭД ИСС в условиях наличия угроз информационной безопасности.

**Научная задача заключается в** разработке метода управления сменой ключей ЭП и сертификатов, минимизирующего математическое ожидание суммарных временных затрат на смену ключевой информации, переиздание сертификата и восстановление доверия к электронным документам.

**Положения, выносимые на защиту.**

1. Модели процесса управления сменой ключевой информации в условиях деструктивных информационных воздействий нарушителя на СППЭД ИСС.
2. Методика оценки временных затрат на переход к новой ключевой информации в СППЭД ИСС с учетом изменения интенсивности обслуживания заявок на получение сертификатов ключа проверки ЭП.
3. Алгоритм имитационного моделирования процесса смены и компрометации ключей ЭП в СППЭД ИСС.
4. Способы получения численных оценок коэффициента готовности СППЭД при организации электронного документооборота в условиях деструктивных информационных воздействий, которые могут привести к компрометации ключей ЭП.

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

**Научная новизна** результатов работы состоит в разработке моделей, методики и алгоритма, позволяющих в отличие от известных подходов разработать схему планирования смены сертификатов ключей проверки ЭП в СППЭД ИСС, учитывающую интенсивность деструктивных информационных воздействий, способных привести к компрометации ключей ЭП, а также готовность УЦ к обслуживанию запросов на издание сертификатов ключей проверки ЭП.

**Практическая значимость** диссертационной работы определяется созданием готовых к непосредственному применению и реализованных для выработки практических требований к действующим УЦ оригинальных моделей и алгоритмов, позволяющих выработать рекомендации по управлению сертификатами ключей проверки ЭП, впервые учитывающие следующий комплекс характеристик СППЭД ИСС:

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

Результаты работ были использованы при подготовке нормативных документов в области применения УЦ и ЭП.

**Реализация:** результаты работы реализованы в в/ч 43753, 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», XIII 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), IX ежегодной международной конференции по проблематике инфраструктуры открытых ключей и электронной цифровой подписи «PKI-FORUM Россия 2011».

**Публикации:** по теме диссертации опубликовано 10 печатных работ, в том числе 4 научных статьи, из них 3 статьи в изданиях, включенных в Перечень ведущих рецензируемых научных журналов, а также 6 тезисов докладов.

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

## 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.

**При заданном коэффициенте готовности эффективное функционирование СППЭД обеспечивается реализацией схемы управления сертификатами и ключами ЭП. Решению задачи построения оптимальной схемы управления сертификатами и ключами ЭП 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;

$\mu_i$ - 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:

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

При ограничениях: компрометация закрытого ключа в результате внешнего воздействия обнаруживается внутри интервала действия ключевой информации $\tau_i$, $i = \overline{0,m}$; 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 $\tau_i$, $0 \le i \le m$, 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.

Решением поставленной задачи являются временные интервалы между сменой ключевой информации $\tau_i$, 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) $\bar{t} = f(m, \tau_0, ..., \tau_m)$.

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

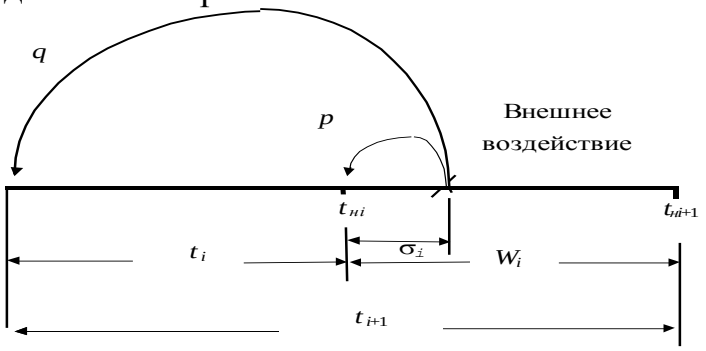


Рис. 1 Процесс восстановления доверия к электронным документам, подписанным скомпрометированными закрытыми ключами

Пусть $\sigma_i$ - случайное время функционирования СППЭД в пределах интервала $\tau_i$ до того как будет обнаружено внешнее воздействие, а $\tau_в$ - представляет собой случайный интервал времени между двумя последовательными компрометациями закрытых ключей. Плотность распределения $\tau_в$ выбрана из модели поступления отказов устройств и системы, являющейся общеупотребительной:

$$f_{\tau_в}(\tau_в) = \lambda e^{-\lambda\tau_в},\ \tau_в \geq 0,\ \lambda\text{-интенсивность компрометаций.}$$

Из этого вытекает, что плотность распределения случайного времени $\sigma_i$ до обнаружения компрометации на интервале τi:

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

Математическое ожидание случайной величины $\sigma_i$ определяется выражением:

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

С учетом модели моментов компрометации $t_i$, $i = \overline{1,m+1}$ является случайным временем, прошедшим от начала регистрации субъекта СППЭД до перехода на i-ю пару ключей.

Тогда для i=1 с учетом времени на восстановления доверия к ЭД - $t_s$ ,получаем

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

Откуда среднее время функционирования до первой смены ключа ЭП

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

Случайное время $t_{i+1}$ до перехода на $i+1$-ю пару ключей определяется наступлением различных событий. При обнаружении компрометации процесс может осуществляться путем смены ключа ЭП (сертификата) субъектом СППЭД или УЦ.

Следовательно, $t_{i+1} = t_i + w_i$, $i = \overline{1,m}$, где

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

и среднее время функционирования до i-й смены сертификата определяется выражением

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

Решая задачу поиска минимума для полученного представления $\bar{t}_{i+1}$ относительно количества m смен сертификата и длительности $\tau_i$ ,получаем рекуррентные выражения:

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

Полученные выражения показывают, что оптимальные интервалы между сменой сертификатов при моделировании моментов компрометации пуассоновским потоком событий должны быть равными за исключением первого, который больше остальных на

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

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

Моменты смены ключевой информации $\{\tau_1, \tau_2, ..., \tau_k, ..., T\}$ составляют определенную последовательность, подлежащую определению. 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:

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

где $R$ - математическое ожидание временных затрат на восстановление доверия к ЭД, подписанными скомпрометированными ключами, и на смену ключевой информации, а $\varphi_t$ - 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 в следующем виде:

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

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 $k$:

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

Последовательность неотрицательных чисел

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

минимизирующая полные ожидаемые потери времени R, находится из условия,

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

и имеет следующий вид

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

Таким образом, последовательность величин $\tau_k$ определяется однозначно, как только выбран момент $\tau_1$.

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 $\tau_k$. Средняя длительность процесса - $t_m$, соответственно m - максимальное количество смен сертификатов.

Средние затраты времени на проведение смены ключей за период $T$ имеют вид:

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

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

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

Полученное выражение является целевой функцией $R$ и представляет собой общее среднее время потерь абонента СППЭД (на смену сертификата и на восстановление доверия).

Порядок расчета оптимальной временной последовательности смены ключевой информации аналогичен.

Разработанные модели в качестве априорной информации требуют не только знания закона распределения между воздействиями, способными привести к

компрометации ключей ЭП, 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 (ЦР), который показал, что временные затраты на получение сертификата нового ключа проверки ЭП существенным образом зависят от того является ли переход на новую ключевую информацию плановым или же осуществляется после компрометации ключа ЭП.

В диссертационной работе 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 ЦР с использованием математического аппарата 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 $\mu_i$, порядок выбора заявок из очередей – «первый пришел, первым обслуживается» (FCFS).

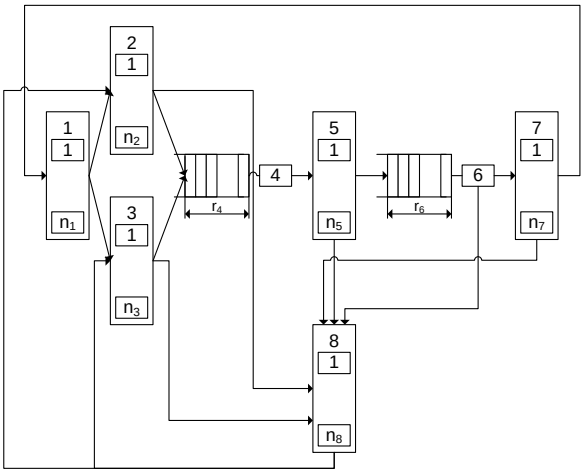


Рис.2. Сеть массового обслуживания, формализующая процесс функционирования Центра регистрации

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 $\tau_i$, 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, выработки ЭП издателем.

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

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 $\theta_{ij}$, где $i, j = \overline{1, M}$. При этом, учитывая, что заявки не покидают сеть, имеем

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

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

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

Интенсивность $\lambda_i$ выходящего из узла $i$ потока заявок равна интенсивности $\mu_i$ обслуживания в узле $i$, умноженной на долю времени, в течение которого канал узла $i$ был занят обслуживанием, равную $1 - p_i(0)$. Используя математический аппарат СеМО, получаем расчетные формулы для определения интенсивности обслуживания заявок на получение сертификатов ключа проверки ЭП в зависимости от функциональных возможностей УЦ (интенсивности обслуживания):

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

откуда, получаем

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

При этом среднее время издания сертификата соответствует суммарному времени обслуживания заявки (поглащения).

**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 в соответствии с результатами, полученными в третьем разделе.

Для преодоления ограничений моделей планирования смены ключевой информации, связанных с допущениями об экспоненциальных законах распределения времени между последовательными компрометациями ключевой информации, экспоненциальном законе распределения времени обслуживания заявок на различных этапах их прохождения в УЦ 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 сертификата от интенсивности поступления заявок);

2) генерируется время до компрометации КИ;

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

4) в зависимости от типа события предпринимаются различные действия. В случае если компрометация ключа ЭП 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 скомпрометированного ключа ЭП.

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 сертификатов ключей проверки ЭП 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 ключей ЭП. Кривая отражает зависимость, полученную с использованием аналитических моделей, а точками показаны результаты имитационного моделирования процесса функционирования.

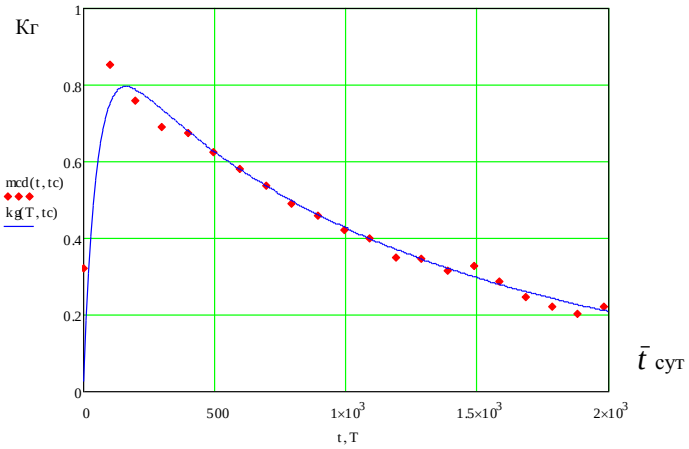


Рис. 3. Зависимость коэффициента готовности систем подтверждения подлинности электронного документооборота от периода действия ключа электронной подписи

Оптимальный период смены сертификатов (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 сертификатов и ключей ЭП.

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 сертификатов с использованием аналитических моделей и имитационного моделирования была получена зависимость коэффициента готовности от математического ожидания времени между компрометациями ключевой информации.

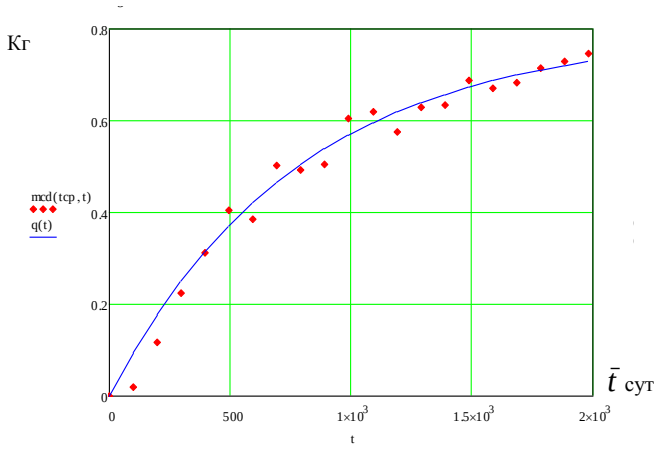


Рис. 4 Зависимость коэффициента готовности от математического ожидания времени между компрометациями ключей электронной подписи

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).

| $\tau_0$ | $\tau_1$ | $\tau_2$ | $\tau_3$ | $\tau_4$ | $\tau_5$ |
|---|---|---|---|---|---|
| 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).

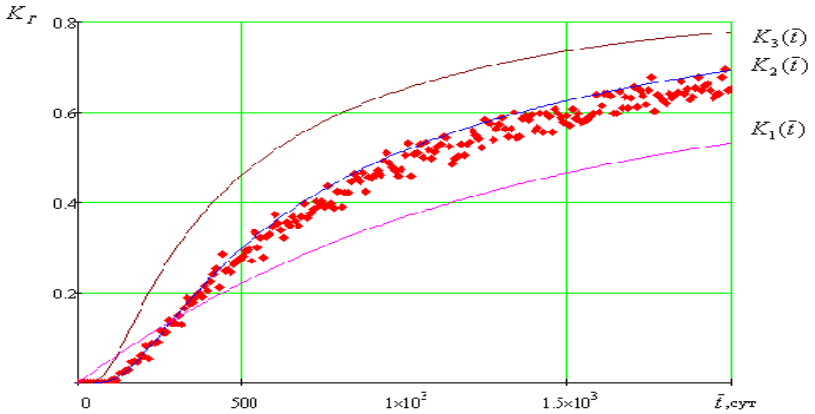


Рис. 5. Зависимость коэффициента готовности от среднего времени между воздействиями для различных стратегий смены ключей электронной подписи

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.

## 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) Предложены способы получения численных оценок коэффициента готовности СППЭД при организации электронного документооборота в условиях деструктивных информационных воздействий, которые могут привести к компрометации ключей ЭП.

5) Получены численные оценки коэффициента готовности СППЭД в условиях моделирования воздействий, которые могут привести к компрометации ключей ЭП, и применительно к функционированию ИСС при организации электронного документооборота показана возможность повысить коэффициента готовности на 12%.

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

## ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ


1. **Аристархов, И. В. О некоторых угрозах информационной безопасности, приводящих к компрометации ключей ЭП/ И.В. Аристархов // Проблемы информационной безопасности, Компьютерные системы. СПб: СПГТУ, 2011. №3, - с. 58-63. (перечень ВАК)**

2. Аристархов, И. В**.** О концепции требований информационной безопасности удостоверяющих центров / И.В**.** Аристархов, А.С. Кузьмин, А.С. Логачев // IX ежегодная международная конференция по проблематике инфраструктуры открытых ключей и электронной цифровой подписи «PKI-FORUM Россия 2011». СПб, 2011. - с. 16.

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

4. Аристархов, И. В. Использование изоляционного подхода в реализации сервисов инфраструктуры открытых ключей./ И.В. Аристархов, А.С. Логачев, С.Е. Прокопьев // Общероссийская конференция «Математика и безопасность информационных технологий» (МАБИТ-2010). Москва: МГУ, 2010. - с. 195-200.

5. Аристархов, И. В. О некоторых проблемах безопасного применения ЭП в системах документооборота специального назначения / И.В. Аристархов, С.Н.Камышев, А.С. Логачев // Труды III Общероссийской научно-практической конференции «Инновационные технологии и технические средства специального назначения. СПб: БГТУ (Библиотека журнала «Военмех. Вестник БГТУ», № 10), 2010. - с. 80-83.

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

7. Аристархов, И. В. Проблемы безопасного применения ЭЦП в системах электронного документооборота / И.В. Аристархов, С.Н. Камышев // Information Security/Информационная безопасность. Москва: издательство «Гротек», 2007. №3, - с. 37-42.

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

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

10. Аристархов, И. В. О требованиях к информационной безопасности удостоверяющих центров / И.В. Аристархов, А.С. Логачев // Материалы XIII Международной конференции «Информатизация и информационная безопасность правоохранительных органов». Москва: Академия управления МВД России, 2004.- с. 4.