О. В. Куликова
Московский инженерно-физический институт (государственный университет)

ОЦЕНКА СТОЙКОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, В КОТОРЫХ ПРИМЕНЯЮТСЯ КЛЮЧИ С ВНЕДРЕННОЙ БИОМЕТРИЧЕСКОЙ ИНФОРМАЦИЕЙ

Приводятся результаты исследования по оценке стойкости к компрометации криптографических ключей систем резервного копирования данных и систем защищенной электронной почты, в которых применяются средства криптографической защиты информации с ключами, выработанными на основе биометрических данных. Выводятся аналитические зависимости, показывающие снижение вероятности компрометации ключей в криптосистемах с внедренной в ключи биометрической информацией по сравнению с традиционными криптосистемами.

Введение

В симметричных криптосистемах секретные ключи с внедренной в них биометрической информацией удается эффективно использовать только тогда, когда процедуры зашифрования и расшифрования осуществляет один субъект, который и является владельцем биометрических данных. На данный момент в современной симметричной криптографии нет метода, позволяющего организовать протокол передачи секретного ключа с внедренной в него биометрической информацией для выполнения процедуры зашифрования и расшифрования другими субъектами криптографической системы. Это связано с тем, что для процесса восстановления ключа необходимо присутствие субъекта, являющегося владельцем биометрических данных, из которых первоначально был получен секретный ключ. Это существенно ограничивает сферу применения биометрических методов для генерации криптографических ключей. Примером симметричных криптосистем, где зашифрование и расшифрование осуществляется одним человеком, являются системы резервного копирования данных. В них для восстановления данных необходим секретный ключ субъекта, которым они были зашифрованы.

Для асимметричных криптосистем важным является тот факт, что секретный ключ не передается другим субъектам, а постоянно хранится у его владельца. В асимметричных криптосистемах биометрические данные можно использовать всегда. Биометрические преобразования позволяют не хранить секретный ключ субъекта, а запрашивать биометрические данные этого субъекта и воспроизводить по ним секретный ключ по мере необходимости использования данного секретного ключа. В качестве примера асимметричной криптосистемы в данной работе рассмотрена система защищенной электронной почты.

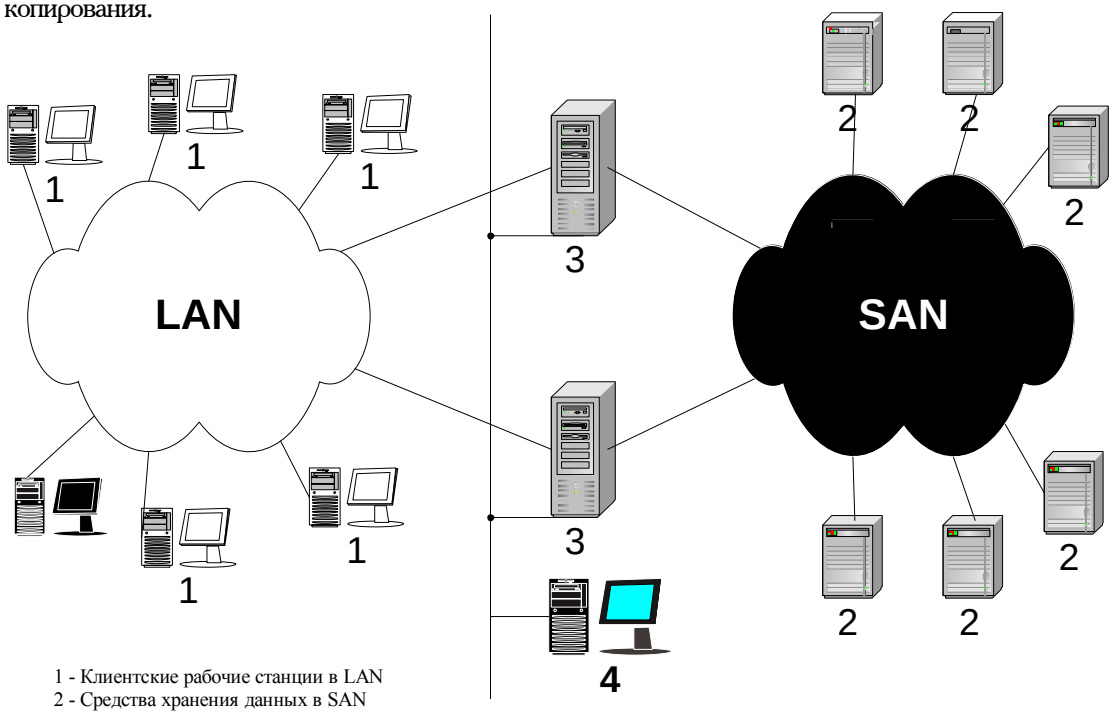
1. Оценка стойкости защищенных систем резервного копирования данных

Система резервного копирования является сложным аппаратно-программным комплексом, основным требованием к которому является высокая доступность его дисковых массивов или ленточных накопителей. На сегодняшний день резервное копирование практически во всех системах резервного копирования, кроме самых мелких, осуществляется на магнитную ленту. Представляется логичным частично или полностью шифровать резервные копии данных с тем, чтобы уменьшить риск несанкционированного доступа к лентам. Однако, известно, что шифрование само по себе не может решить данную проблему в отсутствии безопасной системы управления ключами. Данное требование является крайне важным, так как при небезопасном управлении ключами сводятся на нет все преимущества использования стойкого шифрования.

Исследование рынка существующих программных и аппаратных средств шифрования резервных копий показало, что встроенные в них средства шифрования данных не обеспечивают необходимый уровень безопасности. Поэтому актуальным является исследование по оценке стойкости к компрометации криптографических ключей систем резервного копирования данных, в которых применяются средства

криптографической защиты информации с биометрическими механизмами защиты. В системах резервного копирования данных применение биометрических механизмов возможно для генерации криптографических ключей из биометрических данных пользователей. Такой вариант подразумевает отказ от хранения секретного ключа. Ключ генерируется каждый раз по мере необходимости в нем из биометрических данных участника.

На рис. 1 представлена архитектура сети хранения данных типовой системы резервного копирования.



1 - Клиентские рабочие станции в LAN
2 - Средства хранения данных в SAN
3 - Серверы резервного копирования на шлюзах LAN -SAN
4 - Рабочая станция администратора резервного копирования

Рис. 1. Архитектура сети хранения данных типовой системы резервного копирования

Для оценки вероятности компрометации ключей в системе резервного копирования данных рассматривается такая система, в которой локальная вычислительная сеть состоит из n клиентов, при этом шифрование данных осуществляется на стороне клиента. Оценка проводится для трех вариантов использования ключей:

1) все клиенты зашифровывают и расшифровывают данные на одном ключе, являющимся одинаковым для всех клиентов,

2) каждый клиент зашифровывает и расшифровывает данные на своем уникальном ключе,

3) зашифрование и расшифрование данных в системе осуществляются на ключе, полученном при помощи пороговой схемы разделения секрета.

Оценка вероятности компрометации ключей для обычной системы резервного копирования данных с n клиентами, обладающими одинаковыми ключами (без использования биометрических механизмов защиты). Для системы резервного копирования данных с n участниками, обладающими одинаковыми ключами, в которой не используются биометрические механизмы защиты, задаются следующие вероятности: ρ_{s_i} — вероятности компрометации секретного ключа s участника i, где $i \in \{1,\ldots,n\}$; $P_{enc}(K)$ — вероятность компрометации ключа шифрования участника.

Поскольку события, связанные с компрометацией секретных ключей участников являются независимыми в совокупности событиями [1], т. е. $\rho_{s_1,\ldots,s_i,\ldots,s_n} = \rho_{s_1} \cdot \ldots \cdot \rho_{s_i} \cdot \ldots \cdot \rho_{s_n}$, то вероятность компрометации ключа шифрования i-го участника равна $P_{enc}(K) = \rho_{s_i}$. Для случая равенства вероятностей

компрометации секретных ключей участников (т. е. $\rho_{s_1}=\ldots=\rho_{s_i}=\ldots=\rho_{s_n}=\ldots=\rho$) вероятность компрометации ключа шифрования i—го участника равна $P_{enc}(K)=\rho$.

Оценка вероятности компрометации ключей для системы резервного копирования данных с клиентами, обладающими одинаковыми ключами (ключи сгенерированы из биометрических данных клиентов). Рассмотрение данного случая невозможно, поскольку в силу физиологических особенностей человека его биометрические данные являются уникальными, и нет возможности получить одинаковые ключи для разных участников системы.

Оценка вероятности компрометации ключей для обычной системы резервного копирования данных с n-клиентами, обладающими разными ключами (без использования биометрических механизмов защиты). Для данного случая задаются следующие вероятности: ρ_{s_i}— вероятности компрометации секретного ключа s_i участника i, где $i\in\{1,\ldots,n\}$, $P_{enc}(K)$ — вероятность компрометации ключа шифрования участника.

Вероятность компрометации ключа шифрования i-го участника равна $P_{enc}(K)=\rho_{s_i}$. Для случая равенства вероятностей компрометации секретных ключей участников (т. е. $\rho_{s_1}=\ldots=\rho_{s_i}=\ldots=\rho_{s_n}=\ldots=\rho$) вероятность компрометации ключа шифрования равна $P_{enc}(K)=\rho$.

Оценка вероятности компрометации ключей для системы резервного копирования данных с клиентами, обладающими разными ключами (ключи сгенерированы из биометрических данных клиентов). Для данного случая вероятности компрометации ключей можно задать аналогичным образом: $\rho^{bio}_{s_i}$— вероятности компрометации секретного ключа s_i участника i, где $i\in\{1,\ldots,n\}$, $P^{bio(key)}_{enc}(K)$ — вероятность компрометации ключа шифрования участника.

Вероятность компрометации ключа шифрования участника равна: $P^{bio(key)}_{enc}(K)=\rho^{bio}_{s_i}$. При равенстве вероятностей компрометации ключей $\rho^{bio}_{s_1}=\ldots=\rho^{bio}_{s_i}=\ldots=\rho^{bio}_{s_n}=\ldots=\rho^{bio}_{s}$ вероятность компрометации ключа шифрования участника равна: $P^{bio(key)}_{enc}(K)=\rho^{bio}_{s}$.

На основании полученных результатов можно рассчитать коэффициент повышения стойкости ключей шифрования к компрометации в системе резервного копирования данных при использовании ключей, сгенерированных из биометрических данных ее участников: $K^{\frac{bio(key)+\rho KI}{\rho KI}}=\rho^{bio}_{s_i}/\rho_{s_i}$. При равенстве вероятностей: $\rho^{bio}_{s_1}=\ldots=\rho^{bio}_{s_i}=\ldots=\rho^{bio}_{s_n}=\ldots=\rho^{bio}_{s}$ данный коэффициент равен: $K^{\frac{bio(key)+\rho KI}{\rho KI}}=\rho^{bio}_{s}/\rho$.

Оценка вероятности компрометации ключей, полученных при помощи пороговой схемы разделения секрета (СРС), для обычной системы резервного копирования данных с n-клиентами (без использования биометрических механизмов защиты). Для решения данной задачи рассматривается (t,n)-пороговая СРС, где t-порог. Секретный ключ K делится на доли между n участниками системы резервного копирования данных. Для того, чтобы зашифровать или расшифровать данные на ключе K, необходимо собрать любые t из долей этого ключа. Поскольку восстановление ключа возможно при наличии t долей, следовательно, компрометация ключа K наступает при компрометации любых и более долей ключа. Для оценки вероятности компрометации данного ключа будет использоваться подход на основе методов теории надежности невосстанавливаемых систем [2]. Данный подход можно применить к ключевой системе, в которой ключ состоит из долей. Такая система обладает дробной кратностью резервирования $\frac{n-t}{n-(n-t)}=\frac{n-t}{t}$, где $(n-t)$ — число резервных долей, n — общее число долей. Эта мажоритарная система будет секретной в течение времени T при отказе компрометации не более $(n-t)$ долей. Пусть ρ — вероятность компрометации доли, q — вероятность сохранения секретности доли, $q=1-\rho$.

Вероятность сохранения секретности мажоритарной системы при условии, что все доли имеют одинаковую вероятность компрометации, равна

$$P(T)=\sum_{i=0}^{n-1} C_n^i\cdot p^i(T)\cdot q^{n-1}(T).$$

Тогда вероятность компрометации такой системы будет равна:

$$P_{(t,n)}(T)=1-P(T)=1-\sum_{i=0}^{n-1} C_n^i\cdot p^i(T)\cdot q^{n-1}(T).$$

Оценка вероятности компрометации ключей, полученных при помощи пороговой СРС, для системы резервного копирования данных с n-клиентами (доли ключей сгенерированы из биометрических данных клиентов). Для данного случая вероятности компрометации ключей можно задать аналогичным образом: ρ^{bio} — вероятность компрометации доли, полученной из биометрических данных клиента, q^{bio} — вероятность сохранения секретности доли, полученной из биометрических данных клиента, $q^{bio}=1-\rho^{bio}$, $P^{bio(key)}_{(t,n)}(T)$ — вероятность компрометации ключа шифрования.

Для такой системы все рассуждения проводятся аналогичным образом. Вероятность компрометации ключа шифрования равна:

$$P^{bio}_{(t,n)}(T)=1-P^{bio}(T)=1-\sum_{i=0}^{n-1}C^i_n\cdot(p^{bio})^i(T)\cdot(q^{bio})^{n-i}(T).$$

На основании полученных результатов можно рассчитать коэффициент повышения стойкости ключей шифрования, полученных при помощи пороговой СРС из биометрических данных участников, к компрометации в системе резервного копирования данных:

$$K^{\frac{bio(key)+PKI}{PKI}}_{(t,n)}=\frac{1-P^{bio}(T)}{1-P(T)}=\frac{1-\sum_{i=0}^{n-1}C^i_n\cdot(p^{bio})^i(T)\cdot(q^{bio})^{n-i}(T)}{1-\sum_{i=0}^{n-1}C^i_n\cdot p^i(T)\cdot q^{n-i}(T)}.$$

2. Оценка стойкости систем защищенной электронной почты

Пусть имеется криптосистема, включающая большое число участников, представляющая собой систему защищенной электронной почты. Не ограничивая общности рассуждений, рассматривается два участника системы электронной почты, одному из которых (например, участнику A) необходимо передать другому (например, участнику B) защищенное сообщение. Среди участников этой криптосистемы выделен специальный участник, которому доверяют все остальные, называемый Удостоверяющим центром — (УЦ (Certification Authority)).

Оба участника должны пройти процедуру регистрации в криптосистеме. Для этого они должны взаимодействовать с УЦ, чтобы зарегистрировать свои открытые ключи и получить сертификаты своих открытых ключей. УЦ, в свою очередь должен проверить представленные ему учетные данные, а также знание секретного ключа, соответствующего представленному для регистрации открытому ключу. Участник A, заинтересованный в связи с B, должен однократно приобрести аутентичный открытый ключ УЦ открытых ключей. Впоследствии A получает сертификат B путем извлечения его из открытого общедоступного справочника, который заводится в криптосистеме. Далее A выполняет процедуру проверки сертификата и в случае, если все проверки окончились с положительным результатом, принимает открытый ключ, извлеченный из сертификата B как аутентичный ключ. Участники A и B, приобретя таким образом открытые ключи друг друга, выполняют протокол открытого распределения ключей Диффи-Хеллмана, вырабатывая с его помощью общий секретный ключ для симметричной криптосистемы и используя далее для шифрования сообщений, которыми будут обмениваться эти участники, какой-либо симметричный алгоритм: DES, ГОСТ 28147-89 и др.

На рис. 2 изображен процесс получения и использования сертификатов участниками системы электронной почты.

В системе электронной почты с точки зрения безопасности особый интерес представляют вопросы, связанные с компрометацией секретных ключей шифрования и подписи. Поэтому ниже будет проведена сравнительная оценка вероятностей компрометации секретных ключей шифрования и подписи для системы электронной почты с применением биометрических механизмов защиты и без них.

Оценки вероятности компрометации секретного ключа шифрования для системы электронной почты (без использования биометрических механизмов защиты). Для оценки вероятности компрометации секретного ключа шифрования для системы электронной почты без использования биометрических механизмов защиты задаются следующие вероятности: ρ_{Sqnc} — вероятность

компрометации секретного ключа шифрования участника A, $\rho_{S_B^{enc}}$ — вероятность компрометации секретного ключа шифрования участника B, $\rho_{S_{CA}}$ — вероятность компрометации секретного ключа УЦ, $P_{enc}(K)$ — вероятность компрометации общего секретного ключа шифрования.

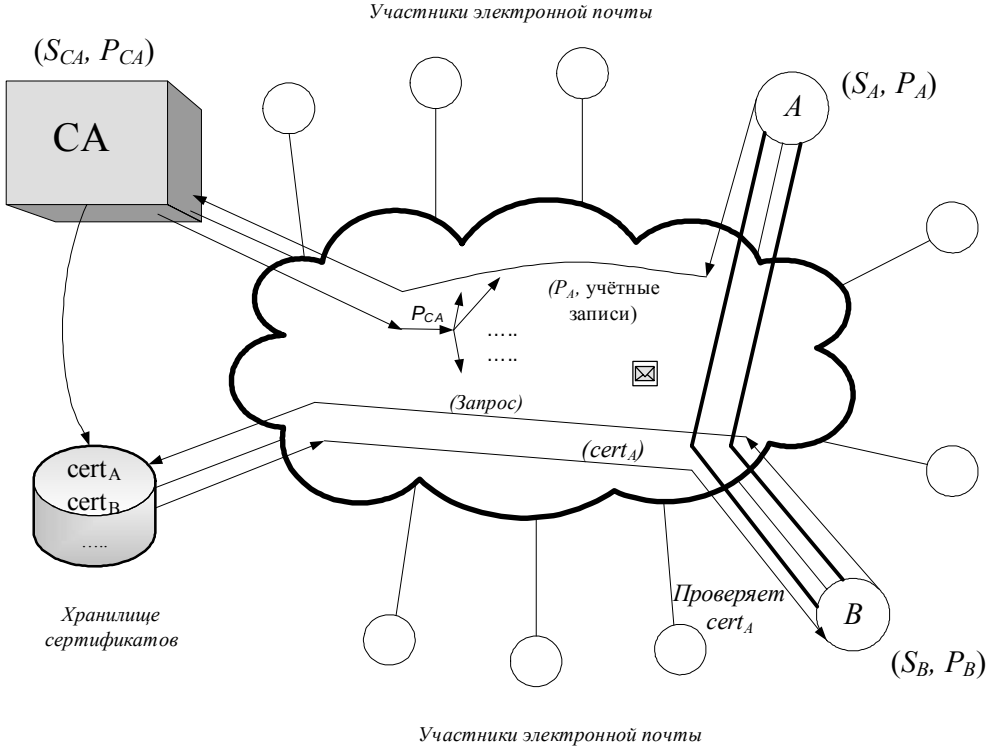


Рис. 2. Процесс получения и использования сертификатов участниками системы электронной почты

Вероятность компрометации ключа шифрования K равна

$$P_{enc}(K)=1-(1-\rho_{S_A^{enc}})(1-\rho_{S_B^{enc}})(1-\rho_{S_{CA}})$$

$$P_{enc}(K)=\rho_{S_A^{enc}}+\rho_{S_B^{enc}}+\rho_{S_{CA}}-\rho_{S_A^{enc}}\cdot\rho_{S_B^{enc}}-\rho_{S_A^{enc}}\cdot\rho_{S_{CA}}-\rho_{S_B^{enc}}\cdot\rho_{S_{CA}}+\rho_{S_A^{enc}}\cdot\rho_{S_B^{enc}}\cdot\rho_{S_{CA}}.$$

Для случая равенства вероятностей компрометации секретных ключей участников A и B (т. е. $\rho_{S_A^{enc}}=\rho_{S_B^{enc}}=\rho$) и вероятностей компрометации открытых ключей участников A и B (т. е. $\rho_{P_A^{enc}}=\rho_{P_B^{enc}}=\rho_{S_{CA}}$) полученное значение вероятности компрометации ключа шифрования K примет вид:

$$P_{enc}(K)=1-(1-\rho)(1-\rho)(1-\rho_{S_{CA}})=1-(1-2\cdot\rho+\rho^2)(1-\rho_{S_{CA}})$$

$$P_{enc}(K)=2\cdot\rho+\rho_{S_{CA}}-2\cdot\rho\cdot\rho_{S_{CA}}-\rho^2+\rho_{S_{CA}}\cdot\rho^2.$$

Оценки вероятности компрометации секретного ключа шифрования для системы электронной почты (ключи сгенерированы из биометрических данных участников). Для данного случая аналогичным образом вводятся следующие вероятности: $\rho_{S_A^{enc}}^{bio}$ — вероятность компрометации секретного ключа шифрования участника A, $\rho_{S_B^{enc}}^{bio}$ — вероятность компрометации секретного ключа шифрования участника B, $\rho_{S_{CA}}^{bio}$ — вероятность компрометации секретного ключа УЦ, $P_{enc}^{bio(key)}(K)$ — вероятность компрометации секретного ключа шифрования при использовании в системе электронной почты ключей, сгенерированных из биометрических данных ее участников.

Вероятность компрометации ключа шифрования равна

$$P_{enc}^{bio(key)}(K)=1-(1-\rho_{S_A^{enc}}^{bio})(1-\rho_{S_B^{enc}}^{bio})(1-\rho_{S_{CA}}^{bio})$$

$$P_{enc}^{bio(key)}(K)=\rho_{S_A^{enc}}^{bio}+\rho_{S_B^{enc}}^{bio}+\rho_{S_{CA}}^{bio}-\rho_{S_A^{enc}}^{bio}\cdot\rho_{S_B^{enc}}^{bio}-\rho_{S_A^{enc}}^{bio}\cdot\rho_{S_{CA}}^{bio}-\rho_{S_B^{enc}}^{bio}\cdot\rho_{S_{CA}}^{bio}+\rho_{S_A^{enc}}^{bio}\cdot\rho_{S_B^{enc}}^{bio}\cdot\rho_{S_{CA}}^{bio}.$$

Для случая равенства вероятностей компрометации секретных ключей A и B (т. е. $\rho_{S_A^{enc}}^{bio}=\rho_{S_B^{enc}}^{bio}=\rho_S^{bio}$), вероятностей компрометации открытых ключей A и B (т. е. $\rho_{P_A^{enc}}^{bio}=\rho_{P_B^{enc}}^{bio}=\rho_{S_{CA}}^{bio}$), полученное значение вероятности примет вид:

$\rho^{bio(key)}_{enc}(K)=1-(1-\rho^{bio}_{S})(1-\rho^{bio}_{S})(1-\rho^{bio}_{S_{CA}})$

$\rho^{bio(key)}(K)=2\cdot\rho^{bio}_{S}-\rho^{bio}_{S_{CA}}+(\rho^{bio}_{S})^2+2\cdot\rho^{bio}_{S}\cdot\rho^{bio}_{S_{CA}}-\rho^{bio}_{S_{CA}}\cdot(\rho^{bio}_{S})^2.$

На основании полученных результатов можно рассчитать коэффициент повышения стойкости ключей шифрования к компрометации в системе защищенной электронной, полученных из биометрических данных участников системы:

$$K_{enc}^{\frac{bio(key)+PKI}{PKI}}=\frac{1-(1-p^{bio}_{S_A^{enc}})(1-p^{bio}_{S_B^{enc}})(1-p^{bio}_{S_{CA}})}{1-(1-p_{S_A^{enc}})(1-p_{S_B^{enc}})(1-p_{S_{CA}})}$$

$$K_{enc}^{\frac{bio(key)+PKI}{PKI}}=\frac{p^{bio}_{S_A^{enc}}+p^{bio}_{S_B^{enc}}+p^{bio}_{S_{CA}}-p^{bio}_{S_A^{enc}}\cdot p^{bio}_{S_B^{enc}}-p^{bio}_{S_A^{enc}}\cdot p^{bio}_{S_{CA}}-p^{bio}_{S_B^{enc}}\cdot p^{bio}_{S_{CA}}+p^{bio}_{S_A^{enc}}\cdot p^{bio}_{S_B^{enc}}\cdot p^{bio}_{S_{CA}}}{p_{S_A^{enc}}+p_{S_B^{enc}}+p_{S_{CA}}-p_{S_A^{enc}}\cdot p_{S_B^{enc}}-p_{S_A^{enc}}\cdot p_{S_{CA}}-p_{S_B^{enc}}\cdot p_{S_{CA}}+p_{S_A^{enc}}\cdot p_{S_B^{enc}}\cdot p_{S_{CA}}}\quad .$$

При равенстве вероятностей $\rho^{bio}_{S_A^{enc}}=\rho^{bio}_{S_B^{enc}}=\rho^{bio}_{S}$, $\rho^{bio}_{\rho_A^{enc}}=\rho^{bio}_{\rho_B^{enc}}=\rho^{bio}_{S_{CA}}$, соответственно, данный коэффициент примет следующий вид:

$$K_{enc}^{\frac{bio(key)+PKI}{PKI}}=\frac{1-(1-p^{bio}_{S})(1-p^{bio}_{S})(1-p^{bio}_{S_{CA}})}{1-(1-p)(1-p)(1-p_{S_{CA}})}$$

$$K_{enc}^{\frac{bio(key)+PKI}{PKI}}=\frac{2\cdot p^{bio}_{S}-p^{bio}_{S_{CA}}+(p^{bio}_{S})^2+2\cdot p^{bio}_{S}\cdot p^{bio}_{S_{CA}}-p^{bio}_{S_{CA}}\cdot(p^{bio}_{S})^2}{2\cdot p-p_{S_{CA}}+p^2+2\cdot p\cdot p_{S_{CA}}-p_{S_{CA}}\cdot p^2}\quad .$$

Оценки вероятности компрометации секретного ключа подписи для системы электронной почты (без использования биометрических механизмов защиты). Аналогичным образом для оценки вероятности компрометации секретного ключа подписи для системы электронной почты без использования биометрических механизмов защиты задаются следующие вероятности: $\rho_{S_A^{sig}}$ — вероятность компрометации секретного ключа подписи участника A, $\rho_{S_{CA}}$ — вероятность компрометации секретного ключа CA, $\rho_{sig}(K)$ — вероятность компрометации секретного ключа подписи.

Вероятность компрометации ключа подписи K равна

$\rho_{sig}(K)=1-(1-\rho_{S_A^{sig}})(1-\rho_{S_{CA}})=\rho_{S_{CA}}+\rho_{S_A^{sig}}-\rho_{S_A^{sig}}\cdot\rho_{S_{CA}}.$

Оценки вероятности компрометации секретного ключа подписи для системы электронной почты (ключи сгенерированы из биометрических данных участников). Для данного случая аналогичным образом вводятся следующие вероятности: $\rho^{bio}_{S_A^{sig}}$ — вероятность компрометации секретного ключа подписи участника A, $\rho^{bio}_{S_{CA}}$ — вероятность компрометации секретного ключа УЦ, $\rho^{bio(key)}_{sig}(K)$ — вероятность компрометации секретного ключа подписи при использовании в системе электронной почты ключей, полученных из биометрических данных участников системы.

Вероятность компрометации ключа подписи равна

$\rho^{bio(key)}_{sig}=1-(1-\rho^{bio}_{S_A^{sig}})(1-\rho^{bio}_{S_{CA}})=\rho^{bio}_{S_A^{sig}}+\rho^{bio}_{S_{CA}}-\rho^{bio}_{S_A^{sig}}\cdot\rho^{bio}_{S_{CA}}.$

На основании полученных результатов можно рассчитать коэффициент повышения стойкости ключей подписи к компрометации в системе защищенной электронной почты, полученных из биометрических данных участников системы:

$$K_{sig}^{\frac{bio(key)+PKI}{PKI}}=\frac{1-(1-p^{bio}_{S_A^{sig}})(1-p^{bio}_{S_{CA}})}{1-(1-p_{S_A^{sig}})(1-p_{S_{CA}})}=\frac{p^{bio}_{S_A^{sig}}+p^{bio}_{S_{CA}}-p^{bio}_{S_A^{sig}}\cdot p^{bio}_{S_{CA}}}{p_{S_A^{sig}}+p_{S_{CA}}-p_{S_A^{sig}}\cdot p_{S_{CA}}}\quad .$$

3. Заключение

Результатом данной работы является оценка стойкости симметричных и асимметричных криптографических систем к компрометации, в которых использованы биометрические технологии для генерации криптографических ключей. Вероятностная оценка компрометации ключей для симметричной криптосистемы, в которой использовались биометрические технологии, проводилась на примере системы резервного копирования данных. Для оценки стойкости асимметричной системы в качестве примера взята система защищенной электронной почты. В соответствии с проведенными оценками рассчитаны

коэффициенты повышения стойкости системы резервного копирования данных и системы защищенной электронной почты к компрометации ключей при использовании биометрии.

Полученные данные позволяют сделать утверждение о повышении криптографической стойкости систем к компрометации за счет введения в эти системы криптографических ключей, с внедренной в них биометрической информацией участников.

СПИСОК ЛИТЕРАТУРЫ:

1. *Севастьянов Б. А.* Курс теории вероятностей и математической статистики. М., 1982. — 256 с.
2. *Половко А. М., Гуров С. В.* Основы теории надёжности. СПб., 2006. —704 с.

Е. А. Лавринов
Московский инженерно-физический институт (государственный университет)

РАЗРАБОТКА МОДЕЛИ И АЛГОРИТМОВ СИСТЕМЫ ДИСТАНЦИОННОГО ВЫПОЛНЕНИЯ КРИПТОГРАФИЧЕСКИХ ОПЕРАЦИЙ

Представлены эффективные протоколы дистанционного шифрования, выполнения проверки целостности данных, генерации и проверки подписи. Разработана модель СКЗИ для дистанционного выполнения криптографических операций.

В настоящее время наиболее уязвимым местом в шифровании является не генерация ключей или использование функций генерации ключей, а управление ключами, используемыми в процессе шифрования. Одни и те же ключи используются для зашифрования и расшифрования данных, поэтому их нужно надежно охранять, чтобы защитить данные. В то же время прикладные программы и пользователи должны иметь доступ к ключам, чтобы расшифровать данные для нормального использования. Эта проблема решается путем физического разделения устройства хранения ключей и устройства, выполняющего криптографические операции. Появляется потребность в криптографических протоколах для дистанционного выполнения операций.

Решением данной проблемы является разработка системы дистанционного выполнения криптографических операций, которая включает в себя следующие протоколы:

1. Протокол дистанционного шифрования данных.
2. Протокол дистанционного выполнения проверки целостности данных.
3. Протокол генерации и проверки ЭЦП.

В качестве устройства хранения ключа удобнее использовать интеллектуальную карту (ИК), которая является важным строительным блоком во многих современных прикладных программах (ПП), обеспечивающих безопасность. В частности, взломозащищенный модуль, низкая стоимость, присущая портативность и бесконтактное соединение с терминалом делают ИК особенно привлекательной для использования ее в качестве хранилища секретных ключей, если терминал является незащищенным. С другой стороны, эти же свойства ограничивают использование ИК. Бесконтактное соединение с