Висновки

Проведення аудиту безпеки інформації потребує нормативно-правового, методичного, математичного та програмного забезпечення. В статті розглянуто питання застосування зон базових думок для надання вербальних оцінок щодо зрілості процесів захисту інформації на основі існуючих стандартів в галузі захисту інформації. Наведено методику визначення границь та значень середніх точок для зон базових думок.

В статті наведено такі нові наукові результати:

- на основі виявленої подібності задач, що вирішуються в теорії нечітких множин та суб'єктивної логіки вперше обґрунтовано можливість побудови СФН вектора думки до зони базової думки для суб'єктивної логіки. Таким чином аналітичний апарат суб'єктивної логіки набув подальшого теоретичного розвитку щодо вирішення задач оцінки зрілості процесів захисту інформації;
- надано визначення СФН та сформульовані задачі побудови СФН;
- вперше визначено перелік властивостей, які повинні мати усі суб'єктивні функції належності;
- згідно з визначеними властивостями СФН, в параметричному вигляді задано родину СФН та побудовано їх графічне представлення для кожної зони базової думки у просторі суб'єктивної логіки;
- визначено алгоритм віднесення вектора думки до зони базової думки та визначення ступеню належності вектора думки до зон базових думок.

Практичне значення одержаних результатів полягає в створенні передумов для формування вербального опису обчислених узагальнених оцінок зрілості процесів захисту інформації та для розробки системи підтримки прийняття рішень начальника служби безпеки інформації щодо зрілості процесів захисту інформації.

*Література: **1**. Леншин А. В. Применение аппарата субъективной логики для оценки безопасности банковских ИТ-систем // Актуальні проблеми та перспективи розвитку фінансово-кредитної системи України: Збірник наукових статей. Харків: Фінарт, 2002, с. 410 – 412 **2**. Потий А. В., Леншин А. В. Оценка защищенности информационно-телекоммуникационных систем с использованием математического аппарата субъективной логики //7-я Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р. **3**. Потій О. В., Лєншин А. В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації //Радиотехника. Тематический выпуск "Информационная безопасность", вып. 141, Харьков, 2005 г., с. 144-160. **4**. Потій О.В., Лєншин А.В. Методика визначення думок експертів відносно зрілості безпеки інформації із застосуванням математичного апарату суб'єктивної логіки //Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, Київ, 2004 р., с. 38-47. **5.** A. Jøsang., S. J. Knapskog. A Metric for Trusted Systems. In Reinhard Posh, editor, Proceedings of the 15th IFIP/SEC International Information Security Conference. IFIP, 1998 **6**. A. Jøsang. A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279–311, June 2001. **7.** Беллман Р., Заде Л. Принятие решений в расплывчатых условиях.- В кн.: Вопросы анализа и процедуры принятия решений.- М.:Мир, 1976. - С. 172-215. **8.** Заде Л. А. Основы нового подхода к анализу сложных систем и процессов принятия решений.- В кн.: Математика сегодня.- М.:Знание, 1974, с. 5-49. **9.** Hong T.-P., Lee C.-Y. Induction of rules and membership functions from training examples. - Fuzzy Sets and Systems, 84, 1996, 33 - 47. **10.** Берштейн Л. С., Целых А. Н., Тимошенко Р. П. Об использовании интервальной функции принадлежности нечеткого множества. Известия высших учебных заведения. Северо - Кавказский регион. Технические науки. Ростов – на – Дону: изд-во Ростовского госуниверситета, №1, 1999г., . с.3-8. **11.** Кофман А. Введение в теорию нечетких множеств. М: Радио и связь, 1982, 432с.*

УДК 681.3.06

КРИТЕРИИ И ПОКАЗАТЕЛИ ОЦЕНКИ КРИПТОПРОТОКОЛОВ. МАТЕМАТИЧЕСКИЙ АППАРАТ СРАВНЕНИЯ ПРОТОКОЛОВ

Дмитрий Балагура

Харьковский национальный университет радиоэлектроники

Аннотация: **Предлагаются критерии оценки криптографических протоколов. Вводятся условные и**

безусловные критерии. Анализируется возможность применения метода иерархий для сравнения криптографических протоколов.
Summary: **Criterions of estimations of cryptoprotocols are proposed. Conditional and unconditional Criterions are introduce. Possibilities of using of methods of hierarchy for comparing cryptographic protocol are analyzed.**
Ключові слова: **Безусловные критерии оценки защищённости протокола, условные критерии оценки защищённости протокола, метод иерархий.**

Введение

Одной из наиболее важных и в то же время недостаточно решенной является задача сравнения свойств различных протоколов при использовании различных полей, размеров полей и при различных ограничениях. Эта задача практически не рассматривалась в печати, поэтому в настоящее время сравнение характеристик и выбор криптографических протоколов не по отдельным параметрам, а по интегральному показателю является весьма актуальным. Важной также является задача выполнения сравнения криптографических протоколов. Для решения этой задачи разработка и формулировка критериев и показателей оценки криптографических протоколов и формирование математического аппарата для их сравнения, на наш взгляд, является весьма важным. Под критерием будем понимать признак, на основе которого осуществляется оценка, определение или классификация чего-нибудь. Предыдущие исследования позволили сделать вывод, что сравнение криптографических алгоритмов можно осуществить с использованием двух составляющих: условных и безусловных критериев. При этом оценку протоколов можно осуществлять в два этапа. На первом этапе они оцениваются по безусловным критериям, а на втором – с использованием условных критериев.

I Критерии оценки и сравнения криптографических протоколов

Анализ состояния применения криптопротоколов, результаты, достигнутые при практическом решении задач разработки и оценки криптопротоколов, результаты, достигнутые при практическом решении задач криптоанализа, позволяют выбрать в качестве основных пять безусловных критериев оценки. Безусловные критерии оценки криптографических протоколов приведены в табл. 1.

Таблица 1 – Безусловные критерии оценки криптографических протоколов

№	Название и сущность критерия	Обозначение
1	Надёжность математической базы в понимании отсутствия возможностей выполнять атаки типа «универсальное раскрытие» за счёт несовершенства математического аппарата, используемого в каждом конкретном типе криптопротокола или слабостей, которые могут быть заложены за счёт специфических свойств общесистемных параметров и ключей. Критерием оценки надёжности математической базы является тот факт, что сложность атаки «универсальное раскрытие» $I_{ур}$ носит экспоненциальный характер, а критерием ненадёжности – субэкспоненциальный или полиномиальный характер сложности.	$W_{\delta 1}$
2	Практическая защищённость криптопреобразований от силовых и аналитических атак, которая достигается за счёт выбора размеров общесистемных параметров и ключей. Критерием практической защищённости криптопреобразований является выбор размеров общесистемных параметров и ключей, при которых сложность атаки $I_{са}$ значительно (на необходимое число порядков) превышает существующие возможности криптоаналитических систем на уровне технологически развитых государств, в том числе с учётом прогноза роста мощностей криптоаналитических систем за счёт развитияматематического и программного обеспечения, а также аппаратных и программно-аппаратных средств.	$W_{\delta 2}$
3	Реальная защищённость от всех известных и потенциально возможных криптоаналитических атак, где под защищённостью понимается тот факт, что все известные криптоаналитические атаки типа «полное раскрытие» носят экспоненциальную сложность $I_{эс}$, а критерием незащищенность – субэкспоненциальный $I_{сэ}$ характер сложности атаки типа «полное раскрытие».	$W_{\delta 3}$

Продовження Таблиці 1

4	Статистическая безопасность криптографического преобразования, под которой понимается статистическая независимость результата криптографического преобразования (выхода), например, зашифрованного блока (криптограммы), от входного блока, который зашифровывается, и личного ключа, который используется (для протоколов направленного шифрования) [1]	$W_{\delta 4}$
5	Отсутствие слабых личных ключей, при которых сложность криптоаналитических атак типа «полное раскрытие и «универсальное раскрытие» меньше, чем сложность атаки для других личных ключей.	$W_{\delta 5}$

Условные критерии оценки криптографических протоколов приведены в табл. 2.

Таблица 2 – Условные критерии оценки криптографических протоколов.

№	Название и сущность критерия	Обозначение
1	Наличие и вид ключевой аутентификации.	K_{y1}
2	Наличие и вид аутентификации субъектов.	K_{y2}
3	Новизна ключей.	K_{y3}
4	Управление ключами.	K_{y4}
5	Эффективность протокола.	K_{y5}
6	Криптоживучесть ключей	K_{y6}
7	Сложность выполнения операции и протокола в целом.	K_{y7}
8	Уровень защищённости при реализации различных видов угроз при разных условиях осуществления криптоаналитических атак и отклонениях свойств общесистемных параметров.	K_{y8}

Сформируем основные принципы вычисления критериев, их сравнения и определения значимости для криптографического протокола.

II Определение значений безусловных критериев и математический аппарат их учёта при анализе криптографических протоколов

Все безусловные критерии не могут выполняться только частично, то есть протокол (криптопреобразование) может либо удовлетворять требованиям (соответствовать критерию) либо нет. При этом невыполнение даже одного из безусловных критериев должно приводить к отказу от использования такого криптопреобразования, так как криптопреобразование является нестойким и его использование может привести к полному взлому системы криптографической защиты информации. С математической точки зрения удовлетворение или не удовлетворение этому критерию, выполнение и не выполнение этого критерия можно описывать при помощи логической переменной $W_{\delta i}$, где i – порядковый номер критерия. Причём все логические переменные принимают значения да или нет, то есть $W_{\delta i} = 0$ или $W_{\delta i} = 1$. Поэтому можно записать

$$\left(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}\right) \in \left(1,0\right) \tag{1}$$

С учётом приведенных выше частичных критериев и условия (1) функцию соответствия криптопреобразования можно записать в виде:

$$f_{фв}(\ ) = \mathrm{W}_{\delta 1} \wedge \mathrm{W}_{\delta 2} \wedge \mathrm{W}_{\delta 3} \wedge \mathrm{W}_{\delta 4} \wedge \mathrm{W}_{\delta 5} \tag{2}$$

Где символ „∧” обозначает операцию конъюнкции булевых переменных.

Таким образом, качество криптографического преобразования может быть оценено с использованием безусловного интегрального критерия – функции соответствия криптопреобразования требованиям

$$f_{фс}(\ ) \in (0,1)$$

и при

$$f_{фс}(\ ) = 1$$

криптографическое преобразование, оценка которого выполняется, соответствует требованиям безусловного критерия.

Предложенный интегральный критерий позволяет установить, соответствует используемое криптопреобразование требованию или нет.

Оценку по каждому из частичных безусловных критериев будем осуществлять с использованием множества показателей, которые поддерживают заданный критерий.

Рассмотрим вначале основные показатели, по которым можно оценить стандарты криптографических преобразований по безусловным критериям.

Оценку надежности математической базы можно осуществить на основе экспертных оценок специалистов-криптологов. При этом должна быть учтена степень открытости проектирования и исследования стандарта или вообще криптографического преобразования. Важным же фактором является возможность или подозрение на её существование в части моделирования криптопреобразований и выполнения криптоанализа с уменьшенной или существенно уменьшенной сложностью. В случае, если для математического аппарата не существует подозрения или возможности на подозрение (на настоящий момент) в части моделирования криптоанализа с существенно уменьшенной сложностью, а также при изучении и анализе протокола использовались принципы открытого рассмотрения, обсуждения и анализа протокола, то принимается решение, что $W_{\delta 1} = 1$ или $W_{\delta 1} = 0$.

Практическую защищённость криптографических преобразований от силовых атак будем оценивать, ориентируясь на размер личного ключа. Под силовой атакой будем понимать направленный перебор личных ключей d_i [2] и/или сеансовых ключей (параметров) k_j. Так как d_i и k_j должны формироваться случайно, равновероятно и независимо, и d_i, k_j входят в интервал от 1 до порядка образующего элемента n (будь-то порядок базовой точки или порядок первообразного элемента), то вероятность подбора с одной попытки $P(1)$ можно оценить как

$$P(1) \geq \frac{1}{n} = \frac{1}{2^m} = 2^{-m}.$$

В k попытках вероятность подбора $P(k)$ можно вычислить как

$$P(k) = \frac{k}{n} = \frac{k}{2^m} = k2^{-m}. \qquad (3)$$

Оценку сложности силовой атаки можно осуществить при помощи оценки сложности выполнения атаки I_a и безопасного времени $t_б$ [3]. Для условия, когда $0 < d_i, k_j < n$, сложность можно оценить как

$$I_a = n = 2^m, \qquad (4)$$

а безопасное время

$$t_б = \frac{I_d}{\gamma K} P_y, \qquad (5)$$

где γ – мощность криптоаналитической системы, $K = 3{,}15 \cdot 10^7\ сек/год$, P_y – вероятность, с которой должен быть успешно осуществлён криптоанализ.

На основе анализа практической защищённости принимается решение, что $W_{\delta 2} = 1$ или $W_{\delta 2} = 0$.

Реальную защищённость криптопреобразований предлагается оценивать определением сложности I_a и безопасного времени $t_б$ осуществления атаки типа полное раскрытие для i-го метода криптоанализа. Детально эти формулы и расчёты по ним будут представлены ниже.

Значение I_a и $t_б$ определяется для всех методов криптоанализа. Если они носят экспоненциальный характер, то защищённость криптопреобразований оценивается как соответствующая требованиям. Если они носят субэкспоненциальный характер, то защищённость криптопреобразований оценивается как не соответствующая требованиям.

Кроме того, даже при экспоненциальном характере для случая рассмотрения разных методов решения дискретного логарифмического уравнения или задачи факторизации, реальную защищённость предлагается оценивать как

$$I_a = \min (I_{a1}, I_{a2}, \ldots, I_{ak}), \quad (6)$$

$$t_б = \min (t_{б1}, t_{б2}, \ldots, t_{бk}), \quad (7)$$

На основе оценки реальной защищённости принимается решение, что $W_{\delta 3} = 1$ или $W_{\delta 3} = 0$.

Четвёртый безусловный критерий $W_{\delta 4}$ используется в основном для протоколов направленного шифрования, в которых применяется блочное симметричное криптопреобразование. Это связано с тем, что при помощи собственно точек эллиптической кривой шифрование не выполняется.

Для блочного криптопреобразования, каким являются практически все криптопреобразования протоколов, необходимо также оценивать вероятность появления коллизий. В [1] предложены оценки вероятности возникновения коллизий для блочных симметричных шифров и хеш-функций. Оценка вероятности возникновения коллизий основывается на парадоксе дня рождения.

В целом, на основе полученных результатов и оценок делается вывод о статистической безопасности алгоритма криптографического преобразования и $W_{\delta 4} = 1$ или $W_{\delta 4} = 0$.

Проведенный анализ показал, что поиск слабых личных ключей или открытых ключей, для которых атаки типа «полное раскрытие» или «универсальное раскрытие» носят субэкспоненциальный характер, является очень сложной задачей.

Первой причиной слабости может стать средство или система генерации ключей. Понятно, что личные ключи должны формироваться (генерироваться) случайно, равновероятно и независимо. Для обеспечения этих свойств необходимо использовать физические источники «белого» шума. Но и в этом случае плотность распределения и его характеристики могут быть искривленными в результате наличия у физического генератора ε-асимметрии, когда вероятности $P(1)$ и $P(0)$ различаются между собой. Например, $P(1) = 0{,}5 + \varepsilon$, а $P(0) = 0{,}5 - \varepsilon$. Наличие достаточной ε-асимметрии позволяет уменьшить сложность атаки грубая сила, которая в этом случае может осуществляться с учётом сдвига распределения, когда изменяется вероятность появления ключа с данным соотношением между числами „1” и „0”. Поэтому первым шагом является предъявление к источнику ключей требования по допустимой величине ε, например, $\varepsilon \le 10^{-5}$. Это требование может быть выполнено за счёт использования физических источников шума и генераторов случайных последовательностей, которые строятся на основе этих источников, а также когда $\varepsilon < \varepsilon_{доп}$.

Таким образом, при анализе ключей в первую очередь необходимо проанализировать источник ключей и ограничить допустимую величину ε-асимметрии.

Слабыми необходимо также считать ключи $d_i(k_i)$, при использовании которых уменьшается сложность решения дискретного логарифма. Слабыми также можно считать такие ключи, вероятность появления которых слишком мала, и которые могут появиться в результате возникновения неисправностей.

Таким образом, наличие или подозрения на наличие слабых ключей, а также эквивалентных ключей должны быть установлены экспертами-криптологами. Если при этом слабые ключи в системе блокируются, и стойкость из-за этого не уменьшается, то такой протокол можно считать как такой, что его алгоритм не имеет слабых ключей. В этом случае безусловный критерий $W_{\delta 5} = 1$, в противном случае $W_{\delta 5} = 0$.

III Показатели и порядок оценки криптографических преобразований по условным критериям

Критерии $K_{y1} - K_{y6}$ являются аналитическими и не требуют математических вычислений для определения значений. Все указанные критерии основываются на свойствах и алгоритмических особенностях конкретного протокола.

Значения критериев K_{y7}, K_{y8} могут быть выражены числовыми значениями, которые сравниваются непосредственно или через какую-либо шкалу предпочтения.

Сложность прямого $I_{пр}$ и обратного $I_{об}$ криптографических преобразований может оцениваться как теоретически, так и экспериментально. При теоретической оценке, например криптографических преобразований в группах точек эллиптических кривых, можно использовать формулы, которые приведены в табл. 3.

Таблица 3 – Теоретическая сложность преобразований в группах точек эллиптических кривых в различных координатах [4]

Координаты	Сложение точек	Удвоение точек
Аффинные	t(A + A) = I + 2M + S	t(2A) = I+2M+2S
Проективные	t(P + P) = 12M + 2S	t(2P) = 7M+5S
Якобиановы	t(y + y) = 12M + 4S	t(2I) = 4M+6S
Чудновского	t(yc + yc) = 11M + 3S	t(2Ic) = 5M+6S
Модифицированные якобиановы	t(ym + ym) = 13M + 6S	t(2Im) = 4M+4S

Однако, эти показатели не окончательные, они являются общепринятыми усреднёнными значениями, «ориентирами» сложности. При выполнении неоднократных вычислений, например, скалярного умножения точки на число, алгоритмы могут быть оптимизированы таким образом, что средние затраты на выполнение одной операции сложения или удвоения могут быть значительно ниже. Наиболее точно показатель сложности (скорости) выполнения того или иного математического действия может быть определён с применением экспериментальной оценки.

Экспериментальная оценка может быть осуществлена с использованием соответствующих средств, которые реализовывают криптопреобразования – программных, программно-аппаратных и аппаратных. При этом, оценка может проводиться методом измерения скорости выполнения тех или иных операций. Пространственную сложность I_y можно оценить через объём памяти, который необходим для выполнения прямых и обратных преобразований, размещения ключей, таблиц, параметров и сертификатов. При формировании аналитического портрета в качестве критерия может приниматься как непосредственное значение скорости выполнения элементарной операции так и протокола в целом (сложности выполнения элементарной операции и протокола в целом). Однако для формирования интегрального критерия для сравнения протоколов необходимо выполнить приведение данного критерия к некоторым условным единицам.

Уровень защищённости при реализации различных видов угроз при разных условиях осуществления криптоаналитических атак и отклонениях свойств общесистемных параметров определяется по наличию возможности выполнения атак на протоколы в случае использования параметров, которые разрешены спецификацией протокола, но при этом являются слабыми в криптографическом смысле. Числовым значением такого критерия будет сложность выполнения атаки при указанных условиях. Во время преобразования приведении полученного значения сложности (времени) выполнения атаки на криптопротокол числовые значения заменяются на числовые значения, соответствующие степени снижения сложности атаки на криптопротокол по сравнению с наиболее быстрыми известными методами криптоанализа.

Рассмотрим основные особенности метода анализа иерархий. Этот метод является систематической процедурой для иерархического представления элементов, определяющих суть данной проблемы. Метод состоит в декомпозиции проблемы на все более простые составляющие части и дальнейшей обработке последовательности суждений лица, принимающего решения по всем сравнениям. В результате может быть выражена относительная степень (интенсивность) взаимодействия элементов иерархии. Эти суждения выражаются затем численно. Метод анализа иерархий включает процедуры синтеза множественных суждений, изучения приоритетности критериев и нахождения альтернативных решений. Следует отметить, что полученные таким образом решения являются оценками в шкале соотношений и соответствуют так называемым жестким оценкам.

Решение проблемы есть процесс поэтапного установления приоритетов. На первом этапе выявляются наиболее важные элементы проблемы, на втором – наилучший способ проверки наблюдений, испытания и оценки элементов; следующим этапом может быть выработка способа применения решения и оценка его качества. Весь процесс подвергается переосмысливанию до тех пор, пока не будет уверенности, что

процесс охватил все важные характеристики, необходимые для представления и решения проблемы. Процесс может быть проведен над последовательностью иерархий: в этом случае результаты, полученные в одной из них, используются в качестве входных данных при изучении следующей. Предложенный метод систематизирует процесс решения такой многоступенчатой задачи.

Рассмотрим основные принципы и методику проведения анализа методом анализа иерархий.

Принцип идентичности и декомпозиции предусматривает структурирование проблем в виде иерархии или сети, что является первым этапом применения метода анализа иерархий (МАИ). В наиболее элементарном виде иерархия строится с вершины (целей), через промежуточные уровни (критерии, от которых зависят последующие уровни) к самому низкому уровню (который обычно является перечнем альтернатив).

Существует несколько видов иерархий: доминантные иерархии, холларии, китайский ящик. Наиболее простой и в то же время наиболее применимой к задачам, рассматриваемым в данном разделе, является доминантная иерархия. Поэтому рассмотрим более подробно именно этот вид иерархий, хотя теория, описанная ниже, распространяется и на другие иерархические формы.

Иерархия считается полной, если каждый элемент заданного уровня функционирует как критерий для всех элементов нижестоящего уровня. В противном случае иерархия – неполная. Нетрудно понять процесс определения весов в случае неполной иерархии, так как используются приоритеты соответствующего элемента, по отношению к которому производится оценка, т. е. иерархия может быть разделена на подиерархии, имеющие общий самый верхний элемент.

После иерархического или сетевого воспроизведения проблемы возникает вопрос: как установить приоритеты критериев и оценить каждую из альтернатив по критериям, выявив самую важную из них.

В МАИ элементы задачи сравниваются попарно по отношению к их воздействию («весу», или «интенсивности») на общую для них характеристику. Проведём парные сравнения, приводящие к матричной форме – квадратной таблице.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \text{K} & a_{1n} \\ a_{21} & a_{22} & a_{23} & \text{K} & a_{2n} \\ a_{31} & a_{32} & a_{33} & \text{K} & a_{3n} \\ \text{M} & \text{M} & \text{M} & & \text{M} \\ a_{n1} & a_{n2} & a_{n3} & \text{K} & a_{nn} \end{pmatrix}$$

Эта матрица имеет свойство обратной симметричности, то есть $a_{ji} = 1/a_{ij}$.

Когда проблемы представлены иерархически матрица составляется для сравнения относительной важности критериев на втором уровне по отношению к общей цели на первом уровне. Подобные матрицы должны быть построены для попарных сравнений каждой альтернативы на третьем уровне по отношению к критериям второго уровня и так далее.

Заполнение квадратных матриц попарных сравнений выполняется по такому правилу. Если элемент E_1 преобладает над элементом E_2, то клетка матрицы, которая соответствует пересечению строки E_1 и столбца E_2, заполняется целым числом, а клетка, которая соответствует пересечению строки E_2 и столбца E_1, заполняется обратным ему числом. Если элемент E_2 преобладает над E_1, то целое число ставится в клетку, которая соответствует строке E_2 и столбцу E_1, а дробь проставляется в клетку, которая соответствует строке E_1 и столбцу E_2. Если элементы E_1 и E_2 преобладают одинаково, то в обеих позициях матрицы ставятся единицы.

Для получения каждой матрицы эксперт или лицо, принимающее решение (ЛПР), выносит $n(n-1)/2$ суждений (здесь n – порядок матрицы попарных сравнений).

Рассмотрим в общем виде пример формирования матрицы попарных сравнений.

Пусть E_1, E_2, …, E_n – множество из n элементов (альтернатив) и v_1, v_2, …, v_n – соответственно их веса, или интенсивности. Сравним попарно вес, или интенсивность каждого элемента с весом или интенсивностью любого другого элемента множества относительно общего для них свойства или цели. В этом случае матрица парных сравнений [E] имеет такой вид:

$[E] =$

	E_1	E_2	...	E_n
E_1	v_1/v_1	v_1/v_2	...	v_1/v_n
E_2	v_2/v_1	v_2/v_2	...	v_2/v_n
...	...	...	...	...
E_n	v_n/v_1	v_n/v_2	...	v_n/v_n

При проведении попарных сравнений необходимо ответить на такие вопросы: какой из двух сравниваемых элементов важнее или имеет большее влияние, какой более вероятен и какой лучше. При сравнении критериев обычно определяют, какой из критериев более важный; при сравнении альтернатив относительно критерия – какая из альтернатив лучше или более вероятна [5].

Попарные сравнения проводятся в терминах преобладания одного элемента над другим. Полученные суждения выражаются в целых числах с учётом девятибальной шкалы (см. табл. 4).

Таблица 4 – Шкала отношений (степени значимости действий)

Степень значимости	Определение	Пояснение
1	Одинаковая значимость	Два действия вносят одинаковый вклад в достижение цели
3	Некоторое преимущество значимости одного действия над другим (слабая значимость)	Существуют аргументы в пользу преимущества одного из действий, но эти аргументы недостаточно убедительны
5	Существенная или сильная значимость	Существуют надёжные данные или логические суждения для того, чтобы показать преимущество одного из действий
7	Очевидная или очень сильная значимость	Убедительное свидетельство в пользу одного действия над другим
2,4,6,8	Промежуточные значения между двумя соседними суждениями	Ситуация, когда необходимо компромиссное решение
Обратные величины приведены выше ненулевых величин	Если действию i при сравнении с действием j приписывается одно из определённых выше ненулевых чисел, то действию j при сравнении с действием i приписывается обратное значение	Если согласованность была определена при получении N числовых значений для создания матрицы

Правомерность этой шкалы доказана теоретически при сравнении со многими другими шкалами [5]. При использовании указанной шкалы ЛПР, сравнивая два объекта в смысле достижения цели, расположенной на вышестоящем уровне иерархии, необходимо поставить в соответствие этому сравнению число в интервале от 1 до 9 или обратное значение чисел. В тех случаях, когда сложно различить сколько промежуточных градаций от абсолютного до слабого преимущества или этого не нужно в конкретной задаче, может использоваться шкала с меньшим числом градаций. В нижнем пределе шкала может иметь только две оценки: 1 – объекты равнозначны; 2 – преимущество одного объекта над другим.

Из группы матриц попарных сравнений мы формируем набор локальных приоритетов, которые выражают относительное влияние множества элементов на элемент примыкающего сверху уровня. Находится относительная сила, величина, ценность, желательность или вероятность каждого отдельного объекта через решение матриц. Для этого необходимо вычислить множество собственных векторов для каждой матрицы, а затем нормализовать результат к единице. Вычисление собственных векторов – не очень сложная, однако весьма трудоёмкая задача. Для её решения наиболее простым является метод вычисления геометрического среднего. Вычислить среднегеометрическое можно путём перемножения всех элементов в каждой строке с последующим извлечением корня n-й степени

$$q_j^{(r-1)} = \sqrt[n]{(v_j^{(r)} / v_1^{(r)}) \times (v_j^{(r)} / v_2^{(r)}) \times \Lambda \times (v_j^{(r)} / v_n^{(r)})}, \quad (8)$$

где r – уровень иерархии, для матрицы которого выполняется расчёт, n – количество элементов в строке, j – порядковый номер строки.

Полученный таким образом столбец нормализуется делением каждого числа на сумму всех чисел (9).

$$\gamma_j^{(r-1)} = \frac{q_j^{(r-1)}}{\sum_{i=1}^{t_r} q_i^{(r-1)}} \quad (9)$$

Иной способ заключается в нормализации элементов каждого столбца матрицы и затем усреднения каждой строки. Таким образом, мы можем определить не только порядок приоритетов каждого отельного элемента, но и величину его приоритета.

После этого из всех нормированных значений формируются промежуточные матрицы, и выполняется «свёртка» иерархии путём перемножения промежуточной матрицы нижнего уровня на нормированный столбец верхнего уровня до определения. «Свёртка» выполняется до того момента, пока не будут получены глобальные значения степени превосходства одной альтернативы над другой.

Предложенный подход позволяет сравнить разные объекты, например, стандарты криптографических преобразований по обобщённому условному критерию и получить количественное значение оценки, определить преимущество одного над другим.

IV Результаты сравнения алгоритмов выработки ключей и транспортировки ключей стандартов ISO/IEC 15946-3, ISO/IEC 11770

Рассмотрим практические аспекты сравнения криптографических протоколов. В качестве главных целей сравнения криптографических протоколов будем рассматривать протоколы стандартов ISO/IEC 15946-3, ISO/IEC 11770. Такой выбор объясняется тем, что эти стандарты являются международными, кроме того, большинство протоколов, описанных в стандарте, практически без изменений применяются и во многих национальных стандартах, что позволяет с уверенностью говорить, о том, что рассматриваемые протоколы на настоящий момент нашли наибольшее применение в мире.

Анализ проведём для двух типов протоколов – протоколы установления общего секрета и протоколы транспортировки секретного ключа.

Кроме того, сравнение рассматриваемых протоколов проведём для трёх вариантов:

- наибольшую значимость имеют скоростные показатели криптографического протокола;
- наибольшую значимость имеют показатели активной безопасности криптографического протокола;
- наибольшую значимость имеет количество раундов криптографического протокола.

Метод иерархий предполагает наличие конечного критерия (цели) X^0 – числового значения интегрального критерия сравнения протоколов. Для определения этого критерия проводится сравнения всех критериев попарно между собой и их привязка к числовым значениям по каждому критерию для каждого протокола. Для упрощения задачи иерархический метод предполагает разделение всех простых критериев на группы критериев. В нашем случае таких групп будет три. Каждую группу представляет свой групповой критерий, при этом групповой критерий в определённой степени влияет на интегральный критерий, влияние критериев может быть различным в случае, когда при отборе протокола по интегральному критерию максимальное внимание уделяется безопасности, скорости или другим характеристиками. Соотношения между групповыми критериями для разных вариантов представлено в табл. 5 – 7.

Обозначим критерий каждой группы как критерий первого порядка: X_1^1 – активная безопасность протокола; X_2^1 – пассивная безопасность протокола; X_3^1 – скоростные показатели протокола.

Критерий каждой группы критериев содержит несколько элементарных критериев, при этом элементарный критерий в определённой степени влияет на свой групповой критерий.

Критерий X_1^1 – «активная безопасность протокола» включает в себя элементарный критерий K_{y1} – «наличие и вид ключевой аутентификации», обозначим его X_1^2; элементарный критерий K_{y2} – «наличие и вид аутентификации субъектов», обозначим его X_2^2; элементарный критерий K_{y1} – «уровень защищённости при реализации различных видов угроз при разных условиях осуществления криптоанализа

и отклонениях свойств общесистемных параметров», обозначим его X_8^2.

Критерий X_2^1 – «пассивная безопасность протокола» включает в себя элементарный критерий K_{y3} – «новизна ключей», обозначим его X_3^2; элементарный критерий K_{y4} – «управление ключами», обозначим его X_2^2; элементарный критерий K_{y6} – «криптоживучесть ключей», обозначим его X_6^2.

Критерий X_3^1 – «скоростные показатели протокола» включает в себя элементарный критерий K_{y5} – «эффективность протокола», обозначим его X_5^2; элементарный критерий K_{y7} – «скорость выполнения элементарной операции», обозначим его X_7^2.

Метод иерархий не предполагает прямого использования при расчёте интегрального критерия числовых значений. Во время подсчёта элементарных критериев числовые значения критерия по каждому из протоколов заменяются на коэффициенты преобладания в соответствии с табл. 4.

Проведём анализ вклада каждого из групповых критериев в интегральный критерий при преобладании того или иного варианта максимальной значимости.

Таблица 5 – Матрица попарных сравнений подцелей 1-го уровня при максимальной значимости скоростных показателей

X^0	X_1^1	X_2^1	X_3^1	$q_j^{(0)}$	$\gamma_j^{(0)}$
X_1^1	1	1/2	1/9	0,381	0,076
X_2^1	2/1	1	1/7	0,659	0,131
X_3^1	9/1	7/1	1	3,98	0,79

Таблица 6 – Матрица попарных сравнений подцелей 1-го уровня при максимальной значимости активной безопасности

X^0	X_1^1	X_2^1	X_3^1	$q_j^{(0)}$	$\gamma_j^{(0)}$
X_1^1	1	9/1	8/1	4,16	0,83
X_2^1	1/9	1	1/2	0,38	0,077
X_3^1	1/8	2/1	1	0,39	0,079

Таблица 7 – Матрица попарных сравнений подцелей 1-го уровня при максимальной значимости количества раундов

X^0	X_1^1	X_2^1	X_3^1	$q_j^{(0)}$	$\gamma_j^{(0)}$
X_1^1	1	9/1	9/1	4,33	0,82
X_2^1	1/9	1	1	0,48	0,09
X_3^1	1/9	1	1	0,48	0,09

Следует отметить, что вклады каждого из элементарных критериев в подцель первого уровня не зависит от выбора максимальной значимости активной безопасности, скоростных показателей или количества раундов, так как этот вклад определён уже групповыми критериями. Поэтому для всех вариантов таблицы вклада элементарных критериев в подцели первого уровня (групповые критерии) будут одинаковыми. В дальнейшем мы не будем приводить матрицы попарных сравнений и расчёты этих матриц, так как они занимают большой объём. Приведём лишь протоколы, сравнение которых проводилось, и результаты сравнения. Результаты сравнения приведены в табл. 8, 9.

Таблица 8 – Результаты сравнения протоколов согласования ключей

№	Название протокола	Максимальная значимость критерия		
		Скорость	Активная безопасность	Количество раундов
1	Неинтерактивный протокол согласования ключей типа Диффи-Хеллмана	0,138	0,075	0,142
2	Интерактивный двухпроходной протокол согласования общего секрета типа Диффи-Хеллмана	0,055	0,032	0,053
3	Интерактивный протокол согласования общего секрета типа Эль-Гамаля	0,070	0,040	0,071
4	Протокол согласования общего секрета типа Диффи-Хеллмана с двумя ключевыми парами	0,045	0,064	0,043
5	Протокол согласования общего секрета типа Диффи-Хеллмана с двумя электронными цифровыми подписями и подтверждением ключей	0,04	0,123	0,038
6	Обобщённая полная модель	0,042	0,048	0,04
7	Протокол согласования ключей типа MQV с одним проходом	0,051	0,063	0,052
8	Протокол согласования ключей типа MQV с двумя проходами	0,045	0,065	0,043
9	Протокол согласования ключей №1	0,0138	0,075	0,142
10	Протокол согласования ключей №2	0,071	0,050	0,072
11	Протокол согласования ключей №3	0,1	0,077	0,1
12	Протокол согласования ключей №4	0,0552	0,032	0,053
13	Протокол согласования ключей №5	0,0431	0,044	0,04
14	Протокол согласования ключей №6	0,0604	0,088	0,059
15	Протокол согласования ключей №7	0,043	0,123	0,042

Таблица 9 – Результаты сравнения протоколов передачи ключей

№	Название протокола	Максимальная значимость критерия		
		Скорость	Активная безопасность	Количество раундов
1	Протокол передачи ключей типа Эль-Гамаля	0,22673	0,10418	0,22966
2	Протокол передачи ключей типа Эль-Гамаля с подписью автора	0,11774	0,15329	0,11821
3	Протокол передачи ключей №1	0,22345	0,13525	0,22904
4	Протокол передачи ключей №2	0,07656	0,07842	0,07691
5	Протокол передачи ключей №3	0,07656	0,07842	0,07791
6	Протокол передачи ключей №4	0,09051	0,07569	0,08604
7	Протокол передачи ключей №5	0,08727	0,18631	0,08444
8	Протокол передачи ключей №6	0,10116	0,18844	0,09878

Выводы

Анализ литературы показал, что сейчас в мире не существует критериев и показателей для оценки криптографических протоколов. Так же проблемным является вопрос сравнения криптографических протоколов, так как зачастую характеристики протоколов не имеют числового выражения. В статье предпринята попытка проанализировать различные характеристики протоколов, построить систему критериев и оценок и сформировать математический аппарат сравнения криптографических протоколов. Показано, что метод иерархий вполне может быть использован для проведения сравнения протоколов при помощи сформулированных критериев. Предложенный математический аппарат является гибким, то есть позволяет сравнивать протоколы при различных значимостях требований и условиях применения. Проведен анализ алгоритмов стандартов ISO/IEC 15946-3, ISO/IEC 11770 для различных условий применения.

Литература: ***1.*** *И. Д. Горбенко, Д. С. Балагура. Исследование свойств и выбор параметров схем шифрования, реализованных на основе Диффи-Хеллмана протоколов. Зб. 2003. Вип. 139.* ***2.*** *Горбенко И. Д., Поляков А. А., Збитнев С. И. Протоколы – примитивы управления ключами в группах точек эллиптичексих кривых // Радиотехника: Всеукр. межвед. науч-тех. сб 2002. Вып. 126. С. 85-96.* ***3****. Горбенко І. Д., Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах. Част. 1. Криптографічний захист інформації. – Харків: ХНУРЕ, 2004. 367 с.* ***4****. J. Lopez, R. Dahab "Fast multiplication on elliptic curves over GF(2^m) without precomputation", 1999.* ***5.*** *Саати Т. Принятие решений: Метод анализа иерархий/ Пер. с англ. - М.: Радио и связь, 1993.*

УДК 681.3.06

ДЕЯКІ МЕТОДИ ЗБІЛЬШЕННЯ ШВИДКОСТІ ВИКОНАННЯ ОПЕРАЦІЙ В ГРУПАХ ТОЧОК НА ЕЛІПТИЧНИХ КРИВИХ В НОРМАЛЬНОМУ БАЗИСІ

Олена Качко, Оксана Мельникова, Дмитро Балагура
Харківський національний університет радіоелектроніки

Анотація: **Аналізуються існуючі алгоритми множення елементів у нормальному базисі. Пропонуються удосконалення алгоритму множення Ітоха і Тсуї. Проводяться практичні дослідження удосконаленої версії.**
Summary: **The being algorithms of multiplication of elements in normal basis are analyzed. The improvements for algorithm of Itoh and Tsui are proposed. The practical research of improved version are led.**
Ключові слова: **Нормальний базис, алгоритм Ітоха і Тсуї, часова складність, просторова складність.**

Вступ

В сучасному суспільстві актуальною стала задача захисту інформації, що формується, обробляється та зберігається у електронному вигляді. У багатьох випадках єдиною можливістю захистити інформацію від несанкціонованого доступу та/або модифікації є криптографічні засоби захисту інформації. Серед різновидів криптографічного захисту інформації особливе місце посідають несиметричні криптографічні системи. До таких систем відносяться криптографічні протоколи в полях та кільцях та криптографічні протоколи в групах точок еліптичних кривих. На сьогоднішній день криптографія в групах точок еліптичних кривих дістала широке поширення в багатьох системах забезпечення захисту інформації. Криптографія, що базується на перетвореннях в групах точок еліптичних кривих, може використовуватись в різних системах, до того ж вона є перспективною для систем, що реалізують інфраструктуру відкритих ключів та криптографічні додатки, що пов'язані з використанням ключових даних, які формуються у структурі відкритих ключів.

Найважливішими параметрами будь-якої криптографічної системи є її безпечність та швидкодія. На теперішній час безпека криптографічних систем, що базуються на криптоперетвореннях в групах точок еліптичних кривих, не викликає сумнівів. Тому величезні зусилля спеціалістів цієї галузі спрямовані на збільшення швидкості обчислень криптографічних перетвореннь в групі точок еліптичних кривих. В світі вже існує багато криптографічних стандартів, що закріплюють використання математичного апарату груп точок еліптичних кривих. Ці стандарти дозволяють використовувати перетворення в групі точок еліптичних кривих, що базуються на простому полі $GF(p)$, на полі розширення двійки $GF(2^m)$, причому для поля $GF(2^m)$ рекомендують використання двох типів базисів: поліноміального та нормального [1 – 4].

Кожний із цих видів та базисів має свої переваги й недоліки. Так перетворення у простому полі, найбільш прості в реалізації, в загальному випадку мають досить високу продуктивність, крім того при реалізації систем на базі таких перетворень існує можливість використання бібліотек, що розроблялись для асиметричної криптографії в полях та кільцях: систем типу RSA, Ель-Гамаля та Діффі-Хеллмана. Перетворення у двійковому вигляді (поліноміальний і нормальний базиси) мають практично таку ж продуктивність, але можуть бути ефективно реалізовані апаратними засобами. Крім того, існують перетворення в оптимальних розширених полях $GF(p^m)$, де p – досить велике просте число спеціального виду, m – невелике просте число. Перетворення над двійковими полями в оптимальному