Д. В. Матюхин (Москва, ТВП). **О некоторых свойствах схем выработки общего ключа, использующих инфраструктуру открытых ключей, в контексте разработки стандартизированных криптографических решений.**

В настоящее время отечественные разработчики средств криптографической защиты информации испытывают потребность в стандартизированном криптографическом решении (национальном стандарте и/или рекомендациях) по выработке общего ключа двумя абонентами по открытому каналу связи. Не вызывает сомнений, что такое решение должно быть реализовано в группе точек эллиптической кривой над конечным простым полем, поскольку данный математический аппарат является одним из наиболее изученных и позволяет обеспечить наилучшее на сегодняшний день сочетание уровня криптографической стойкости и быстродействия схем с открытым ключом. Также очевидно, что вариант классической схемы Диффи–Хеллмана, в котором ключевая пара хотя бы одного из абонентов является сеансовой, подходит не для всех моделей нарушителя. Поэтому среди стандартизируемых или рекомендуемых схем выработки общего ключа (ВОК) должны присутствовать схемы, использующие долговременные ключевые пары и инициатора (A), и ответчика (B), что, в свою очередь, предполагает наличие сертификатов соответствующих открытых ключей. Учитывая наметившуюся в последнее время тенденцию к гармонизации национальных и международных стандартов в области криптографической защиты информации, представляется целесообразным рассмотреть возможность использования в качестве основы для таких схем соответствующих механизмов выработки общего ключа (key agreement mechanism), определяемых международным стандартом ISO/IEC 11770-3: 2007.

В работе, представленной данным докладом, проведен сравнительный анализ указанных механизмов с точки зрения возможности их модификации, при которой долговременные открытые ключи абонентов (P_A и P_B) могут соответствовать разным эллиптическим кривым, а также с точки зрения количества пересылок и стойкости к следующим угрозам: 1) чтение назад по отношению к A (B, A и B); 2) имперсонификация при компрометации ключа (key-compromise impersonation — KCI); 3) подмена источника (unknown key-share — UKS, source-substitution).

Результаты анализа сведены в таблицу. Они позволяют сделать вывод, что среди стандартизированных на международном уровне схем выработки общего ключа, в которых абоненты используют долговременные ключи, наиболее предпочтительными для разработки отечественного стандартизированного решения с точки зрения рассмотренных свойств представляются схемы типа STS и MTI/A0.

Тип схемы	Diffie-Hellman	STS-MAC	Full Unified Model	MQV	MQV	MTI/A0
Число пересылок	0	3	2	2	3	2
Работает, если P_A и P_B на разных кривых	нет	да[1])	нет	нет	нет	да[2])
Защита от чтения назад	нет	A и B	A и B	A и B	A и B	A, B
Защита от KCI	нет	да	нет	v да	да	да
Защита от UKS	нет[3])	да	нет[3])	нет[5])	да	нет[3),4)]

где: [1]) требуется еще одна кривая, согласованная A и B; [2]) в 2011 году Н. П. Варновским и А. А. Татузовым доказана стойкость схемы в некоторой математической модели; [3]) если при получении сертификата открытого ключа нет проверки знания абонентом соответствующего секретного ключа; [4]) защиту без проверки

обеспечивает модификация с тем же количеством пересылок; [5])если абонент может получить сертификат открытого ключа в процессе ВОК.

Работа выполнена при финансовой поддержке Академии криптографии Российской Федерации.