О РАСШИРЕНИИ НАПРАВЛЕНИЙ СЕРТИФИКАЦИИ И ЭКСПЕРТИЗЫ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

О.В. Соловей, А. Л. Костевич

Научно–исследовательский институт прикладных проблем математики и информатики БГУ
Минск, Беларусь
E-mail: solovey@bsu.by, kostevich@bsu.by

В статье описываются новые направления сертификации и экспертизы средств криптографической защиты информации, возникшие в Республике Беларусь в связи с принятием новых технических правовых актов, а также вызванные проблемами совместимости информационных продуктов на базе инфраструктуры открытых ключей.

Ключевые слова: защита информации, методы испытаний, инфраструктура открытых ключей, форматы данных

Испытательная лаборатория НИИ прикладных проблем математики и информатики Учреждения Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики» (НИИ ППМИ) проводит сертификационные испытания и экспертизу средств криптографической защиты информации (СКЗИ) с 2001 года. Основными задачами испытательной лаборатории являются:

- проведение сертификационных испытаний СКЗИ на соответствие требованиям действующих в Республике Беларусь стандартов СТБ 1176.2 на процедуры выработки и проверки электронной цифровой подписи, СТБ 1176.1 на функцию хэширования, ГОСТ 28147 на алгоритм шифрования и контроля целостности;
- проведение отдельных экспертиз СКЗИ по поручениям органа по сертификации.

НОВЫЕ НАПРАВЛЕНИЯ СЕРТИФИКАЦИИ И ЭКСПЕРТИЗЫ

В связи с введением в действие профиля защиты СТБ П 34.101.27 «Информационные технологии. Методы и средства безопасности. Профиль защиты программных средств криптографической защиты информации» и для совершенствования методов сертификационных испытаний СКЗИ потребовалась доработка методик испытаний и инструментальных средств проведения испытаний.

Ранее для проведения сертификационных испытаний программных реализаций криптографических алгоритмов (далее – программ) в испытательной лаборатории в 2001 году были разработаны методики испытаний и программный комплекс автоматизации тестирования (программный комплекс «Экзаменатор»). Методики испытаний

включали проверки по анализу программной документации и исходных текстов программы, а также наборы тестов для тестирования программы.

При доработке методик в них были внесены изменения, направленные на приведение методик испытаний в соответствие с профилем защиты СТБ П 34.101.27. Для анализа программной документации в дополнение к проверкам на соответствие ЕСПД были включены проверки, отражающие специфику испытаний СКЗИ и учитывающие требования семейств ADV_IMP и ADV_HLD профиля защиты СТБ П 34.101.27. Наборы тестов были приведены в соответствие с требованиями класса ATE «Тестирование» СТБ П 34.101.27. В частности, для алгоритма СТБ 1176.2 были разработаны тесты, покрывающие тестирование алгоритма для всех уровней стойкости, а для алгоритма ГОСТ 28147 были добавлены тесты, основанные на известных математических свойствах алгоритма. К проверкам по анализу исходных текстов программы были добавлены проверки на корректность работы программы в многопоточном режиме.

С учетом опыта разработки методик испытаний программных реализаций криптографических алгоритмов СТБ 1176.2, СТБ 1176.1 и ГОСТ 28147 дополнительно были разработаны методики испытаний программных реализаций алгоритмов РД РБ 07040.1202 и СТБ П 34.101.31. Данные методики могут использоваться при экспертизе указанных алгоритмов.

В последнее время, как правило, на испытания представляются СКЗИ, в которых используются программные реализаций криптографических алгоритмов, прошедшие сертификационные испытания, и для которых требуется провести анализ корректности реализации механизмов безопасности (механизма аутентификации, механизма управления криптографическими ключами и др.). Проведении экспертизы таких СКЗИ предлагается проводить по одному из двух направлений: 1) экспертиза на соответствие заданию по безопасности, разработанного в соответствии с профилем защиты СТБ П 34.101.27; 2) экспертиза на соответствие реализации механизмов безопасности программной документации. Проведение экспертизы на соответствие заданию по безопасности согласуется с международной практикой и обеспечивает всестороннюю проверку СКЗИ, однако требует от разработчика внедрения системы качества разработки в соответствии с Общими критериями, что не всегда может быть экономически оправдано для компаний с небольшим числом сотрудников. Экспертиза на соответствие реализации механизмов безопасности программной документации может быть проведена лишь для СКЗИ с небольшим объемом исходных текстов программ, что характерно для «малофункциональных» СКЗИ. Для данного направления экспертизы требуется не только проверка корректности реализации механизмов безопасности, но и проведение экспертами анализа проектных решений, заявленных в документации. Считаем, что для «многофункциональных» СКЗИ экспертиза должна проводиться на соответствие заданию по безопасности, а для «малофункциональных» СКЗИ – на соответствие реализации механизмов безопасности программной документации.

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

В связи с широким распространением информационных продуктов и технологий на базе инфраструктуры открытых ключей (ИОК) большую актуальность приобрел вопрос совместимости продуктов различных производителей. Традиционно проблема совместимости в ИОК решается использованием стандартных форматов дан-

ных: сертификатов открытых ключей и списков отозванных сертификатов (стандарт RFC 2459, 3280, 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile»), подписанных и зашифрованных сообщений (стандарты RFC 2630, 3211, 3369 «Cryptographic Message Syntax») и др.

К сожалению, в Республике Беларусь достаточно долго отсутствовали рекомендации для разработчиков СКЗИ по использованию единых идентификаторов криптографических алгоритмов и форматов данных. Это остро поставило проблему совместимости информационных продуктов и технологий на базе ИОК различных производителей.

Переход Республики Беларусь на международные стандарты для форматов данных ИОК позволяет решить проблему совместимости. При этом требуется разработка методов оценки соответствия (экспертизы или сертификации) СКЗИ требованиям упомянутых стандартов. При разработке методов оценки соответствия следует учитывать достаточную сложность описания и реализации как самих форматов данных ИОК, так и используемой в них кодировки ASN.1. Также следует учитывать возможность использования в оцениваемых СКЗИ существующих библиотек функций, осуществляющих кодирование информации согласно ASN.1 и дальнейшее ее преобразование к форматам данных ИОК (например, Microsoft CryptoAPI). Это существенно затрудняет или делает невозможным применение методов (статического и динамического) анализа исходных текстов для оценки СКЗИ. Будем также учитывать, что преобразование информации перед или после обращения к криптографическим алгоритмам к стандартным форматам не снижает стойкости используемых криптографических алгоритмов.

Поэтому в качестве метода оценки соответствия СКЗИ требованиям стандартов на форматы данных ИОК предлагается использовать независимое функциональное тестирование компонент СКЗИ, выполняющих кодирование информации согласно ASN.1 и дальнейшее ее преобразование к форматам данных ИОК. Это в полной мере соответствует Общим критериям оценки безопасности информационных технологий по СТБ 34.101.3 (семейство ATE_IND «Независимое тестирование») и принятой международной практике (программа NIST PKI Testing по тестированию компонент ИОК [1]). Реализация предлагаемого подхода требует разработки набора тестовых данных, в частности сертификатов, списков отозванных сертификатов, подписанных сообщений, предусматривающих различные практические ситуации: отозванные сертификаты, файлы с нарушенной целостностью, просроченные сертификаты и др. Оценка соответствия будет заключаться в проверке корректности результатов обработки в СКЗИ подготовленного набора данных.

ЛИТЕРАТУРА

1. Public Key Interoperability Public Key Interoperability Test Suite (PKITS) Certification Path Validation // NIST, 2004. Avail. at http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/PKITS.pdf