ПРОБЛЕМА ВЫБОРА МЕТРИК ПРОВЕРКИ КОРРЕКТНОСТИ ВСТРАИВАНИЯ ПРОГРАММНЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

И.А. НЕЗДОЙМИНОВ

При разработке программного обеспечения средств криптографической защиты информации очень большое внимание уделяется правильности реализации криптографических алгоритмов. Как правило, программные средства криптографической защиты информации сертифицируются уполномоченными государственными органами. В то же время, как показывает практика, большинство уязвимостей средств криптографической защиты информации появляются из-за неверного встраивания в конечный продукт.

Таким образом, проблема проверки корректности встраивания остро стоит при проведении сертификационных испытаний и нуждается в исследовании, формализации требований и введении критериев оценки.

Исследования корректности встраивания программных средств криптографической защиты информации является трудоемким и долгим процессом. При сертификации обычно используется экспертный метод

тестирования, что требует привлечения опытных и дорогостоящих специалистов в области криптографии и разработки программного обеспечения для исследования исходных кодов.

Особое внимание необходимо уделить проблеме выбора требований для определения основных «проблемных мест». На основании выбранных требований необходимо разработать критерии оценки и метрики.

В докладе описаны проблемы выбора требований и метрик, предложены методы проверки корректности встраивания программных средств криптографической защиты информации в конечный продукт. Исследования проводятся на существующих в РБ программных продуктах, использующих программные средства криптографической защиты информации. Работа продолжается в части разработки экспертных и расчетных методов тестирования.