

ОПЫТ ИСПОЛЬЗОВАНИЯ СВОБОДНО РАСПРОСТРАНЯЕМЫХ РЕШЕНИЙ ДЛЯ АНАЛИЗА ПРОГРАММНОГО КОДА НА ОТСУТСТВИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

А.А. ПЕРЕПЁЛКИН

Существующие на рынке информационных технологий (ИТ) автоматизированные системы анализа и поиска недеklarированных возможностей (НДВ) в программных и программно-аппаратных продуктах построены по специализированным методикам оценки, которые применяются в аккредитованных испытательных лабораториях, при оценке специализированной продукции по уровню контроля на НДВ. Однако, при создании продуктов ИТ, предназначенных для защиты информации, имеющей ценность для собственника системы, разработчик и оценщик должны убедиться в отсутствии в них НДВ.

При создании программных и аппаратно-программных продуктов защиты ИТ часто оказывается удобным использование уже имеющихся наработок и программных решений, существующих в фондах разработчиков так называемых «открытых кодов». Зачастую наследование программного кода происходит не только в виде отдельно взятых библиотек, но и в виде решений, содержащих миллионы строк кода программного или микропрограммного кода. В подобном случае анализ такого продукта становится сложным, так как открытый код, как правило, плохо документирован. Вместе с возможными ошибками в родительском проекте в новый продукт может переходить и масса НДВ. Большинство из них недеklarированно по халатности разработчика, но существует и вероятность наследования злонамеренно вставленных НДВ, которые, как правило, структурно организованы так, чтобы максимально скрыть себя.

На сегодняшний день фонд свободно распространяемых программных средств располагает широким спектром инструментария, позволяющим решать задачи анализа программных средств защиты информации для выявления НДВ. Этот доклад содержит краткое описание и методы применения подобных средств.