М. А. Стюгин, *канд. техн. наук, Сибирский федеральный университет, г. Красноярск, styugin@gmail.com*

Повышение защищенности информационных систем на основе технологий защиты от исследования[1]

В данной работе приводится методология повышения безопасности информационных систем на основе технических решений по защите информационных систем от внешнего исследования. В целях обобщения разработан алгоритм получения защищенной от исследования системы путем использования методов размывания и технологий движущейся цели. Разработан метод оценки изменения уровня защищенности при применении указанных методов, на основе которого получены количественные оценки эффективности предложенных решений.

Ключевые слова: защита информации, защита от исследования, технология движущейся цели, размывание параметров систем, оценка рисков.

Введение

В настоящей статье представлены существенная проблема безопасности современных информационных систем и способ ее решения на основе группы методов и технологий, полученных в течение последних пяти лет и изложенных в работах [1–17].

Анализ информационных процессов с точки зрения безопасности необходимо провести на уровне формализованных моделей. Формализованные модели и доказательства их безопасности строятся с учетом предположений и ограничений, накладываемых на модель. Такие условия и ограничения можно найти в формальном анализе криптографических информационных систем [18], моделях политик управления доступом [19], анализе информационных потоков [20] и других дисциплинах. Однако повсеместное усложнение информационных систем не позволяет провести их полную формализацию и удостовериться в адекватности реализации формализованных моделей на практике.

Для примера рассмотрим абсолютно секретный шифр Вернама (one-time pad) [18]. На уровне формальной модели доказано, что шифртекст не раскрывает абсолютно никакой информации относительно исходного текста. Однако на уровне реализации шифр-система может иметь множество уязвимостей. Например, это могут быть утечки по побочным каналам, в результате чего злоумышленник может измерить импульсные сигналы и восстановить ключ шифрования или внутренние параметры генератора псевдослучайных чисел, используемого для его получения. Возможно, администратор информационной системы самостоятельно передаст исходное сообщение злоумышленнику или злоумышленник внедрит собственный ключ шифрования при помощи удаленной инъекции

[1] Работа выполнена при поддержке гранта Президента Российской Федерации МК-5025.2016.9 и гранта РФФИ проект № 16-29-09456 офи_м.