

Испытания и контроль программных ресурсов

Алексей Марков, зам. начальника аттестационного центра и центра сертификации МО РФ,
Сергей Щербина, зам. начальника отдела МО РФ

Уязвимость программных ресурсов (ПР) определена объективными причинами:

- чрезвычайной сложностью программных средств (ПС);
- динамичностью развития технологий;
- легкостью модификации кода.

Основные угрозы ПР

К недостаткам мер по устранению угроз следует отнести отсутствие между ними внутреннего единства. Так, процедуры администрирования не связаны с результатами сертификации, которая может и не производиться (если нет исходных кодов). Поэтому необходим подход, объединяющий испытания и контроль ПР.

В таблице представлены основные реализационные и эксплуатационные угрозы ПР.

Испытания по требованиям безопасности

Сертификация

Имеются 2 основных вида сертификационных испытаний ПС:

- на соответствие классу защищенности информации от несанкционированного доступа (НСД);
- на отсутствие недеklarированных возможностей (НДВ).

Недостатком испытаний первого вида является отставание нормативной базы. Согласно руководящим документам (РД) Гостехкомиссии РФ, под понятие "средства защиты информации" подпадают только комплексные средства защиты от несанкционированного доступа и межсетевые экраны (МЭ). Что делать со средствами VPN, IDS, антивирусами и т.д. – пока не ясно.

Устранение указанных недостатков возможно в случае апро-

бации ГОСТа 15408-02 и сертификации профилей защиты (по аналогии с РД). Однако вопрос, сократит ли сроки испытаний применение нового стандарта (879 страниц в оригинале), остается дискуссионным.

Для испытаний ПР на отсутствие НДВ имеется РД Гостехкомиссии РФ, определяющий формирование и проверку маршрутов программ. Данный подход эффективен для структурно несложного программного обеспечения. Для больших комплексов использование его проблематично. К примеру, мистер Майерс 30 лет назад демонстрировал программу из 100 строк, число маршрутов которой больше числа атомов во Вселенной. Остается надеяться, что сертифицируемая Windows 2003 (50 млн операторов) не относится к подобным программам.

Аттестация

Аттестация необходима для тех объектов информатизации, где обрабатываются сведения, представляющие собой государственную тайну.

Недостатком аттестации остается то, что в ней декларируется неизменность условий функционирования, которые с точки зрения безопасности меняются с появлением очередной уязвимости (а таких для корпоративной сети может быть на практике до 1500 в год!).

Специальные проверки

На сертификацию принимается ПО, разработанное юридическим лицом, зарегистрированным на территории Российской Федерации, которое имеет соответствующие лицензии и права. На программное обеспечение должна быть со-

ставлена документация, в том числе исходные тексты программ. Что делать с программным ресурсом, для которого по каким-то причинам сертификацию проводить нельзя? Об этом законодательство умалчивает.

ПРЕДЛАГАЕТСЯ разработать систему спецпроверок программных ресурсов на отсутствие ПЗ (по аналогии с аппаратными средствами).

Назрела необходимость в построении единой системы оценки и контроля безопасности программных ресурсов. При этом основными направлениями должны быть:

- 1) совершенствование нормативной базы испытаний ПР с учетом требований по контролю безопасности, а также угроз ПР;
- 2) введение системы спецпроверок ПР;
- 3) разработка новых подходов к сертификации ПР на отсутствие недеklarированных возможностей (программных закладок). ●

Действенной мерой по оценке безопасности ПР является сертификация, но ее возможности ограничены нормативно-техническими рамками. Требования к контролю безопасности ПР отсутствуют или сводятся к антивирусной проверке. Предлагается рассмотреть проблему оценки и контроля безопасности ПР в комплексе на этапах внедрения и эксплуатации.

Угрозы	Меры по устранению	Типовые методы
Наличие программных закладок (явно идентифицируемых как злонамеренные)	Сертификация СВТ (аттестация ОИ)	Эвристические методы
Наличие недеklarированных возможностей	Сертификация СВТ (аттестация ОИ)	Структурный анализ
Ошибки политики безопасности	Сертификация АС, аттестация ОИ	Анализ рисков
Нарушения конфигурирования	Администрирование	Анализ конфигураций и сканирование
Нарушения целостности среды (наличие несанкционированных программ)	Администрирование	Антивирусный контроль
Наличие опубликованных уязвимостей	Администрирование	Отслеживание уязвимостей (bugtracking)