УДК 621.3

И.Г. Дровникова[1], В.П. Алферов[2], С.А. Змеев[2], Е.А. Рогозин[2]
([1]Воронежский институт МВД России, [2]Воронежский Государственный Технический Университет; e-mail: idrovnikova@mail.ru)

АНАЛИЗ ТРЕБОВАНИЙ ГОСТ Р ИСО/МЭК 15408-2002 ДЛЯ ВЫЯВЛЕНИЯ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Проведён сравнительный анализ требований международного стандарта ГОСТ Р ИСО/МЭК 15408-2002 и руководящего документа ФСТЭК №114 от 4 июня 1999 г., а также Государственных стандартов ЕСПД и ЕСКД. Сделан вывод о возможности применения стандарта для выявления недекларированных возможностей программного обеспечения.

Ключевые слова: недекларированные возможности (НДВ) программного обеспечения, автоматизированная система, защита информации.

I.G. Drovnikova, V.P. Alferov, S.A. Zmeev, E.A. Rogozin

ANALYSIS OF REQUIREMENTS OF GOST R ISO / IEC 15408-2002 TO REVEAL UNDECLARED FEATURES SOFTWARE

A comparative analysis of the requirements of international standard GOST ISO / IEC 15408-2002 and guidance document FSTEC № 114 of June 4 1999 y., as well as State standards ESPD and ESKD. The conclusion about the possibility of applying a standard for identifying undeclared software features.

Key words: undeclared software features, automated system, data protection.

Статья поступила в редакцию Интернет-журнала 11 марта 2014 г.

Одной из современных тенденций защиты информации является переход к использованию международного стандарта ГОСТ Р ИСО/МЭК 15408-2002 "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий". В этом стандарте отказались от концепции фиксированного набора классов защищенности. Место класса в ***общероссийском классификаторе (ОК)*** занял ***профиль защиты (ПЗ)***, а за термином "класс" закреплено новое значение – набор функциональных или гарантийных требований, охватывающих те или иные задачи обеспечения безопасности.

Из требований классов составляются ПЗ, конкретные виды которых в новом стандарте не рассматриваются. Даются только общие правила их составления и оценки. Кроме ПЗ, предназначенного для оценки требований безопасности независимо от реализации информационного продукта или системы, для оценки конкретных изделий в ОК вводится близкое ПЗ понятие ***"цель безопасности" (ЦБ)*** или техническое задание по безопасности. При использовании ОК, а также нормативных документов, разработанных в их развитие, жизненный цикл ***автоматизированных систем (АС)*** принят состоящим из четырех стадий: разработка / интеграция, установка, эксплуатация системы и модификация. Меры безопасности автоматизированной системы должны подвергаться оценке в течение всего жизненного цикла системы.

На стадии разработки/интеграции первым действием по обеспечению ***безопасности информации (БИ)*** должна быть идентификация рисков для АС. Риски, считающиеся неприемлемыми, должны уменьшаться или устраняться средствами обеспечения БИ, интегрированными в систему. Следом за оценкой риска и идентификацией рисков, которые должны быть устранены, доверенное должностное лицо организации, а именно аттестующее лицо, должно рассмотреть предполагаемые остаточные риски, общее количество имеющихся остаточных рисков и подтвердить, что они являются приемлемыми.

После этого проектируется автоматизированная система с использованием программных и аппаратных изделий, физических мер, коммерческих программ и технических мер безопасности. Проект автоматизированной системы должен быть записан в ***задание по безопасности (ЗБС)***. В ЗБС содержится описание требований по безопасности, включая риски, которым надо противодействовать, и цели безопасности, которые необходимо реализовать с использованием технических и эксплуатационных мер безопасности.

Цели безопасности системы конкретизируются в перечне технических и эксплуатационных мер обеспечения безопасности. Для корректности в ЗБС необходимо обозначать цели безопасности, которые определяют все риски, идентифицированные как неприемлемые. В ЗБС должны обозначаться требования по безопасности, полностью удовлетворяющие целям безопасности без каких-либо дополнений.

В проектной документации АС должны быть определены конкретные контрмеры безопасности самой автоматизированной системы, отвечающие всем требованиям по безопасности, определенным в ЗБС. Этими контрмерами могут быть функции безопасности, оборудование, процедуры или правила. Контрмеры безопасности в системе должны адекватно контролироваться, управляться и использоваться. Их реализация должна контролироваться посредством тестирования системы или проверки документации. Функционирование контрмер безопасности должно быть адекватно описано в руководстве.

В отечественной нормативной документации предусмотрено проведение контроля отсутствия недекларированных возможностей [1] на этапе сертификационных испытаний. Данным документом вводится ряд проверок, обязательно выполняемых при проведении сертификационных испытаний.

Отказ от руководящего документа [1] и использование вместо него ОК делают актуальной задачу сравнительного анализа руководящего документа ФСТЭК [1] и ОК.

Требования, предъявляемые к составу и содержанию документации, представляемой заявителем для проведения испытаний ***программного обеспечения систем защиты информации (ПО СЗИ)***, представленные в РД НДВ, соответствуют требованиям к составу и содержанию документации, содержащихся в ОК (Класс FDV. Разработка).

В частности, содержание документа "Спецификация (ГОСТ 19.202-78)" соответствует семейству класса ADV_FSP – "Функциональная спецификация". Содержание документа "Описание программы (ГОСТ 19.402-78)" соответствует содержанию семейств класса ADV_FSP – "Функциональная спецификация", ADV_IMP – "Представление реализации", ADV_SPM – "Моделирование политики безопасности". Содержание документа "Описание применения (ГОСТ 19.502-78)" соответствует содержанию семейств класса ADV_IMP – "Представление реализации" и ADV_SPM – "Моделирование политики безопасности". Содержание документа "Пояснительная записка (ГОСТ 19.404-79)" соответствует содержанию ADV_HL – "Проект верхнего уровня" и ADV_SPM – "Моделирование политики безопасности". Содержание документа "Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)" соответствует содержанию семейств класса ADV_IMP – "Представление реализации".

Таким образом, требования ОК в части состава и содержания документации, представляемой заявителем для проведения испытаний ПО СЗИ, полностью соответствует требованиям РД НДВ. Применение ОК при проведении сертификационных испытаний в части требований к составу и содержанию документации, представляемой для испытаний, эквивалентно применению РД НДВ.

Требования к содержанию испытаний ПО СЗИ, предъявляемые ОК, соответствуют требованиям к содержанию испытаний, предъявляемых РД НДВ, частично. В частности, целью семейства класса ATE_DPT "Глубина" ОК является противостояние риску пропуска ошибки при разработке ***объекта оценки (ОО)***. Дополнительно компоненты этого семейства позволяют с большей вероятностью обнаружить любой внесенный злонамеренный код, особенно потому, что тестирование в большей степени касается внутренней структуры систем безопасности объектов.

Целевым назначением семейства класса ATE_DPT "Глубина" является получение гарантированной оценки отсутствия ошибок в программном коде ПО СЗИ и отчасти гарантированной оценке отсутствия недекларированных возможностей. По цели и содержанию семейства класса ATE_DPT соответствует ГОСТу 28195-89 "Оценка качества программных средств. Общие положения" не применяемому при сертификационных испытаниях. Однако целью требования доверия семейства класса ATE_DPT.3 – Тестирование на уровне реализации ОК является обеспечение высокоуровневого описания внутренних действий ФБО.

Тестирование на уровне подсистем для демонстрации наличия любых недостатков обеспечивает доверие, что подсистемы ФБО были правильно реализованы. Модули ФБО обеспечивают описание внутренних действий ФБО. Тестирование на уровне модулей для демонстрации наличия любых недостатков обеспечивает доверие, что модули ФБО были правильно реализованы. Представление реализации ФБО обеспечивает детализированное описание внутренних действий ФБО.

Тестирование на уровне реализации для демонстрации наличия любых недостатков обеспечивает доверие, что реализация ФБО была выполнена правильно. Таким образом, требования доверия семейства класса ATE_DPT.3 – Тестирование на уровне реализации ОК можно интерпритировать как требование низкоуровневой верификации правильности выполнения функций безопасности. При этом подрозумевается также и обнаружение НДВ. Однако применение данного требования доверия при проведении сертификационных испытаний потребует уточнения механизмов контроля исходного состояния ПО, конкретизации технологии статического и динамического анализа исходных текстов программ.

В частности необходимо детализировать понятие правильности реализации модулей ФБО до связей функциональных объектов по управлению, связей функциональных объектов по информации, заданных конструкций в исходных текстах, маршрутов выполнения функциональных объектов.

Также необходимо предусмотреть технологию контроля соответствия исходных текстов ПО его объектному (загрузочному) коду и анализа алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т.п., построенных по исходным текстам контролируемого ПО.

В части динамического анализа исходных текстов программ ОК имеют требование семейства класса ATE_COV – Покрытие, частично соответствующее требованию сопоставления фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа. При этом для применения ОК при проведении сертификационных испытаний контроля выполнения функциональных объектов необходимо введение нового требования семейства класса в рамках документа, уточняющего ОК, или формулировки данного требования при формулировании задания по безопасности.

Таким образом, в части требований к содержанию испытаний, предъявляемых РД, НДВ ОК соответствуют частично. Формулировка основных видов испытаний, проводимых при проведении сертификации ПО СЗИ по РД, НДВ в ОК в прямой постановке отсутствует. В этой связи применение ОК невозможно без существенного уточнения и доработки в части расширения понятия "правильности выполнения модулей", введения новых требований доверия семейств классов. Также необходимо отметить несоответствие уровней контроля НДВ, соответствующего используемым в России уровням конфиденциальности информации и оценочных уровней доверия ОК.

Исходя из сказанного, применение ОК для сертификационных испытаний, проводимых в соответствии с РД НДВ, в части требований к составу и содержанию документации, представляемой заявителем для проведения испытаний, эквивалентно РД НДВ. Применение ОК для сертификационных испытаний, проводимых в соответствии с РД НДВ, в части требований к содержанию испытаний, потребует существенной доработки и уточнения данного документа для учёта более содержательных требований РД НДВ.

Литература

1. Руководящий документ "Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей". Утверждён приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

2. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий.