Новая редакция Методики выявления уязвимостей и недекларированных возможностей в программном обеспечении. *Версия 3.0*

Дмитрий Пономарев

С благодарностью за вклад в общее Дело:

- В. С. Лютикову, Д. Н. Шевцову, И. С. Гефнер и коллективу сотрудников 2 управления ФСТЭК России
- В. А. Падаряну, А. В. Хорошилову и коллективу ИСП РАН
- А. В. Кузнецову и коллективу НТЦ «Фобос-НТ»
- рабочей группе по созданию ГОСТ «Композиционный анализ программного обеспечения» и ряду других заинтересованных инженеров-экспертов
- студентам ФСТЭК-групп кафедры ИУ10 МГТУ им. Н. Э. Баумана

Задачи, подлежащие решению (выборка):

- добиться консистентности текста с текстами ГОСТов, инф. писем, иных документов
- усилить акцент на «РБПО у разработчика», при этом конкретизировать задачи ИЛ
- ввести требования к номенклатуре, качеству, детализации материалов сертификационных испытаний
- расширить, конкретизировать методологию определения и нотирования поверхности атаки
- актуализировать требования к видам исследований, удалить «артефакты» прошлых версий
- стандартизовать работу со сторонними компонентами - Композиционный анализ и Центр исследований безопасности системного ПО
- упростить алгоритм работы с потенциальными и актуальными уязвимостями
- добиться атомарности требований и внутренней консистентности текста
- ввести требование наличия исходных кодов в т. ч. для испытаний по 6 уровню контроля

Важная информация

Дальнейшие слайды не являются цитированием утвержденного и введенного в действие нормативно-правового документа

Приведенные выдержки текста отражают текущий статус дискуссии авторов по освещаемым вопросам и могут быть скорректированы в финальной редакции

Приведенные выдержки текста затрагивают вопросы испытаний и исследований по 6-4 уровню контроля

1.1 Общие положения

Методика определяет требования к составу и содержанию исследований по выявлению уязвимостей и недекларированных возможностей (далее – НДВ)
в общесистемном и прикладном программном обеспечении (далее – объект оценки, ОО), рассчитанного на выполнение на процессорных архитектурах общего назначения, как входящего в состав программно-аппаратного средства защиты информации, так и работающего самостоятельно

1.2 Общие положения

Методика определяет состав исходных данных, предоставляемых разработчиком ОО, включая результаты реализации процессов жизненного цикла программного обеспечения в соответствии с Требованиями Доверия, ГОСТ Р 56939 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (далее – ГОСТ РБПО) и иных национальных стандартов в области разработки безопасного программного обеспечения

1.3 Общие положения

Методика определяет требования к подготовке исследовательского стенда и проведению исследований, проводимых испытательными лабораториями и разработчиками (далее – экспертами) в рамках сертификационных испытаний программных, программно-аппаратных средств защиты информации и защищенных программных, программно-технических средств, а также при внесении изменений в ранее сертифицированные средства

2.1 Общие требования к проведению исследований ВУ и НДВ

К недостаткам архитектуры относятся уязвимости архитектуры и потенциально опасные функциональные возможности, например, заведомо избыточные внешние интерфейсы или избыточные функции сторонних компонентов программного обеспечения

2.2 Общие требования к проведению исследований ВУ и НДВ

Разработчик ОО предоставляет эксперту следующие исходные данные:

...

исходный код ОО

2.3 Общие требования к проведению исследований ВУ и НДВ

Разработчик ОО предоставляет эксперту следующие исходные данные:
…
перечень программных компонентов (далее – ППК), содержащий информацию о сторонних программных компонентах ОО в соответствии с уровнем контроля, объем и форма представления ППК должны отвечать требованиям, приведенным в Приложении 1

2.4 Общие требования к проведению исследований ВУ и НДВ

Разработчик ОО предоставляет эксперту следующие исходные данные:

…

сведения о прохождении программными компонентами сертификационных испытаний, в случае включения в состав ОО компонентов из состава ранее сертифицированных по равному или более высокому уровню контроля дистрибутивов (например, операционной системы) – при включении в состав ОО компонентов без проведения статического и динамического анализа; сведения должны быть представлены в формате и объеме, позволяющем эксперту выполнить оценку, например:

– документ и пункт в эксплуатационной документации сертифицированного дистрибутива (например, комплектность поставки в формуляре), содержащий упоминание компонента

…

подготовленные разработчиком ОО планы статического анализа, тестирования модулей, фаззинг-тестирования

2.5 Общие требования к проведению исследований ВУ и НДВ

В случае, если разработчик ОО заявляет об отсутствии возможности реализации угроз безопасности для некоторого подмножества выявленных актуальных недостатков ОО, т.е. оценивает их как неактуальные, эксперт практически подтверждает возможность реализации угроз безопасности на испытательном стенде

Достаточно подтверждения экспертом возможности реализации угроз в отношении одного недостатка безопасности из числа тех, которые разработчик отнес к неактуальным, для того, чтобы трактовать оценки разработчика об отсутствии возможности реализации угроз не соответствующими действительности. Все оспариваемые разработчиком недостатки оцениваются как актуальные и подлежат устранению

2.6 Общие требования к проведению исследований ВУ и НДВ

Не требуется фиксировать значения контрольных сумм дистрибутива, исполняемых файлов и файлов исходных кодов (в соответствии с уровнем контроля) в документации и акте отбора образцов ОО до момента успешного завершения испытаний ОО

Дистрибутив ОО, подвергаемый испытаниям, считается промежуточным (не эталонным) до момента успешного завершения испытаний ОО

Предоставление эталонного дистрибутива и соответствующих ему зафиксированных значений контрольных сумм в составе документации ОО эксперту, а также акта отбора образцов ОО, в орган по сертификации (если применимо) и ФСТЭК России не требуется до момента успешного завершения испытаний ОО

2.7 Общие требования к проведению исследований ВУ и НДВ

Эксперт оценивает представленные разработчиком ОО результаты анализа ОО, проводимого в соответствии с Требованиями Доверия, ГОСТ РБПО и иных национальных стандартов в области разработки безопасного ПО в целях использования в испытаниях ОО результатов, полученных разработчиком

2.8 Общие требования к проведению исследований ВУ и НДВ

Для подтверждения всех видов инструментальных исследований ОО, в материалах испытаний ОО должны быть представлены технические результаты выполненных исследований, а именно: файлы конфигураций и журналы (логи) запуска инструментов анализа, журналы (логи) работы с результатами анализа, разметка результатов анализа, скриншоты и т. п

Каждое размеченное предупреждение должно быть снабжено комментарием, поясняющим принятое решение. Комментарий должен быть достаточен, чтобы другой участник процессов сертификационных испытаний мог понять основания для принятого решения без проведения тщательного анализа исходного кода ОО. Формулировка пояснений общего вида, таких как «Не эксплуатируемо», «Не несёт угроз безопасности информации», «Не применимо» и т. п., а также применение единообразной групповой разметки общего вида в отношении не полностью идентичных причин срабатывания анализатора, не допускается и расценивается как некачественно выполненная разметка

3.1.1 Анализ документации и иных исходных данных

В общем случае в поверхность атаки должны входить:
- подпрограммы (функции), реализующие интерфейсы, которые непосредственно доступны потенциальному нарушителю
- подпрограммы (функции) ПО, которые не могут быть непосредственно вызваны потенциальным нарушителем через доступные ему интерфейсы, но их входные данные потенциальный нарушитель способен гарантированно сформировать определенным образом

К интерфейсам ОО, непосредственно доступным для атаки потенциальным нарушителям, следует относить все интерфейсы всех режимов безопасного функционирования ОО, перечисленные в документации ОО, для которых одновременно выполняются следующие условия...

3.1.2 Анализ документации и иных исходных данных

Модельный пример анализа поверхности атаки приведен в Приложении 2

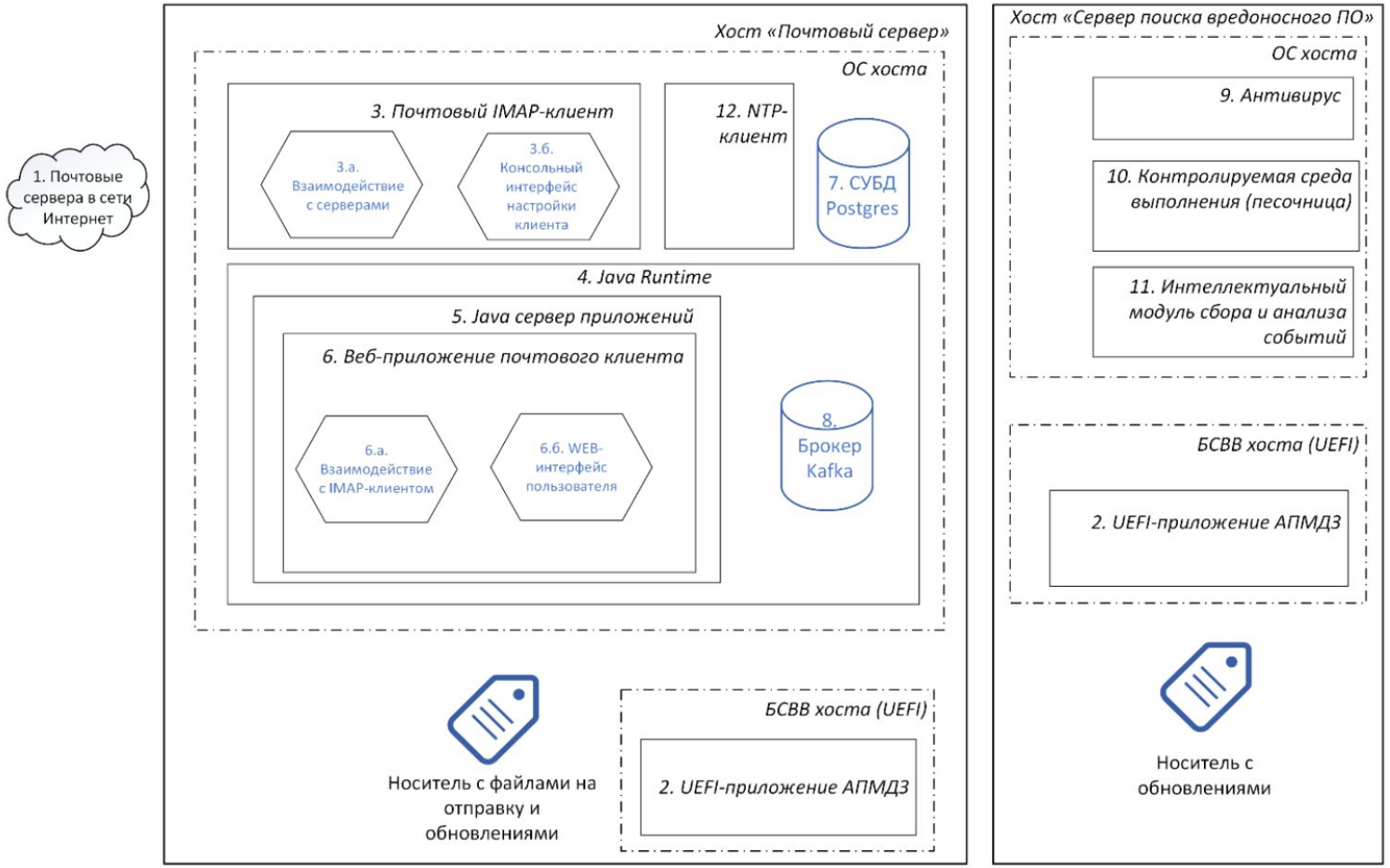

Рисунок П.1 – Схема архитектуры модельного примера

3.1.3 Анализ документации и иных исходных данных

Эксперт проверяет, что разработчик ОО выделил в составе подлежащих анализу модулей участки кода, взаимодействующие с данными, поступающими от потенциального нарушителя (парсеры, анализаторы; в том числе в составе кода веб-приложений), и имеющие высокую сложность, сформировал на их основе синтетические цели для фаззинг-тестирования

Достаточность состава выделенных целей определяется экспертом непосредственно в ходе проведения исследований ДАО.2 с фиксацией выделенных целей в протоколах испытаний, без требования внесения изменений в методику испытаний

3.1.4 Анализ документации и иных исходных данных

Эксперт проверяет, что для определения поверхности атаки разработчиком ОО применялись инструментальные средства. Сам эксперт при проведении анализа поверхности атаки ОО также должен использовать инструментальные средства определения поверхности атаки

3.1.5 Анализ документации и иных исходных данных

Эксперт описывает в методике (протоколе) испытаний поверхность атаки в графической нотации, в объеме сущностей не меньшем чем:

а) подсистемы;

б) модули, входящие в указанные подсистемы с указанием используемых языков программирования

в) реализованные модулями интерфейсы, доступные потенциальному нарушителю (внешний нарушитель до 4 УД включительно – непосредственно доступные интерфейсы...).

При наличии в ОО также в описание включаются:

г) веб-платформы (веб-приложения) – требуется отобразить соответствующие подсистемы и модули, их реализующие

д) интерпретаторы и среды выполнения кода с управляемой памятью, если исполняемый ими код реализует функции безопасности средства защиты информации – требуется отобразить подсистемы и модули, их реализующие с указанием используемого языка программирования

Для подготовки описания рекомендуется использовать нотацию, представленную в Приложении 3

3.2.1 Подготовка исследовательского стенда

Эксперт формирует перечень сред выполнения динамических исследований ОО, предписанных разделами КАО.2, ДАО.1, ДАО.3 настоящей Методики и методикой функционального тестирования ОО, включающий не менее чем одного представителя для каждого семейства сред функционирования

Отнесение к семейству среды функционирования определяется парой характеристик: семейство ОС, система управления пакетами

3.2.2 Подготовка исследовательского стенда

Эксперт выполняет контролируемую сборку дистрибутивов ОО с целью выявления и устранения:

– обращений сборочной среды к недоверенным репозиториям исходных кодов

– использования в сборочном процессе не подвергавшихся требуемым видам анализа версий исходных кодов

– включения в состав дистрибутива исполняемых файлов, не собираемых разработчиком из исходных кодов

До момента устранения всех недостатков безопасности и успешного прохождения всех видов исследований дистрибутив ОО рассматривается как промежуточный дистрибутив ОО; после – как эталонный дистрибутив ОО

3.2.3 Подготовка исследовательского стенда

Эксперт проводит сравнение контрольных сумм дистрибутива ОО и исполняемых файлов установленного ОО с контрольными суммами, зафиксированными в документации ОО. Контрольные суммы должны быть рассчитаны в соответствии с ГОСТ 34.11-2012 (алгоритм «Стрибог»)

Контрольное суммирование требуется выполнять средствами сертифицированной ОС либо сертифицированным средством контрольного суммирования

Проведение исследований по выявлению уязвимостей и недекларированных возможностей

в силу ограниченности времени доклада далее успеем рассмотреть ~20% от значимых нововведений в Методики версии 3.0

4.1 Проведение исследований по выявлению уязвимостей и недекларированных возможностей

Анализ архитектуры ОО включает:

а) анализ архитектуры ОО статическими методами (КАО.1)

б) анализ архитектуры ОО динамическими методами (КАО.2)

4.2 Проведение исследований по выявлению уязвимостей и недекларированных возможностей

...если разработчик выполняет работы в Центре исследований безопасности системного ПО (далее – Центр исследований), то допускается использовать результаты Центра исследований для сертификации ОО: методики проведения статического анализа и готовую разметку результатов статического анализа программных компонент с открытым исходным кодом

Эксперт проверяет, что статический анализ в отношении таких компонент ОО выполнялся разработчиком ОО в соответствии с методикой Центра исследований

Эксперт проверяет, что для предупреждений, полученных для таких компонент и не входящих в состав разметки предупреждений Центра исследований выполнена разметка в соответствии с требованиями Центра исследований

В отношении этих размеченных предупреждений выполняется выборочная проверка...

Важно - в отношении фаззинг-тестирования аналогичные по сути требования !

4.3 Проведение исследований по выявлению уязвимостей и недекларированных возможностей

Если предоставленные разработчиком ОО исходные данные отвечают требованиям (пп. 4.2.3.1. - 4.2.3.3. Методики), то эксперт проводит выборочную проверку разметки результатов статического анализа из состава исходных данных

Проверка выполняется в отношении контрольной выборки предупреждений, составленной из различных типов предупреждений и для различных модулей из числа подвергавшихся статическому анализу

Для каждого из использованных статических анализаторов суммарный размер контрольной выборки должен быть не менее чем 50 предупреждений

Для каждого программного модуля (программного пакета) из состава ОО в состав контрольной выборки включается не менее 5 предупреждений

Важно - в отношении фаззинг-тестирования аналогичные по сути требования !

4.4 Проведение исследований по выявлению уязвимостей и недекларированных возможностей

При оценке исходных данных эксперт проверяет, что используемый разработчиком ОО статический анализатор отвечает требованиям ГОСТ Р 71207-2024

Благодарим за внимание!

Встреча РБПО-сообщества ФСТЭК России и ИСП РАН на ТБ Форум **уже завтра!**

Информационные ресурсы РБПО-сообщества ФСТЭК России и ИСП РАН в **Телеграм**