ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, СЕТЬ ИНТЕРНЕТ

Научная статья

УДК 006.91 + 346.544.4

DOI: 10.36535/0236-1914-2022-07-1

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ТРАНСПОРТНЫХ СИСТЕМ ПРИ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЯХ

Лозовецкий Вячеслав Владимирович
(Московский Государственный Технический Университет им. Н.Э. Баумана, Мытищинский филиал)
lozovetsky@mail.ru,

Титов Михаил Юрьевич
(МИРЭА - Российский Технологический Университет)
mtitov_u@list.ru,

Губсков Юрий Анатольевич
(Институт автоматики и информационных технологий, ТГТУ)
gubtambov@yandex.ru

Аннотация. *Предлагаются способы, методы и средства для проведения сертификации в информационных системах транспортных сетей с целью выбора подходов и инструментария для работы в нестандартных ситуациях в условиях постоянно меняющейся нормативно-методической базы. Рассматриваемый вид сертификации ограничивается методами и методиками анализа уязвимостей и не декларированных возможностей и предназначен для исследования программного- и программно-аппаратного обеспечения. Представлены подходы к сертификационным испытаниям с использованием инструментария собственной разработки, который позволяет выделить основные параметры, необходимые для сборки программного обеспечения и его исследования, и производить синтаксический анализ программного обеспечения, написанного на различных языках программирования.*

Ключевые слова: *сертификация, нормативно-методическая база, инструментарий, информационная безопасность, транспортная система, программное обеспечение, язык программирования, экспериментальный стенд.*

Для цитирования: Лозовецкий В.В., Титов М.Ю., Губсков Ю.А. Методы и средства защиты программного обеспечения транспортных систем при сертификационных испытаниях // ТРАНСПОРТ: Наука, Техника, Управление. 2022. № 7. С. 3-10. DOI: 10.36535/0236-1914-2022-07-1.

INFORMATION TEXNOLOGY, INTERNET

Scientific article

METHODS AND MEANS OF PROTECTION OF SOFTWARE OF TRANSPORT SYSTEMS DURING CERTIFICATION TESTS

Lozovetsky Vyacheslav. V.
(Bauman Moscow State Technical University, Mytishchi Branch)
lozovetsky@mail.ru,

Titov Mikhail Yu.
(MIREA - Russian Technological University)
mtitov_u@list.ru,

Gubskov Yuri A.
(Institute of Automation and Information Technology)
gubtambov@yandex.ru

Abstract. *Methods, methods and tools are proposed for carrying out certification in information systems of transport networks in order to select approaches and tools for working in non-standard situations in an ever-changing regulatory and methodological framework. The considered type of certification is limited to methods and techniques for analyzing vulnerabilities and undeclared capabilities and is intended for the study of software and software and hardware. Approaches to certification tests are presented using tools of our own design, which allows you to select the main parameters necessary for assembling software and its research, and to parse software written in various programming languages.*

Key words: *certification, regulatory framework, tools, information security, transport system, software, programming language, experimental stand.*

For citation: Lozovetsky V.V., Titov M.Yu., Gubskov Yu.A. Methods and means of protection of software of transport systems during certification tests//«TRANSPORT: Science, Equipment, Management». Scientific Information Collection. 2022. № 7. P. 3-10. DOI: 10.36535/0236-1914-2022-07-1.

Введение

Сертификация продуктов и систем информационных технологий актуальна для управления транспортом, а также имеет большое значение, как для народного хозяйства в целом, так и для оборонного комплекса страны. В случае транспорта одной из ключевых проблем, с которой в последнее время сталкиваются субъекты транспортной инфраструктуры не только в сфере дорожного хозяйства, но и в области различных видов транспорта, при обеспечении безопасности дорожного движения, является организация и выполнение на объектах транспортной инфраструктуры требований Правительства РФ от 26.09.2016 г № 969 "Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации средств обеспечения транспортной безопасности" [1]. В значительной мере это относится к обязательной сертификации программного- и программно-аппаратного продукта, используемого в технических средствах для обеспечения транспортной безопасности, установленных непосредственно на объектах (по схеме сертификации № 4). В РФ не создается в широких масштабах программное и программно-аппаратное обеспечение, используемое в системах передачи информации в транспортной сети, в мобильных телефонах, в компьютерах и других средствах вычисли-тельной техники. В нашей стране необходимость в такой продукции возрастает в геометрической прогрессии. С другой стороны мы вынуждены сейчас жить в условиях ограничений по импорту данных средств ПО и нуждаемся в импортозамещении.

Постановка задачи

Наилучшим выходом из такой ситуации является сертификация куп-ленных, а также отечественных продуктов ИТ с учётом требованиям безопасности информации, что позволило бы решить проблемы, которые по-являются при сертификации продуктов и систем ИТ, используемых в транспортных системах. В первую очередь такие проблемы связаны с трудоёмкостью испытаний программного и программно-аппаратного обеспечения при сертификации по упомянутой выше схеме № 4, что требует принятия решения – изменить или отменить процедуру сертификации по данной схеме.

Ряд сертифицируемых ОС может содержать в себе миллионы исходных текстов программ. В частности, некоторые версии дистрибутивов Linux SUSE были собраны из около трёх миллионов исходных текстов программ, что требует исследования около одной тысячи исходных текстов в день, для завершения такой работы за год. Выход из этой ситуации только один – автоматизация труда эксперта, и своевременное их прогнозирование. В работе предложены пути решения указанных проблем на базе западных, так называемых, "Общих критериях" и на предложениях о создании отечественных критериев, основанных, как на Общих критериях, так и на моделировании информационных потоков в продуктах и системах ИТ. Такой подход основан на методологии IDEF по информационному моделированию бизнес-процессов и отличается от традиционных подходов наглядностью, высокой технологичностью, а также возможностью отследить движение информации в любой реализации информа-ционных технологий с учётом предъявляемых к ним требованиям безопасности информации. Проблему оценки эффективности защиты информации в системах ИТ предлагается решить с помощью её модели в системе, в условиях воздействия на нее средств реализации угроз безопасности информации. Использование такой модели на практике поможет определить набор реализаций методов и средств защиты информации, наиболее целесообразной по критерию эффективность-стоимость для конкретной системы. Одним из основных документов, описывающим понятия и способы определения соответствия различных продуктов, в том числе продуктов информационных технологий, необходимым требованиям является Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании», в котором определены понятия аттестации, сертификации и декларации соответствия. Для осуществления сертификации СЗИ по требованиям безопасности информации в ФСТЭК России разработано и используется «Положение о сертификации средств защиты информации по требованиям безопасности информации» от 27 октября 1995 г., №199 [1].

По линии ФСТЭК России осуществляются различные типы сертификации: сертификация программного текста ПО на отсутствие не декларированных возможностей, программных или программно- аппаратных СЗИ на соответствие определённым показателям защищённости. Такими СЗИ могут быть межсетевые экраны или другие средства вычислительной техники. Сравнительно недавно стала входить в силу сертификация по Общим критериям (ГОСТ Р ИСО/МЭК 15408), что свидетельствует о том, что большая часть сертификации будет осуществляться по ним. Многие типы СЗИ сейчас уже сертифицируются (если речь идёт не о сертификации на отсутствие не декларированных возможностей) по Общим критериям: электронные замки, антивирусы, системы обнаружения вторжений. Для про-ведения сертификации по линии ФСТЭК России основным документом является «Положение о сертификации средств защиты информации по требованиям безопасности информации» от 27 октября 1995 г., №199. Оно устанавливает организационную структуру системы сертификации СЗИ с учётом требований безопасности информации, функции субъектов сертификации, её порядок, государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, за нормативными и документам по сертификации СЗИ.

Положение разработано в соответствии со следующими основными документами:

- законом Российской Федерации от 10 июня 1993 г., № 5151-1 "О сертификации продукции и услуг" с изменениями и дополнениями;

- законодательством Российской Федерации, 1996 г., № 1, ст. 4; 1998, № 10, ст. 1143; 1998, № 31, ст. 3832); Законом Российской Федерации от 21 июля 1993 г., № 5485-1 "О государственной тайне" с изменениями и дополнениями;

- Федеральным законом от 20 февраля 1995 г. № 24-ФЗ "Об информации, информатизации и защите информации";

- законом Российской Федерации от 7 февраля 1992 г., № 2300/1-1 "О защите прав потребителей";

- Федеральным законом "Об участии в международном информационном обмене" от 4 июля 1996 г., № 85-ФЗ и рядом других документов.

Существует два основных типа отбора образца продукции на сертификацию, которые связаны с процессом получения эталонных образцов продукции, необходимых для сертификации. Эталонный образец программного обеспечения – это дистрибутив ПО, который считается сертифицированным после положительных сертификационных испытаний. Он может быть получен во время сертификационных испытаний после контрольной сборки из представленных на испытания исходных текстов ПО (первый тип отбора образца). Такой дистрибутив отбирается на дальнейшие испытания в соответствии с Актом отбора образца, подписываемым аккредитованной испытательной лабо-раторией и разработчиком сертифицируемой продук-ции или заявителем на данную сертификацию [2, 3]. При этом составляется Акт о проведении контрольной сборки эталонного дистрибутива ПО, в котором говорится, что разработчик или заявитель соглашаются с тем, что эталонный образец будет собираться во время сертификационных испытаний и, что сборка проходит в присутствии представителя разработчика или заявителя. Второй тип связан с получением на основании Акта отбора собранного ранее эталонного образца и подписывается представителями аккреди-тованной испытательной лаборатории, разработчика сертифицируемой продукции или заявителя на данную сертификацию. Причина такого отбора может быть различной и связана с тем, что либо собранный для испытаний стенд не позволяет собрать дистрибутив в приемлемые сроки, либо для сбора дистрибутива требуются дополнительные проверки, которые испытательный стенд не может произвести по каким-либо причинам.

В процессе отбора образца с файлов сертифицируемого ПО снимаются контрольные суммы с использованием сертифицированных средств расчёта контрольных сумм. Например, может использоваться программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.2, имеющая сертификат соответствия № 1548 от 15.01. 2008 г.

На рис. 1 приведен простейший испытательный стенд, который используется для исследования объекта сертификации на не декларированные возможности.

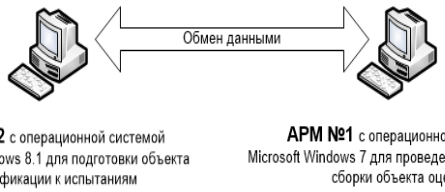

Рис. 1. Испытательный стенд

Для компиляции и сборки достаточно одного компьютера (на стенде АРМ №1), а второй (АРМ №2) используется, как вспомогательный.

При испытаниях должны быть проведены следующие проверки:

- Оценка работоспособности всех устройств, используемых при испытаниях.
- Оценка работоспособности операционных систем (например, как показано на рисунке 1: операционных систем Windows 7 и Windows 8.1), используемых на испытательном стенде.
- Соответствие фактического состава программно-аппаратной среды стенда требованиям к эксплуатации объекта сертификации.
- Оценка достаточности программно-аппаратной среды стенда для проведения сертификационных испытаний.

На стенде устанавливаются и проверяются следующие программные средства:

1) программа фиксации и контроля исходного состояния программно-го комплекса ФИКС или другое сертифицированное средство для подсчёта контрольных сумм файлов ПО;

2) средства разработки ПО КПМ: Microsoft Visual Studio версии: Microsoft Visual Studio для языков программирования Microsoft Visual Studio – C, C++ или другое необходимое средство для компиляции и сборки;

3) анализаторы исходных текстов программ: анализатор для исходных текстов C и C++ программ, версия 2.0 (далее «АИСТ-С» версии 2.0), АК-ВС (разработки компании «Эшелон»), программа FortyAges-analyzer v0.3, предназначенная для автоматизации процесса сравнения имен файлов исходных текстов, представленных в логах компиляции, с именами файлов исходных текстов в списках, определённых с помощью программы ФИКС.

На АРМ № 2 стенда фиксируются контрольные суммы исходных текстов программ ПО и/или остальных файлов объекта сертификации с помощью программы ФИКС, и анализируются результаты испытаний. АРМ № 1 можно использовать для удобства при компиляции и сборки ПО. После копирования на жесткий диск АРМ № 1 файлов исходных текстов программ в соответствии со списком в Акте отбора образца, осуществляется компиляция и сборка дистрибутива ПО из отобранных файлов исходных текстов программ. В результате может быть получен эталонный дистрибутив (если он не был передан ранее на испытания по акту отбора образца) или со-бранный заново соответствующий эталонному, так называемый, пересобранный дистрибутив и файлы логов компиляции и сборки ПО, тексты которых и сборки содержат в себе информацию об обращении компилятора к необходимым для сборки файлам исходных текстов. Для установления факта безошибочной сборки бинарных файлов анализируются логи компиляции и сборки по поиску ключевых слов error и warning. Сборка выполнена успеш-но, если в её процессе для установления этого факта уровень компилятора признается допустимым и нет ни одной ошибки компилятора при компиляции и сборке объекта сертификации. Рассчитываются контрольные суммы файлов эталонного или пересобранного дистрибутива. Если собран эталонный дистрибутив, то образец продукции ПО идентифицируется как эталонный. Если он не может интерпретироваться как эталонный, то возможны два варианта развития событий. В первом случае, если контрольные суммы файлов эталонного дистрибутива, который был собран до испытаний, совпадают с файлами пересобранного в процессе испытаний, то считается, что эталонный и пересобранный дистрибутивы идентичны. Во втором случае, если контрольные суммы не совпадают, то в последующих испытаниях необходимо

доказать, что эталонный и пересобранный дистрибутивы идентичны. Необходимо иметь в виду, что в любом случае (или в большинстве случаев) при каждой новой сборке собираемые файлы отличаются в отображении новой даты и времени, в теле исполняемого бинарного файла при сборке в другое время и в другую дату, по этой же причине могут не совпадать смещения в секциях и сегментах данных в исполняемых файлах. Это может произойти, если при последующих сборках произойдёт дефрагментация памяти компьютера и у свободных участков памяти изменятся адреса и изменятся смещения в секциях и сегментах данных. В программировании такая команда, как "allocate" при обращении к ней в разное время может выделять память по разным адресам свободной памяти в компьютере [5]. В процессе испытаний проверяются на отсутствие не декларированных возможностей документы, представленные в таблице 1.

Таблица 1

Перечень документов для испытаний

№ п/п	Требуемые документы
1	Спецификация (ГОСТ 19.202-78)
2	Описание программы (ГОСТ 19.402-78)
3	Описание применения (ГОСТ 19.502-78)
4	Тексты программ, входящих в состав программного обеспечения (ГОСТ 19.401-78)
5	Пояснительная записка (ГОСТ 19.404-79)

Контроль исходного состояния испытуемого ПО производится путём контрольного суммирования сертифицируемого ПО. Если эталонный дистрибутив ПО был собран в процессе контрольной сборки, то результаты фиксации его исходного состояния должны быть зафиксированы в Акте отбора образца, в котором заявитель, разработчик ПО и испытательная лаборатория договариваются о том, что собранный в процессе испытаний дистрибутив является эталонным. В нём подтверждается, что во время испытаний он собирался в присутствии заявителя или разработчика. В противном случае эта-лонный дистрибутив мог быть собран заранее до испытаний и представлен по Акту отбора образца для испытательной лаборатории. Результаты этого контроля (контрольные суммы всех файлов ПО, используемых при сертификации, которые были представлены на сертификацию на основании акта отбора образца), должны совпадать с контрольными суммами всех файлов ПО, представленными в документе Описание программы. Основными результатами являются рассчитанные значения контрольных сумм загрузочных модулей и файлов исходных текстов программ, входящих в состав.

Контрольные суммы отобранного на испытания эталонного дистрибутива ПО должны совпадать с контрольными суммами соответствующих файлов дистрибутива, представленных в документе Описание программы, который предоставляется от заявителя на сертификацию или от разработчика ПО.

Из дистрибутива ПО должны быть выделены, так называемые, неизменяемые исполняемые файлы и файлы библиотек. В ряде случаях рекомендуется не выделять все файлы дистрибутива или большую их часть в качестве неизменяемых, поскольку их могут быть тысячи по количеству. Следует выбирать наиболее представительные неизменяемые файлы для отражения их в формуляре, которые должны составить ядро области сертификации. Файлы, используемые только для работы со шрифтами, не влияют на безопасность ПО и не рассматриваются, как относящиеся к объекту сертификации СЗИ.

Контрольные суммы неизменяемых исполняемых файлов и библиотек (они могут совпадать с файлами эталонного дистрибутива) должны быть отражены в формуляре (или паспорте) на продукт ИТ (ПО). Контрольные суммы исходных текстов сертифицируемого ПО фиксируются в Акте отбора образца, и должны совпадать с представленными в Описании программы.

Контроль исходного состояния ПО заключается в фиксации исходного состояния ПО и в сравнении полученных результатов со значениями, приведёнными в документации. Результатами фиксации исходного состояния ПО должны быть значения контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО. Они рассчитываются для каждого файла, входящего в состав сертифи-цируемого ПО, и сравниваются с соответствующими контрольными суммами в документации.

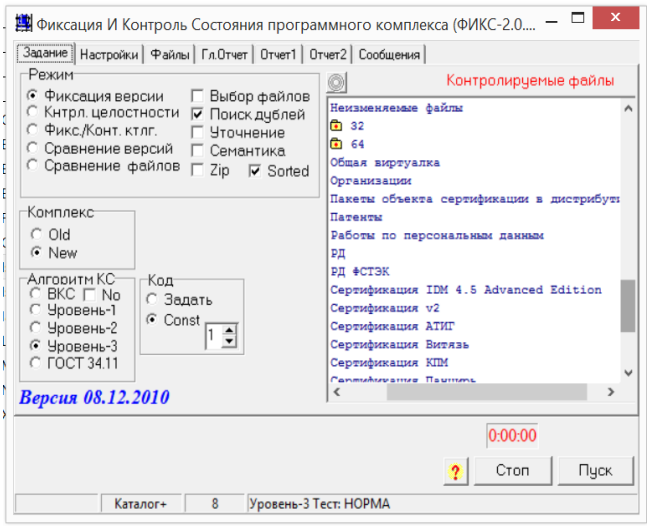

Рис. 2. Интерфейс программы ФИКС

Производится фиксация исходного состояния программного обеспечения ПО путём расчета контрольных сумм всех бинарных файлов из состава объекта оценки, а также всех файлов исходных текстов из состава объекта оценки. С помощью программы ФИКС (например, на АРМ №2 рисунок 1) выполняется подсчет значений контрольных сумм для каждого файла, присутствующего на дистрибутивном носителе информации. При использовании программы ФИКС необходимо настроить её алгоритм по алгоритму «Уровень-3, программно» (рисунок 2), навести курсор на папку в дереве файловой системы в программе ФИКС, получить отчёт о контрольных суммах и нажать на кнопку «Пуск». После окончания работы программы получить отчёт о контрольных суммах, требуемых для анализа. С помощью ФИКС рассчитываются значения контрольных сумм для неизменяемых файлов библиотек и бинарных исполняемых файлов объекта оценки, установленных в системе после установки дистрибутива (например, на АРМ №1, рисунок 1). Расчет контрольных сумм неиз-

меняемых файлов библиотек и бинарных исполняемых файлов производится после их контрольной сборки и установки эталонного дистрибутива, который по согласованию с заявителем может считаться эталонным, а контрольная сборка должна осуществляться во время отбора образца.

После контрольной сборки исполняемых файлов необходимо зафиксировать их контрольные суммы с помощью программы ФИКС, сформировать отчеты программ ФИКС, фиксирующие контрольные суммы файлов ПО. Рассчитанные значения контрольных сумм файлов, находящихся на дистрибутивных носителях и исходных текстов объекта оценки, фиксируют исходное состояние ПО.

Программа испытаний и проверок ОО с определенными заводскими номерами, например, №№ 122, 123 состоит из испытаний на отсутствие в ОО НДВ и АУ в соответствии с требованиями безопасности информации по определённому уровню контроля. В связи с тем, что ОО с различными заводскими номерами должны быть идентичны, испытания могут быть проведены на ОО № 122, а идентификация ОО с заводским № 123 будет производиться путем сличения полученных контрольных сумм ПО для обоих ОО. Система показателей соответствия ОО требованиям безопасности информации устанавливается с учётом требований ФСТЭК России в соответствии с уровнями доверия контроля. Испытания ОО по выявлению НДВ и АУ проводятся в три этапа: подготовка к проведению испытаний ОО, проведение испытаний ОО, оформление результатов испытаний ОО, составление протокол испытаний и технического заключения [4, 6]. При подготовке к испытаниям анализируются комментарии разработчика к исходному коду с целью выявления потенциально опасных функциональных возможностей. Результаты анализа позволяют проверить комментарии разработчика к исходному коду.

Основную информацию, связанную с комментариями, предоставляет FortyAges-analyzer v0.4 путем поиска в файлах с исходными кодами ОО соответствующих конструкций и отражения информации о конструкциях в отчете своей работы, что в полной мере компенсирует недостаточное количество комментариев в программе ОО. Анализируется описания программы и пояснительной записки к эскизному и (или) техническому проектам для выявления опасных функциональных возможностей [7, 9].

В соответствии с рекомендациями «Описание программы», ОО произ-водит сканирование ресурсов компьютера для моделирования матрицы доступа, получает информацию о структуре ресурсов АРМ и сохраняет ее в памяти ПЭВМ. ОО осуществляет считывание прав доступа файловой системы NTFS. При сканировании дисков с файловой системой NTFS ОО считывает установленные права доступа и преобразует их в формат, используемый для представления прав доступа в соответствии с ПРД. ОО осуществляет построение дерева ресурсов и по данным сканирования автоматически строит иерархическую структуру, аналогичную структуре ресурсов АРМ, получает список локальных и доменных пользователей, списки учетных записей пользователей, зарегистрированных на АРМ и на контроллере домена (в случае, если АРМ входит в состав домена). Пользователи регистрируются в проекте разделения доступа (ПРД определяются в матрице доступа) наравне с другими субъектами доступа. После построения дерева ресурсов администратор регистрирует в ПРД пользователей и устанавливать их уровни допуска. ОО предоставляет возможности по моделированию разрешительной системы. Администратор устанавливает права доступа пользователей к объектам доступа. Проводится анализ вышеперечисленных действий для выявления ли потенциально опасных функциональных возможностей ОО. Информация, необходимая для анализа и соответствующая пояснительной записки к эскизному и или техническому проектам, может находиться в следующих документах ОО: «Требования к проектированию»; «Представление реализации средства».

Для представленного ОО не требуется реализации механизмов защиты. ОО не реализует политики управления доступом пользователей к ресурсам, функционал управления информационными потоками, не содержит специальных мер защиты, характерных для средств защиты информации и это может быть отображено в документе «Требования к проектированию».

Подготовка испытательный стенда (рисунок 1) проводится также с учётом следующих требований:

1) при проведении исследований исходными данными должны быть: дистрибутив, документация, исходные тексты программы ПО, а также результаты испытаний;

2) в ходе подготовки исследований собирается экспериментальный стенд в соответствии со схемой, представленной на рисунке 1, включающий технические, программные и инструментальные средства;

3) производится развёртывание и настройка сред функционирования ОО, а также необходимого ПО;

4) установка, конфигурирование и настройка ОО осуществляется в соответствии с эксплуатационной документацией на него;

5) для отобранных с целью проведения сертификационных работ файлов исходных текстов, неизменяемых исполняемых файлов и файлов дистрибутива ОО с определенными заводскими номерами рассчитываются контрольные суммы (КС) с помощью средств фиксации и контроля исходного состояния программного комплекса. КС можно рассчитать, например, с помощью программы «ФИКС», версия 2.0.2 (ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, тех. поддержка до 15.01.2025). Для всех отобранных экземпляров с определенными заводскими номерами все КС должны быть идентичны, КС неизменяемых исполняемых файлов и файлов дистрибутива должны соответствовать КС, приведенным в формуляре для ОО.

После проверки проводится анализ дистрибутива ОО (а также исполняемых файлов), в том числе среды функционирования ОО с использованием не менее двух сертифицированных средств антивирусной защиты от различных разработчиков с поддержкой актуальных баз данных угроз.

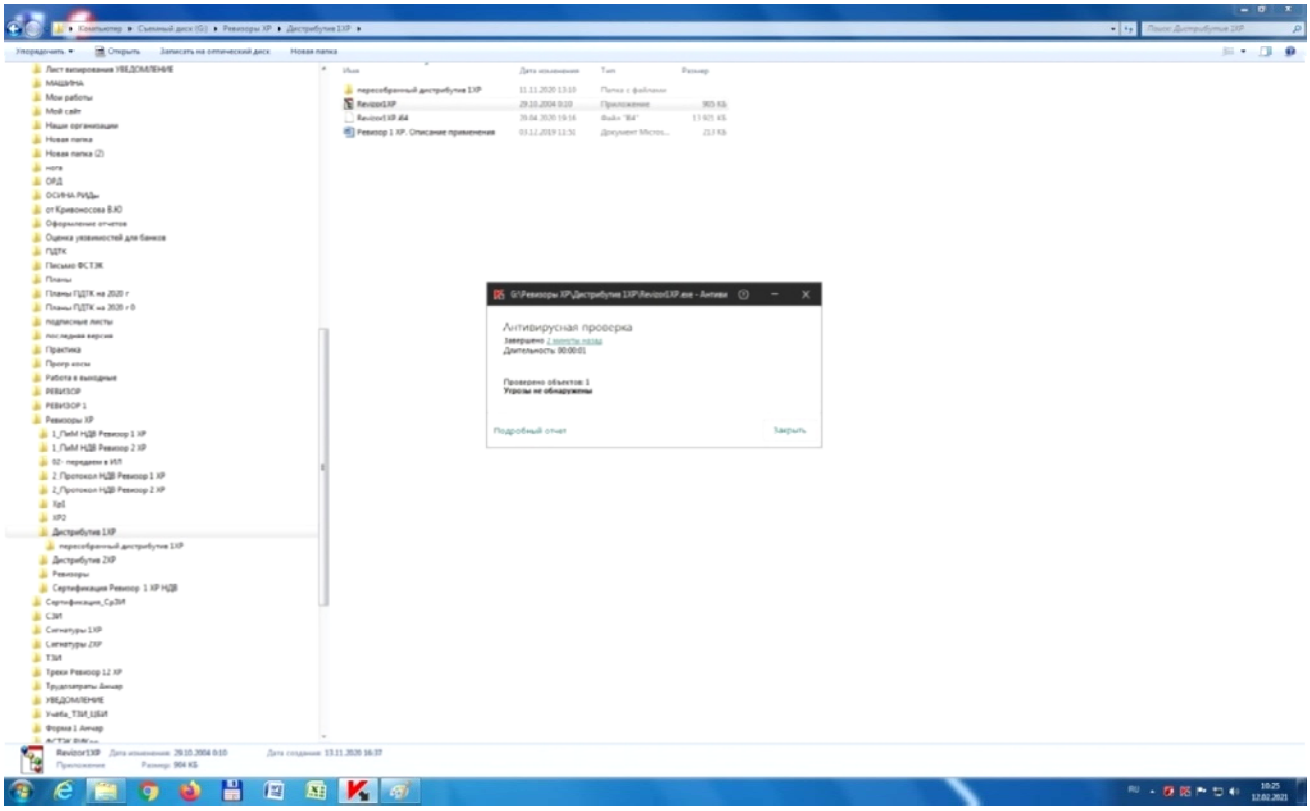

Рис. 3. Результат проверки исполняемого файла ОО с помощью программного изделия «Kaspersky Endpoint Security для Windows»

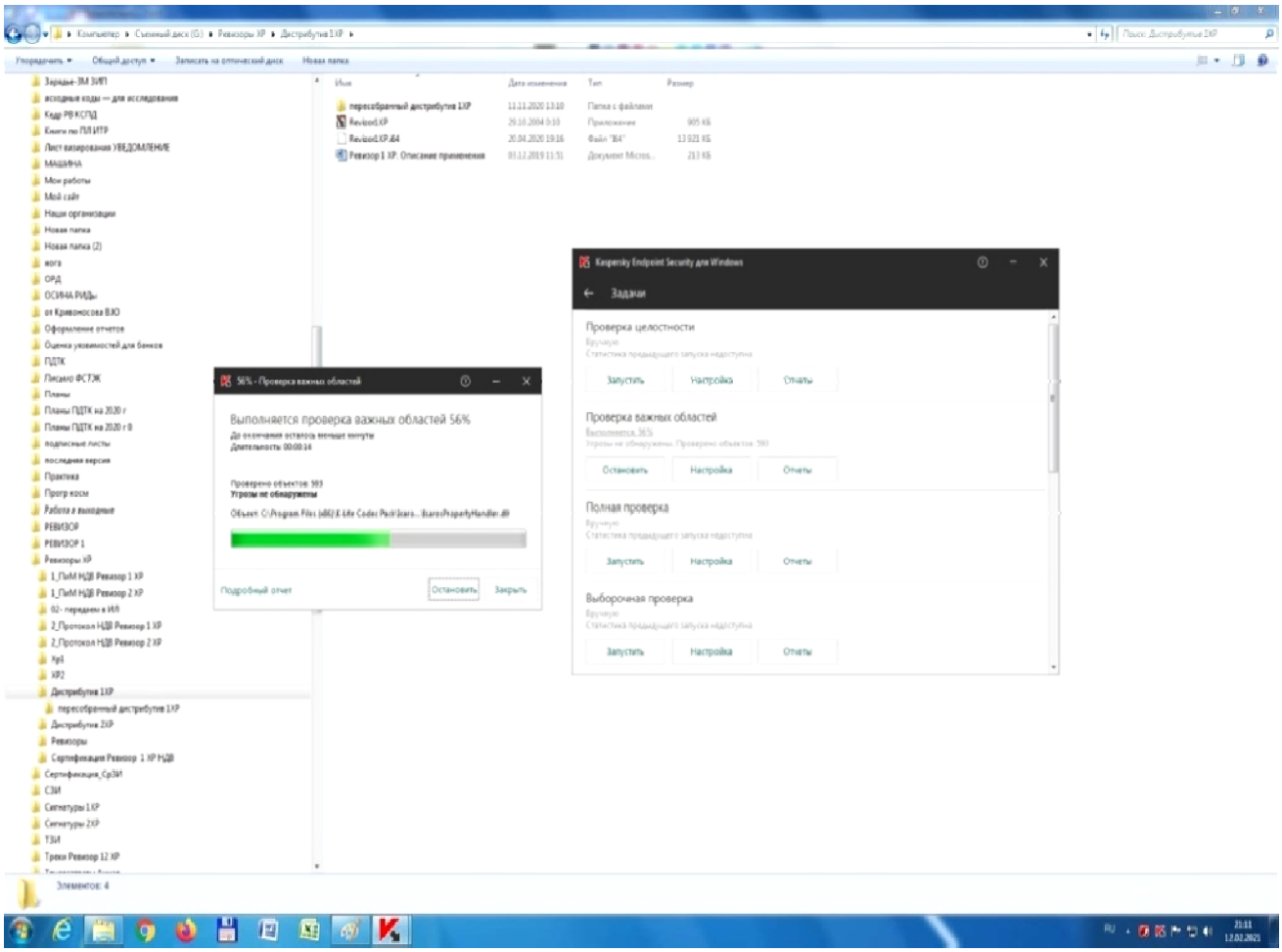

Рис. 4. Проверка среды функционирования ОО с помощью программного изделия «Kaspersky Endpoint Security для Windows»

С этой целью можно использовать следующие антивирусные программы: программное изделие «Kaspersky Endpoint Security для Windows» (сертификат соответствия ФСТЭК России № 4068 до 22.01.2024) и «Программное обеспечение Dr.Web ENTERPRISE SECURE SUITE» версия 11.5, сертификат ФСТЭК России № 3509 выдан 25 января 2016, действует до 27 января 2024. На рисунке 3 показан результат проверки исполняемого файла ОО с помощью антивирусной программы «Kaspersky Endpoint Security для Windows». Из рисунка 3 следует, что угрозы не обнаружены. С помощью антивирусной программы «Kaspersky Endpoint Security для Windows» можно проверить среду функционирования ОО (рисунок 4). На данном этапе испытаний (подготовки к проведению испытаний) должна быть произведена проверка выполнения компиляции и сборки ОО, а также получена лабораторная сборка ОО. Результат проверки среды функционирования ОО показал, что угрозы не обнаружены.

С этой целью для компилируемых языков (например, Паскаль) могут быть произведены следующие действия: запущено средство разработки (например, Delphi 7) [11]; выбран проект для ОО в Delphi 7; выбрано меню «Project» -> «Build»; после сборки в определенном каталоге появится исполняемый файл ОО, который является продуктом компиляции и сборки ОО; закрыт проект (меню «File» -> «Close All») [12]; после копирования на жесткий диск ПЭВМ № 1 испытательного стенда файлов исходных текстов программ в соответствии со списком в акте отбора ОО должна быть произведена успешная компиляция и сборка дистрибутива ОО из отобранных файлов исходных текстов программ [10, 13].

Выводы

После испытаний осуществляется экспертиза участков исходного кода. При помощи анализатора исходных текстов программ можно получить сведения о связях между информационными и функциональными объектами с указанием их принадлежности функциональным объектам.

В рамках испытаний должен быть проведен анализ ПО, который может показать используются или нет в данном ПО небезопасные конструкции, например, такие как ShellExecute.

Следует провести ручной анализ ПО с использованием комментариев к исходном кодам ОО, которые передаются его разработчиком. Если они не были получены, не обязательно останавливать испытания до предоставления разработчиком комментариев в исходные тексты ПО в случае применения анализатора исходных текстов программы FortyAges-analyzer v0.4.

Используя полученные при испытаниях данные, а также комментарии к языковым конструкциям, следует в ручном режиме проверить исходные коды ОО и функционирование найденных небезопасных конструкций[1].

Список источников

1. Калугин О.А. Сложности сертификации. Спецпроект транспортная безопасность. www. secuteck.ru; - 2020. - апрель-май. - С. 36 - 37.

2. Экспертиза программной документации на соответствие требованиям Государственных стандартов ГОСТ Р ИСО/МЭК 12119-2000 (п. 3.2), ГОСТ Р ИСО 9127-94 (п.п. 5, 6.1, 6.3-6.5);

3. Кошевая И. П. Метрология. Стандартизация. Сертификация: учебник / И. П. Кошевая, А. А. Канке. – М.: ФОРУМ, 2009. – 414 с. – (Профессиональное образование) .– Библиогр.: с.406–411 .– ISBN 978–5–8199–0293–6.

4. Волков В. И. Основы теории и практики экспертной деятельности - М.: АМИ, 2002.

5. Джодж С., Ваймерских А. Всеобщее управление качеством: стратегии и технологии, применяемые сегодня в самых успешных компаниях. (TQM).- СПб., «Виктория плюс», 2002 г. - 256 с.

6. Крейг Р. Дж. ИСО 9000 - Руководство по получению сертификата о регистрации. Пер. с англ. - М.: РИА «Стандарты и качество», -2000.

7. Крылова Г.Д. Основы стандартизации, сертификации, метрологии: Учебник для вузов - 2-е изд., перераб. и доп. -М.: ЮНИТИ-ДАНА, 2001.

8. Лифиц И.М. Основы стандартизации, метрологии, сертификации Учебник для вузов. - М.: Юрайт, 1999.

9. Москвин В. А. Управление качеством в бизнесе: Рекомендации для руководителей предприятий, банков, риск - менеджеров. - М.: Финансы и статистика, 2006. - 384с.: ил.

10. Роберт В. Пич, Бил Пич, Дайана Риттер Справочник по использованию ISO 9001 - стандарта систем качества: Пер. с анг. - К. [Укр. ассоц. качества], 2003. - 184 с.

11. Сборник законов и иных нормативных правовых актов Российской Федерации по вопросам сертификации продукции и услуг (Вып. 2, дополненный)/ Всероссийский научно-исследовательский, институт сертификации Госстандарта России. - М., 1995. - 104 с.

12. Сергеев А. Г., Латышев М. В. Сертификация: Учебное пособие для студ. вузов. - М.: «Логос», 2000.

13. Система сертификация ГОСТ Р. Основные положения и порядок сертификации услуг/ Комитет Российской Федерации по стандартизации, метрологии и сертификации. - М.,1995.

14. "Криптором по антивирусу" журнал Хакер № 168, 2021г.

Информация об авторах

Лозовецкий Вячеслав Владимирович – доктор техн. наук, профессор;

Титов Михаил Юрьевич – к.т.н., с.н.с., доцент кафедры КБ-1 «Защита информации» института кибербезопасности и цифровых технологий;

[1] ©Лозовецкий В.В., Титов М.Ю., Губсков Ю.А., 2022

Губсков Юрий Анатольевич – к.т.н., доцент кафедры «Информационные системы и защита информации».

Information about the authors

Lozovetsky Vyacheslav. V. – Doctor (Techю), Professor;

Titov Mikhail Yuryevich – Ph. (Tech.), Senior Researcher, Associate Professor of the Department of KB-1 "Information Protection" of the Institute of Cybersecurity and Digital Technologies;

Gubskov Yuri Anatolyevich – Ph. (Tech), Associate Professor of the Department "Information Systems and Information Protection".

Статья поступила в редакцию 15.03.2022, одобрена после рецензирования 28.04.2022, принята к публикации 13.05.2022.

The article was submitted 15.03.2022, approved after reviewing 28.04.2022, accepted for publication 13.05.2022.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Authors contribution: All authors have made an equivalent contribution to the preparation of the publication. The authors declare that there is no conflict of interest.