УДК 006.91 + 346.544.4
DOI: 10.18698/2542-1468-2022-5-145-157
Шифр ВАК 2.3.7

СЕРТИФИКАЦИЯ ПРОГРАММНОГО И ПРОГРАММНО-АППАРАТНОГО ОБЕСПЕЧЕНИЯ ТРАНСПОРТНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Е.Г. Комаров[1], В.В. Лозовецкий[1]✉, В.В. Лебедев[2], А.В. Архипенко[3]

[1]МГТУ им. Н.Э. Баумана (Мытищинский филиал), 141005, Московская обл., г. Мытищи, ул. 1-я Институтская, д. 1
[2]РТУ — МИРЭА, 107996, Москва, ул. Стромынка, д. 20
[3]Сочинский международный инновационный университет, 354000, г. Сочи, ул. Орджоникидзе, д. 10а

lozovetsky@mail.ru

Рассмотрены способы, методы и средства для проведения сертификации программного и программно-аппаратного обеспечения в информационных системах в целях выбора подходов и инструментария для работы в нестандартных ситуациях в условиях постоянно изменяющейся нормативно-методической базы и возможных угроз их информационной безопасности. Представлены рекомендации к сертификационным испытаниям с использованием инструментария собственной разработки, который позволяет выделить основные параметры, необходимые для сборки программного обеспечения и его исследования, и провести синтаксический анализ программного обеспечения, написанного на различных языках программирования. На основе программы испытаний и проверок объекта оценки в соответствии с требованиями безопасности информации в условиях определенного уровня контроля предложены методы проведения сертификационных исследований, показаны преимущества методики с использованием имевшегося в распоряжении и рекомендуемого инструментария. В целях экономии указаны некоторые известные бесплатные и свободно распространяемые средства, а также эффективные и недорогие программные продукты.
Ключевые слова: сертификация, нормативно-методическая база, инструментарий, объект оценки, анализ угроз, информационная безопасность, программное обеспечение, язык программирования, экспериментальный стенд

Ссылка для цитирования: Комаров Е.Г., Лозовецкий В.В., Лебедев В.В., Архипенко А.В. Сертификация программного и программно-аппаратного обеспечения транспортных информационных систем в соответствии с требованиями безопасности // Лесной вестник / Forestry Bulletin, 2022. Т. 26. № 5. С. 145–157.
DOI: 10.18698/2542-1468-2022-5-145-157

Вопросы сертификации продуктов и систем информационных технологий актуальны, в частности, для управления транспортом, а также имеют важное значение как для народного хозяйства в целом, так и для оборонного комплекса страны.

Известно, что в РФ не создается в широких масштабах программное и программно-аппаратное обеспечение для известных продуктов информационных технологий (ИТ), в частности, распространенное общесистемное программное обеспечение (ПО), используемое в мобильных телефонах, в компьютерах и в других средствах вычислительной техники. Необходимость такой продукции возрастает для РФ в геометрической прогрессии.

Наилучшим выходом из сложившейся ситуации является сертификация закупленных, а также отечественных продуктов ИТ с учетом требований безопасности информации. Это позволило бы разрешить проблемы, которые появляются при сертификации продуктов и систем ИТ. В первую очередь такие проблемы связаны с трудоемкостью испытаний программного и программно-аппаратного обеспечения при сертификации. Иногда сертификации затягиваются до полугода и более, что часто напрямую не связано с квалификацией экспертов, а зависит непосредственно от объемов задач, стоящих перед специалистами по испытаниям такой продукции.

Сертифицируемые операционные системы (ОС) могут содержать миллионы исходных текстов программ. В частности, некоторые версии дистрибутивов Linux SUSE собраны почти из 3 млн исходных текстов программ, и тогда эксперту в течение рабочего дня необходимо исследовать около 1000 исходных текстов, для завершения работы за год. Необходимо также исследовать и другие типы файлов в ОС, например, бинарные файлы, которых в ОС может быть десятки тысяч.

Материалы и методы

Выход из описанной выше ситуации только один — автоматизация труда эксперта и их заблаговременное предвидение. В работе предлагаются эффективные методы сертификации, основанные, как на западных, так называемых, «Общих критериях», так и на отечественных критериях, учитывающих Общие критерии и возможность моделирования информационных потоков в продуктах и системах ИТ. Такой подход основан, в том числе, на методологии IDEF по информа-

ционному моделированию бизнес-процессов, и отличается от традиционных как наглядностью, так и высокой технологичностью, возможностью отследить движение информации в любой реализации информационных технологий с учетом предъявляемых к ним требованиям безопасности информации.

Проблему оценки эффективности защиты информации в системах ИТ предлагается решить с помощью модели оценки эффективности защиты информации в системе в условиях воздействия на нее средств реализации угроз безопасности информации. Использование такой модели на практике поможет определить набор методов и средств защиты информации, наиболее целесообразных по критерию эффективность — стоимость для конкретной системы.

Общие положения при сертификации с учетом требований безопасности информации. Одним из основных документов, описывающих понятия и способы определения соответствия различных продуктов, в том числе продуктов информационных технологий, необходимым требованиям, является Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». В этом законе определены понятия аттестации, сертификации и декларации соответствия. В руководящих документах Федеральной службы по техническому и экспортному контролю (ФСТЭК) России нет регламента по декларации соответствия системы защиты информации (СЗИ) требованиям безопасности информации, но существует регламент на аттестацию и сертификацию.

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, в соответствии с которым осуществляются различные типы сертификации: сертификация программного текста ПО на отсутствие не декларированных возможностей, сертификация программного или программно-аппаратного СЗИ на соответствие определенным показателям защищенности. Такими СЗИ могут быть межсетевые экраны или другие средства вычислительной техники. Сравнительно недавно стала входить в силу сертификация по так называемым Общим критериям (ГОСТР ИСО/МЭК 15408). Тенденции сертификации по линии ФСТЭК говорят о том, что в скором времени большая часть сертификации будет осуществляться по Общим критериям. Многие типы СЗИ уже сертифицируются (если речь идет не о сертификации на отсутствие не декларированных возможностей) по Общим критериям, например электронные замки, антивирусы, системы обнаружения вторжений. Остались еще отдельные руководящие документы ФСТЭК России, например, руководящие документы (РД), регламентирующие сертификацию не по Общим критериям, а по межсетевым экранам, однако тенденция развития подходов к сертификации указывает на то, что вскоре подобные РД будут переведены на методологию Общих критериев.

Рассмотрим более подробно отдельные документы ФСТЭК РФ, регламентирующие процессы сертификации, среди которых основным является «Положение о сертификации средств защиты информации по требованиям безопасности информации» от 27 октября 1995 г. № 199. Данное положение устанавливает организационную структуру сертификации средств защиты информации с учетом требований безопасности информации, функции субъектов сертификации, порядок сертификации, государственного контроля и надзора, инспекционного за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, общие требования к нормативным и методическим документам по сертификации средств защиты информации. В приложениях к данному положению приведены перечень средств защиты информации, подлежащих сертификации в системе сертификации, формы заявок на проведение сертификации и продление срока действия сертификата, решения по заявке на проведение сертификации (продлению срока действия сертификата), сертификата и лицензии на применение знака соответствия.

Положение было 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;

– Собранием законодательных актов Российской Федерации, 1996, № 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;

– Постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» с изменениями и дополнениями, внесенными на основании Правил по проведению сертификации в Российской Федерации, утвержденных Постановлением

АРМ № 2 с операционной системой Microsoft Windows 8.1 для подготовки объекта сертификации к испытаниям

АРМ № 2 с операционной системой Microsoft Windows 7 для проведения компиляции и сборки объекта оценки

Рис. 1. Испытательный стенд: АРМ — автоматизированное рабочее место
Fig. 1. Test bench: AWP — workstation

Госстандарта России от 16 февраля 1994 г., № 3 и зарегистрированных в Министерстве юстиции Российской Федерации 21 марта 1994 г., регистрационный номер 521 (Российские вести, от 30 марта 1994 г., № 56), и Порядка проведения сертификации продукции в Российской Федерации, утвержденного Постановлением Госстандарта России от 21 сентября 1994 г. № 15 и зарегистрированного в Министерстве юстиции Российской Федерации 5 апреля 1995 г., регистрационный номер 826 (Российские вести, от 1 июня 1995 г., № 100).

Отбор образцов продукции на сертификацию. Существует два основных типа отбора образца продукции на сертификацию. Эти типы связаны с процессом получения эталонных образцов продукции, необходимых для сертификации. Эталонный образец программного обеспечения — это дистрибутив ПО, который будет считаться сертифицированным после положительных сертификационных испытаний. Эталонный образец ПО можно получить в процессе сертификационных испытаний после контрольной сборки этого эталонного дистрибутива из представленных на испытания исходных текстов ПО (это первый тип отбора образца). Полученный таким образом дистрибутив отбирается на дальнейшие испытания в соответствии с Актом отбора образца, подписываемым аккредитованной испытательной лабораторией и разработчиком сертифицируемой продукции либо заявителем на данную сертификацию [1–3].

При первом типе отбора составляется Акт о проведении контрольной сборки эталонного дистрибутива ПО, свидетельствующий, что разработчик или заявитель соглашаются с тем, что эталонный образец будет собираться во время сертификационных испытаний, а также, что сборка проходит в присутствии представителя разработчика или заявителя.

Второй тип отбора связан с получением на основании Акта отбора образца собранного ранее разработчиком эталонного образца. Такой Акт отбора образца подписывается аккредитованной испытательной лабораторией и разработчиком сертифицируемой продукции либо заявителем на данную сертификацию. Причина такого отбора может быть различной, но, как правило, она 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 провести по каким-либо причинам [4].

Второй тип отбора сопряжен в последующих испытаниях со значительными трудностями, поскольку требуются доказательства, что собранный заново в процессе испытаний дистрибутив идентичен по функциональности с эталонным дистрибутивом. Эти доказательства привести нелегко, ведь необходимо доказать, что при новой сборке не было привнесено в ПО чего-либо, что может нарушить безопасность ПО. По этой причине при сертификации рекомендуется использовать (по возможности) первый тип отбора.

С файлов сертифицируемого ПО в процессе отбора образца снимаются контрольные суммы с использованием сертифицированных средств расчета контрольных сумм. Например, может использоваться программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.2 (далее — ФИКС), имеющая сертификат соответствия № 1548 от 15 января 2008 г.

На рис. 1 приведен простейший вариант испытательного стенда для проведения сертификации, который отвечает требованиям, предъявляемым к исследованию объекта сертификации на не декларированные возможности. Для компиляции и сборки (как правило) достаточно одного компьютера (на стенде АРМ № 1), второй компьютер (АРМ № 2) используется как вспомогательный.

В процессе испытаний необходимо осуществить следующие проверки:

– работоспособности всех устройств, используемых во время испытаний;

– работоспособности операционных систем (например, операционных систем Windows 7 и Windows 8.1, как показано на рис. 1), используемых на испытательном стенде;

– соответствия фактического состава программно-аппаратной среды стенда требованиям к эксплуатации объекта сертификации;

– достаточности программно-аппаратной среды стенда для проведения сертификационных испытаний.

На стенде, как правило, устанавливаются и проверяются следующие программные средства:

1) программа фиксации и контроля исходного состояния программного комплекса ФИКС или другое сертифицированное средство для подсчета 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, например анализатор для исходных текстов C и C++ программ, версия 2.0 (далее — «АИСТ-С» версии 2.0, АИСТ), или другие анализаторы, например АК-ВС (разработки компании «Эшелон») либо программа FortyAges-analyzer v0.3, предназначенная для автоматизации процесса сравнения имен файлов исходных текстов, представленных в логах компиляции, с именами файлов исходных текстов, представленных в списках, определенных с помощью программы фиксации и контроля исходного состояния программного комплекса ФИКС.

На АРМ № 2 испытательного стенда можно фиксировать контрольные суммы исходных текстов программ ПО и/или остальных файлов объекта сертификации с помощью программы ФИКС, анализировать результаты испытаний. АРМ № 1 можно использовать в целях удобства только для компиляции и сборки ПО. После копирования на жесткий диск АРМ № 1 испытательного стенда файлов исходных текстов программ в соответствии со списком в Акте отбора образца обычно проводятся компиляция и сборка дистрибутива испытуемого ПО из отобранных файлов исходных текстов программ.

Эталонный дистрибутив может быть получен (если он не был передан ранее на испытания по акту отбора образца) или собранный заново соответствующий эталонному — так называемый пересобранный дистрибутив, в результате успешной компиляции и сборки дистрибутива ПО на АРМ №1 испытательного стенда. На этом этапе получают файлы логов компиляции и сборки ПО. Тексты логов компиляции и сборки содержат в себе информацию об обращении компилятора к необходимым для сборки файлам исходных текстов.

Эксперт должен провести анализ логов компиляции и сборки для установления факта безошибочной сборки бинарных файлов. Анализ осуществляется по поиску ключевых слов error и warning в логах компиляции и сборки. Сборка выполнена успешно, если уровень предупреждений компилятора признается допустимым и нет ни одной ошибки компилятора при компиляции и сборке объекта сертификации.

Таблица 1

Документы, проверяемые при испытаниях на отсутствие не декларированных возможностей

Documents checked during tests for the absence of undocumented features

Требуемые документы
Спецификация, ГОСТ 19.202–78
Описание программы, ГОСТ 19.402–78
Описание применения, ГОСТ 19.502–78
Тексты программ, входящих в состав программного обеспечения, ГОСТ 19.401–78
Пояснительная записка, ГОСТ 19.404–79

Таблица 2

Спецификация (ГОСТ 19.202–78)

Specification (GOST 19.202–78)

Требования
Спецификация должна содержать разделы: «Документация»; «Комплексы»; «Компоненты»
В раздел «Документация» вносят программные документы на программу, кроме спецификации и технического задания, в порядке возрастания кода вида документа, входящего в обозначение. Далее записывают заимствованные программные документы в порядке возрастания кодов организаций (предприятий) — разработчиков и далее в порядке возрастания вида документа, входящего в обозначение
В разделах «Комплексы» и «Компоненты» указывают полное наименование программы, наименование и вид документа

Далее рассчитываются контрольные суммы (например, с помощью ФИКС) файлов эталонного или пересобранного дистрибутива. Если в процессе сертификационных испытаний собран эталонный дистрибутив, то образец продукции ПО однозначно идентифицируется как эталонный.

Если собранный при испытаниях дистрибутив нельзя (по каким-либо причинам) интерпретировать 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 дистрибутива, 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, что сделать весьма не просто. При этом необходимо иметь в виду, что в любом случае (или в подавляющем большинстве случаев) при каждой новой

Таблица 3

Описание программы (ГОСТ 19.402–78)

Description of the program (GOST 19.402–78)

Требования
В разделе «Общие сведения» следует указать: обозначение и наименование программы; программное обеспечение, необходимое для функционирования программы
В разделе «Функциональное назначение» должны быть указаны классы решаемых задач и (или) назначение программы и сведения о функциональных ограничениях на применение
В разделе «Описание логической структуры» должны быть указаны: алгоритм программы; используемые методы; структура программы с описанием функций составных частей и связи между ними. Описание логической структуры программы выполняют с учетом текста программы на исходном языке
В разделе «Используемые технические средства» указывают типы электронных вычислительных машин и устройств, которые используются при работе
В разделе «Вызов и загрузка» должны быть указаны: способ вызова программы с соответствующего носителя данных; входные точки в программу
В разделе «Входные данные» должны быть указаны: характер, организация и предварительная подготовка входных данных; формат, описание и способ кодирования входных данных
В разделе «Выходные данные» должны быть указаны: характер и организация выходных данных; формат, описание и способ кодирования входных данных

Таблица 4

Описание применения (ГОСТ 19.502–78)

Description of application (GOST 19.502–78)

Требования
Наличие аннотации и содержания
В разделе «Назначение программы» указывают назначение, возможности программы, ее основные характеристики, ограничения, накладываемые на область применения программы
В разделе «Условия применения» указываются условия, необходимые для выполнения программы (требования к необходимым для данной программы техническим средствам, и другим программам, общие характеристики входной и выходной информации, а также требования и условия организационного, технического и технологического характера и т. п.)
В разделе «Описание задачи» должны быть указаны определения задачи и методы ее решения
В разделе «Входные и выходные данные» должны быть указаны сведения о входных и выходных данных

сборке собираемые файлы отличаются. Отличия могут быть 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. Такое может произойти, например, в случаях, если через некоторое время после первой сборки при последующих сборках произойдет дефрагментация памяти компьютера и у свободных участков памяти изменятся адреса. При этом могут измениться смещения в секциях и сегментах данных. Например, в программировании такая команда, как allocate при обращении к ней в разное время может выделять память по разным адресам свободной памяти в компьютере.

Таблица 5

Тексты программ (ГОСТ 19.401–78)

Program texts (GOST 19.401–78)

Требования
Настоящий стандарт устанавливает требования к содержанию и оформлению программного документа «Текст программы», определенного ГОСТ 19.101–77
Структуру и оформление документа устанавливают в соответствии с ГОСТ 19.105–78
Основная часть документа должна состоять из текстов одного или нескольких разделов, которым даны наименования

Таблица 6

Пояснительная записка (ГОСТ 19.404–79)

Explanatory note (GOST 19.404–79)

Требования
В разделе «Введение» указывают наименование программы и (или) условное обозначение темы разработки, а также документы, на основании которых ведется разработка с указанием организации и даты утверждения
В разделе «Назначение и область применения» указывают назначение программы, краткую характеристику области применения программы
Раздел «Технические характеристики» должен содержать следующие подразделы: постановка задачи на разработку программы, описание применяемых математических методов и, при необходимости, описание допущений и ограничений, связанных с применяемым математическим аппаратом; описание алгоритма и (или) функционирования программы с обоснованием выбора схемы алгоритма решения задачи, возможные взаимодействия программы с другими программами; описание и обоснование выбора метода организации входных и выходных данных; описание и обоснование выбора состава технических и программных средств на основании проведенных расчетов и (или) анализов, распределение носителей данных, которые использует программа.
В разделе «Ожидаемые технико-экономические показатели» указывают технико-экономические показатели, обосновывающие преимущество выбранного варианта технического решения, а также, при необходимости, ожидаемые оперативные показатели
В разделе «Источники, использованные при разработке» указывают перечень научно-технических публикаций, нормативно-технических документов и других научно-технических материалов, на которые есть ссылки в основном тексте

Проверка документации, представленной на сертификацию. В процессе испытаний проверяются следующие документы (табл. 1). Информация, которая должна быть представлена в документах, представлена в табл. 2–6.

Состав и содержание представленной документации должны удовлетворять требованиям, установленным в руководящем документе ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (РД НДВ) (Гостехкомиссия России, 1999) [5, 6].

Контроль исходного состояния программного обеспечения. Контроль исходного состояния испытуемого ПО производится путем контрольного суммирования сертифицируемого ПО. Если эталонный дистрибутив ПО получен в процессе контрольной сборки, во время испытаний, то результаты фиксации его исходного состояния должны быть зафиксированы в акте отбора образца. Одновременно создается акт контрольной сборки дистрибутива, в котором заявитель, разработчик ПО и испытательная лаборатория договариваются о том, что собранный в процессе испытаний дистрибутив является эталонным. В нем подтверждается, что эталонный дистрибутив во время испытаний собирался в присутствии заявителя или разработчика. В противном случае эталонный дистрибутив мог быть собран заранее, до проведения испытаний, и представлен по акту отбора образца для испытательной лаборатории.

Результаты контроля исходного состояния испытуемого ПО (контрольные суммы всех файлов ПО, используемых при сертификации, которые были представлены на сертификацию на основании акта отбора образца) должны совпадать с контрольными суммами (КС) всех файлов ПО, которые представлены в документе «Описание программы». Основными результатами фиксации исходного состояния ПО являются рассчитанные значения КС загрузочных модулей и файлов исходных текстов программ, входящих в состав ПО.

Контрольные суммы отобранного на испытания эталонного дистрибутива ПО должны совпадать с КС соответствующих файлов дистрибутива, представленных в документе «Описание программы», который предоставляет заявитель на сертификацию или разработчик ПО.

Из дистрибутива ПО следует выделить так называемые неизменяемые исполняемые файлы и файлы библиотек, которые не изменяются в процессе функционирования ПО ни по их длинам, ни по КС, и относятся к объекту сертификации. В некоторых случаях рекомендуется не выделять все файлы дистрибутива или, например, большую их часть в качестве неизменяемых, поскольку их могут быть тысячи. На наш взгляд следует выбирать наиболее представительные неизменяемые файлы для отражения их в формуляре, в первую очередь, составляющие ядро области сертификации.

Некоторые файлы в дистрибутиве ПО могут не относиться к объекту сертификации, например, не связанные с функциями безопасности информации. Примером могут служить файлы, которые используются только для работы со шрифтами, явно не влияющие на безопасность ПО и не рассматривающиеся в качестве относящихся к объекту сертификации средств защиты информации.

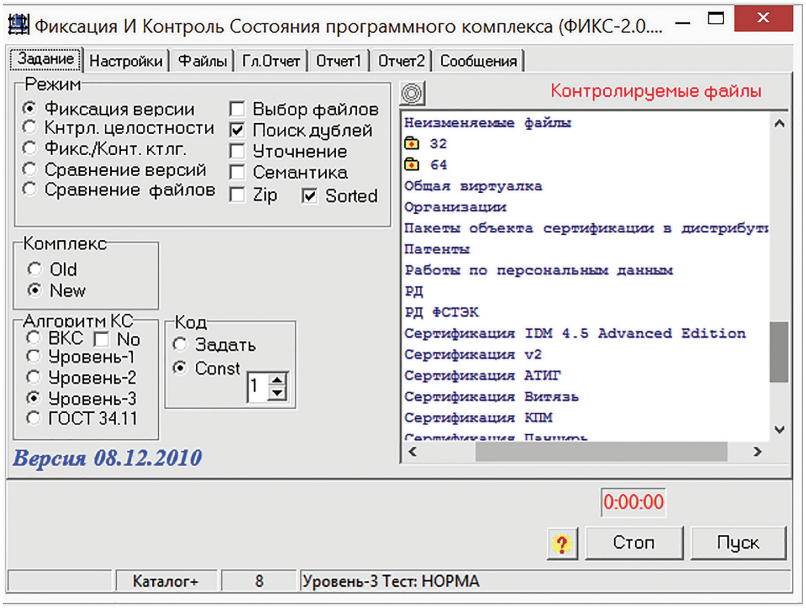

Рис. 2. Интерфейс программы ФИКС
Fig. 2. FIKS program interface

Контрольные суммы неизменяемых исполняемых файлов и библиотек (эти файлы могут точно совпадать с файлами эталонного дистрибутива) отражаются в формуляре (или паспорте) на продукт ИТ (ПО).

Контрольные суммы исходных текстов сертифицируемого ПО фиксируются в акте отбора образца и должны совпадать с теми, что представлены в документе «Описание программы».

Контроль исходного состояния ПО заключается в фиксации исходного состояния ПО и последующем сравнении полученных результатов со значениями, приведенными в документации. Результатом фиксации исходного состояния ПО служат рассчитанные значения КС загрузочных модулей и исходных текстов программ, входящих в состав ПО. Контрольные суммы рассчитываются для каждого файла, входящего в состав сертифицируемого ПО. Результат контроля — это результат сравнения рассчитанных КС файлов, входящих в состав ПО, с соответствующими КС, декларированными в документации.

Проводится фиксация исходного состояния программного обеспечения ПО. Для этого эксперт осуществляет расчет КС всех бинарных файлов, а также всех файлов исходных текстов из состава объекта оценки (ОО). Программа ФИКС (например, на АРМ № 2, как показано на рис. 1) должна подсчитать значения контрольных сумм для каждого файла, присутствующего на дистрибутивном носителе информации.

Если для подсчета КС эксперт использует программу ФИКС, то он должен запустить ее и настроить работу программы на необходимый алгоритм подсчета КС, например, алгоритм «Уровень-3, программно» (рис. 2). Далее эксперт наводит курсор на необходимую папку в дереве файловой системы в программе, и нажимает на кнопку «Пуск». Дождавшись окончания работы программы ФИКС, эксперт получает отчет о КС, необходимых для анализа.

С помощью программы ФИКС рассчитываются значения КС для неизменяемых файлов библиотек и бинарных исполняемых файлов ОО, установленных в системе после установки дистрибутива (например, на АРМ № 1, см. рис. 1). Расчет КС неизменяемых файлов библиотек и бинарных исполняемых файлов проводится после их контрольной сборки и установки эталонного дистрибутива.

Дистрибутив ПО, полученный во время контрольной сборки, может считаться эталонным при согласовании с заявителем. По этой причине контрольную сборку следует осуществлять во время отбора образца. После контрольной сборки исполняемых файлов фиксируются их КС с помощью программы ФИКС.

Необходимо сформировать отчеты программы ФИКС, фиксирующие КС файлов ПО. Все отчеты следует прилагать к протоколу испытаний. Рассчитанные значения КС файлов, находящихся на дистрибутивных носителях и исходных текстах ОО, фиксируют исходное состояние ПО.

Программа испытаний и проверок. Предположим, что программа испытаний и проверок ОО с определенными заводскими номерами, например, №№ 122, 123 состоит из испытаний на отсутствие в ОО недекларированных возможностей (НДВ) и анализа угроз (АУ) в соответствии с требованиями безопасности информации по

определенному уровню контроля. В связи с тем, что ОО с различными заводскими номерами должны быть идентичны, испытания могут быть проведены на ОО с № 122, а идентификация ОО с № 123 будет проводиться путем сличения полученных контрольных сумм ПО для ОО № 122 и № 123.

Система показателей соответствия ОО требованиям безопасности информации устанавливается с учетом требований ФСТЭК России согласно уровню доверия контроля в соответствии с методическими документами.

Испытания ОО по выявлению НДВ и АУ проводятся в три этапа:

1) подготовка к проведению испытаний;

2) проведение испытаний;

3) оформление результатов испытаний.

По окончанию испытаний следует составить протокол испытаний и техническое заключение [7, 8].

Результаты испытаний. На этапе подготовки к проведению испытаний необходимо провести анализ документации и подготовку испытательного стенда.

Анализ документации подразумевает выявление потенциально опасных функциональных возможностей ОО, при этом проверяется следующая документация:

– формуляр;

– описание применения;

– инструкция по установке и эксплуатации ПО;

– спецификация;

– технические условия;

– текст программы и ее описание;

– требования к модели безопасности;

– описание архитектуры безопасности;

– функциональная спецификация;

– требования к проектированию;

– представление реализации средства;

– средства, применяемые для разработки;

– требования к управлению конфигурацией;

– документация по безопасной разработке;

– руководство пользователя;

– руководство администратора;

– тестовая документация;

– требования по поддержке безопасности средства;

– реализация требований к программе в части соответствия стандарту разработки безопасного ПО.

При подготовке к испытаниям важно выполнить анализ комментариев разработчика к исходному коду, направленный на выявление потенциально опасных функциональных возможностей. Для этого эксперт проверяет комментарии разработчика к исходному коду.

Если исходный программный код ОО окажется закомментированным не в достаточной мере, то этот недостаток можно устранить, применив синтаксический анализ программного кода, который осуществляется с помощью анализатора исходных текстов программ — FortyAges-analyzer v0.4, содержащего базу данных языковых конструкций различных языков программирования с описанием основных возможностей таких конструкций и с информацией об их возможном небезопасном применении.

Таким образом, основную информацию, связанную с комментариями, предоставляет анализатор FortyAges-analyzer v0.4 путем поиска в файлах с исходными кодами ОО соответствующих конструкций и отражения информации о них в отчете о своей работе, что в полной мере компенсирует недостаточное количество комментариев в программе ОО.

Применяемые конструкции в программе ОО и их описание представлены в примере, описанном ниже в виде отчетов анализатора FortyAges-analyzer v0.4:

```
RegQueryValueEx
// RegQueryValueEx получает значение параметра из раздела
// реестра. Это может быть число, строка и другие типы данных.
// При чтении строковых типов данных используйте ключевое
// слово ByVal перед lpData, для других типов данных ByVal
// использовать необязательно sizeof
// sizeof – возвращает число байт,
//занимаемых параметром
RegQueryValueEx
// RegQueryValueEx получает значение параметра из раздела
// реестра. Это может быть число, строка и другие типы данных.
// При чтении строковых типов данных используйте ключевое
// слово ByVal перед lpData, для других типов данных ByVal
// использовать необязательно
ShellExecute
// ShellExecute используется в случаях, когда вы хотите, чтобы
// WINDOWS сама решала, как обрабатывать тот или иной документ
//по имени этого документа. Функция способна открывать, печатать
//файл или запускать программу. Под Win 95/98/ME эта функция
// также откроет папку Мой компьютер или Проводник с указанным
// каталогом. Если выполняющая программа определена, Windows
// запустит ту программу. Если файл документа определен, Windows
```

```
//откроет или напечатает его, используя связанную программу
// ShellExecute — является небезопасной конструкцией, поскольку на
//ее основе можно организовать программные закладки
```

При подготовке к испытаниям выполняется анализ описания программы и пояснительной записки к эскизному и (или) техническому проектам, направленный на выявление потенциально опасных функциональных возможностей [9, 10].

Эксперт осуществляет анализ документа «Описание программы». В соответствии с данным документом ОО проводит сканирование ресурсов компьютера для моделирования матрицы доступа. При сканировании ОО получает информацию о структуре ресурсов АРМ, сохраняет ее в памяти ПЭВМ и осуществляет считывание прав доступа файловой системы NTFS. При сканировании дисков с файловой системой NTFS объект оценки считывает установленные права доступа, преобразует их в формат, используемый для представления прав доступа в соответствии с правилами разделения доступа (ПРД) и осуществляет построение дерева ресурсов. По результатам сканирования ОО автоматически строит иерархическую структуру, соответствующую структуре ресурсов АРМ, предоставляет получение списка локальных и доменных пользователей и получает списки учетных записей пользователей, зарегистрированных как непосредственно на АРМ, так и на контроллере домена (в случае, если АРМ входит в состав домена). Эти пользователи регистрируются в проекте разделения доступа (ПРД определяются в матрице доступа) наравне с другими субъектами доступа. Объект оценки позволяет определять права пользователей. После построения дерева ресурсов администратор может регистрировать пользователей в ПРД и устанавливать их уровни допуска. Объект оценки предоставляет возможности по моделированию разрешительной системы. Администратор устанавливает права доступа пользователей к объектам доступа. Объект оценки позволяет создавать отчеты на основе информации о субъектах и объектах доступа и формировать их на основе информации, содержащейся в ПРД.

Требуется выполнить анализ перечисленных выше действий для выявления потенциально опасных функциональных возможностей ОО. Информация, необходимая для анализа и соответствующая пояснительной записке 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. Объект оценки не реализует политику управления доступом пользователей к ресурсам и функционал управления информационными потоками, не содержит специальных мер защиты, характерных для средств защиты информации, и это может быть отображено в документе «Требования к проектированию».

Кроме того, ОО не содержит подсистем, реализующих функции безопасности средства, поддерживающих выполнение функций безопасности и не влияющих на выполнение функций безопасности, т. е. подсистем, которые взаимодействуют (оказывают влияние, не оказывают влияния или иным образом взаимодействуют) с функциями безопасности средства.

Эксперту необходимо выполнить анализ документа «Представление реализации средства».

Далее для этого осуществляется подготовка испытательного стенда (см. рис. 1) с учетом следующих требований:

1) наличие при проведении исследований таких исходных данных, как дистрибутив, документация, исходные тексты программы ПО, результаты испытаний;

2) формирование исследовательского стенда по схеме (см. рис. 1) с техническими, программными и инструментальными средствами, указанными в табл. 1;

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

4) установка, конфигурирование и настройка ОО в соответствии с документацией по его эксплуатации;

5) расчет КС в целях проведения сертификационных работ файлов исходных текстов, неизменяемых исполняемых файлов и файлов дистрибутива ОО с определенным заводским номером с помощью средств фиксации и контроля исходного состояния программного комплекса.

Контрольные суммы можно рассчитать, например, применяя программу «ФИКС» (версия 2.0.2) (ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, техническая поддержка до 15.01.2025 г.). Для всех отобранных экземпляров с определенными заводскими номерами все КС должны быть идентичны. Контрольные суммы неизменяемых исполняемых файлов и файлов дистрибутива должны соответствовать КС, приведенным в формуляре для ОО [11].

После проверки выполняется 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.

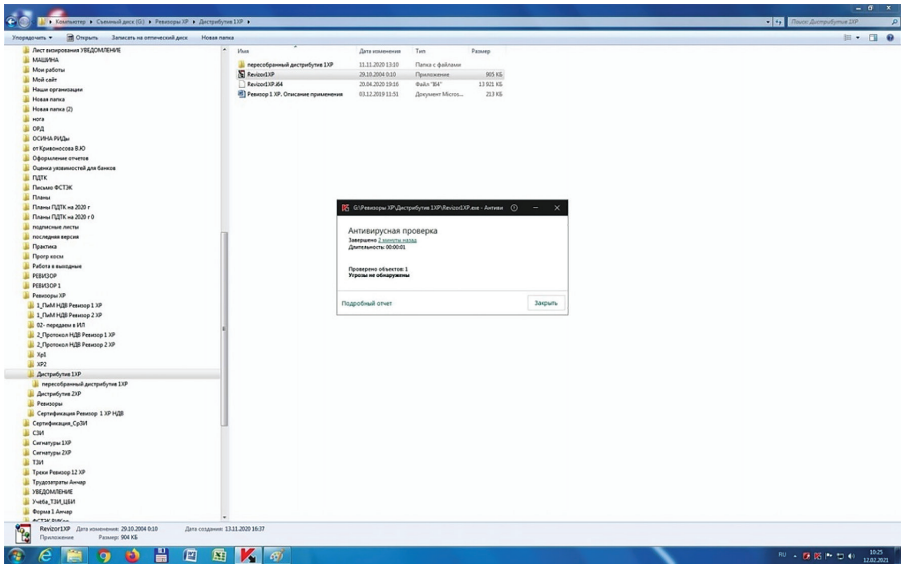

Рис. 3. Результат проверки исполняемого файла объекта оценки с помощью программного изделия «Kaspersky Endpoint Security для Windows»
Fig. 3. The result of checking the executable file of the evaluation target using the software product «Kaspersky Endpoint Security for Windows»

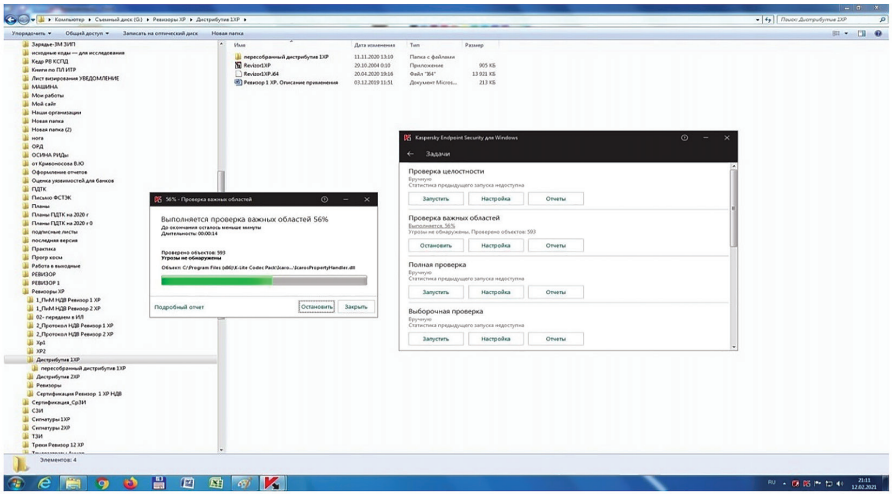

Рис. 4. Проверка среды функционирования объекта оценки с помощью программного изделия «Kaspersky Endpoint Security для Windows»
Fig. 4. Checking the operating environment of the evaluation target using the «Kaspersky Endpoint Security for Windows» software product

На рис. 3 представлен результат проверки исполняемого файла ОО с помощью антивирусной программы. Из рис. 3 следует, что угрозы не обнаружены.

С помощью антивирусной программы «Kaspersky Endpoint Security для Windows» можно проверить среду функционирования ОО (рис. 4).

На данном этапе проведения испытаний (подготовки к проведению испытаний) проводится проверка выполнения компиляции и сборки ОО, а также осуществляется лабораторная сборка ОО.

С этой целью для компилируемых языков (например, Паскаль) выполняют следующие действия [12]:

– запуск средства разработки (например, Delphi 7);

– выбор проекта для ОО в Delphi 7;

– выбор меню «Project» → «Build»;

– после сборки в определенном каталоге появится исполняемый файл ОО, который является продуктом компиляции и сборки ОО;

– закрыть проект (меню «File» → «Close All») [13];

После копирования на жесткий диск ПЭВМ № 1 испытательного стенда файлов исходных текстов программ в соответствии со списком в акте отбора ОО проводится успешная компиляция и сборка дистрибутива ОО из отобранных файлов исходных текстов программ [14 –17].

Выводы

В целях выявления архитектурных уязвимостей кода и опасных функциональных объектов в ПО необходимо выполнить его ручной анализ.

Описанные выше испытания показали возможность осуществления экспертизы участков исходного программного кода. С помощью анализатора исходных текстов программ можно получить сведения о связях между информационными и функциональными объектами с указанием их принадлежности функциональным объектам.

Анализ ПО может показать, используются ли в данном ПО небезопасные конструкции, например ShellExecute. По полученным результатам проводится ручной анализ ПО. Для этого эксперт использует комментарии к исходным программным кодам ОО, представляемым разработчиком ПО. Анализатор исходных текстов программы FortyAges-analyzer v0.4 позволяет, например, для языка программирования, Паскаль, а также языков С, С++, комментировать исходные тексты программы.

Список литературы

[1] Дроботун Е. Криптором по антивирусу // Хакер, 2013. № 168 (1). С.82–85.

[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). URL: https://docs.cntd.ru/document/1200025075 (дата обращения 09.10.2021).

[3] Кошевая И.П., Канке А.А. Метрология. Стандартизация. Сертификация. М.: ФОРУМ, 2009. 414 с.

[4] Аграновский А.В., Хади Р.А. Новый подход к защите информации – системы обнаружения компьютерных угроз // Jet Info, 2007. № 04(167). С. 2–22.

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

[6] Калугин О.А. Сложности сертификации // Security and IT. Management, 2020. № 36. С. 37.

[7] Волков В.И. Основы теории и практики экспертной деятельности. М.: АМИ, 2003. 192 с.

[8] Крейг Р.Дж. ИСО 9000. Руководство по получению сертификата о регистрации. М.: Стандарты и качество, 2001. 183 с.

[9] Крылова Г.Д. Основы стандартизации, сертификации, метрологии. М.: ЮНИТИ-ДАНА, 2001. 711 с.

[10] Москвин В.А. Управление качеством в бизнесе: рекомендации для руководителей предприятий, банков, риск-менеджеров. М.: Финансы и статистика, 2006. 384 с.

[11] Постановления Правительства РФ от 26.09.2016 г. № 969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности». URL: https://base.garant.ru/71500596/ (дата обращения 09.10.2021).

[12] Сборник законов и иных нормативных правовых актов Российской Федерации по вопросам сертификации продукции и услуг. М.: ВНИИ сертификации Госстандарта России, 1995. 104 с.

[13] Сергеев А.Г., Латышев М.В. Сертификация. М.: Логос, 2000. 536 с.

[14] Пич Р.В., Пич Б., Риттер Д. Справочник по использованию ISO 9001 – стандарта систем качества. Киев: Украинская ассоциация качества, 2003. 184 с.

[15] Система сертификации ГОСТ Р. Основные положения и порядок сертификации услуг / Комитет Российской Федерации по стандартизации, метрологии и сертификации. URL: https://docs.cntd.ru/document/5200306 (дата обращения 09.10.2021).

[16] Лифиц И.М. Основы стандартизации, метрологии, сертификации. М.: Юрайт, 1999. 285 с.

[17] Бороздина А.Г. Определение состава документации, сопровождающей жизненный цикл программ для ЭВМ // Вестник ВНИИДАД, 2021. № 1. С. 36–50.

[18] Кошевая И.П., Канке А.А. Метрология. Стандартизация. Сертификация. М.: ФОРУМ, 2009. 414 с.

Сведения об авторах

Комаров Евгений Геннадиевич — д-р техн. наук, профессор МГТУ им. Н.Э. Баумана (Мытищинский филиал), fuzzykom@gmail.com

Лозовецкий Вячеслав Владимирович✉ — д-р техн. наук, профессор МГТУ им. Н.Э. Баумана (Мытищинский филиал), lozovetsky@mail.ru

Лебедев Владимир Владимирович — канд. техн. наук, доцент РТУ — МИРЭА, voval_matr@mail.ru

Архипенко Андрей Валентинович — канд. техн. наук, Сочинский международный инновационный университет, andrei-arhipenko@mail.ru

Поступила в редакцию 04.04.2022.
Одобрено после рецензирования 11.07.2022.
Принята к публикации 15.08.2022.

CERTIFICATION AND IDENTIFICATION OF POSSIBLE THREATS TO INFORMATION SECURITY OF SOFTWARE AND FIRMWARE

E.G. Komarov[1], V.V. Lozovetsky[1]✉, V.V. Lebedev[2], A.V. Archipenko[3]

[1]BMSTU (Mytishchi branch), 1, 1st Institutskaya st., 141005, Mytishchi, Moscow reg., Russia
[2]Russian Technological University — MIREA, 20, Stromynka st., 107996, Moscow, Russia
[3]Sochi International Innovative University, 10a, Ordzhonikidze st., 354000, Sochi, Russia

lozovetsky@mail.ru

A number of methods, methods and tools are proposed for certification of software and firmware in information systems in order to select approaches and tools for working in non-standard situations in a constantly changing regulatory and methodological framework and possible threats to their information security. The type of certification under consideration is limited to methods and techniques for analyzing vulnerabilities and undeclared capabilities. This type of certification is intended for software research. Not all possible aspects related to this type of certification have been considered, however, the novelty and advantages of the approaches are based on some original approaches in cases where it is not clear how to present sets of input data for testing. Approaches to certification tests are presented using tools of our own design, which allows you to identify the main parameters necessary for assembling software and its research, and to parse software written in various programming languages. Based on the program of testing and verification of the object of assessment in accordance with the requirements of information security under a certain level of control, methods for conducting certification studies are proposed, the advantages of approaches using the available and proposed tools are shown. To save on the purchase of tools, some well-known, free and freely distributed tools, as well as effective and inexpensive software products, are proposed for use in tests.

Keywords: certification, regulatory and methodological framework, tools, object of assessment, threat analysis, information security, software, programming language, experimental stand

Suggested citation: Komarov E.G., Lozovetsky V.V., Lebedev V.V., Archipenko A.V. *Sertifikatsiya programmnogo i programmno-apparatnogo obespecheniya transportnykh informatsionnykh sistem v sootvetstvii s trebovaniyami bezopasnosti* [Certification and identification of possible threats to information security of software and firmware]. Lesnoy vestnik / Forestry Bulletin, 2022, vol. 26, no. 5, pp. 145–157. DOI: 10.18698/2542-1468-2022-5-145-157

References

[1] Drobotun E. *Kriptorom po antivirusu* [Antivirus cryptor]. Header, 2013, no. 168 (1), pp. 82–85.
[2] *Ekspertiza programmnoy dokumentatsii na sootvetstvie trebovaniyam Gosudarstvennykh standartov GOST R ISO/MEK 12119–2000 (p. 3.2), GOST R ISO 9127–94 (p.p. 5, 6.1, 6.3–6.5)* [Examination of software documentation for compliance with the requirements of State Standards GOST R ISO/IEC 12119–2000 (clause 3.2), GOST R ISO 9127–94 (clauses 5, 6.1, 6.3–6.5)]. Available at: https://docs.cntd.ru/document/1200025075 (accessed 09.10.2021).
[3] Koshevaya I.P., Kanke A.A. *Metrologiya. Standartizatsiya. Sertifikatsiya* [Metrology. Standardization. Certification]. Moscow: Forum, 2009, 414 p.
[4] Agranovskiy A.V., Khadi R.A. *Novyy podkhod k zashchite informatsii – sistemy obnaruzheniya komp'yuternykh ugroz* [A new approach to information security - computer threat detection systems]. Jet Info, 2007, no. 04 (167), pp. 2–22.
[5] George S., Weimerskikh A. *Vseobshchee upravlenie kachestvom: strategii i tekhnologii, primenyaemye segodnya v samykh uspeshnykh kompaniyakh (TQM)* [Total Quality Management: Strategies and Technologies Used in Today's Most Successful Companies (TQM)]. St. Petersburg: Viktoriya plyus [Victoria plus], 2002, 256 p.
[6] Kalugin O.A. *Slozhnosti sertifikatsii* [Difficulties of certification]. Security and IT Management, 2020, no. 36, p. 37.
[7] Volkov V.I. *Osnovy teorii i praktiki ekspertnoy deyatel'nosti* [Fundamentals of the theory and practice of expert activity]. Moscow: AMI, 2003, 192 p.
[8] Craig R.J. *ISO 9000. Rukovodstvo po polucheniyu sertifikata o registratsii* [ISO 9000. Guidelines for obtaining a certificate of registration]. Moscow: Standarty i kachestvo [Standards and quality], 2001, 183 p.
[9] Krylova G.D. *Osnovy standartizatsii, sertifikatsii, metrologii* [Fundamentals of standardization, certification, metrology]. Moscow: UNITI-DANA, 2001, 711 p.
[10] Moskvin V.A. *Upravlenie kachestvom v biznese: Rekomendatsii dlya rukovoditeley predpriyatiy, bankov, risk-menedzherov* [Quality management in business: Recommendations for business leaders, banks, risk managers]. Moscow: Finansy i statistika [Finance and statistics], 2006, 384 p.
[11] *Postanovleniya Pravitel'stva RF ot 26.09.2016 g. № 969 «Ob utverzhdenii trebovaniy k funktsional'nym svoystvam tekhnicheskikh sredstv obespecheniya transportnoy bezopasnosti i Pravil obyazatel'noy sertifikatsii tekhnicheskikh sredstv obespecheniya transportnoy bezopasnosti»* [Decree of the Government of the Russian Federation of September 26, 2016 No. 969 «On approval of the requirements for the functional properties of technical means of ensuring transport security and the Rules for mandatory certification of technical means of ensuring transport security». Available at: https://base.garant.ru/71500596/ (accessed 09.10.2021).
[12] *Sbornik zakonov i inykh normativnykh pravovykh aktov Rossiyskoy Federatsii po voprosam sertifikatsii produktsii i uslug* [Collection of laws and other normative legal acts of the Russian Federation on the issues of certification of products and services]. Moscow: VNII sertifikatsii Gosstandarta Rossii [VNII certification of the State Standard of Russia], 1995, 104 p.
[13] Sergeev A.G., Latyshev M.V. *Sertifikatsiya* [Certification]. Moscow: Logos, 2000, 536 p.
[14] Pich R.V., Pich B., Ritter D. *Spravochnik po ispol'zovaniyu ISO 9001 – standarta sistem kachestva* [A guide to the use of ISO 9001 – a quality system standard]. Kyiv: Ukrainskaya assotsiatsiya kachestva [Ukrainian Association for Quality], 2003, 184 p.

[15] *Sistema sertifikatsiya GOST R. Osnovnye polozheniya i poryadok sertifikatsii uslug/ Komitet Rossiyskoy Federatsii po standartizatsii, metrologii i sertifikatsii* [Certification system GOST R. Basic provisions and procedure for certification of services. Committee of the Russian Federation for Standardization, Metrology and Certification]. Available at: https://docs.cntd.ru/document/5200306 (accessed 09.10.2021).
[16] Lifits I.M. *Osnovy standartizatsii, metrologii, sertifikatsii* [Fundamentals of standardization, metrology, certification]. Moscow: Yurayt, 1999, 285 p.
[17] Borozdina A.G. *Opredelenie sostava dokumentatsii, soprovozhdayushchey zhiznennyy tsikl programm dlya EVM* [Determination of the composition of the documentation accompanying the life cycle of computer programs]. Vestnik VNIIDAD, 2021, no. 1, pp. 36–50.
[18] Koshevaya I.P., Kanke A.A. *Metrologiya. Standartizatsiya. Sertifikatsiya* [Metrology. Standardization. Certification]. Moscow: FORUM, 2009, 414 p.

Authors' information

Komarov Evgeniy Gennadievich — Dr. Sci. (Tech.), Professor of the BMSTU (Mytishchi branch), fuzzykom@gmail.com

Lozovetskiy Vyacheslav Vladimirovich✉ — Dr. Sci. (Tech.), Professor of the BMSTU (Mytishchi branch), lozovetsky@mail.ru

Lebedev Vladimir Vladimirovich — Cand. Sci. (Tech.), Associate Professor of the RTU — MIREA, voval_matr@mail.ru

Arkhipenko Andrey Valentinovich — Cand. Sci. (Tech.), Sochi International Innovative University, andrei-arhipenko@mail.ru

Received 04.04.2022.
Approved after review 11.07.2022.
Accepted for publication 15.08.2022.

Вклад авторов: все авторы в равной доле участвовали в написании статьи
Авторы заявляют об отсутствии конфликта интересов
Authors' Contribution: All authors contributed equally to the writing of the article
The authors declare that there is no conflict of interest