МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.Н.Бегаев, С.В.Кашин, С.А.Зимненко

СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ В РАЗЛИЧНЫХ СИСТЕМАХ СЕРТИФИКАЦИИ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки (специальности) 11.04.03 «Проектирование электронных средств в защищенной интегрированной среде» в качестве учебного пособия для реализации основных профессиональных образовательных программ высшего образования магистратуры

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2018

Бегаев А.Н., Кашин С.В., Зимненко С.А., Сертификация программного обеспечения и автоматизированных систем в различных системах сертификации. – СПб: Университет ИТМО, 2018. – 45 с.

Рецензент: Кременчуцкий Александр Лазаревич, профессор, к.т.н.

Учебное пособие содержит теоретический материал, посвященный основным принципам, методам и средствам проведения сертификационных испытаний. В пособии приведена нормативно-правовая база в области сертификации средств защиты информации (СЗИ).

Учебное пособие для формирования кругозора, требуемого для работы, содержит материалы законодательного, справочного, информационного содержания.

Учебное пособие предназначено для студентов, обучающихся по направлениям 11.04.03 «Конструирование и технология электронных средств» по дисциплинам «Сертификация программного обеспечения и автоматизированных систем в различных системах сертификации (Минобороны, ФСТЭК, ФСБ)».

Рекомендовано к печати Советом мегафакультета КТиУ (протокол №2 от 14 февраля 2018 года).

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО является участником программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО заключается в становлении исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информационные технологии сегодня лежат в основе фундаментальных изменений, происходящих в обществе, поэтому нет сферы человеческой деятельности, которая не зависела бы от рынка информации и не нуждалась в использовании новейших информационных технологий.

Использование информационных технологий, обладающих современными информационными возможностями, тесно связано с проблемными ситуациями, имеющими место в области профессиональной деятельности будущих специалистов.

Сертификация по требованиям информационной безопасности является важнейшим этапом создания средства защиты информации, либо защищенного системного средства. Это обусловливается тем, что именно процедура сертификации призвана дать объективную (по крайней мере, максимально к средствам защиты в соответствующих приложениях) оценку эффективности средства защиты.

Именно наличие сертификата, соотносящего заявляемые разработчиком возможности средства защиты, с определенными требованиями, в большой мере (а в некоторых случаях, практически в полном объеме) определяет эти возможности, являясь необходимым или достаточным, условием использования той или иной технологии.

ГЛАВА 1 ОБЩИЕ СВЕДЕНИЯ О СЕРТИФИКАЦИИ

1.1 Понятие сертификации

Под сертификацией понимается комплекс действий с целью подтверждения соответствия третьей стороной, относящийся к продукции, процессам, системам или персоналу.

Ключевые особенности сертификации:

1. Сертификация проводится на соответствие заданным требованиям, а именно техническим регламентам, положениям стандартов, сводов правил, условиям договоров и другим требованиям, определенным в нормативных документах и соответствующей документации. Поэтому область сертификации и ее результат однозначно определены конкретными нормативными документами, а не требованиями и рекомендациями по повышению качеству или защищенности вообще.

2. В случае положительно результата процесс сертификации заканчивается выдачей официального письменно оформленного удостоверения – сертификата соответствия, а сертифицированная продукция подлежит маркировке знаком соответствия системы сертификации. В некоторых системах сертификации можно встретить еще одно официальное удостоверение – заключение, которое применяется для случаев, когда орган по сертификации затрудняется выдать общепринятый сертификат соответствия.

3. Сертификация является деятельностью третьей стороны, т.е. должна быть обеспечена независимость оценки соответствия, максимально исключающая любые формы аффилированности или сговора.

4. Сертификация может быть добровольной и обязательной. Сертификация средств защиты информации по требованиям безопасности информации является обязательной.

5. Так как в стране действует несколько систем сертификации, то эти системы определяют некоторые свои правила и процедуры проведения оценки соответствия, включая аккредитацию органов по сертификации и испытательных лабораторий, разумеется, в рамках российского законодательства и своей компетенции.

Таким образом, сертификация средств защиты информации по требованиям безопасности информации представляет собой обязательное независимое подтверждение соответствия СЗИ требованиям нормативных документов по защите информации с учетом правил федеральных органов (Минобороны, ФСБ, ФСТЭК) в рамках их компетенции. Следует отметить, что федеральные органы по сертификации трактуют СЗИ в широком смысле, как средство защиты от угроз информационной безопасности и ее составных свойств: целостности, доступности, конфиденциальности и др. В этом смысле под понятие СЗИ при самой общей модели угроз подпадает

любое изделие в защищенном исполнении, например, «безопасное» от программных закладок ПО.

В таблице 1 приведены примеры объектов сертификации в области информационной безопасности, к которым определены требования в открытых нормативных документах.

Таблица 1 Требования к объектам сертификации

Объекты сертификации по требованиям безопасности информации	Объект сертификации средств защиты информации
Продукция	Средства защиты информации Средства вычислительной техники Профили защиты Межсетевые экраны Средства обнаружения вторжений Средства антивирусной защиты Средства криптографической защиты информации Средства защиты персональных данных
Системы	Автоматизированные системы
Системы менеджмента	Системы менеджмента (управления) безопасности

Следует прокомментировать таблицу 1. Например, несмотря на то, что сертификация систем в ФСТЭК проводится в форме аттестации объектов информатизации, последняя реально (при защите конфиденциальной информации) таковой не является, т.к. не полностью соблюдается самый главный закон сертификации о третьей стороне. Несмотря на то, что сформулированы требования к системам менеджмента информационной безопасности (серия ГОСТ 27000), они не нашли отражение в нормативно-методических документах обязательных систем сертификации. В жизни и в документах регуляторов можно встретить классы общепринятых СЗИ, таких как: средства контент анализа, средства контроля утечек, средства анализа защищенности, средства управления и мониторинга, средства доверенной загрузки, генераторы паролей, защищенные BIOS, средства безопасности программных приложений, средства безопасности виртуализации, средства безопасности облачных технологий, средства защиты в промышленных системах и системах высокой готовности и др., однако требования к ним либо пока отсутствуют, либо (в противоречие 2-му правилу Керкгоффса) не подлежат публичному информированию или обсуждению.

Согласно Доктрине информационной безопасности РФ19 сертификация СЗИ является важнейшим методом обеспечения безопасности страны, а значит, государственную важность приобретает

совершенствование мер, направленных на повышение эффективности и достоверности результатов сертификации СЗИ [34]. Именно поэтому процесс сертификации включает несколько уровней независимых проверок: экспертизу заявки в федеральном органе, проведение испытаний в аккредитованной испытательной лаборатории, проверку материалов испытаний в аккредитованном органе по сертификации и др. При этом обеспечивается независимость между участниками сертификации: аккредитованным органом по сертификации, аккредитованной испытательной лабораторией и другими заинтересованными сторонами.

1.2 Правила и участники сертификации

Согласно Постановлению Правительства РФ 1995 г. № 608, руководство системами сертификации возложено на федеральные органы по сертификации: Минобороны России, ФСБ России и ФСТЭК России.

В общегражданском плане регулирование рынка не криптографических СЗИ в стране возложено на ФСТЭК России, а рынка криптографических СЗИ - на ФСБ России.

Участниками сертификации являются федеральный орган по сертификации, аккредитованный орган по сертификации, аккредитованная испытательная лаборатория, заявитель на сертификацию, которым может быть разработчик, изготовитель или поставщик.

Порядок проведения сертификации выглядит следующим образом.

1. Заявитель подает в федеральный орган заявку на проведение сертификационных испытаний.

Заявителем может являться организация-разработчик, изготовитель, поставщик СЗИ или потребитель. Он:

- Подаёт во ФСТЭК России заявку на сертификацию;
- Указывает в технической документации сведения о сертифицируемой технике защиты информации, нормативных документах, которым она должна соответствовать, обеспечивает доведение этой информации до потребителя.

Заявитель, если он выступает в качестве организации-разработчика или изготовителя СЗИ, должен иметь лицензию ФСТЭК России на соответствующий вид деятельности.

Поставщик СЗИ или потребитель, в рамках работ по сертификации, иметь соответствующие лицензии не обязаны.

2. Федеральный орган определяет аккредитованную испытательную лабораторию и орган по сертификации, что фиксируется в решении на сертификацию.

По отношению к Заявителю ФСТЭК России выполняет следующие практически важные функции:

- Рассматривает заявки на сертификацию, принимает по ним решения, определяет схему проведения сертификации средств

защиты информации и испытательный центр (лабораторию) с учётом предложений Заявителя и назначает орган по сертификации;

- Выдаёт сертификаты и, в зависимости от схемы сертификации, знаки соответствия.

3. Испытательная лаборатория проводит сертификационные испытания.

ФСТЭК России ведёт реестр аккредитованных органов по сертификации и испытательных лабораторий.

Основные выполняемые функции испытательной лаборатории:

- осуществляет отбор образцов средств защиты информации для проведения сертификационных испытаний;
- разрабатывает программы и методики сертификационных испытаний, осуществляет сертификационные испытания средств защиты информации, оформляет протоколы сертификационных испытаний и технические заключения.

На практике встречается, что организация может являться одновременно и органом по сертификации и испытательной лабораторией. Однако в процессе сертификации конкретного продукта организация может выступать только в одной ипостаси – одновременно совмещать и ту и другую роль при сертификации запрещено.

4. Материалы испытаний (программа и методика, протоколы испытаний, техническое заключение) передаются в орган по сертификации, который проводит их независимую экспертизу.

Орган по сертификации выполняет контрольные функции и проверяет корректность работ, проведённых испытательной лабораторией. Таким образом, реализуется принцип невозможности выполнения критичных функций одним субъектом.

Основные функции, выполняемые органом по сертификации:

- проводит экспертизу технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний;
- оформляет экспертное заключение по сертификации средств защиты информации и представляет их в федеральный орган по сертификации – ФСТЭК России.

5. Федеральный орган по сертификации на основании положительного технического заключения органа по сертификации оформляет сертификат соответствия. В случае выявления каких-либо несоответствий федеральный орган может провести дополнительную экспертизу с привлечением экспертов из различных аккредитованных лабораторий и органов по сертификации.

1.3 Схемы сертификационных испытаний. Инспекционный контроль

В области защиты информации применяются следующие схемы сертификации СЗИ:

- сертификация единичного образца СЗИ;
- сертификации партии СЗИ;
- сертификация серия (типового образца) с предварительной проверкой производства.

Сертификационные испытания можно классифицировать по методу тестирования:

- функциональное тестирование продукта или системы по методу «черного ящика»;
- структурное тестирование исходного кода ПО.

В первом случае при испытаниях используются:

- традиционные нормативные документы (например, руководящие документы Гостехкомисии России);
- документация (например, ТУ);
- задание по безопасности - документ, разрабатываемый в соответствии с метастандартом ГОСТ ИСО 15408.

Особенность структурного тестирования состоит в том, что оно проводится в форме статического и динамического анализа исходного кода программ и касается только вопросов внутренней безопасности продукта (контроля отсутствия недекларированных возможностей).

Как ранее отмечалось, документом, подтверждающим положительные результаты сертификационных испытаний, является сертификат соответствия, в котором указаны самые важные моменты: идентификационные характеристики20, на соответствие каким документам проведены испытания, срок действия, документ (обычно ТУ или формуляр), в котором определены ограничения на использование СЗИ и зафиксированы контрольные суммы и др.

Перечень аккредитованных испытательных лабораторий ФСТЭК России и ФСБ России, аккредитованных органов по сертификации ФСТЭК, открытые реестры сертифицированных СЗИ, правовые акты и нормативно-методические документы ФСТЭК и ФСБ можно посмотреть на веб-порталах указанных ведомств: www.fstec.ru и clsz.fsb.ru.

Требования к сертификации определены федеральными законами, постановлениями Правительства, стандартами и кодексами, а требования к проверкам (сертификационным испытаниям, инженерным или тематическим исследованиям) определены в нормативных документах или в соответствующей документации.

1.4 Законодательно-правовые основы сертификации

Законодательные и правовые требования определяют, когда сертификация необходима, а также ответственность за несоблюдение этих требований.

При определении обязательности сертификации СЗИ удобно провести классификацию защищаемого информационного ресурса и объектов информатизации.

В качестве признаков классификации информационного ресурса выделяют два: принадлежность к государственному информационному ресурсу и уровень ограниченности доступа.

Для государственного информационного ресурса требования устанавливает и контролирует сам собственник (государство). В других случаях могут быть неоднозначности.

Назовем основные случаи, когда сертификации СЗИ в нашей стране обязательна:

- защищаемая информация составляет сведения, отнесенные к государственной тайне;
- защищаемая информация ограниченного доступа, но не отнесенная к государственной тайне, при условии, что она относится к государственному информационному ресурсу;
- защищаемая информация относится к персональным данным и составляет личную и семейную тайну;
- к защите объектов информатизации (систем, комплексов) определены требования по оценке соответствия независимо от видов тайн.

Таблица 2 Основание для требования по сертификации средств защиты информации

Информационный ресурс	Государственная тайна	Личная, семейная тайна	Другие тайны	Открытая общедоступная информация
Государственный информационный ресурс	Да	Да	Да	Для систем общего пользования и для специфических систем
Негосударственный информационный ресурс	–	Да	Только для специ-фичес-ких систем	Только для специфических систем

Следует сказать, что с практической точки зрения обязательность сертификации СЗИ диктуется обычно двумя обстоятельствами. Первое связано с требованиями заказчика, который формулирует их к разработке, поставке, внедрению защищенной информационной системы.

Другой случай связан с необходимостью быть уверенным в защищенности объекта с формальной точки зрения, когда требуется заполучить какой-нибудь официальный документ о подтверждении соответствия информационной системы требованиям российского законодательства. В настоящее время в области информационной безопасности таким документом является аттестат соответствия. Никто не выпишет такой аттестат без сертифицированных СЗИ.

Согласно Закону № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. То же самое можно сказать и про использование несертифицированных СЗИ.

Что касается административных нарушений в области защиты информации, то следует в первую очередь отметить Главу 13 действующего КоАП, в котором весьма интересны для изучения следующие статьи:

- ст. 13.6. Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи;
- ст. 13.12. Нарушение правил защиты информации;
- ст. 13.13. Незаконная деятельность в области защиты информации.

Так, в ст. 13.12 определены административные штрафы для случая использования несертифицированных СЗИ, включая конфискацию СЗИ, а при отягчающих обстоятельствах и высшую меру административного наказания – приостановление деятельности.

Про УК РФ возникает речь, если внедрение и использование несертифицированных СЗИ квалифицируется как деяние, повлекшее некоторое преступление. Например, согласно ст. 274 УК РФ нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации может ограничить свободу на пять лет. Вопросы нарушения правил и условий, халатности, утраты, разглашения тайн при автоматизированной обработке в той или иной степени отражены в 19, 22, 24, 26-33 главах УК РФ.

Отдельно следует назвать ст. 171 (незаконное предпринимательство), касающуюся деятельности с нарушением обязательных лицензионных требований и условий, в нашем случае, читай, при разработке, внедрении и сертификации СЗИ.

Надо понимать, что ответственность за возникшие проблемы в области защиты информации, кроме органов по сертификации и испытательных лабораторий, возлагается также на владельца объекта информатизации, уполномоченного владельцем (по договору) лицо и разработчика.

Вопросы для контроля

1. Что понимают под сертификацией?
2. Основные отличия сертификации от лицензирования и аттестации.
3. Сколько участников входит в процесс сертификации ФСТЭК?
4. Как долго федеральный орган по сертификации может рассматривать заявку на сертификацию?
5. Может ли заявитель указать лабораторию для сертификации?
6. Может ли заявитель указать орган по сертификации?
7. Кто принимает решения о необходимости сертификации по требованиям того или иного документа?
8. Может ли заявитель не быть разработчиком ПО?
9. Перечислите основные этапы сертификации.
10. Что такое NDA? Почему оно необходимо?
11. Виды сертификационных испытаний.
12. Назовите основные отличия инспекционного контроля от сертификационных испытаний.

ГЛАВА 2 ОСНОВНЫЕ РУКОВОДЯЩИЕ НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ

В настоящее время наиболее используемыми в области технической защиты информации (в полном объеме или фрагментарном) во всех системах сертификации являются «традиционные» руководящие документы Гостехкомиссии России, разработанные в незапамятные времена прошлого века, но остающиеся актуальными до сих пор. Наиболее представительными из них следует назвать следующие четыре:

1. РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1992 г.);
2. РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1997 г.);
3. РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (Гостехкомиссия России, 1992 г.);
4. РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (Гостехкомиссия России, 1999 г.).

Первые три документа касаются требований по защите информации, предъявляемых к средствам и системам, и используются при функциональном тестировании (по методу «черного ящика»).

Четвертый документ касается внутренней безопасности программных продуктов (защищенности от уязвимостей) и используется при оценке соответствия структурными методами (по методу «белого ящика»)

2.1 Сертификация АС

Документ «РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» определяет требования к защищенности информации в АС. Следует сказать, что данный документ может быть основным в случае сертификации системы, но только дополнительным – в случае аттестации. Это связано с тем, что требования по аттестации уточнены специальными нормативными документами ФСТЭК России и национальными стандартами ограниченного доступа.

Документ устанавливает требования к группам подсистем безопасности:

- подсистеме управления доступом (включая идентификацию, аутентификацию и авторизацию);
- подсистеме протоколирования;
- криптографической системе;
- подсистеме обеспечения целостности, а также подсистеме физической защиты, администрирования, тестирования и резервирования.

В РД определены девять классов защищенности АС от несанкционированного доступа к информации (таблица 2). Каждый класс задается определенной совокупностью минимальных требований по защите. Классы разбиты на три группы, различающиеся особенностями обработки информации в АС.

Третья группа («3А», «3Б») классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности.

Вторая группа («2А», «2Б») классифицирует АС, в которых пользователи имеют одинаковые права доступа ко всей информации АС, обрабатываемой на носителях различного уровня конфиденциальности.

Первая группа («1А», «1Б», «1В», «1Г», «1Д») классифицирует многопользовательские АС, в которых одновременно обрабатывается информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС.

В рамках выделенных групп установлено упорядочение требований по защите в зависимости от степени конфиденциальности информации. Класс, имеющий высшую степень защищенности для конкретной группы, отмечается литерой «А» («1А», «2А», «3А»).

Согласно п. 2.18 документа, при разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) «3А», «2А», «1А», «1Б», «1В» и использовать сертифицированные СВТ:

- не ниже 4 класса - для класса защищенности АС «1В»;
- не ниже 3 класса - для класса защищенности АС «1Б»;
- не ниже 2 класса - для класса защищенности АС «1А».

Следует обратить внимание на то, что в специальных документах ФСТЭК, используемых при аттестации, требования к п.4.6 таблицы 2 однозначно усилены, а к п.3 могут быть снижены за счет ассиметричных мер.

Таблица 3 – Классы защищенности автоматизированных систем

п/п	Подсистемы и требования	Классы								
		3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1	**Подсистема управления доступом**									
1.1	Идентификация, проверка подлинности и контроль доступа субъектов:									
	в систему	+	+	+	+	+	+	+	+	+
	к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
	к программам	-	-	-	+	-	+	+	+	+
	к томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
1.2	Управление потоками информации			-	+	-	-	+	+	+
2	**Подсистема регистрации и учета**									
2.1	Регистрация и учет:									
	входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+	+	+	+	+	+	+	+
	выдачи печатных (графических) выходных документов	-	+	-	+	-	+	+	+	+
	запуска (завершения) программ и процессов (заданий, задач)	-	-	-	+	-	+	+	+	+
	доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-	-	+	-	+	+	+	+
	доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
	изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
	создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2	Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4	Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+
3	**Криптографическая подсистема**									
3.1	Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+

2.2 Сертификация СВТ

Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливает требования к составу документации, а также номенклатуру показателей защищенности средств вычислительной техники (СВТ), описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.

В рамках документа под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, и предназначенных для предотвращения или существенного затруднения несанкционированного доступа к информации. СВТ как комплексное средство защиты информации от НСД может включать ряд подсистем (механизмов) безопасности, таких как: идентификация, аутентификация, разграничение доступом, контроль целостности, протоколирование и другие механизмы противодействия актуальным угрозам информационной безопасности. В данном РД не предъявляются требования к средствам криптографической защиты информации (СКЗИ), которые, однако, могут быть использованы дополнительно.

Следует заметить, что данный РД релевантен по отношению к стандарту ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

Документ определяет 7 классов защищенности. Каждый класс характеризуется заданными значениями показателей защищенности СВТ, которые описываются соответствующими требованиями (таблица 3). Формально требования можно разделить на 4 группы:

- требования к подсистемам идентификации, аутентификации, авторизации (п.п. 1-4, 6-8 в таблице 3);
- требования к подсистеме протоколирования (п.п.5, 10);
- требования к гарантиям разработки (п.п.9,11-17);
- требования к документации (п.п.18-21).

Обозначения: "-" - нет требований к данному классу; "+" - новые требования, "=" - требования совпадают с предыдущими; серым фоном выделены требования к защите сведений, составляющих гостайну.

Таблица 4 – Показатели защищенности средств вычислительной техники

п/п	Показатель защищенности	Класс защищенности					
		6	5	4	3	2	1
1	Дискреционный принцип контроля доступа	+	+	+	=	+	=
2	Мандатный принцип контроля доступа	-	-	+	=	=	=
3	Очистка памяти	-	+	+	+	=	=
4	Изоляция модулей	-	-	+	=	+	=
5	Маркировка документов	-	-	+	=	=	=
6	Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
7	Сопоставление пользователя с устройством	-	-	+	=	=	=
8	Идентификация и аутентификация	+	=	+	=	=	=
9	Гарантии проектирования	-	+	+	+	+	+
10	Регистрация	-	+	+	+	=	=
11	Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
12	Надежное восстановление	-	-	-	+	=	=
13	Целостность КСЗ	-	+	+	+	=	=
14	Контроль модификации	-	-	-	-	+	=
15	Контроль дистрибуции	-	-	-	-	+	=
16	Гарантии архитектуры	-	-	-	-	-	+
17	Тестирование	+	+	+	+	+	=
18	Руководство для пользователя	+	=	=	=	=	=
19	Руководство по КСЗ	+	+	=	+	+	=
20	Тестовая документация	+	+	+	+	+	=
21	Конструкторская (проектная) документация	+	+	+	+	+	+

Требования к СВТ варьируются по уровню и глубине в зависимости от соответствующего класса защищенности. С точки зрения принципиальных моментов безопасности информации можно выделить три группы СВТ:

- СВТ с гарантированной (верифицированной) защитой информации - класс 1;
- СВТ с полным (мандатным) управлением доступом – классы 2-4;
- СВТ с избирательным (дискретным) управлением доступом – классы 5, 6.

Формально в РД определены 7 классов, но к 7-му классу (в таблице 2.4 не показан) требования не предъявляются, 5-ый класс предусмотрен для защиты информации конфиденциального характера, с 4-го по 2-ой класс - для защиты сведений, составляющих государственную тайну

(соответственно секретных сведений, совершенно секретных, особой важности), 6 и 123 – в настоящее время в РФ не имеют юридической значимости.

2.3 Сертификация МЭ

Документ «Р.Д. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации» разработан для оценки соответствия средств межсетевой защиты (межсетевых экранов), используемых для безопасного разграничения доступа между сегментами сетей.

В РД под межсетевым экраном (МЭ) понимается локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС.

Указанным документом определены 12 показателей защищенности МЭ, требования к реализации которых задают класс защищенности МЭ (табл.5).

Таблица 5 – Показатели защищенности межсетевых экранов

п/п	Показатель защищенности	Класс защищенности				
		5	4	3	2	1
1	Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
2	Идентификация и аутентификация	-	-	+	=	+
3	Регистрация	-	+	+	+	=
4	Администрирование: идентификация и аутентификация	+	=	+	+	+
5	Администрирование: регистрация	+	+	+	=	=
6	Администрирование: простота использования	-	-	+	=	+
7	Целостность	+	=	+	+	+
8	Восстановление	+	=	=	+	+
9	Тестирование	+	+	+	+	+
10	Руководство администратора защиты	+	=	=	=	=
11	Тестовая документация	+	+	+	+	+
12	Конструкторская (проектная) документация	+	=	+	=	+

К каждому классу защищенности МЭ сопоставлено в соответствие требование по защите категории информации ограниченного доступа. Иначе говоря, для того, чтобы АС возможно было аттестовать, объект информатизации должен быть защищен от внешней среды межсетевым экраном не ниже следующего класса:

- 5 класс для АС «1Д», «2Б», «3Б»;
- 4 класс для АС «1Г»;
- 3 класс для АС «1В», а также «2А», «3А» в случае обрабатываемой информации с грифом «секретно»;
- 2 класс для АС «1Б», а также «2А», «3А» в случае обрабатываемой информации с грифом «сов.секретно»;
- 1 класс для АС «1А», а также «2А», «3А» в случае обрабатываемой информации с грифом «особой важности».

2.4 Сертификация ПО

Документ «РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» определяет требования к структурному анализу ПО с целью выявления недекларированных возможностей (НДВ), под которыми понимаются неописанные в документации функциональные возможности, при использовании которых возможно нарушение уровня безопасности системы. В РД указаны два вида структурного анализа: статический и динамический, что подразумевает необходимость предоставления исходных текстов ПО и спецификаций (в данном случае документации, выполненной в соответствии с ГОСТ).

Документ определяет четыре уровня контроля отсутствия НДВ, в зависимости от этого предъявляются требования к содержанию проверок, составляющих статический и динамический анализ, а также к составу документации (таблица 4). Уровни контроля соответствуют уровню ограниченности доступа к информации, а именно: 4-ый уровень контроля соответствует средствам защиты информации конфиденциального характера, с 3-го по 1-ый - соответственно средствам защиты секретных сведений, совершенно секретных, особой важности.

Как видно из таблицы 4, основное содержание статического анализа составляют процедуры идентификации исходного и загрузочного кода, а также процедуры декомпозиции кода программы вплоть до перечня маршрутов (путей), представляющих собой последовательность выполняемых функциональных объектов. Динамический анализ представляет собой проверку соответствия реальных маршрутов с перечнем маршрутов, полученным на этапе статического анализа.

Следует обратить внимание на контроль по 2-му уровню, так как здесь предусмотрены проверки по безопасности кода, а именно контроль

конструкций (предполагается, что это фрагменты потенциально опасного кода) и анализ критических (потенциально небезопасных) маршрутов.

Таблица 5 – Уровни контроля отсутствия недекларированных возможностей

№	Наименование требования	Уровень контроля			
		4	3	2	1
Требования к документации					
1	Контроль состава и содержания документации				
1.1	Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2	Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3	Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4	Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
1.5	Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
Требования к содержанию испытаний					
2	Контроль исходного состояния ПО	+	=	=	=
3	Статический анализ исходных текстов программ				
3.1	Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2	Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3	Контроль связей функциональных объектов по управлению	-	+	=	=
3.4	Контроль связей функциональных объектов по информации	-	+	=	=
3.5	Контроль информационных объектов	-	+	=	=
3.6	Контроль наличия заданных конструкций в исходных текстах	-	-	+	+
3.7	Формирование перечня маршрутов выполнения функциональных объектов	-	+	+	=
3.8	Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
3.9	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	-	-	+	=
4	Динамический анализ исходных текстов программ				
4.1	Контроль выполнения функциональных объектов	-	+	+	=
4.2	Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=
5	Отчетность	+	+	+	+

Вопросы для контроля

1. Перечислите основные руководящие документы в области сертификации СЗИ.
2. Какие существуют этапы при отбора образца продукции при проведении сертификационных испытаний?
3. Основные положения руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
4. Основные положения руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
5. Основные положения руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации».
6. Основные положения руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

ГЛАВА 3 ПОРЯДОК СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

3.1 Подготовка к проведению сертификационных испытаний программного обеспечения в системе сертификации ФСТЭК

Отбор образца

Отбор образцов для проведения сертификационных испытаний является важной операцией, направленной на обеспечение достоверности и обоснованности результатов обязательного подтверждения соответствия продукции (получения сертификата).

Отбор образцов производится в соответствии с требованиями, устанавливающими методы отбора и сертификационных испытаний, в количестве, необходимом для проведения исследований (испытаний).

Основными артефактами при отборе образца являются:

1) документация;
2) дистрибутив;
3) исходные тексты.

При отборе образца необходимо обратить особое внимание на:

1. Внутренние регламенты компаний-разработчиков:

a) Конфиденциальность передаваемых материалов – необходимо составить соглашение о неразглашении (NDA);

b) Внутренний аудит итоговых материалов испытательной лаборатории и их фильтрация (пример: исключение фрагментов исходных текстов).

2. Требования законодательства.

3. Полноту предоставленных материалов – их достаточность для проведения сертификационных испытаний. Например, отсутствие программных компонентов, отдельных типов документов и др.

4. Соответствие материалов требованиям испытательной лаборатории и органа по сертификации – присутствие иностранного языка в документации, соответствие ГОСТам и т.д.

Подходы по обеспечению доступа испытательной лаборатории к материалам образца заключаются в:

- полном проведении сертификации на территории испытательной лаборатории в РФ;
- доступе к материалам образца на территории российской компании или филиала иностранной компании;
- доступе к материалам образца на территории иностранной компании.

Проведение испытаний

Контроль отсутствия недекларированных возможностей ПО СЗИ является наиболее проблемным, трудоемким и ответственным видом

испытаний. Для того чтобы выполнить все требования, указанные в таблице 4, рассмотрим порядок проведения испытаний на отсутствие НДВ для 2-го уровня контроля.

Общий порядок проведения сертификационных испытаний на отсутствие НДВ приведен на рисунке 1.

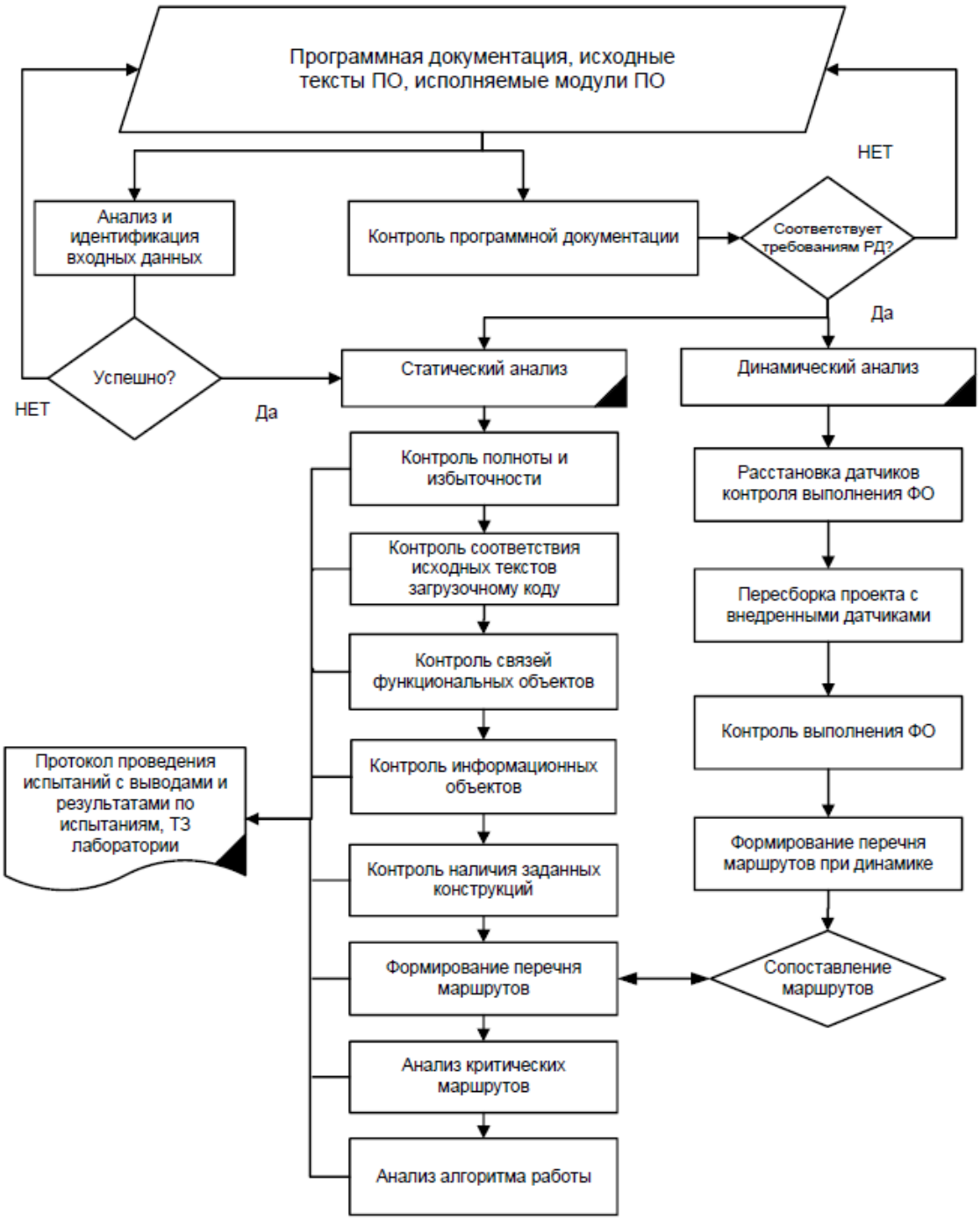


Рисунок 1 – Схема проведения сертификационных испытаний

Порядок проведения контроля полноты и отсутствия избыточности исходных текстов ПО приведен на рисунке 2.

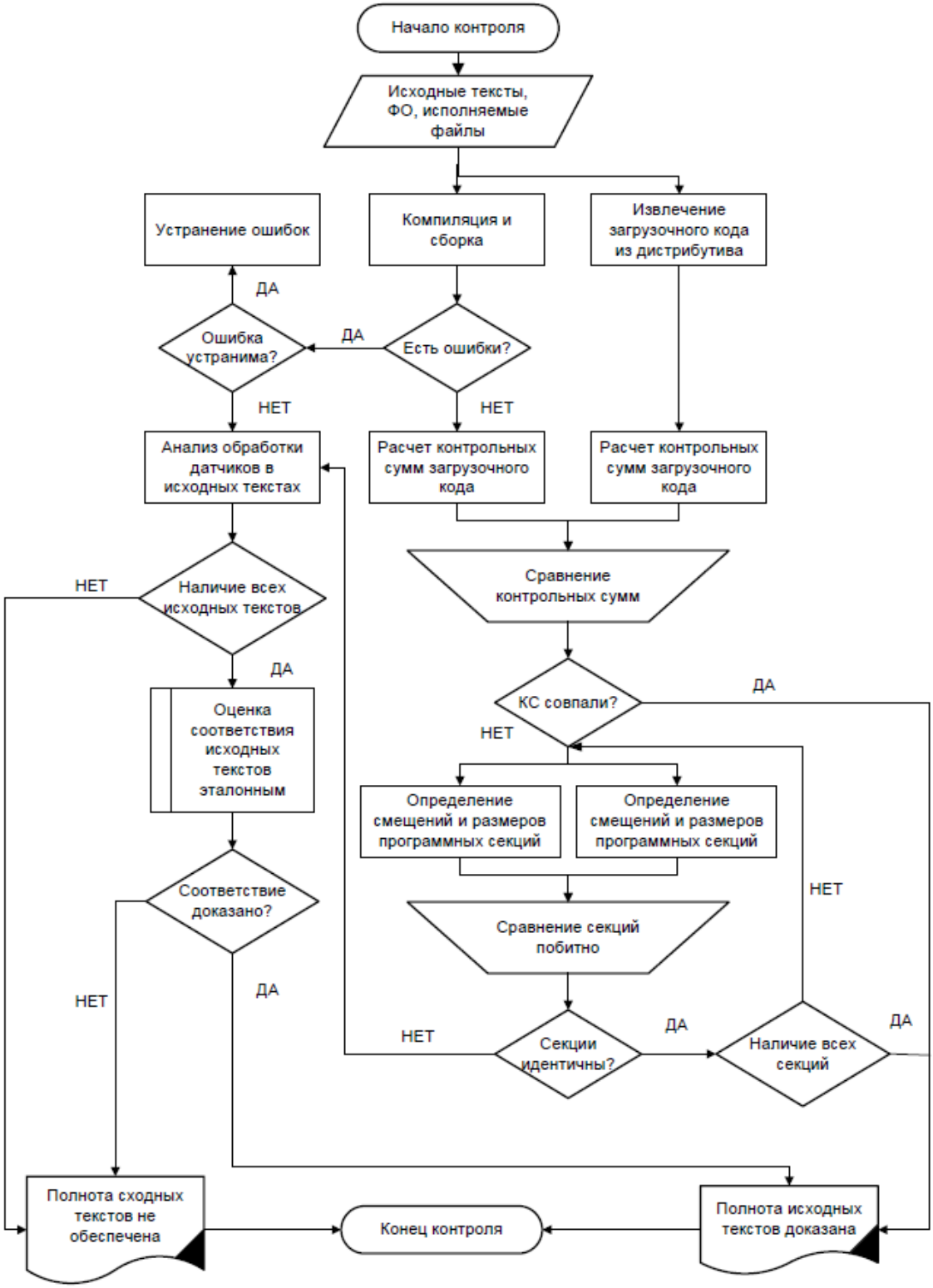


Рисунок 2 – Схема анализа полноты и отсутствия избыточности исходных текстов

Контроль отсутствия недекларированных возможностей включает в себя:

1) контроль состава и содержания документации:

- основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО);

- основные сведения о назначении компонентов, входящих в состав ПО, параметрах, обрабатываемых наборов данных (подсхемах баз данных), формируемых кодах возврата, описание используемых переменных, алгоритмов функционирования.

2) контроль исходного состояния ПО

- дистрибутив;
- исполняемые модули ПО;
- исходные тексты;
- информацию по сторонним компонентам (наименование, разработчик, назначение, список модулей).

3) статический анализ исходных текстов программ:

- контроль наличия заданных конструкций в исходных текстах:

- синтаксический;
- семантический.

4) динамический анализ исходных текстов программ:

- вставка датчиков в исходные тексты продукта;
- полная пересборка исходных текстов продукта со вставленными датчиками;
- функциональное тестирование собранного дистрибутива, сбор лога отработки датчиков;
- сопоставление трасс из лога отработки датчиков с данными статического анализа.

5) отчетность.

Оформление материалов является следующим шагом при контроле отсутствия недекларированных возможностей и состоит из:

- программы и методики проведения сертификационных испытаний;
- протоколов проведения сертификационных испытаний;
- технического заключения по результатам проведения сертификационных испытаний.

Органы по сертификации средств защиты информации согласовывают и оформляют экспертное заключение по сертификации средств защиты информации и представляют его в федеральный орган по сертификации, который проводит экспертизу заключения и выдает сертификат соответствия.

3.2 Подготовка стенда для сборки и проведения сертификационных испытаний программного обеспечения в системе сертификации ФСТЭК

Для фактической возможности проведения испытательной лабораторией работ по сертификации необходимо подготовить и предоставить следующее:

1. Полный комплект исходных текстов программ, входящих в состав программного обеспечения (ПО);

2. Дистрибутив программного обеспечения;

3. Стенд компиляции и сборки программного обеспечения;

4. Программную документацию, оформленную в соответствии с требованиями ЕСПД, в следующем составе:

- Спецификация (ГОСТ 19.202-78), содержащая сведения о составе ПО и документации на него;
- Описание программы (ГОСТ 19.402-78), содержащее основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО), логической структуре и среде функционирования ПО, а также описание методов, приемов и правил эксплуатации средств технологического оснащения при создании ПО;
- Описание применения (ГОСТ 19.502-78), содержащее сведения о назначении ПО, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы;
- Формуляр (ГОСТ 19.501-78, ГОСТ 2.610—2006) на изделие;
- Технические условия (ГОСТ 2.114-95) на изделие;
- Эксплуатационную документацию на изделие (Руководство администратора / пользователя);
- Стенд для проверки функционирования изделия в части соответствия требованиям технических условий.

Стенд для компиляции и сборки программного обеспечения и для проверки функционирования изделия в части соответствия требованиям технических условий может представлять собой готовый образ виртуальной машины.

Сборочный стенд должен предусматривать:

- Обеспечение полного цикла компиляции и сборки;
- Обеспечение сетевой изоляции сборочного стенда;
- Возможности по установке дополнительных средств аудита.

Документация на сборочный стенд включает:

- аппаратную конфигурацию стенда;
- программную конфигурацию стенда;
- программную конфигурацию инструментов сборки (компиляторы, линковщики, обфускаторы, оптимизаторы, IDE, CVS, системы управления сборкой).

Этапы работ испытательной лаборатории могут быть представлены в следующем виде:

1. Готовность продукта к представлению на сертификационные испытания.

2. Отбор образца для проведения испытаний (Акт отбора образца).

3. Проведение контрольной сборки ПО (Протокол контрольной сборки).

4. Разработка и согласование спецификаций стендов (Спецификации).

5. Сборка и настройка стендов (Материалы в Программу и методику - ПМИ).

6. Разработка и согласование ПМИ с Органом по сертификации.

7. Проведение испытаний по требованиям ТУ (Протокол).

8. Проведение испытаний по требованиям РД НДВ (Протокол).

9. Оформление и отправка отчетных материалов (Техническое заключение).

Отбор образца продукции, как упоминалось выше, осуществляется по Акту отбора образца, и представляет собой передачу исходных файлов ПО с указанием в Акте следующей информации:

- Наименование Заявителя;
- Наименование испытательной лаборатории;
- Цель отбора;
- Наименование продукции;
- Единица измерения и объем выборки;
- Дата отбора;
- Место отбора;
- Условия отбора;
- Результат наружного осмотра образцов;
- Результат идентификации образцов (с указанием перечня документации, файлов и их контрольных сумм).

Контрольная сборка: проведение контрольной сборки ПО подразумевают собой процедуры, при которых по предоставленным Заявителем инструкциям испытательной лабораторией из исходных кодов собирается / компилируется ПО.

Возможен вариант, когда Заявитель передаёт в лабораторию уже подготовленный стенд с собранным и настроенным ПО – в этом случае лаборатория сверяет, что контрольные суммы файлов, получившиеся при сборке, совпадают с контрольными суммами соответствующих файлов готового стенда.

Ещё одна причина, по которой должна производится контрольная сборка – в процессе компиляции или сборки с использованием специального ПО осуществляется контроль за отсутствием несанкционированных вызовов, обращений, подключением сторонних библиотек и т. п. действий, не указанных в документации

3.3 Проведение сертификационных испытаний межсетевых экранов

Сертификационные испытания межсетевых экранов, как правило, проводятся на соответствие требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссиия России, 1997 г., далее по тексту РД МЭ). Особенностью данного типа сертификации является предъявление указанным руководящим документом единых требований защищенности ко всем существующим типам межсетевых экранов (фильтрам пакетов, прокси-серверам, шлюзам приложений). При этом межсетевой экран (МЭ), отвечающий требованиям второго класса защищенности указанного руководящего документа, должен сочетать в себе функции всех трех типов МЭ. Данная особенность формулирует особые требования к стенду сертификационных испытаний, поскольку стенд должен быть собран таким образом, чтобы эксперт, проводящий сертификационные испытания, имел возможность проверки всех требований РД МЭ и однозначной трактовки результатов испытаний для всех типов МЭ.

Основным назначением МЭ является фильтрация данных (пакетов и соединений) на различных уровнях семиуровневой модели OSI (от сетевого уровня до уровня приложений) на основании тех или иных параметров. В связи с этим, стенд сертификационных испытаний должен предоставлять эксперту возможность генерации пакета (установления соединения) с произвольными параметрами и проводить анализ влияния настроек МЭ на результат испытаний (пропущен ли пакет через МЭ или установлено ли соединение). МЭ, в соответствии с определением, приведенным в РД МЭ, обеспечивает взаимодействие как минимум двух вычислительных сетей (далее по тексту – ВС). Таким образом, в процессе выполнения сертификационных испытаний эксперту необходимо осуществлять генерацию и анализ результата прохождения пакета или установления соединения «по разные стороны» МЭ (то есть генератор пакетов и анализатор трафика должны располагаться в разных вычислительных сетях). Поэтому простейшая схема стенда сертификационных испытаний должна включать генератор пакетов (соединений), МЭ, анализатор трафика. Для проверки установления соединений, генератор пакетов должен иметь возможность установки соединений, а анализатор трафика – универсальный сервер, способный обслуживать любой произвольно заданный порт или прикладной сервис.

Для проведения сертификационных испытаний испытательной лабораторией используется комплекс тестирования МЭ, который включает в себя автоматизированное рабочее место эксперта, одновременно соединенное с генератором и анализатором трафика.

Комплекс тестирования МЭ предоставляет возможность выполнения тестов на сетевом, транспортном и прикладном уровнях модели TCP/IP. Основная задача комплекса тестирования МЭ – моделирование определенных сетевых событий и визуализация происходящих процессов. Причина такого решения в том, что корректно выполнить моделирование реальной сети можно только для множества наиболее общих проверок. Комплекс тестирования МЭ предоставляет средства генерации трафика по заданным экспертом параметрам, а также средства визуализации результата прохода трафика через тестируемое изделие. Комплекс позволяет просматривать общую статистику в виде круговой диаграммы (пример диаграммы приведен на рисунке 3), при формировании которой эксперту предоставляется возможность выбора параметров пакета, по которым будет осуществляться формирование диаграммы. Круговая диаграмма предоставляется отдельно для пакетов, полученных в той же ВС, где они были отправлены, и для пакетов, переданных МЭ. Если сравнение круговых диаграмм не дает однозначного ответа на вопрос, какие пакеты были пропущены через МЭ, а какие нет, эксперт имеет возможность сравнить списки пакетов с указание параметров заголовков и содержимого (данных). В списках каждый пакет может быть однозначно идентифицирован по полю «Packet ID».

На основе анализа полученных результатов прохождения тестового трафика через МЭ и их сопоставления с результатами, при которых изделие считается соответствующим определенному требованию, формируется вывод о корректности реализации в МЭ проверяемого механизма защиты.

Комплекс не предназначен для автоматического формирования заключения о выполнении МЭ заданных требований. Соответствующее решение принимает эксперт на основе анализа результатов тестирования и представленной документации.

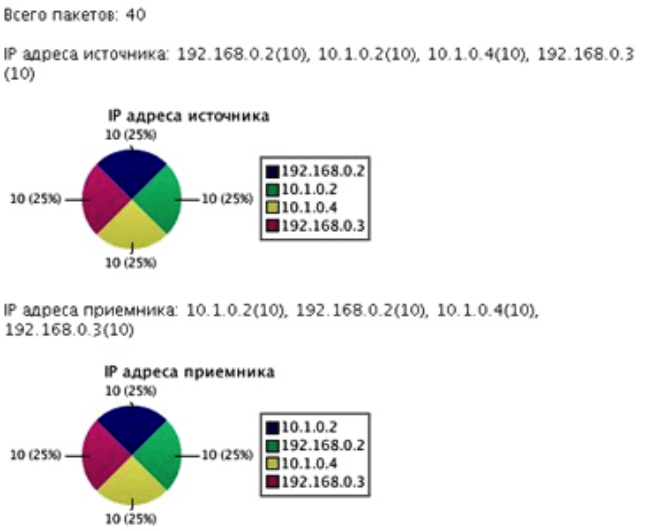


Рисунок 3 – Пример диаграммы статистики отправленных и полученных пакетов, формируемых комплексом тестирования МЭ

3.4 Проведение сертификационных испытаний на отсутствие недекларированных возможностей (программных закладок), анализ безопасности программного кода с использованием анализатора исходных текстов «АК-ВС 2»

Документ «РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» определяет требования к анализу ПО с целью выявления недекларированных возможностей (НДВ), под которыми понимаются неописанные в документации функциональные возможности, при использовании которых возможно нарушение уровня безопасности системы. В РД указаны два вида структурного анализа: статический и динамический, что подразумевает необходимость предоставления исходных текстов ПО и спецификаций (документации, выполненной в соответствии с ГОСТ).

Документ определяет четыре уровня контроля отсутствия НДВ, в зависимости от этого предъявляются требования к содержанию проверок, составляющих статический и динамический анализ, а также к составу документации (рисунок 1). Уровни контроля соответствуют уровню ограниченности доступа к информации, а именно: 4-ый уровень контроля соответствует средствам защиты информации конфиденциального характера, с 3-го по 1-ый -соответственно средствам защиты секретных сведений, совершенно секретных, особой важности.

Как видно на рисунке 4, основное содержание статического анализа составляют процедуры идентификации исходного и загрузочного кода, а также процедуры декомпозиции кода программы, включая перечень маршрутов (путей), представляющих собой последовательность выполняемых функциональных объектов. Динамический анализ представляет собой проверку соответствия реальных маршрутов с перечнем маршрутов, полученным на этапе статического анализа.

Следует обратить внимание на контроль по 2-му уровню, так как здесь предусмотрены проверки по безопасности кода, а именно контроль конструкций (предполагается, что это фрагменты потенциально опасного кода) и анализ критических (потенциально небезопасных) маршрутов.

Статический анализ исходных текстов программ				
Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
Контроль связей функциональных объектов по управлению	-	+	=	=
Контроль связей функциональных объектов по информации	-	+	=	=
Контроль информационных объектов	-	+	=	=
Контроль наличия заданных конструкций в исходных текстах	-	-	+	+
Формирование перечня маршрутов выполнения функциональных объектов	-	+	+	=
Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	-	-	+	=

Рисунок 4 – Структурный (статистический) анализ исходных текстов программ

В программе «АК-ВС 2» доступны русский и английский язык, который автоматически используется исходя из языкового окружения локальной операционной системы.

При успешной авторизации открывается вкладка “Projects”, где представлены все загруженные проекты (рисунок 5). Предложенная таблица включает:

- “ID” -уникальный номер проекта в списке проектов;
- “Name” -название проектов;
- “Status” -стадия, на которой находится проект.

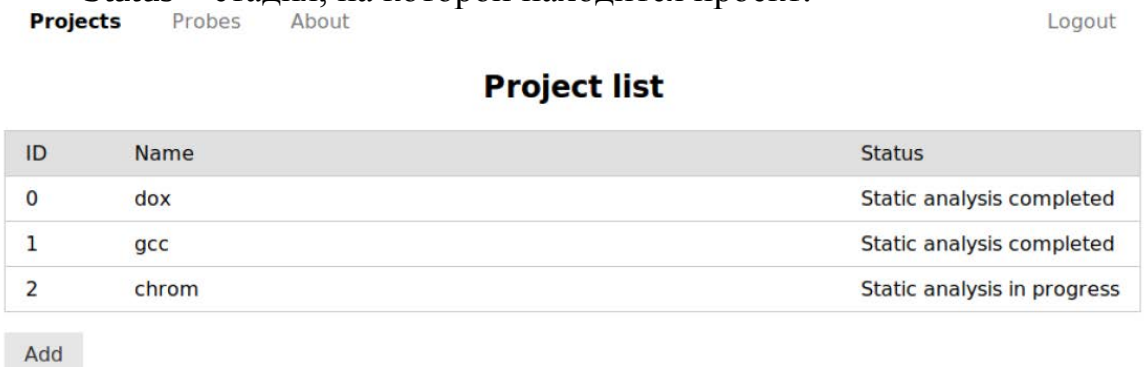


Рисунок 5 – Общий вид панели «АК-ВС 2»

При нажатии на кнопку «Add» в нижней части вкладки открывается страница добавления нового проекта (рисунок 6).

Рисунок 6 – Добавление проекта

Для добавления нового проекта необходимо заполнить следующие поля:

1. “Project name” -название проекта должно состоять из латинских букв, цифр и нижнего подчеркивания.
2. “Control level” -уровень контроля необходимо выбирать в соответствии с выбранным классом в РД "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей".
3. “Signature analyzer” -возможность выбора сигнатурного анализатора.
4. “Dynamic analysis” -возможность проведения динамического анализа.

Для проведения статического анализа необходимо ввести название проекта и уровень контроля, после чего нажать кнопку “submit”. В появившемся вкладке можно увидеть информацию, заполненную ранее, которую можно сбросить или удалить. Сброс настроек позволяет обнулить загруженные ранее файлы. “Удаление” полностью стирает проект. Необходимо выбрать архив с исходным кодом и загрузить его (рисунок 7).

Рисунок 7 – Загрузка исходных кодов

После загрузки исходных кодов вам будет предложено загрузить архив с конфигурационным файлом и используемыми сторонними заголовочными файлами.

После загрузки поле “статус” изменится и начнется подготовка отчетов программы “АК-ВС 2” (рисунок 8).

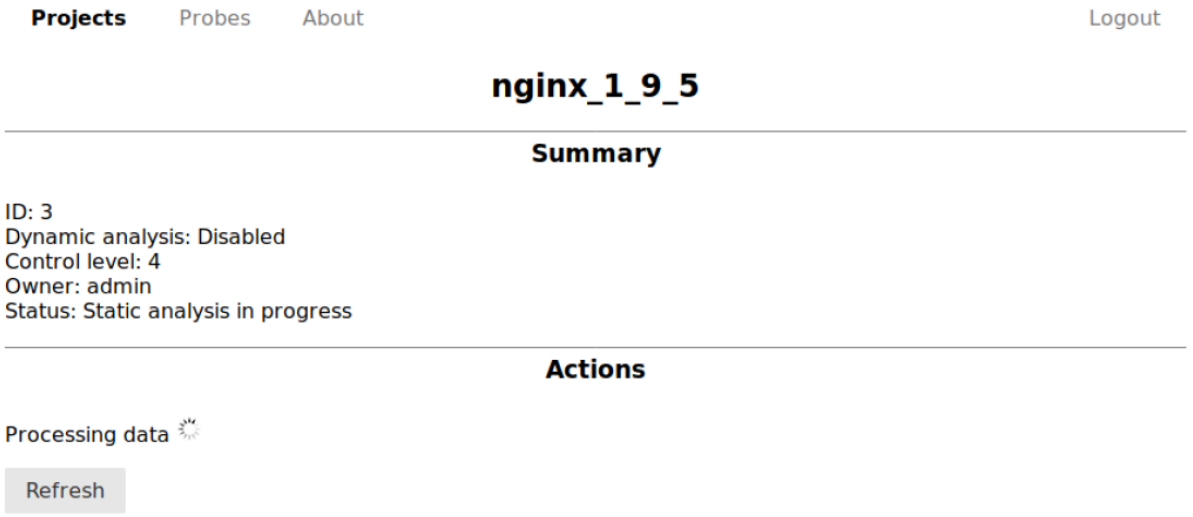


Рисунок 8 –Подготовка отчетов

После окончания процесса генерации отчетов появляются дополнительные пункты, позволяющие просмотреть полученные отчеты или загрузить их на локальный компьютер. При необходимости можно посмотреть логи работы “АК-ВС 2”. При открытии вкладки с отчетами отображается список сгенерированных отчетов по статическому анализу проекта доступных для просмотра (рисунок 9).

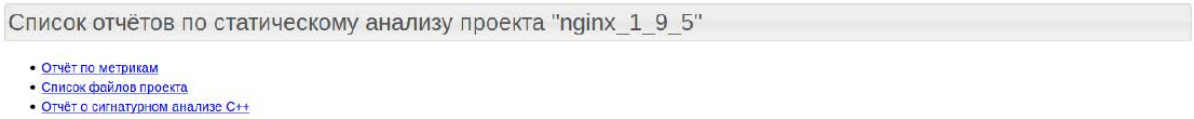
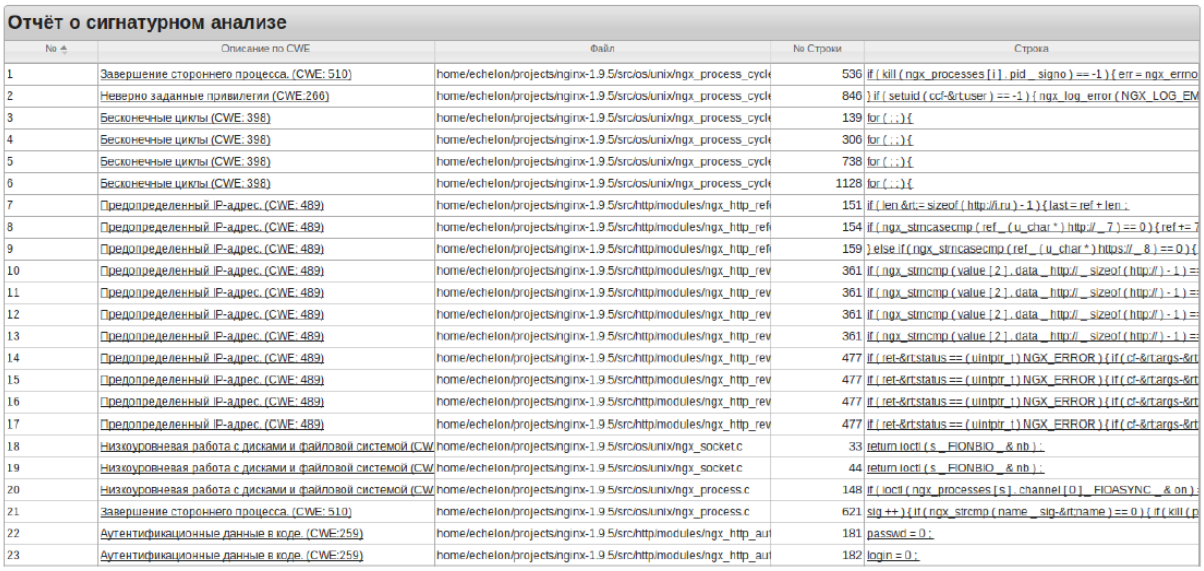


Рисунок 9 – Добавление проекта

Для открытия отчета необходимо выбрать его из предложенного списка и кликнуть по нему. Приведем пример одного из таких отчетов “отчет о сигнатурном анализе” (рисунок 10). В приведенном ниже списке можно увидеть обнаруженные уязвимости с указанием номера в реестре уязвимостей, выявленных в исследуемом проекте.



Отчёт о сигнатурном анализе

№	Описание по CWE	Файл	№ Строки	Строка
1	Завершение стороннего процесса. (CWE: 510)	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process_cycl	536	if (kill (ngx_processes [i] . pid _ signo) == -1) { err = ngx_errno
2	Неверно заданные привилегии (CWE:266)	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process_cycl	846	} if (setuid (cc[-&rt;user) == -1) { ngx_log_error (NGX_LOG_EM
3	Бесконечные циклы (CWE: 398)	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process_cycl	139	for (; ;) {
4	Бесконечные циклы (CWE: 398)	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process_cycl	306	for (; ;) {
5	Бесконечные циклы (CWE: 398)	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process_cycl	738	for (; ;) {
6	Бесконечные циклы (CWE: 398)	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process_cycl	1128	for (; ;) {
7	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_ref	151	if (len &rt;= sizeof (http://i.ru) - 1) { last = ref + len ;
8	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_ref	154	if (ngx_strncasecmp (ref _ (u_char *) http:// _ 7) == 0) { ref += 7
9	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_ref	159	} else if (ngx_strncasecmp (ref _ (u_char *) https:// _ 8) == 0) {
10	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	361	if (ngx_strncmp (value [2] . data _ http:// _ sizeof (http://) - 1) ==
11	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	361	if (ngx_strncmp (value [2] . data _ http:// _ sizeof (http://) - 1) ==
12	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	361	if (ngx_strncmp (value [2] . data _ http:// _ sizeof (http://) - 1) ==
13	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	361	if (ngx_strncmp (value [2] . data _ http:// _ sizeof (http://) - 1) ==
14	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	477	if (ret-&rt;status == (uintptr_t) NGX_ERROR) { if (cf-&rt;args-&rt
15	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	477	if (ret-&rt;status == (uintptr_t) NGX_ERROR) { if (cf-&rt;args-&rt
16	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	477	if (ret-&rt;status == (uintptr_t) NGX_ERROR) { if (cf-&rt;args-&rt
17	Предопределенный IP-адрес. (CWE: 489)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_rev	477	if (ret-&rt;status == (uintptr_t) NGX_ERROR) { if (cf-&rt;args-&rt
18	Низкоуровневая работа с дисками и файловой системой (CW	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_socket.c	33	return ioctl (s _ FIONBIO _ & nb) ;
19	Низкоуровневая работа с дисками и файловой системой (CW	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_socket.c	44	return ioctl (s _ FIONBIO _ & nb) ;
20	Низкоуровневая работа с дисками и файловой системой (CW	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process.c	148	if (ioctl (ngx_processes [s] . channel [0] _ FIOASYNC _ & on)
21	Завершение стороннего процесса. (CWE: 510)	home/echelon/projects/nginx-1.9.5/src/os/unix/ngx_process.c	621	sig ++) { if (ngx_strcmp (name _ sig-&rt;name) == 0) { if (kill (p
22	Аутентификационные данные в коде. (CWE:259)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_aut	181	passwd = 0 ;
23	Аутентификационные данные в коде. (CWE:259)	home/echelon/projects/nginx-1.9.5/src/http/modules/ngx_http_aut	182	login = 0 ;

Рисунок 10 – Добавление проекта

Вопросы для контроля

1. Общий порядок проведения сертификации СЗИ.
2. Виды сертификационных испытаний.
3. Каким образом происходит контрольная сборка ПО?
4. Что необходимо подготовить и передать испытательной лаборатории для возможности сертификации программного обеспечения?
5. Можно ли использовать несертифицированную операционную систему на испытательном стенде для проведения сертификационных работ?
6. Зачем нужно обеспечить изолированность сборочного стенда от доступа к сети Интернет?
7. Можно ли использовать чужие модули при работе сертифицируемого ПО? Если можно, то укажите условия, которые должны быть выполнены.
8. Можно ли использовать в качестве аппаратной платформы сборочного стенда ноутбук?

9. Обязательно ли при каждой сертификации производить контрольную сборку сертифицируемого ПО?
10. Что подразумевается под полным циклом компиляции?
11. Что делать есть исходные тексты к сертифицируемой программе отсутствуют?

ЗАКЛЮЧЕНИЕ

Таким образом, сертификация средств защиты информации позволяет минимизировать актуальные угрозы, а также повысить эффективность функционирования предприятия в части информационной безопасности.

Изложенный материал позволяет студентам получить:

- представления и знания об основных терминах, употребляемых в контексте сертификации средств защиты информации;
- представление об участниках сертификационных испытаний и об основных правилах их проведения;
- основную нормативно-правовую базу в области сертификации средств защиты информации;
- представление и знания о возможном порядке проведения сертификационных испытаний в системе сертификации ФСТЭК.

Полученные знания и представления могут быть использованы студентами при подготовке выпускных квалификационных работ, в процессе дальнейшего обучения в Университете ИТМО по выбранному направлению подготовки.

СПИСОК ЛИТЕРАТУРЫ

1. О техническом регулировании [Текст]: Федеральный закон от 27 декабря 2002 г. № 184-ФЗ
2. О информации, информационных технологиях и о защите информации [Текст]: Федеральный закон от 27 июля 2006 г. № 149-ФЗ
3. О государственной тайне [Текст]: Закон от 21 июля 1993 г. № 5485-1
4. Об органе по сертификации средств защиты информации по требованиям безопасности информации [Текст] / типовое положение от 5 января 1996 г. № 3
5. Об испытательной лаборатории [Текст] / типовое положение от 25 ноября 1994 г.
6. О сертификации средств защиты информации [Текст] / постановление Правительства Российской Федерации от 26 июня 1995 г. N 608
7. О сертификации средств защиты информации по требованиям безопасности информации [Текст] / положение от 27 октября 1995 г.
8. По аттестации объектов информатизации по требованиям безопасности информации [Текст] / типовое положение от 05 января 1996 г.
9. Об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации [Текст] / типовое положение от 25 ноября 1994 г.
10. Методика определения угроз безопасности информации в информационных системах [Текст] / методический документ (проект) 2015 г.
11. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Текст] / руководящий документ от 30 марта 1992 г.
12. Средства вычислительной техники Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. [Текст] / руководящий документ от 30 марта 1992 г.
13. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Текст] / руководящий документ от 25 июля 1997 г.
14. Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей [Текст] / руководящий документ от 4 июня 1999 г. N 114)
15. Марков, А.С. Методы оценки несоответствия средств защиты информации [Текст] / А.С. Марков, В.Л. Цирлов, А.В. Барабанов. – Москва: Радио и связь, 2012. – 192 с.

16. Практика проведения оценки соответствия в форме сертификации (в системе сертификации ФСТЭК для средств защиты информации по требованиям безопасности информации РОСС RU.0001.01БИОО) [Текст]. – Москва, 2014. – 38 с.
17. Семкин, С.Н. Основы правового обеспечения защиты информации [Текст]: учебник для вузов / С.Н. Семкин, А.Н. Семкин. – Горячая Линия: Телеком, 2008. – 238 с.
18. Гатчин, Ю.А. Теория информационной безопасности и методология защиты информации [Текст] / Ю.А.Гатчин, В.В. Сухостат. – Санкт-Петербург: СПбГУ ИТМО, 2010. – 98 с.
19. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Текст] / В.Ф. Шаньгин. – Москва: ДМК Пресс, 2012. – 592 с.
20. Гатчин, Ю.А. Основы информационной безопасности [Текст] / Ю.А.Гатчин, Е.В. Климова. – Санкт-Петербург: СПбГУ ИТМО, 2009. – 85 с.
21. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Текст]: учебное пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. – Санкт-Петербург: СПб: Университет ИТМО, 2016. – 168 с.
22. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30-33.
23. Барабанов А.В., Марков А.С., Цирлов В.Л., Корсунский А.С. Инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации / Автоматизация процессов управления. 2012. № 1. С. 10-14.
24. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации "Общим Критериям" / Информационные технологии. 2015. Т. 21. № 4. С. 264-270.
25. Бегаев А.Н., Тарасюк М.В. Контроль безопасности программного кода в составе объекта информатизации / Защита информации. Инсайд. 2013. № 5 (53). С. 63-67.
26. Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. М.: Изд. «Вооружение. Политика. Конверсия», 1996. 280 с.
27. Марков А., Никулин М., Цирлов В. Сертификация средств защиты персональных данных: революция или эволюция / Защита информации. Инсайд. 2008. № 5 (23). С. 20-25.
28. Марков А., Цирлов В. Сертификация программ: мифы и реальность / Открытые системы. СУБД. 2011. № 6. С. 26.
29. Марков А.С., Рауткин Ю.В. Сертификация средств защиты информации по требованиям безопасности информации. новая парадигма /

Информационные и математические технологии в науке и управлении. 2016. № 1. С. 94-102.
30. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации / Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.
31. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. СПб.: Изд-во Политехн. ун-та, 2017. 454 с.
32. Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации / Спецтехника и связь. 2011. № 3. С.48-53.
33. Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации / Правовая информатика. 2015. № 3. С. 19-23.
34. Барабанов А.В., Марков А.С., Цирлов В.Л. Испытания межсетевых экранов по требованиям безопасности информации: Учебное издание. М.: НЦПИ при Минюсте России, 2017. 44 с.
35. Барабанов А.В., Марков А.С., Цирлов В.Л. Разработка методики испытаний межсетевых экранов по требованиям безопасности информации //Вопросы защиты информации. 2011. № 3. С.19-24.
36. Богораз А.Г., Пескова О.Ю. Методика тестирования и оценки межсетевых экранов / Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 148-156.
37. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения / Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.
38. Барабанов А.В., Федичев А.В. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации / Вопросы кибербезопасности. 2016. № 2 (15). С. 2-8.
39. Горюнов М.Н., Юдичев Р.М., Фадин А.А. Внедрение сертификации в жизненный цикл программного обеспечения / Защита информации. Инсайд. 2016. № 3 (69). С. 28-35.
40. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах / Вопросы кибербезопасности. 2014. № 1 (2). С. 40-48.
41. Марков А.С., Барабанов А.В., Фадин А.А. Выявление недекларированных возможностей в декомпилированных текстах программного обеспечения / Известия Института инженерной физики. 2010. Т. 4. № 18. С. 24-26.
42. Марков А.С., Матвеев В.А., Фадин А.А., Цирлов В.Л. Эвристический анализ безопасности программного кода / Вестник Московского

государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2016. № 1 (106). С. 98-111.
43. Марков А.С., Фадин А.А. Статический сигнатурный анализ безопасности программ / Программная инженерия и информационная безопасность. 2013. № 1. С. 50-56.
44. Марков А.С., Фадин А.А., Цирлов В.Л. Концептуальные основы построения анализатора безопасности программного кода / Программные продукты и системы. 2013. № 1. С. 10.
45. Мельников П.В., Горюнов М.Н., Анисимов Д.В. Подход к проведению динамического анализа исходных текстов программ / Вопросы кибербезопасности. 2016. № 3 (16). С. 33-39.
46. Осовецкий Л.Г. Технология выявления недекларированных возможностей при сертификации промышленного программного обеспечения по требованиям безопасности информации / Вопросы кибербезопасности. 2015. № 1 (9). С. 60-64.
47. Осовецкий Л.Г., Ефимова А.В. Гарантии выявления недекларированных возможностей в промышленном программном обеспечении / Известия Института инженерной физики. 2016. Т. 2. № 40. С. 59-63.
48. Поляков С.А., Карасев С.В. Особенности получения информации о ходе выполнения программы (трассы) с использованием аппаратного окружения / Вопросы кибербезопасности. 2016. № 3 (16). С. 40-44.
49. Самарин Н.Н. Виды потенциально-опасных возможностей, реализуемых вредоносным кодом / Успехи современной науки и образования. 2016. Т. 4. № 9. С. 199-202.
50. Markov A., Fadin A., Shvets V., Tsirlov V. The experience of comparison of static security code analyzers / International Journal of Advanced Studies. 2015. V. 5. N 3. P. 55-63.
51. Markov A.S., Fadin A.A., Tsirlov V.L. Multilevel metamodel for heuristic search of vulnerabilities in the software source code / International Journal of Control Theory and Applications. 2016. V. 9. No 30. P. 313-320.
52. Барабанов А. Инструментальные средства проведения испытаний систем по требованиям безопасности информации / Защита информации. Инсайд. 2011. № 1 (37). С. 49-51.

ПРИЛОЖЕНИЕ А

Практическое задание 1

1. Ознакомиться с процессом сертификации в системе сертификации ФСТЭК.
2. Ознакомиться с нормативными документами, регламентирующими работу испытательной лаборатории.
3. Ознакомиться с процессом сертификации программного обеспечения в системе сертификации ФСТЭК.
4. Составить соглашение о неразглашении (NDA) между испытательной лабораторией и заявителем.
5. Выбрать любое свободное программное обеспечение (ПО). Далее необходимо найти всю возможную информацию о продукте (техническую и функциональную) необходимую для его дальнейшей сертификации.
6. Определить используемую общественную лицензию, под которой распространяется выбранное ПО, и обозначить основные отличия от других существующих лицензий.
7. Определить достаточность найденных материалов для проведения сертификации. Описать каких входные данные дополнительно необходимы для проведения сертификационных работ.
8. Составить заявку на сертификацию в федеральный орган по сертификации, которая должна включать:
   - наименование заявителя;
   - наименования продукции, которую Заявитель просит сертифицировать;
   - перечень нормативных и методических документов, на соответствие требованиям, которых Заявителю необходимо сертифицировать продукцию;
   - предложения Заявителя по выбору испытательной лаборатории, которая будет проводить сертификационные испытания;
   - дополнительные условия или сведения.
9. Составить решения от федерального органа по сертификации, которое должно включать:
   - наименование Заявителя, адрес Заявителя;
   - наименование сертифицируемой продукции;
   - схема проведения сертификации;
   - перечень нормативных и методических документов, на соответствие требованиям, которых должна проводиться сертификация;
   - наименование испытательной лаборатории, назначенной для проведения последующего инспекционного контроля;

- орган по сертификации, назначенный для проведения экспертизы результатов сертификационных испытаний;
- вариант оплаты работ.

Практическое задание 2

1. Создать на основе виртуальной машины сборочный стенд для проведения сертификационных работ программного обеспечения в системе сертификации ФСТЭК.
2. Составить акт отбора образца программного обеспечения, которое используется при сертификации.
3. Произвести контрольную сборку программного обеспечения и рассчитать контрольные суммы для загрузочного кода.
4. Описать используемые модули ПО и информацию по сторонним компонентам (наименование, разработчик, назначение, список модулей).
5. Описать документацию на сборочный стенд.

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

НАПРАВЛЕНИЕ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТИ) 11.04.03 «ПРОЕКТИРОВАНИЕ ЭЛЕКТРОННЫХ СРЕДСТВ В ЗАЩИЩЕННОЙ ИНТЕГРИРОВАННОЙ СРЕДЕ»

Направление подготовки (специальности) 11.04.03 «Проектирование электронных средств в защищенной интегрированной среде» реализуется как профессиональная образовательная программа высшего образования магистратуры в Университете ИТМО. Кафедра проектирования и безопасности компьютерных систем осуществляла подготовку магистрантов в области информационной безопасности компьютерных систем по данному направлению подготовки.

ИСТОРИЯ РЕАЛИЗАЦИИ НАПРАВЛЕНИЯ

1945-1966 РЛПУ (кафедра радиолокационных приборов и устройств). Решением Советского правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения. Приказом по институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д.т.н., профессор С.И. Зилитинкевич (до 1951 г.). Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. – радиоинженер (специальность 0705).

В разные годы кафедрой заведовали доцент Б.С. Мишин, доцент И.П. Захаров, доцент А.Н. Иванов.

1966–1970 КиПРЭА (кафедра конструирования и производства радиоэлектронной аппаратуры). Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско-технологической направленностью. Оканчивающим институт по этой специальности

присваивалась квалификация инженер-конструктор-технолог РЭА.

Заведовал кафедрой доцент А.Н. Иванов.

1970–1988 КиПЭВА (кафедра конструирования и производства электронной вычислительной аппаратуры). Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых ответственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям – автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой: д.т.н., проф. В.В. Новиков (до 1976 г.), затем проф. Г.А. Петухов.

1988–1997 МАП (кафедра микроэлектроники и автоматизации проектирования). Кафедра выпускала инженеров-конструкторов-технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям-разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. С.А. Арустамов, затем снова проф. Г.А. Петухов.

С 1996 г. кафедрой заведует д.т.н., профессор Ю.А. Гатчин.

1997–2011 ПКС (кафедра проектирования компьютерных систем). Кафедра выпускала инженеров по специальности 210202 «Проектирование и технология электронно-вычислительных средств». Область профессиональной деятельности выпускников включала в себя проектирование, конструирование и технологию электронных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации. Кроме того, кафедра готовила специалистов по защите информации, специальность 090104 «Комплексная защита объектов информатизации». Объектами профессиональной деятельности специалиста по защите информации являются методы, средства и системы обеспечения защиты информации на объектах информатизации.

В 2009 и 2010 годах кафедра заняла второе, а в 2011 году – почетное

первое место в конкурсе среди кафедр университета.

С **2011 года ПБКС** (кафедра проектирования и безопасности компьютерных систем). Кафедра осуществляет подготовку бакалавров и магистров по направлениям 090900 «Информационная безопасность» (с 2013 г. коды направления: для бакалавров 10.03.01, для магистров 10.04.01) и 211000 «Конструирование и технология электронных средств» (с 2013 г. коды направления: для бакалавров 11.03.03, для магистров 11.04.03), а также продолжает подготовку инженеров по специальностям 090104 и 210202.

С 2017 года кафедрой заведовал к.т.н., доцент Д.А. Заколдаев.

За время своего существования кафедра выпустила более 4750 инженеров, специалистов, бакалавров и магистров. На кафедре защищено 100 кандидатских и 16 докторских диссертаций.

В связи с реорганизацией структуры мегафакультета компьютерных технологий и управления, факультета безопасности информационных технологий, одним из подразделений которых являлась кафедра ПБКС, осуществление руководства направлением подготовки (специальности) 11.04.03 «Проектирование электронных средств в защищенной интегрированной среде» возложено на отдел «дирекция образовательных программ факультета безопасности информационных технологий».

.