Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ
(ФГБОУ ВПО ТУСУР)
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

УТВЕРЖДАЮ
заведующий каф.КИБЭВС
_____ А.А. Шелупанов
"___"_____ 2013г.

КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА

Отчет по групповому проектному обучению
Группа КИБЭВС-1208

Ответственный исполнитель
Студент гр. 520-1
_____ Никифоров Д. С.
"___"_____ 2013г.

Научный руководитель
Аспирант каф.КИБЭВС
_____ Гуляев А. И.
"___"_____ 2013г.

2013

РЕФЕРАТ

Курсовая работа содержит 30 страниц, 0 таблиц, 3 источников.

КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА, ФОРЕНЗИКА, ЛОГИ, QT, ЖУРНАЛЬНЫЕ ФАЙЛЫ, XML, GIT.

Объектом разработки является автоматизированная система для исследования образов жёстких дисков.

Цель работы - создание автоматизированной системы, предназначенной для экспертизы образов жёстких дисков.

Задачей, поставленной на данный семестр, стало написание автоматизированного экспертизного комплекса, имеющего следующие возможности:

1) сбор и анализ событий системных журналов операционной системы;
2) сбор и анализ информации из журналов истории браузеров;
3) сбор и анализ истории переписки мессенджеров;
4) сбор и анализ событий журнальных файлов приложений;
5) обнаружение сетевых параметров системы;
6) поиск файлов по имени.

Достигнутые результаты:

Пояснительная записка выполнена в текстовом редакторе Vim.

Список исполнителей

Моргуненко А.В. – документатор.

Никифоров Д.С. – программист, ответственный исполнитель, ответственный за написание части системы, работающей с логами системы.

Поляков И.Ю. – программист, ответственный за написание части системы, работающей с логами мессенджеров.

Пономарёв А.К. – аналитик.

Содержание

1 Введение

Компьютерно-техническая экспертиза является классом инженерно-технических экспертиз, проводимых в целях поиска криминалистически значимой информации на носителях, её всестороннего исследование, и, как следствие, получения доказательственной информации и установления фактов, имеющих значение для уголовных, гражданских и административных дел, сопряжённых с использованием компьютерных технологий. Для проведения компьютерных экспертиз необходима высокая квалификация экспертов, так как при изучении представленных носителей информации, попытке к ним доступа и сбора информации возможно внесение в информационную среду изменений или полная утрата важных данных.

Компьютерная экспертиза, в отличие от компьютерно-технической экспертизы, затрагивает только информационную составляющую, в то время как аппаратная часть и её связь с программной средой не рассматривается.

На протяжении предыдущих семестров нами были рассмотрены такие направления компьютерной экспертизы, как исследование файловых систем, сетевых протоколов, организация работы серверных систем, механизм журналирования событий. Также нами были изучены основные задачи, которые ставятся перед сотрудниками правоохранительных органов, которые проводят компьютерную экспертизу, и набор чуществующих утилит, способных помочь эксперту в проведении компьютерной экспертизы. Было выявлено, что существует множество разрозненных программ, предназначенных для просмотра лог-файлов системы и таких приложений, как мессенджеры и браузеры, но для каждого вида лог-файлов необходимо искать отдельную программу. Так как ни одна из них не позволяет эксперту собрать воедино и просмотреть все логи системы, браузеров и мессенджеров, было решено создать для этой цели собственный автоматизированный комплекс, которому на данный момент нет аналогов.

2 Назначение и область применения

Разрабатываемый комплекс предназначен для автоматизированного сбора информации из журналов операционных систем и приложений.

3 Технические характеристики

3.1 Постановка задачи

Для того, чтобы уменьшить время проведения компьютерной экспертизы, необходимо автоматизировать части этого процесса. В данном семестре мы занимались автоматизацией сбора информации из лог-файлов операционной системы Windows. В результате были автоматизированы такие процессы, как сбор информации из журнальных файлов системы и сбор информации из файлов, в которых хранится история переписки мессенджеров skype и pidgin.

3.2 Выбор единого формата выходных файлов

XML - eXtensible Markup Language или расширяемый язык разметки. XML разрабатывался как язык с простым формальным синтаксисом, удобный для создания и обработки документов программами и одновременно удобный для чтения и создания документов человеком. Задумка языка в том, что он позволяет дополнять данные метаданными, которые разделяют документ на объекты с атрибутами. Это позволяет упростить программную обработку документов, так как структурирует информацию.

4 Архитектура

4.1 Основной алгоритм

В ходе разарботки был применен видоизменнённый шаблон проектирования Factory method.

Данный шаблон относится к классу порождающих шаблонов. Шаблоны данного класса - это шаблоны проектирования, которые абстрагируют процесс инстанцирования (создания экземпляра класса). Они позволяют сделать систему независимой от способа создания, композиции и представления объектов. Шаблон, порождающий классы, использует наследование, чтобы изменять инстанцируемый класс, а шаблон, порождающий объекты, делегирует инстанцирование другому объекту. Основной алгоритм представлен на рисунке 1.

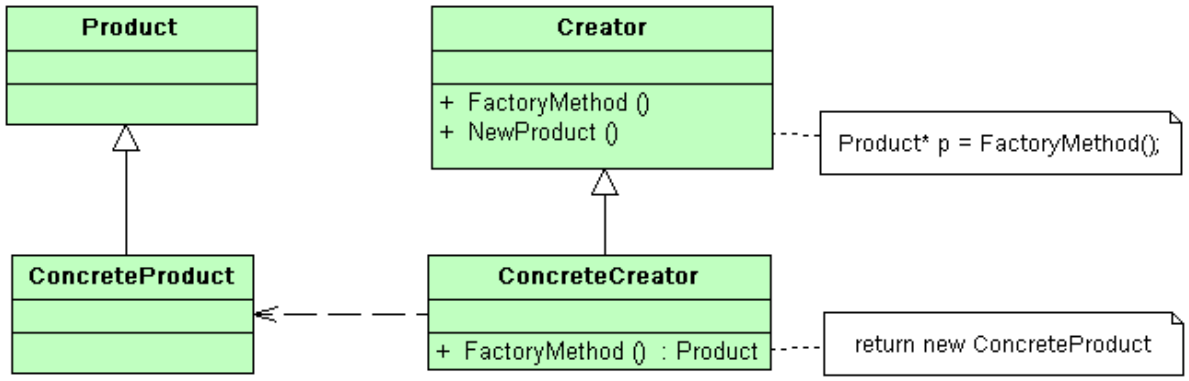

Рисунок 1 – Основной алгоритм

Использование данного шаблона позволило нам разбить наш проект на независимые модули, что весьма упростило задачу разработки, так как написание алгоритма для конкретного таска не влияло на остальную часть проекта. При разработке был реализован базовый класс для работы с образом диска. Данный клас предназначался для формирования списка настроек, определения операционной системы на смонтированном образе и инстанционировании и накапливание всех необходимых классов-тасков в очереди тасков. После чего каждый таск из очереди отправлялся на выполнение. Блоксхема работы алгоритма (ЗАПИЛИТЬ БЛОКСХЕМУ!!!)

Каждый класс-таск порождался путем наследования от базового абстрактного класса который имеет 8 методов и 3 атрибута:

1) QString manual() - возвращает справку о входных параметрах данного

таска;

2) void setOption(QStringList list) - установка флагов для поданных на вход параметров;
3) QString command() - возвращает команду для инициализации такска вручную;
4) bool supportOS(const coex::typeOS &os) - возвращает флаг указывающий на возможность использования данного таска для конкретной операционной системы;
5) QString name() - возвращает имя данного таска;
6) QString description() - возвращает краткое описание такска;
7) bool test() - ??????????????????????????????;
8) bool execute(const coex::config &config) - запуск таска на выполнение;
9) QString m_strName - хранит имя таска;
10) QString m_strDescription - хранит описание таска;
11) bool m_bDebug - флаг для параметра –debug;

5 Разработка программного обеспечения

5.1 Сбор и анализ истории переписки мессенджеров

Для упрощения разобьем задачу, на подзадачи

1) определить места хранения переписки пользователя;
2) определить формат хранения переписки;
3) разработать парсер для каждого из возможных форматов;
4) выделить важную информацию их каждой записи;
5) автоматизировать процесс поиска журнальных файлов;
6) производить сохранение полученных информации формат XML.

5.2 Определить формат хранения переписки

Приложение «skype» хранит переписку локально на машинах пользователей или же возможна синхронизация с машин других пользователей [2]. Формат хранения SQLite.

По умолчанию файлы распологаются в каталоге: “WINDOWS_DRIVE”/Users/”U

Основная интересующая нас информация находится в main.db.

main.db содержит 18 таблиц:

- "DbMeta"
- "Contacts"
- "LegacyMessages"
- "Calls"
- "Accounts"
- "Transfers"

- "Voicemails"
- "Chats"
- "Messages"
- "ContactGroups"
- "Videos"
- "SMSes"
- "CallMembers"
- "ChatMembers"
- "Alerts"
- "Conversations"
- "Participants"
- "VideoMessages"

Таблицы которые нам интересны, на данный момент:

- "Contacts"
- "Messages"
- "Chats"

Приложение «pidgin» хранит лог файлы локально на машине пользователя в формате HTML и TXT. По умолчанию лог файли хранятся в .HTML файле. Настройки программы и подключенных аккаунтов в XML, но особой ценности на данный момент не представляют. По умолчанию файлы распологаются в каталоге: “WINDOWS_DRIVE”/Users/”USER_WIN_NAME”/AppData/Roaming/.purple/log
Основная интересующая нас информация хранится в файлах с такой маской имени YEAR-MONTH-DATE.TIME.html пример:2013-03-02.004915+0700NOVT.htm

5.3 Определить места хранения переписки пользователя

Определение месторасположения файлов переписки происходит следующим образом. Для при монтированному образу запускается модуль который сужает область поиска, сканируя только нужные места в образе (к примеру не всю папку %ProrgamFiles, а только %ProrgamFiles/Skype). Сканированием папки занимается класс QDirIterator. После вызова происходит поочередный обход по каждому файлу в директории и под директории. Проверка полученного имени файла осуществляется по маске, если реакция на маску положительная, происходит добавление в список обрабатываемых файлов.

5.4 Парсинг найденых файлов

В зависимости от обрабатываемых логов, запускается нужный модуль. Из полученного ранее списка, найденные файлы поочередно открываются и парсятся. Методами класса QstringList происходит резанье строк и добавление в список. Для парсинга полученного списка используется регулярные вырожения использующие класс QRegExp.

5.5 Сохранение полученного в XML

Соранение полученных данных происходит в ранее выбраный формат XML. Для этого используется класс QXmlStreamReader и QxmlStreamWriter. Класс QXmlStreamWriter представляет XML писателя с простым потоковым API.

QXmlStreamWriter работает в связке с QXmlStreamReader для записи XML. Как и связанный класс, он работает с QIODevice, определённым с помощью setDevice ().

Класс QXmlStreamReader представляет собой быстрый синтаксически корректный XML анализатор с простым потоковым API. QXmlStreamReader является быстрым и более удобным для замены в Qt анализатора SAX (смотри-

те QXmlSimpleReader), а в некоторых случаях он даже более предпочтителен, чем использование DOM дерева (смотрите QDomDocument). QXmlStreamReader считывает данные с QIODevice (смотрите setDevice()) или с необработанного QByteArray (смотрите addData()). Вместе с QXmlStreamWriter Qt обеспечивает связанный класс для записи XML.

5.5.1 Работа с xml-файлами

XML - eXtensible Markup Language или расширяемый язык разметки. XML разрабатывался как язык с простым формальным синтаксисом, удобный для создания и обработки документов программами и одновременно удобный для чтения и создания документов человеком. Задумка языка в том, что он позволяет дополнять данные метаданными, которые разделяют документ на объекты с атрибутами. Это позволяет упростить программную обработку документов, так как структурирует информацию.

5.6 Отчёт Димы

5.7 Введение

Одной из задач на данный семестр стала задача поиска и переработки журнальных файлов Windows. Сложность данной задачи состоит в том, что все системные события хаписываются в журналы с особой структурой. Существует множество софта, позволяющего просматривать записи из данных журналов, но ни один из рассмотренных проектов не предоставлял открытый исходный код своего приложения. Но обо всем по порядку
Для решения данной задачи необходимо было разобрастся с такими проблеамами как:

1) определить места хранения журнальных файлов операционной системы
2) изучить какие события записываются в журналы и отбросить ненужные журналы
3) разобраться со структурой журнальных файлов
4) выделить важную информацию их каждой записи журнала
5) автоматизировать процесс поиска журнальных файлов
6) реализовать конвертр журнальных файлов в формат XML

Рассмотрим подробнее каждый этап.

5.8 Журнльные файлы операционной системы

Во всех операционных системах Windows начиная с XP есть папка config, в данной папке помимо всего прочего находятся бинарные файлы без расширений из которых формируется реестр системы, а так же файлы с расширением .log и .evt. Как раз эти файлы и являются журналами в которые система записывает

некоторые произошедшие события. Какие именно события пишутся зависит от настройки самой системы.

В файлы с расширением .log пишется системная информация, размер этих файлов всегда равен 1КБ. А вот файлы с расширением .evt сожержат информацию о подключении/отключении устройств, запуске/остановке программ, ошибок при работе программ, существует так же журнал загрузки операционной системы, журнал обновления системы. Так же опционально можно включить такие журналы как например журналы безопасности и обнаруденных угроз.

5.9 структур .evt файлов

Файл представляет из себя строки данныйх переменной длинны. Из сторонних источников стало извиестно что некоторые поля данных имеют определенное значение. А именно:
Первые 4 байта содержат длинну события в файтах, после длинны идет 4 байтный системный код сообщения. Затем 4байтовы номер записи, после него дата создания записи, время созания, идентификатор события, тип события и так далее.

Ниже приведен список полей записи, преднозначенной для счтиывания одного события из журнального файла.

quint32 Length;
quint32 Reserved;
quint32 RecordNumber;
quint32 TimeGenerated;
quint32 TimeWritten;

quint32 EventID;

quint16 EventType;

quint16 NumStrings;

quint16 EventCategory;

quint16 ReservedFlags;

quint32 ClosingRecordNumber;

quint32 StringOffset;

quint32 UserSidLength;

quint32 UserSidOffset;

quint32 DataLength;

quint32 DataOffset;

Из сторонних источников стало известно о пяти типах событий (поле EventType)

значение - тип события

1) 0x0001 - Error event
2) 0x0010 - Failure Audit event
3) 0x0008 - Success Audit event
4) 0x0004 - Information event
5) 0x0002 - Warning event

У поля EventID удалось определить четыре значения:

1) 0x00 - Success
2) 0x01 - Informational

3) 0x02 - Warning

4) 0x03 - Error

Среди множества полей записи события были выделены поля содержащие информацию о типе события, времени возникновения события и создания записи, пользователя от имени которого была сделана запись, а так же поле Data - поле с бинарными данными в которых записана подробная информация о событии.

5.10 Автоматизация процесса поиска .evt файлов

Так как комплекс работает с оброзом жесткого диска, то программе достаточно указать папку в которой находятся искомы файлы. Для поиска же можно взять список всех файлов папки и отфилтровать их по расширению .evt. Данную операцию можно сделать при помощи инструметов QDirItherator и QFileInfo из набора библиотек QT.

Первый инструмент необходим для получения списка файлов в папке config, а второй позволяет просматривать информацию о файлах. При просмотре иноформации будут отобраны пути до файлов с расширением .evt. После чего список путей будет передан передан процедуре обработки файлов. Которая конвертирует каждый .evt файл в XML и сохранит в дирриктворию с результатами работы. Для чтения файла используется инструмент QDataStream, а для записи в XML документ QXmlSreamWriter.

На данный момент полностью реализован комплекс для работы с журнальными файлами windows XP

5.11 описание используемых инструментов

Для работы с файловыми системами в QT существует несколько библиотек. В данном проекте активно используются две:

1) QDirIterator
2) QDir

QDirIterator — библотека, предназначенная для работы с файловой системой начиная с определенной директории как точки входа. Создав объект данного типа с указанием директории мы получим все пути которые существуют в файловой системе и начинаются с указанной директории. Данный объект поддерживает фильтрацию которая помогает выделять только необходимую информацию, исключая то, что нас не интересует, например можно вывести список только файлов находящихся в данной директории или поддиректориях, или исключить вывод символьных ссылок. Объекты данного типа используются для поиска файлов или папок на образе исследуемого диска.

QDir — библиотека позволяющая работать с конкретной директорией. Создав объект данного типа с указанием директории мы получим доступ к этой директории в программе и сможем работать в ней (просматривать содержимое; удалять, создавать или копировать файлы; создавать поддиректории). Данный объект так же поддерживать разные наборы фильтров выходных данных которые могут отсеивать ненужную информацию.

Так же данные библиотеки позволяют создавать объект QFile, который позволяет работать с файлом, путь к которому передается как параметр при создании, данный объект позволяет получить базовую информацию о файле, такую

как относительный или абсолютный путь до этого файла, размер файла, тип файла или его имя. Так же позволяет перемещать или копировать данный файл.

Работа с xml-файлами

XML - eXtensible Markup Language или расширяемый язык разметки. XML разрабатывался как язык с простым формальным синтаксисом, удобный для создания и обработки документов программами и одновременно удобный для чтения и создания документов человеком. Задумка языка в том, что он позволяет дополнять данные метаданными, которые разделяют документ на объекты с атрибутами. Это позволяет упростить программную обработку документов, так как структурирует информацию.

В QT для работы с xml-документами используется две библиотеки:

1) QxmlStreamReader
2) QxmlStreamWriter

Данные библиотеки позволяют создавать потоки для чтения и записи XML файлов и предоставляют набор функций для разбиения файлов на элементы и создания структур данных по записям в xml-файлах.

Команды для записи же позволяют записывать данные в файл автоматически дополняя методанные. Для этого существует набор команд при помощи которых создается xml-файл с заголовком, команды по созданию элемента, команды по добавлению атрибутов в элемент, команды записи конца элемента и конца файла.

6 Отчёт Лёши

6.1 Некоторые аспекты сертификации программных средств объектов информатизации по требованиям информационной безопасности

Под информационной безопасностью объектов информатизации в общем случае понимается такое их состояние, при котором исключается нанесение неприемлемого ущерба субъектам информационных отношений при применении последними средств информатизации. Следовательно, для оценки информационной безопасности объектов информатизации важно оценить сначала степень информационной безопасности средств информатизации, применяемых на объектах информатизации, в том числе всех их компонентов.

Одной из важнейших составляющих любого объекта информатизации являются применяемые программные средства различного назначения, которые существенно влияют на информационную безопасность объекта информатизации в целом.

В настоящее время достаточно полно регламентирована законодательными актами и распорядительными документами организация работ по сертификации средств защиты информации. Разработаны и представлены в виде нормативных документов (Государственных стандартов и Руководящих документов Гостехкомиссии России) требования к защиты информации автоматизированных систем и их компонентов (вычислительных и программных средств). Отработаны методы их проверки и создано достаточно большое количество программных средств для проведения испытаний. Однако в основной их части требования касаются средств и методов защиты информации от несанкционированного доступа, а также проверок на отсутствие закладных деструктивных элементов в таких программных средствах.

В то же время информационная безопасность средств информатизации определяется не только их защищенностью от несанкционированного доступа. Одной

из важнейших составляющих является выполнение средством информатизации заданных функций в различных условиях функционирования, в том числе при воздействии внешних деструктивных факторов.

Действительно, стержневой характеристикой качества любого средства информатизации является его функциональная пригодность. Ибо, если средство информатизации не решает в заданном объеме и с заданным качеством установленных для него задач, то нет смысла обеспечивать защиту от несанкционированного доступа и нецелесообразно его применять по назначению, так как только по этой причине результаты его использования могут привести к непредсказуемым последствиям и нанести пользователю неприемлемый ущерб.

В рамках Системы сертификации «Росинфосерт» разрабатывается подход к сертификации средств информатизации по требованиям информационной безопасности, сущность которого основана на действующей нормативно-методической базе Системы сертификации «Росинфосерт». Эта нормативно-методическая база дорабатывается с учетом требований Федерального закона «О техническом регулировании», в том числе в части вычислительных и программных средств, а также компьютерных систем в целом.

В ФЗ «О техническом регулировании» определены типы технических регламентов, в которых должны быть сформулированы требования по обеспечению биологической, механической, пожарной, промышленной, химической и др. видов безопасности применительно к продукции, работам и услугам. К сожалению, не попали в этот список требования по обеспечению информационной безопасности. Очевидно, Законодатель считает ее составной частью всех остальных видов безопасности.

Согласно закону, безопасность продукции определяется ее характеристиками, безопасность работ и предоставляемых услуг определяется применением безопасной продукции и безопасностью методов использования этой продукции при работах и предоставлении услуг. Фактически безопасность продукции является

одной из составляющих ее качества.

Таким образом, информационная безопасность средств информатизации должна оцениваться в рамках общей оценки их качества, как один из показателей качества продукции.

При рассмотрении вопросов информационной безопасности исследуется и оценивается безопасность информационных ресурсов (данных, программ и их совокупности), которые, в свою очередь нельзя рассматривать в отрыве от вычислительных средств, на которых они размещены и реализованы. То есть предметом рассмотрения должны быть вычислительные средства с реализуемыми на них информационными ресурсами.

Таким образом, требования информационной безопасности следует применять к многоуровневому программно-вычислительному комплексу как единому целому (рисунок 2):

В характеристики качества (в том числе и в информационную безопасность) такого комплекса компоненты каждого уровня вносят свою составляющую. Например, недостаточная надежность технических компонентов вычислительных средств может компенсироваться программно-алгоритмическими решениями. В конечном счете, следует рассматривать в качестве основного показателя качества комплекса безопасность его функционирования.

Поскольку 100% безопасности функционирования любого комплекса определенной структуры быть не может, то можно говорить о безопасности комплекса лишь в вероятностном смысле. Это в полной мере относится к компонентам любого уровня.

В общем случае для прикладных программных средств безопасное функционирование означает:

- полное и точное выполнение всех заданных функций;
- обеспечение целостности и сохранности;

– обеспечение защиты от неправильных действий пользователя, от некорректных входных данных, от случайных сбоев вычислительных средств;

– простой и удобный интерфейс.

Эти составляющие обеспечивают как аппаратные средства, так и операционная среда, Однако, центральным моментом оценки качества прикладных программных средств должна являться оценка их собственных функциональных характеристик, но, прежде, чем провести оценку качества прикладных программных средств, следует убедиться в том, что характеристики остальных составляющих комплекса соответствуют предъявляемым к ним требованиям, в том числе требованиям информационной безопасности.

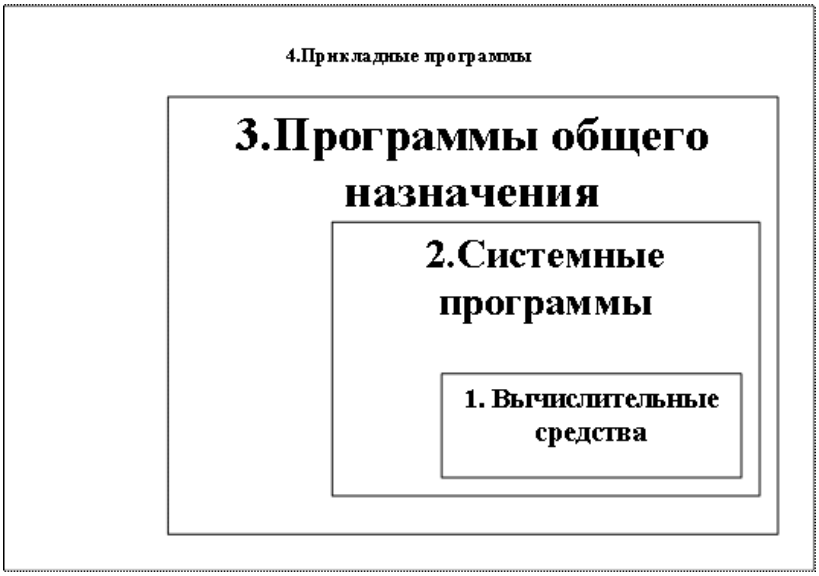

Рисунок 2 – Многоуровневый программно-вычислительный комплекс

В свете всего сказанного предлагается следующая этапность оценки:

1-й этап – осуществляется оценка выполнения требований к качеству комплекса на первом уровне. Здесь исследуются и оцениваются характеристики преимущественно технических средств с использованием широкой номенклатуры специальных или специализированных тестов.

2-й этап – осуществляется оценка уже программно – аппаратного комплекса, включающего средства 1-го и 2-го уровней (технические средства и системные

программные средства). При исследованиях и оценках используются имитаторы (в том числе программные) сигналов внешних устройств и функционирования программ общего назначения.

3-й этап – осуществляется оценка программно – аппаратного комплекса, включающего средства 1-го, 2-го и 3-го уровней (технические средства, системные программные средства и программные средства общего назначения). При оценках также используются независимые имитаторы сигналов внешних устройств, функционирования программ общего назначения и прикладных программ.

И, наконец, на 4-м этапе осуществляется оценка характеристик качества всего программно-вычислительного комплекса в целом. При этом используются результаты всех предыдущих этапов, что повышает достоверность и доверие к полученным оценкам.

Обязательные требования к продукции (работам и услугам) по действующему законодательству Российской Федерации устанавливаются Техническими регламентами, принимаемыми в качестве Федеральных законов. Сегодня необходимость технического регламента, устанавливающего обязательные требования по информационной безопасности к программно-вычислительным комплексам очевидна. При этом основным инструментом контроля соблюдения таких требований является сертификация (подтверждение соответствия). Место Системы сертификации в рамках проведения единой технической политики России в области решения задач информатизации поясняется рисунком 3.

Регистрация в реестре Системы сертифицированной продукции и выдача сертификата соответствия заявителю. Применение результатов сертификации продукции можно проиллюстрировать примером проведения тендера на поставку средств информатизации для государственных нужд. Схема проведения такого тендера представлена на рисунке 4.

Отбор участников тендера целесообразно проводить на основе анализа результатов их деятельности, одним из объективных показателей которой является

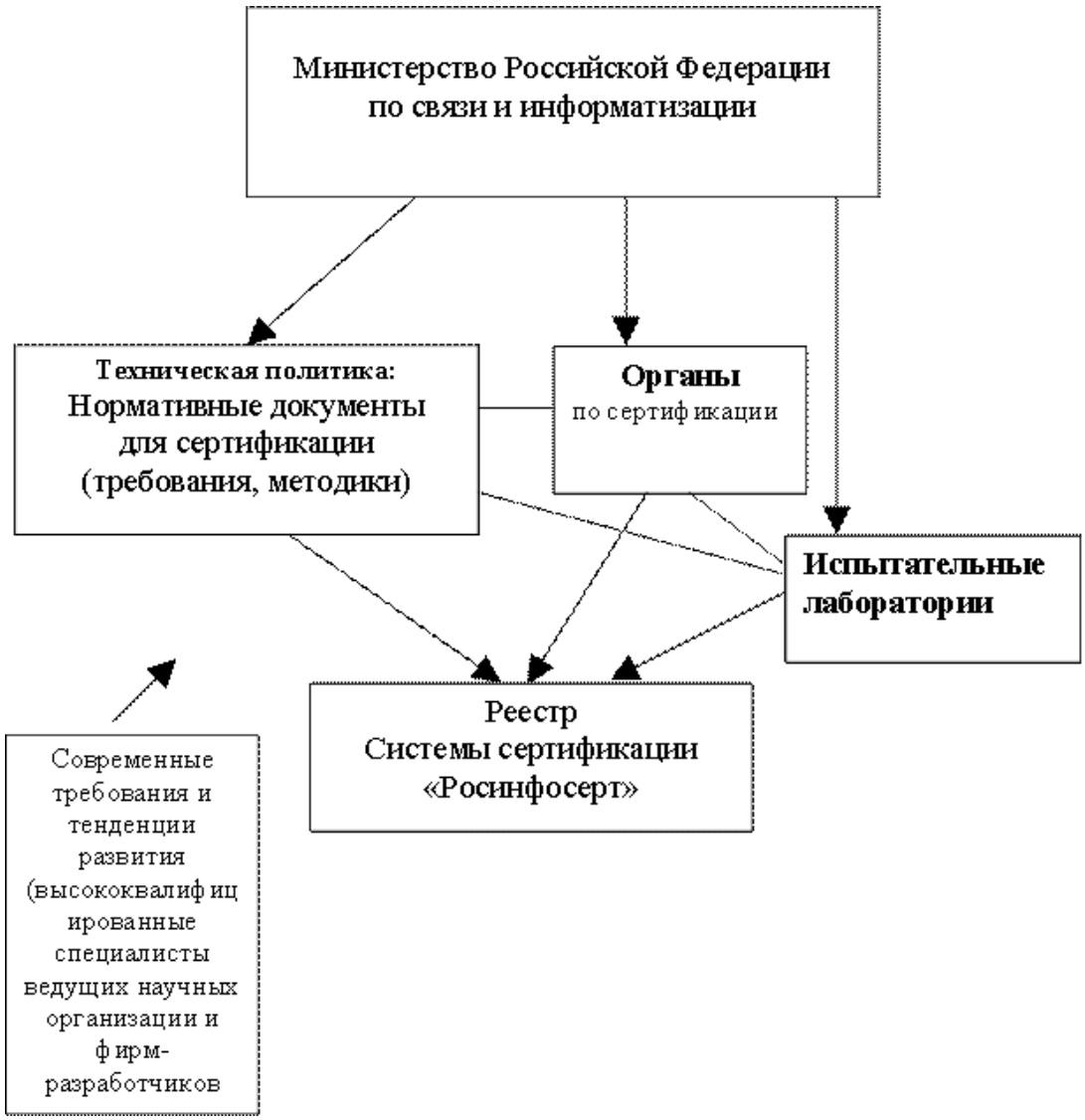

Рисунок 3 – Система сертификации при проведении единой технической политики

сертификат соответствия системы менеджмента качества организации требованиям международных стандартов ИСО 9001 – 2001, а также наличие в номенклатуре выпускаемой продукции сертифицированных продуктов, характеристики которых представлены в Реестре Системы. Такой подход ставит барьер недобросовестным поставщикам и некачественной продукции на рынок средств информатизации России.

В этом случае нормативно-правовое обеспечение применения сертификации для реализации обязательных требований информационной безопасности составляют следующие документы:

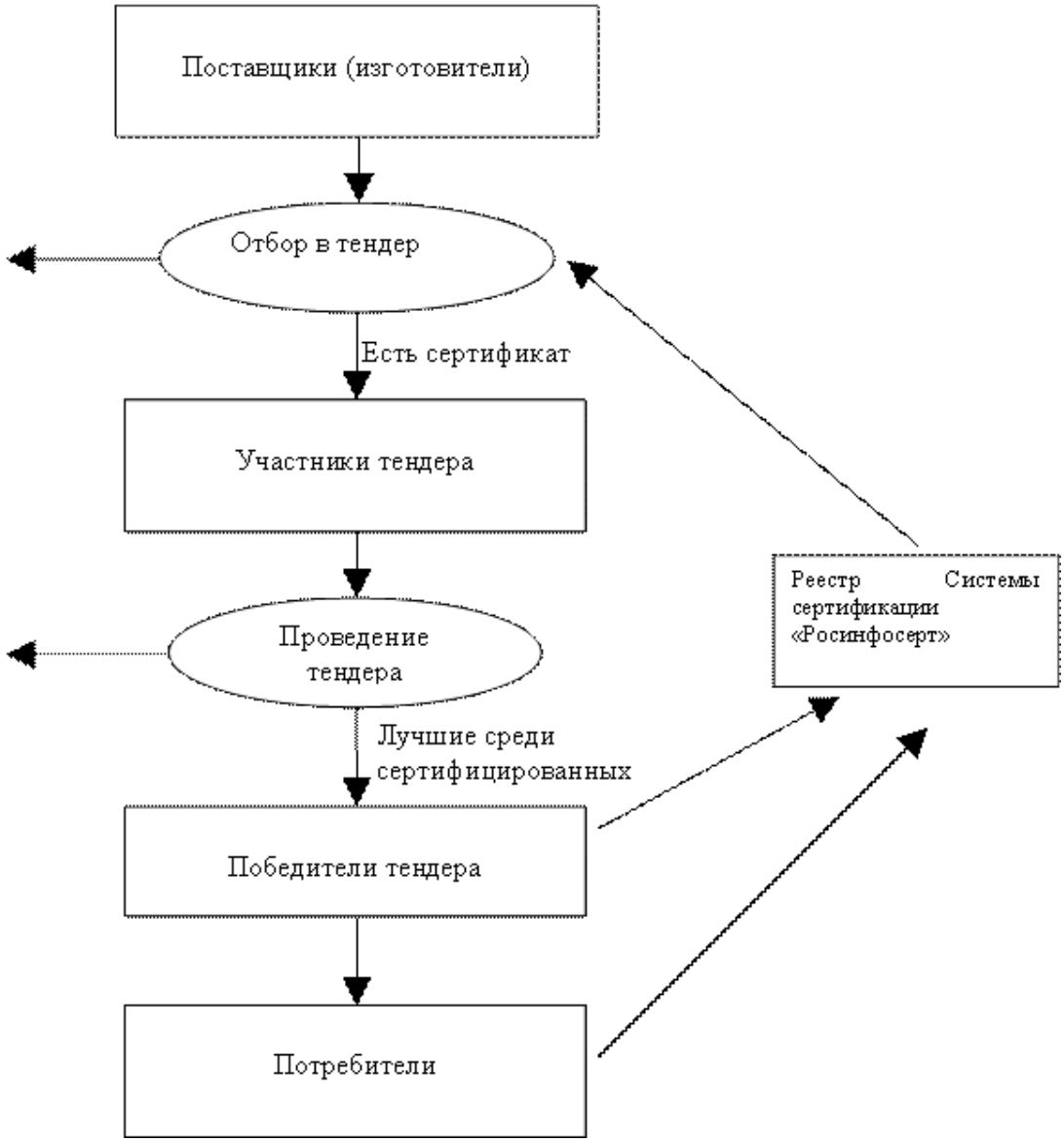

Рисунок 4 – Схема проведения тендера на поставку средств информатизации для государственных нужд

1) Соглашение о взаимодействии в области сертификации средств информатизации между Минсвязи России и субъектом равного уровня. Такое соглашение является необязательным, но желательным документом, который регламентирует взаимоотношения руководства Системы сертификации, ее органов и испытательных лабораторий с потенциальными поставщиками и потребителями средств информатизации, впрямую не подчиняющимися Минсвязи России.

2) Распоряжение (постановление, приказ) субъекта об утверждении Поло-

жения о порядке использования средств информатизации для решения своих задач.

3) Положение о порядке использования субъектом средств информатизации, устанавливающее систему показателей и правил отбора и применения поставляемых для государственных нужд средств информатизации.

4) Нормативный документ для сертификации, содержащий состав характеристик средства информатизации, их допустимые значения и способы оценки. Этот документ носит статус стандарта организации, утверждается Минсвязи России по согласованию с субъектом.

7 Заключение

В результате проделанной работы были достигнуты следующие результаты: типа ссылка [3] типа вторая ссылка [1]

В дальнейшей работе планируется:

– добавление части системы, работающей с логами браузеров.

Список использованных источников

1 Федотов, Н. Н. Форензика - компьютерная криминалистика / Николай Николаевич Федотов. — Юрид. мир, 2007. — P. 432.

2 Chat history on skype [электронный ресурс]. — 2012. — http://community.skype.com/t5/Security-Privacy-Trust-and/Is-chat-history-stored-on-Skype-servers/td-p/472379.

3 Qt documentation [электронный ресурс]. — 2013. — http://doc.crossplatform.ru/qt/.

Приложение А

(Обязательное)

Компакт-диск

Компакт-диск содержит:

– электронную версию пояснительной записки в форматах *.tex и *.pdf;

– индивидуальные ежемесячные отчеты студентов;

– групповые ежемесячные отчёты.