## *1. Наименование продукта*

Система управления правами на интеллектуальную собственность в цифровом виде ALMAZ III.

## *2. Назначение*

Система защиты ALMAZ III является системой класса DRM (Digital Rights Management) предназначенной для:

1) защиты программного обеспечения от нелегального (нелицензионного) использования;
2) защиты критически важных алгоритмов или их элементов от исследования методами обратного проектирования (reverse engineering);
3) управления лицензиями на отдельные компоненты и модули программного обеспечения;
4) защиты баз данных от нелегального тиражирования и использования;
5) разграничения доступа к информации в системах электронного документооборота, и информации, распространяемой через Интернет.

## *3. Краткие сведения о продукте*

Система построена на основе электронного микропроцессорного ключа ALMAZ III с интерфейсом USB. Внешний вид электронного ключа приведен на рисунке 1. Электронный ключ содержит защищенную память, аппаратно реализованные стойкие алгоритмы шифрования на основе международных стандартов, защищенную java-машину. Электронный ключ также содержит другие технические решения (на физическом и алгоритмическом уровнях), направленные на затруднение и предотвращение эмуляции ключа программными или аппаратными средствами, расшифровку зашифрованных баз данных злоумышленником и т.п.

Рисунок 1. – Внешний вид электронного ключа ALMAZ III

Наличие в электронном ключе ALMAZ III защищенной виртуальной машины позволяет разработчику защищаемого приложения создавать собственные функции электронного ключа, которые будет невозможно проанализировать любыми стандартными и нестандартными средствами. Возможен только анализ по входам и выходам.

Для управления лицензиями на отдельные модули защищенной программы, электронный ключ содержит 256 аппаратных алгоритмов шифрования, из которых 248 могут быть включены или отключены. Система поддерживает удаленное управление всеми элементами защиты электронного ключа в безопасном режиме.

Для управления лицензиями на программное обеспечение система существует в локальном и сетевом вариантах. Локальный вариант предназначен для защиты программы на одном компьютере, тогда как сетевой ограничивает количество одновременно запущенных программ в пределах сети. В сетевом варианте дополнительно возможно ограничение на количество запущенных программ определенного вида.

Существуют специальные версии системы, направленные на защиту баз данных.

Благодаря отсутствию потребности в установке драйверов система идеально подходит для защиты документов, размещаемых на веб-ресурсах.

## *4. Краткие технические характеристики*

Аппаратный ключ защиты подключается к ПЭВМ при помощи шины USB и соответствует спецификации версии 2.0, которая обеспечивает:

- plug & play инсталляцию;
- горячее подключение и отключение электронного ключа без перезагрузки системы;
- возможность одновременного подключения до 127 устройств;
- не требует установки драйверов (распознается ОС как HID устройство);
- совместим с ОС Microsoft Windows 98 / Me / 2000 / XP / 2003 Server / Vista / 2008 Server / 7 (x86 и x64), Linux с ядром 2.6 и выше;
- гарантия на электронный ключ – 3 года.

Аппаратный ключ содержит:

- уникальный серийный номер, доступный только для чтения;
- 512 байт защищенной памяти, из которых 480 байт могут использоваться разработчиком для любых целей, а 32 байта содержат информацию о текущей конфигурации ключа. Механизм чтения памяти содержит элементы защиты от эмуляции на основе несимметричной криптографии;
- 256 аппаратных 128-и битовых алгоритмов шифрования на основе стандарта AES, из которых 248 являются управляемыми и могут быть включены или отключены;
- защищенную виртуальную java-машину с объемом защищенного ПЗУ 1024 байта (в версиях с поддержкой технологии DBShield и автодекрементным счетчиком — 512 байт) и ОЗУ 1024 байта. Байт код хранится в упакованном виде, что значительно увеличивает размер программы, которую можно разместить в ограниченном ПЗУ;
- дополнительные механизмы противодействия полной расшифровке баз данных (только в версии для защиты баз данных).

Взаимодействие с электронным ключом осуществляется посредством статических и динамических библиотек, а также элементов COM-технологии. Поддерживаются следующие языки программирования/среды разработки: C, C++ (Microsoft Visual Studio, Borland Builder), Delphi, C# (.NET), Visual Basic, Java.

## *5. Ключевые технологии системы защиты ALMAZ III*

### *5.1. Технология защиты программного обеспечения ALMAZ TrustedExecution*

Основными уязвимостями программного обеспечения являются:

- простота внесения в программное обеспечение модификаций;
- простота копирования программного обеспечения;
- в случае известной архитектуры аппаратной платформы, на которой работает ПО, возможность исследования и восстановления алгоритмов работы программы (возможность относительно простого обратного проектирования).

Осуществление надежной защиты программного обеспечения на открытой аппаратной платформе потребителя является очень сложной задачей. Основная сложность заключается в наличии у злоумышленника полных знаний о самой платформе и возможности отслеживать ход работы программы вплоть до каждой ее инструкции на реальной платформе, а также путем ее

полной или частичной виртуализации. Поэтому никакие антиотладочные меры не могут обеспечить достаточно длительный безопасный период эксплуатации программы.

Для того чтобы создать защищенную программу можно пойти несколькими путями, которые направлены либо на устранение некоторой уязвимости, либо на затруднение ее использования до такой степени, что ее использование становится нецелесообразным. Принципиально устранить уязвимости программного обеспечения можно только с помощью внедрения в существующую информационную модель некоторого элемента, которому можно доверять. Очевидно, что в качестве доверенного элемента наиболее эффективно использовать аппаратное средство, так как для любой программы будут существовать те же самые уязвимости, что и для защищаемой.

Для защиты программного обеспечения на существующих архитектурах наиболее оптимальной является модель недоверенного узла с доверенным элементом, где в качестве доверенного элемента выступает безопасный сопроцессор. Основную часть защищенной программы выполняет центральный процессор, а небольшую часть, содержащую критические алгоритмы и данные – безопасный сопроцессор. Такой вариант исполнения системы защиты не требует изменений в архитектуре существующего парка вычислительной техники и позволяет устранить основные уязвимости ПО для наиболее критичных частей защищенной программы.

Злоумышленник не имеет доступа к внутренним параметрам доверенного элемента и может обмениваться с ним информацией только через тот же канал, что и защищенная программа. В качестве такого доверенного элемента используется электронный ключ ALMAZ III.

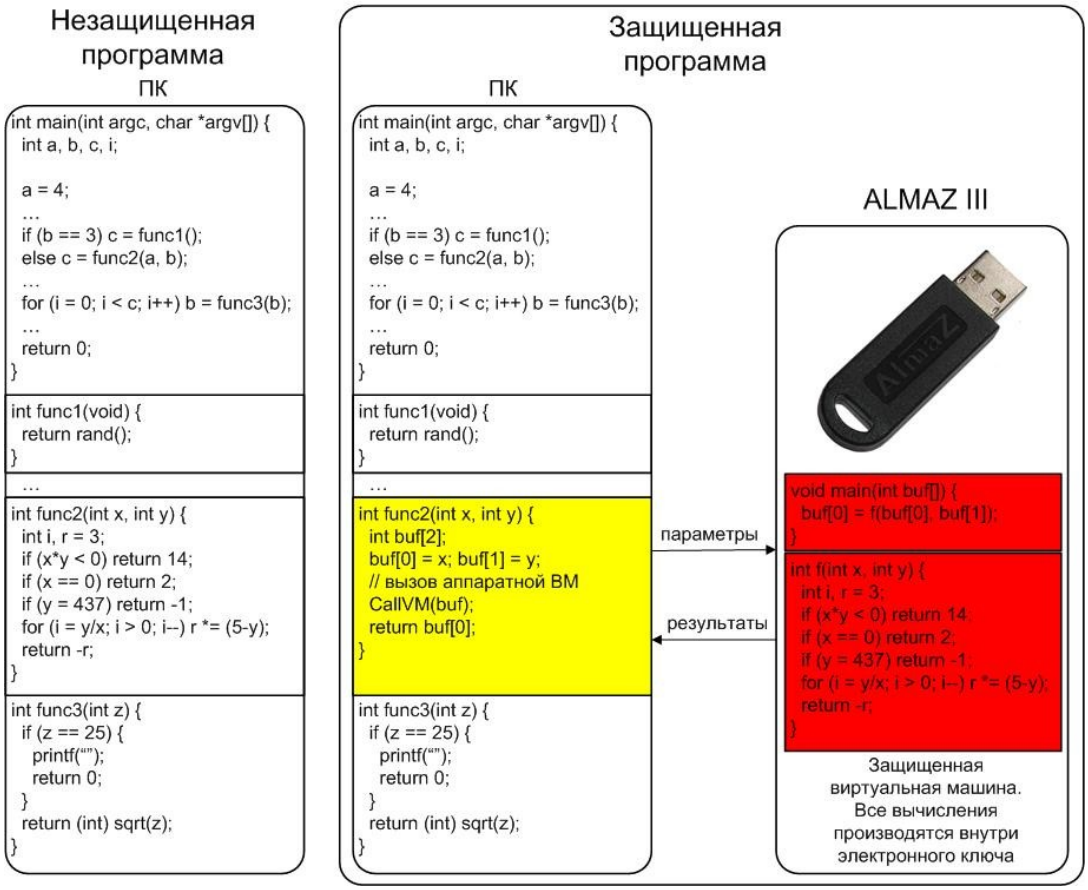


Рисунок 2. – Схема защиты ПО с применением технологии ALMAZ TrustedExecution

Для упрощения разработки программ для доверенного элемента, в электронный ключ ALMAZ III встроена защищенная виртуальная java-машина. Благодаря этому, разработчики могут просто и быстро разрабатывать собственные программы для электронный ключа с использованием стандартных средств разработки на java (в том числе – бесплатного JDK).

Злоумышленник не имеет доступа к программе защищенной java-машины и может проводить ее анализ только по принципу «черного ящика», т.е. анализируя входы и выходы. В нетривиальном случае такая задача является NP-полной и при достаточной длине входов – вычислительно неразрешимой.

Данная технология получила название ALMAZ TrustedExecution.

### *5.2. Технология защиты баз данных ALMAZ DBShield*

Многие программы содержат в своем составе базы данных. Причем, во многих случаях, именно информация, содержащаяся в этих базах данных, и представляет основную ценность. В таких системах сама программная часть зачастую является всего лишь интерфейсом пользователя, позволяющим пользователю получать необходимую информацию из базы данных и выполнять над ней некоторые действия. Защита только программной части в таких ситуациях не всегда достаточно эффективна, поскольку злоумышленник, имея в своем распоряжении полную базу данных, относительно легко может создать свой модуль, реализующий интерфейс пользователя.

Для решения задач защиты программного обеспечения, содержащего в себе базы данных, специалистами нашей компании была разработана технология DBShield для системы защиты ALMAZ III. Основным элементом технологии DBShield является электронный ключ ALMAZ III, с использованием аппаратных алгоритмов шифрования которого зашифровываются записи базы данных.

Основными особенностями данной технологии является применение аппаратного ключа не просто для шифрования базы данных, но и для противодействия попыткам злоумышленника расшифровать записи базы данных. Электронный ключ в процессе расшифрования записей базы данных оценивает типы, последовательность, интенсивность и другие параметры запросов и на основании некоторых критериев принимает решение о формировании данных запросов легальной программой или злоумышленником. В случае если запросы сформированы злоумышленником, шифратор базы данных аппаратного ключа может быть отключен/изменен, а пользователю предоставлена новая зашифрованная база данных, процесс расшифровки которой злоумышленнику придется начинать заново.

В данное время технология ALMAZ DBShield является практически единственным эффективным решением защиты баз данных от нелегального копирования, которое обеспечивает существенное затруднение полной расшифровки базы данных злоумышленником, а в отдельных случаях позволяет гарантировать безопасное время, в течение которого база данных не будет полностью расшифрована.

### *5.3. Система защиты электронных документов ALMAZ DocShield*

Использование электронных ключей ALMAZ III с системой DocShield позволяет построить эффективную и легко администрируемую систему разграничения доступа пользователей к корпоративной информации, а также информации распространяемой через интернет.

Основным элементом системы DocShield является электронный ключ ALMAZ III, с использованием аппаратных алгоритмов которого выполняется шифрование документов. Каждый пользователь получает электронный ключ ALMAZ III, в котором в зависимости от полномочий данного пользователя включены или отключены определенные алгоритмы шифрования. В соответствии с включенными алгоритмами пользователь может расшифровать и прочитать документы, доступ к которым ему разрешен.

При необходимости, администратор безопасности может удаленно изменить настройки электронного ключа, включить или отключить определенные алгоритмы шифрования.

Система ALMAZ DocShield состоит из трех элементов:

- утилиты настройки ключей пользователей, по умолчанию поддерживающей 32 уровня доступа в иерархическом или произвольном порядке;
- утилиты защиты документов, позволяющей шифровать публикуемые документы и задавать для них параметры доступа;
- утилиты просмотра или plug-in модуля для стандартных программ, обеспечивающих работу пользователя с защищенными документами.

Схематически процесс создания и работы с защищенными документами показан на рисунке 3.


Рисунок 3. – Процесс создания и работы с защищенными документами.

### *5.4. Автодекрементный счетчик*

Автодекрементный счетчик используется с целью ограничения количества запусков либо времени использования программы (количества просмотров электронных документов). Разработчик или поставщик защищенного программного продукта (защищенных электронных документов) устанавливает начальное значение счетчика перед отправкой электронного ключа потребителю. При достижению декрементным счетчиком значения 0 в процессе эксплуатации все функции электронного ключа ALMAZ III за исключением чтения памяти и удаленного обновления блокируются. Счетчик может быть установлен в новое значение путем выполнения удаленного обновления памяти ключа в безопасном режиме. После записи в счетчик нового значения (отличного от 0) полная функуиональность электронного ключа будет восстановлена.

Счетчик может работать в следующих режимах: автоматический декремент, декремент по событию и смешанный.

В случае использования режима автоматического декремента значение счетчика уменьшается на 1 через определенный интервал времени (от 5-и минут до 24-х часов), а также при каждой подаче электропитания на электронный ключ. При использовании счетчика в таком режиме необходимо учитывать, что при отсутствии электропитания счетчик работать не будет, т.е. он не является часами реального времени.

При использовании режима декремента по событию счетчик декрементируется при вызове одного из аппаратных алгоритмов шифрования. В таком режиме наиболее эффективно реализуется защита с ограничением по количеству запусков программы либо по количеству загруженных (прочитанных) электронных документов.

В смешанном режиме работают оба выше приведенных сценария.