Инновационное решение 2

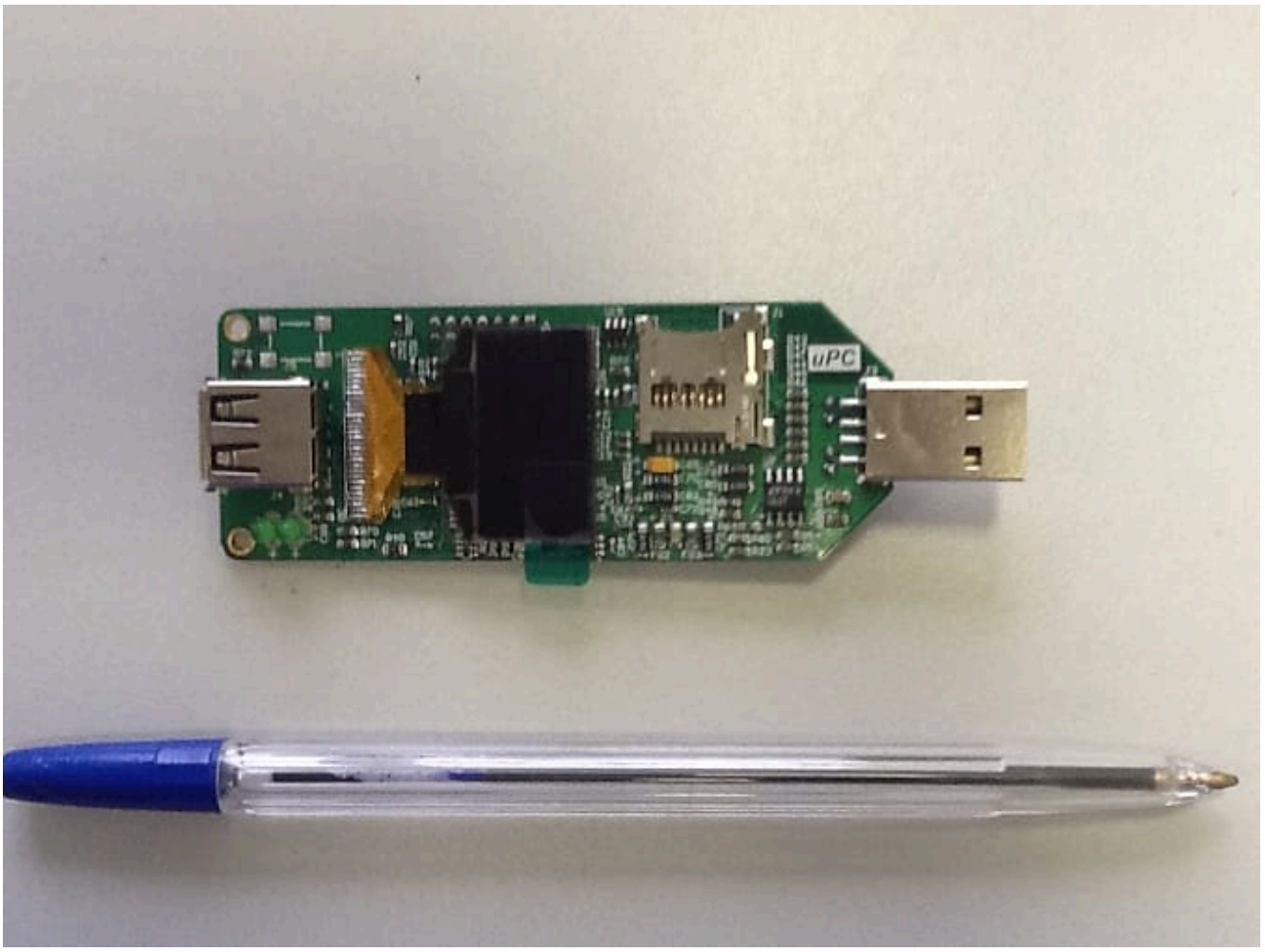
Перспективный микроминиатюрный персональный компьютер с защитой информации µPC ™ как уникальная платформа для обработки персональных данных

ООО «НЦПР» (Технический бюллетень)

Выпуск-02

Настоящая статья посвящена уникальной российской инновационной разработке, не имеющей аналогов в мире и позволяющей в полном объеме реализовать требования отечественного и зарубежного законодательств в области обеспечения безопасности персональных данных и некоторых видов конфиденциальной информации в медицинской, фармацевтической и банковской сферах, в государственных учреждениях, коммерческих организайиях и силовых структурах. Содержащаяся в статье информация может быть интересна сотрудникам кадровых подразделений и подразделений информационной безопасности государственных и частных предприятий, а также производителям автоматизированных кадровых информационных систем.

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» определил новый порядок работы, связанный с «обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях» (часть 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ). Вопросы практического соблюдения требований 152-ФЗ широко обсуждались специалистами, которые сделали однозначное заключение о том, что технические сложности, связанные с точным выполнением всех требований закона, потребует от операторов персональных данных внесения серьезных изменений в действующие бизнес-процессы и существенных финансовых затрат. Это явилось одной из основных причин задержек в выполнении вышеуказанных требований и, как результат, привело к его массовым нарушениям.



Микроминиатюрный компьютер с защитой информации µPC™

Перспективный микроминиатюрный компьютер с защитой информации µPC™ российской компании Flexlab (ООО «НЦПР») проектировался и создавался как универсальная защищенная платформа для обработки персональных данных и другой конфиденциальной информации, полностью удовлетворяющая самым жестким российским и международным требованиям к обеспечению безопасности информации. Он представляет собой компьютер нового типа, выполненный в форм-факторе USB-флэш, имеющий собственную встроенную систему установки и удаления программ, аутентификации пользователя и защиты от атак злоумышленников и вредоносных программ-вирусов.

µPC™ использует современный высокопроизводительный процессор, как и широко представленные на рынке планшетные компьютеры, смартфоны и коммуникаторы, однако, в отличие от них, он не имеет экрана и устройства ввода данных, поскольку с технической точки зрения поддержка экрана и устройства ввода данных отнимает ощутимую долю производительности процессора во время выполнения сложных графических задач. В µPC™ функции отображения и ввода данных с клавиатуры реализованы иначе, что позволило решить одновременно несколько задач:

- освободить процессор от работы с экраном и направить всю его вычислительную мощность на выполнение программ;
- добиться максимальной миниатюризации изделия при сохранении вычислительной мощности, соизмеримой с мощностью современного смартфона или планшетного компьютера;

- обеспечить беспрецедентную степень защиты данных и программ за счет наличия изолированной памяти для выполнения программ пользователя;
- позволить его использование совместно с любыми средствами отображения и ввода данных без модификации встроенного программного обеспечения;
- максимально снизить стоимость изделия и технической платформы.

Для решения задач отображения и ввода данных µPC™ использует любой внешний компьютер-донор, имеющий экран, клавиатуру и мышь со штатными драйверами периферийных устройств или даже обычный современный телевизор с соответствующим интерфейсом. µPC™ подключается к компьютеру-донору через разъем USB и получает от него питание.

При подключении µPC™ он распознается, как USB-флэш накопитель. На этом накопителе размещены файлы автозапуска autorun.inf для Windows-систем и autorun.sh для Unix-систем. В зависимости от того, какая операционная система установлена на компьютере-доноре, будет запущен соответствующий файл. Если политика безопасности компьютера-донора запрещает автоматический запуск программ со съемных носителей, соответствующий файл автозапуска µPC™ может быть выполнен в ручном режиме.

Файл автозапуска загружает соответствующий вариант программы Launcher, который настраивает соединение между µPC™ и компьютером-донором, после чего µPC™ начинает восприниматься последним как обычная сетевая карта. Кроме того, Launcher перенаправляет графическую информацию из µPC™ в окна, создаваемые на экране компьютера-донора, а в собственном окне отображает кнопки управления (иконки), позволяющие запускать приложения µPC™.

При нажатии на кнопки запускается соответствующее выбранное приложение, для которого на экране компьютера-донора создается отдельное окно. Таким образом, за счет средств ввода-вывода компьютера-донора обеспечивается полноценная работа пользователя с приложениями µPC™.

Для завершения работы с µPC™ достаточно отключить его от компьютера-донора. В момент отключения µPC™ пропадает напряжение питания, но это не вызывает потерю несохраненных данных, так как µPC™ имеет встроенный аккумулятор, обеспечивающий штатное завершение работы. После переключения на аккумуляторное питание в µPC™ завершаются все ранее запущенные приложения и сохраняются все ранее открытые документы. Процедура завершения работы занимает всего несколько секунд, что не требует частого заряда аккумулятора, который производится автоматически при подключении к компьютеру-донору.

µPC™ имеет жидкокристаллический индикатор, отображающий текущее состояние. Во время запуска и завершения работы индикатор отображает соответствующую информацию: «Загрузка» или «Завершение работы». В процессе работы на индикатор выводится информация о запущенных приложениях, имеющемся свободном дисковом пространстве, уровне заряда аккумулятора и другие справочные данные.

µPC™ может оснащаться дополнительными встроенными компонентами, включая разъем для карты памяти микро-SD, 3G или LTE модем, USB разъем для подключения внешних устройств, модуль WiFi/Bluetooth, микрофон.

Основу защиты µPC™ от внешних атак составляет собственная система установки/удаления программ и идентификации пользователя. Он не может быть заражен вирусами или хакерскими эксплойт-программами, поскольку такие программы не могут быть выполнены в памяти µPC™ из-за применения

следующих технических решений:

- дисковое пространство изделия может быть зашифровано;
- система установки и удаления программ модифицирована таким образом, что в памяти может быть установлена и выполнена только та программа, которая была предварительно зашифрована соответствующим уникальным ключом, подходящим только для данного изделия;
- ключ хранится во встроенном электронном идентификаторе Rutoken с формированием электронной цифровой подписи, который на сегодня признан не вскрываемым;
- обмен любыми данными и программами с внешними источниками осуществляется в зашифрованном виде;
- при обмене с внешними источниками ключ шифрования не передается в канале обмена данными;
- аппаратная платформа изделия не содержит консольных или отладочных портов для перехвата управления;
- программная платформа изделия не включает поддержку консольных или отладочных портов, которые могли бы обеспечить проникновение или перехват управления.

Реализованные в µPC™ инновационные технические решения позволяют с уверенностью утверждать следующее:

- демонтаж компонентов изделия не позволяет свободно считать содержимое флэш-памяти из-за наличия шифрования;
- преднамеренный взлом защиты самим пользователем индивидуального изделия не влияет на безопасность других компьютеров и не позволяет выработать общий метод взлома;
- с помощью изделия можно установить безопасное соединение для обмена данными по любому открытому каналу связи из любого не доверенного места.

Подобная степень защиты данных и программ открывает для µPC™ множество применений, где важна сохранность персональных данных пользователя, достоверность получаемой информации и безопасность удаленных соединений, в том числе, через открытую сеть Интернет.

Платформа µPC™ позволяет организовать корректную обработку персональных данных в любой организации, учреждении или на предприятиях, использующих современные автоматизированные кадровые информационные системы практически всех известных разработчиков. Возможности изделия позволяют разместить на нем и соответствующим образом защитить ключевые персональные данные, а хранение всей информационной базы организовать в имеющейся информационной системе в обезличенном виде. В этом случае становится невозможным без использования размещенных в µPC™ данных определить принадлежность информации к конкретному субъекту персональных данных, что позволяет полностью обезличить их на время хранения и привязывать к конкретным субъектам только в период их обработки. Тем самым обеспечивается соблюдение требования 152-ФЗ о том, что «Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных… Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки…».

Миниатюрные размеры µPC™ позволяют также организовать трансграничную передачу персональных данных с полным соблюдением требований 152-ФЗ.

На основе µPC™ создаются различные специализированные решения для групповых и индивидуальных приложений, связанных с необходимостью защиты информации, в первую очередь, для медицинских учреждений, банков и страховых компаний, операторов связи, силовых структур, а также государственных и частных компаний с удаленными офисами, не имеющими закрытых каналов связи.

Например, для обеспечения связи сотрудников банков или страховых компаний с удаленными отделениями, либо для обеспечения переводов денежных средств, применяются специальные решения для защиты информации (токены, электронная цифровая подпись) в сочетании с незащищенными вычислительными средствами, такими как компьютер в отделении банка или на стороне клиента. Такое сочетание защищенных и незащищенных средств не решает проблем информационной безопасности при удаленных соединениях. Чтобы удовлетворить всем требованиям государственного регулятора, банки вынуждены внедрять сложные системы и компьютерные сети, обладающие необходимыми средствами обеспечения конфиденциальности и безопасности. Применение µPC™ многократно сокращает затраты на развертывание безопасных каналов удаленного доступа, так как позволяет использовать любые незащищенные компьютерные сети. Обладая изолированной средой выполнения программ, µPC™ обеспечивает пользователю формирование реальной доверительной зоны на любом неконтролируемом службой безопасности рабочем месте. Для этого достаточно для каждого участника системы персонализировать отдельный µPC™ и внести в уже имеющиеся базы данных соответствующую ему пару «закрытый — открытый ключ». В результате появляется возможность организации надёжных защищенных удаленных транзакций с использованием на рабочих местах пользователей обычных незащищенных компьютеров, включая блокнотные и планшетные.

В медицине для проведения клинических исследований при удовлетворении всех требований стандарта CFR 21 Part 11 недостаточно предоставить только специальное оборудование или программное обеспечение. Чтобы удовлетворить всем требованиям государственного регулятора исследования должны проводиться с использованием программно-технических средств, обладающих необходимыми средствами обеспечения конфиденциальности и безопасности. На практике, пока ни одно из заявленных производителями средств такого класса, за исключением µPC™, не удовлетворяет в полной мере требованиям вышеуказанного стандарта. То же относится и к разработкам перспективных лекарств в фармацевтике. Обеспечиваемый µPC™ уровень безопасности позволяет обрабатывать медицинские, фармацевтические и биометрические данные без угрозы их компрометации.

Применение µPC™ в службах общественной безопасности позволяет организовать безопасный удаленный доступ к ведомственной информационной системе с любого незащищенного рабочего места по открытому каналу связи, существенно расширяя возможности собственных технологических сетей обмена данными.

Краткая техническая информация о различных вариантах исполнения µPC™ представлена ниже:

Процессор: Cortex-A8/A15 720MHz/1.3GHz

Память: DDR2/DDR3 256MB/2GB, NAND Flash 512MB/4GB

Интерфейсы: WiFi, 3G/LTE, Bluetooth

Разъемы: microSD, USB OTG

Индикация: OLED 0,96″ 128x64

Операционная система: Linux, Android

Токен: Rutoken с неизвлекаемым ключом, уникальным для каждого изделия, с формированием ЭЦП

ВЫВОДЫ:

1. Микроминиатюрный персональный компьютер с защитой информации uPC™, защищенный патентами РФ и США, в сочетании с разработанной для него инфраструктурой информационной безопасности, на сегодня является единственным в мире техническим решением, обладающим одновременно компактностью исполнения и беспрецедентной системой защиты информации, удовлетворяющей самым жестким современным требованиям защиты персональных данных.
2. Применеиени компьютера uPC™ и сопуствующей инфраструктуры позволяет в полной мере удовлетворить требования регулятора по обеспечению защиты персональных данных, предусмотренные, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», а также выполнить условия по обеспечен ию медицинских клинических исследований и фармацевтических разработок, определенные действующим законодательством.

Сноски