Защита данных. Новые подходы и решения.

Ренат Юсупов

Москва, 10 ноября 2010

Оглавление

Несанкционированный доступ

Электронные замки (аппаратно-программные модули доверенной загрузки - АПМДЗ) решают следующие задачи:

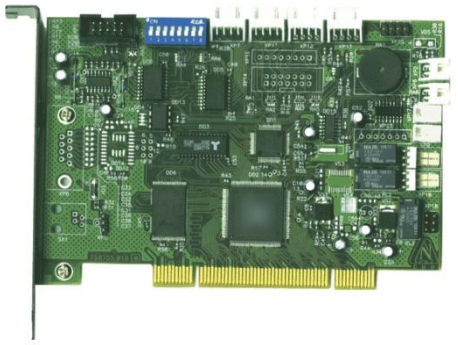
- Предотвращение несанкционированного доступа к ресурсам компьютера
- Предотвращение загрузки операционной системы с внешнего носителя
- Контроль целостности программной среды компьютера
- Регистрация событий доступа к ресурсам компьютера (в том числе несанкционированного)

Электронный замок (АПМДЗ)

«Традиционные» АПМДЗ выполняются в виде специализированного контроллера, подключаемого к компьютеру посредством шины PCI/PCI-X, PCI-E

ПАК «Соболь»

АМДЗ Аккорд-5.5.e



АПМДЗ «КРИПТОН-ЗАМОК»

Архитектурные недостатки АПМДЗ
на основе внешнего контроллера

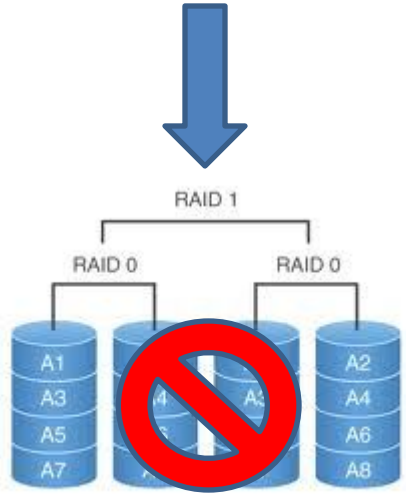
Для использования АПМДЗ необходима установка платы внешнего контроллера в слот PCI/PCI-X. Данный контроллер выполняет все функции АПМДЗ

Установка внешних устройств и дополнительного программного обеспечения на компьютеры связана с неудобствами, временными и финансовыми затратами

Архитектурные недостатки АПМДЗ
на основе внешнего контроллера

Внешний контроллер АПМДЗ использует «перехват» управления для блокирования загрузки операционной системы компьютера после окончания процедуры POST

RAID-контроллеры для работы используют механизмы, сходные с механизмами АПМДЗ. При их совместном использовании злоумышленник имеет возможность обхода защитных механизмов АПМДЗ



kraftway
ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ

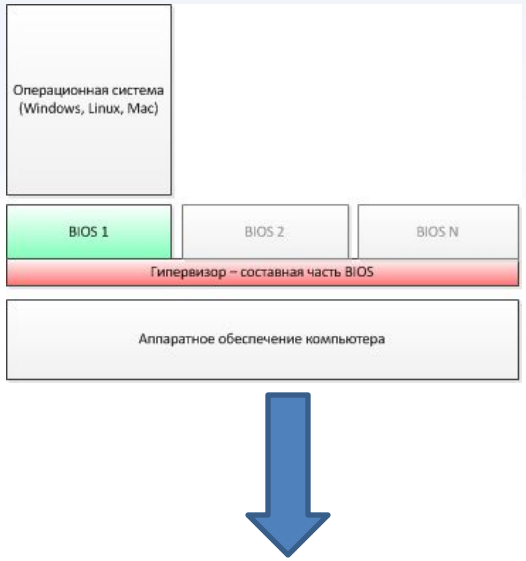
Архитектурные недостатки АПМДЗ
на основе внешнего контроллера

Для осуществления контроля целостности внешние платы АПМДЗ используют собственные средства работы с жесткими дисками компьютера

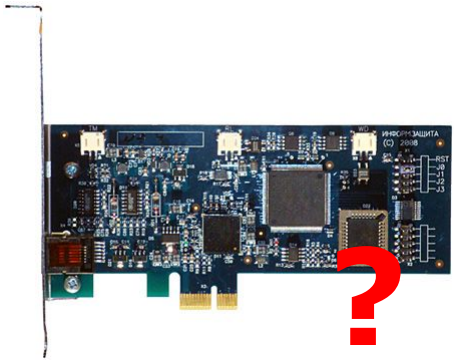
Это накладывает ограничения на работу с RAID-массивами, нестандартными конфигурациями, жесткими дисками большого объема

Архитектурные недостатки АПМДЗ
на основе внешнего контроллера

АПМДЗ не в состоянии контролировать наличие гипервизора уровня BIOS



При внедрении стороннего кода, который подменяет содержание жесткого диска или эмулирует наличие определенных устройств, АПМДЗ на основе стороннего контроллера становится бесполезным



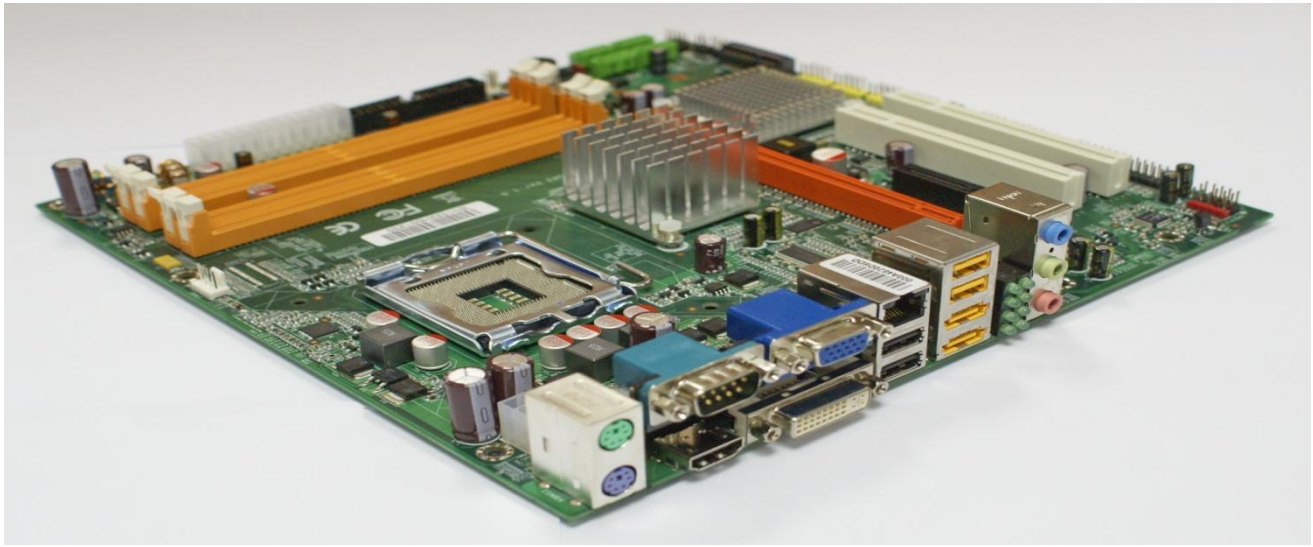
Защищенный компьютер

Для противодействия современным угрозам и соответствия уровню развития техники, а так же для максимального удобства использования и управления средствами защиты компаниями **Kraftway** и **Aladdin** был разработан Защищенный компьютер:

- Современная аппаратная платформа и программное обеспечение (Intel Core 2, Windows XP/Vista)
- Модифицированный BIOS
  - Интеграция с TSM для защиты от НСД
  - Разграничение прав доступа к секциям BIOS, TSM (защита от перезаписи, ограничение прав чтения)
  - Защита от несанкционированной модификации CMOS (область хранения настроек BIOS)
  - Ограничение доступа к BIOS SETUP
- embedded TSM (Trusted Security Module)
  - Строгая двухфакторная аутентификация
  - Журнал регистрации событий

Материнская плата Kraftway KWG 43

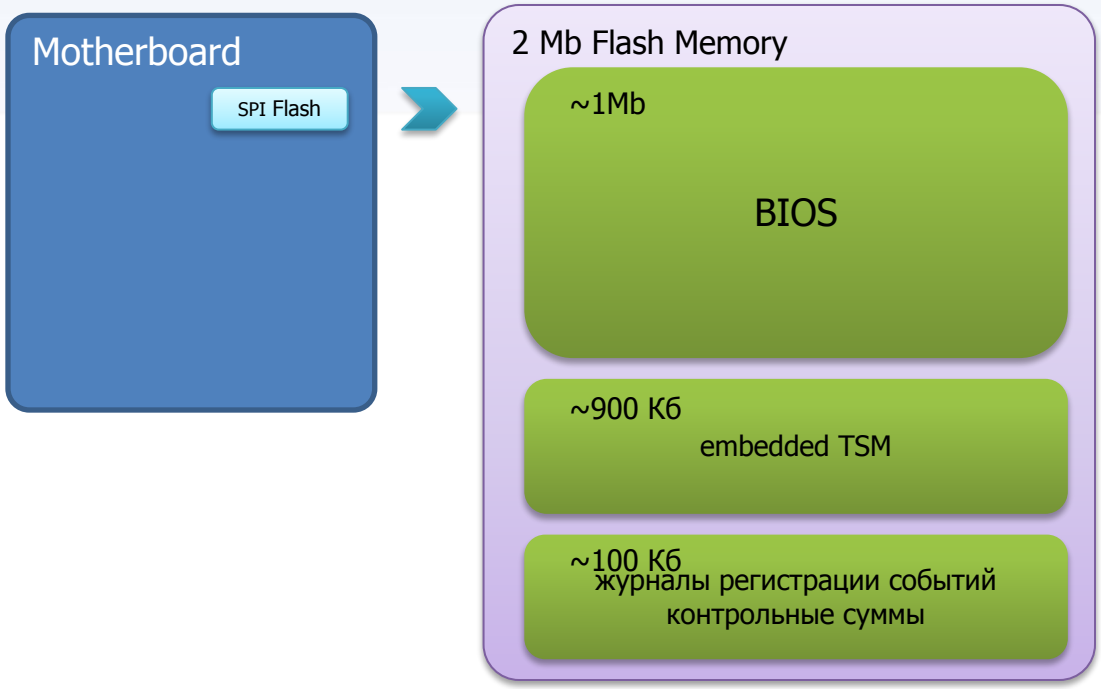
- Производство осуществляется на сертифицированной площадке на территории России, что гарантирует отсутствие недекларированных возможностей, закладок и гипервизоров уровня BIOS



- Имеет полностью русифицированный BIOS, обладает развитыми возможностями управления и самодиагностики

Особенности реализации

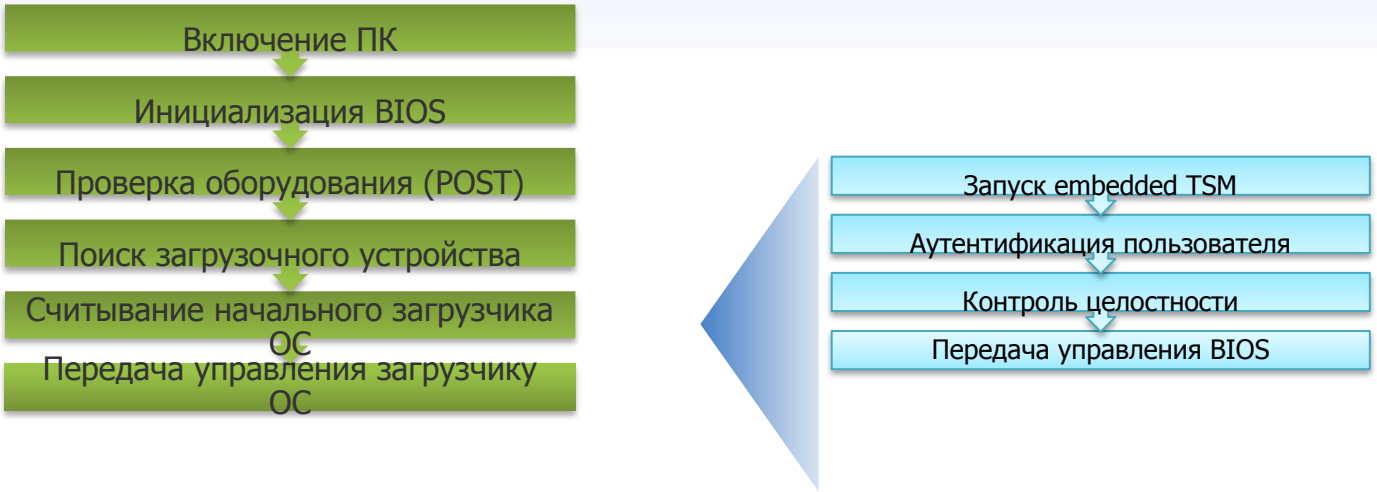
В момент загрузки «Доверенный BIOS» проверяет целостность CMOS и загружаемых компонентов, которые располагаются в SPI Flash материнской платы KWG-43



После прохождения процедуры Power On Self-Test (POST) вызывается на исполнение модуль TSM

Работа TSM на этапе загрузки

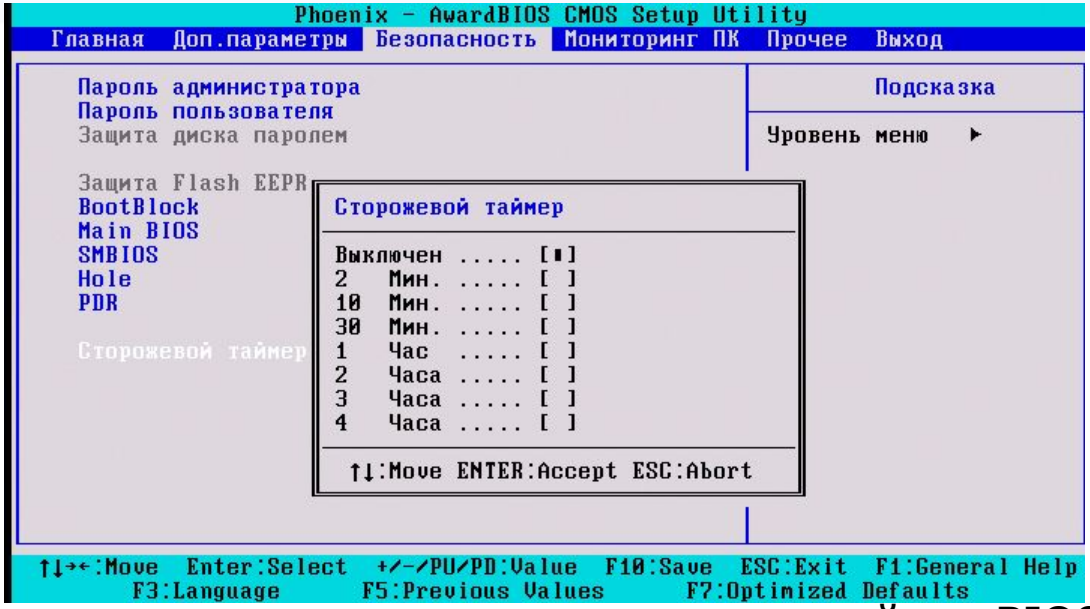
Благодаря тесной интеграции TSM с BIOS материнской платы обеспечивается максимальная безопасность и совместимость со всеми используемыми аппаратными средствами



Обратная передача управления BIOS для дальнейшей загрузки компьютера осуществляется только после аутентификации пользователя

Управление доверенной загрузкой

- Режим доверенной загрузки включается и отключается посредством специальных настроек BIOS SETUP



- После включения этого режима доступ к настройкам BIOS SETUP возможен только для Администратора

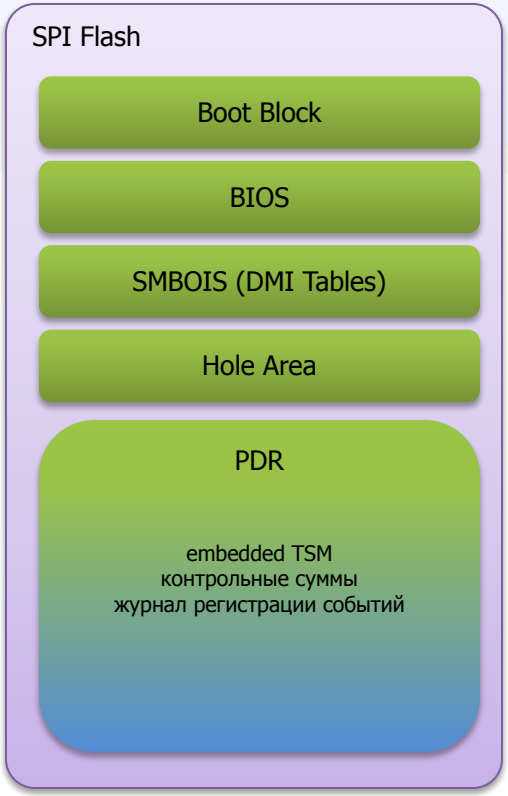
Обеспечение безопасности кода

В SPI Flash материнской платы KWG43 логически выделены пять регионов, которые независимо друг от друга могут быть защищены от записи:

- Boot Block
- Main BIOS
- SMBIOS Area (DMI Tables)
- Hole Area

  для хранения кода инициализации памяти и копии Video ROM, используемой для процедуры BIOS Recovery
- PDR - Platform Data Region

  для хранения кода TSM, журнала и контрольных сумм



Защита кода приложения TSM осуществляется программно-аппаратными средствами материнской платы

Ролевая модель
Идентификация, аутентификация и авторизация

- Администратор
  - изменение настроек BIOS посредством BIOS SETUP
  - включение/отключение TSM посредством BIOS SETUP
  - продолжение загрузки компьютера
  - изменение настроек TSM
  - управление пользователями TSM
  - изменение пароля подключенного пользователя
  - выработка и запись дополнительного аутентификатора
  - просмотр журнала событий
  - инициализация контроля целостности программной среды компьютера
  - запрос сводной информации о версии, настройках, содержании хранилища TSM

- Пользователь
  - продолжение загрузки компьютера
  - многофакторная аутентификация
    - Идентификатор пользователя – USB-ключ eToken
    - Аутентификатор – пароль пользователя
  - изменение пароля пользователя

Контроль целостности

Подсистема контроля целостности обеспечивает контроль следующих объектов:

- Файлы на компьютере для файловых систем NTFS/FAT32/FAT16;
- Критичные секторы жестких дисков:
  - ✔ Master Boot Record;
  - ✔ 62 сектора после Master Boot Record;
  - ✔ Volume (Partition) Boot Sector для каждого раздела жесткого диска;
  - ✔ Extended Boot Record для каждого раздела жесткого диска.

Режимы контроля целостности для пользователей:

- **Жесткий**, при нарушении загрузка операционной системы блокируется
- **Мягкий**, при нарушении загрузка операционной системы не блокируется

Журнал регистрации событий

- TSM осуществляет регистрацию всех событий доступа к компьютеру
- Журнал регистрации содержит информацию о следующих событиях:
  - Успешная аутентификация
  - Неуспешная аутентификация с сохранением ID предъявленного eToken
  - Изменения в учетных записях пользователей
  - Блокировка/разблокировка пользователей
  - Изменение настроек TSM
  - События подсистемы контроля целостности
  - Включение/отключение TSM
  - Информация о служебных событиях TSM
- Журнал регистрации событий TSM предоставляет полную информацию о событиях доступа к компьютеру, в том числе о попытках несанкционированного доступа
- Служебная информация о пользователях (имя, описание, серийный номер eToken), а так же журналы регистрации событий хранятся в энергонезависимой памяти

Сертификация

- embedded TSM:
  - Сертификат соответствия требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля **отсутствия недекларированных возможностей**» (Гостехкомиссия России, 1999) по **3 уровню контроля**;
  - Сертификат соответствия требованиям Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 5 февраля 2010 г. № 58, - для применения **в ИСПДн до 1 класса включительно**.
  - Сертификат соответствия требованиям руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Гостехкомиссия России, 1992г., для применения **в АС до класса 1В включительно**
  - Сертификат соответствия требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели **защищенности от несанкционированного доступа** к информации" (Гостехкомиссия России, 1992) – по **4 классу**.

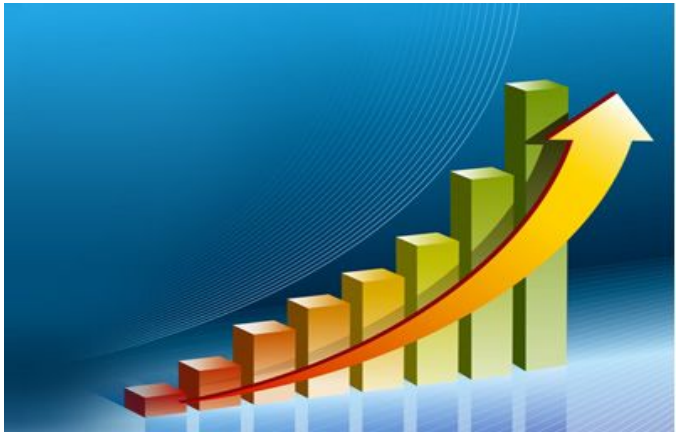
- Электронный ключ eToken 5:
  - Сертификат соответствия ФСТЭК России № 1883 от 11.08.2009 года на применение в **АС до класса 1Г включительно и ИСПДн до 1 класса включительно**.

- Операционная система компьютера:
  - MS Windows XP Professional: Сертификат № 844/2 / Сертификат № 844/3 на соответствие Заданию по Безопасности и имеет оценочный уровень доверия **ОУД 1 (усиленный)** в соответствии с руководящим документом "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий" (Гостехкомиссия России, 2002);
  - MS Windows Vista Business/Ultimate: Сертификат 1516/1 на соответствие Заданию по Безопасности и имеет оценочный уровень доверия **ОУД 1 (усиленный)** в соответствии с руководящим документом "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий" (Гостехкомиссия России, 2002);

Перспективы развития

- Защищенный компьютер
  - Интеграция в серверные решения
  - Интеграция в терминальные решения
  - Перенос на другие аппаратные платформы (AMD, Intel Core i*)

- embedded TSM
  - Удаленное управление
  - Централизованное администрирование
  - Интеграция криптографических функций
  - Поддержка расширенного модельного ряда смарт-карт и считывателей



Базальт БД

Моноблочный ПК для безопасной работы в двух независимых сетях.

kraftway®
ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ

Требования по защите данных

- **Указ Президента РФ от 17 мая 2008 г. № 351**
  - Не допускается подключение к сети Интернет средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну

- **Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) от 30.08.2002 г.**
  - использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
  - использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
  - использование сертифицированных средств защиты информации;
  - развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
  - электромагнитная развязка между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация;
  - Информация, составляющая служебную тайну и персональные данные, может обрабатываться только в изолированных ЛВС;

Типовое решение

Одно рабочее место

ПК №1 для работы в защищенной сети

Защищенная сеть

ПК №2 для работы в сети Интернет

Незащищенная сеть

- Два компьютера на одном рабочем месте
  - Защищенный ПК для работы с данными
  - Незащищенный ПК для выхода в Интернет
- Недостатки типового решения
  - Дополнительное рабочее место
  - Увеличенное энергопотребление
  - Затраты на техническое обслуживание

Постановка задачи

- Создание единого устройства для работы в двух независимых сетях в компактном и эргономичном исполнении.
- Минимизация уровня ЭМ излучения.
- Ограничение физического доступа к устройствам съёма информации.
- Использование общего комплекта мультимедийных и периферийных устройств для работы в независимых сетях.

Типичное рабочее место

Одно рабочее место

ПК №1 для работы в защищенной сети

Защищенная сеть

ПК №2 для работы в сети Интернет

Незащищенная сеть

- Для обеспечения возможности работы и в защищенной сети и с данными из незащищенной сети, например с данными из сети Интернет обычно используется два независимых ПК, каждый в полной комплектации.
- Основная причина – в недостаточной защищенности критичных данных от внешних информационных угроз.
- Два ПК на одном рабочем месте помимо низкой эргономики влекут за собой ряд дополнительных работ как по обслуживанию так и по подготовке данного оборудования к возможности использования на таких рабочих местах.

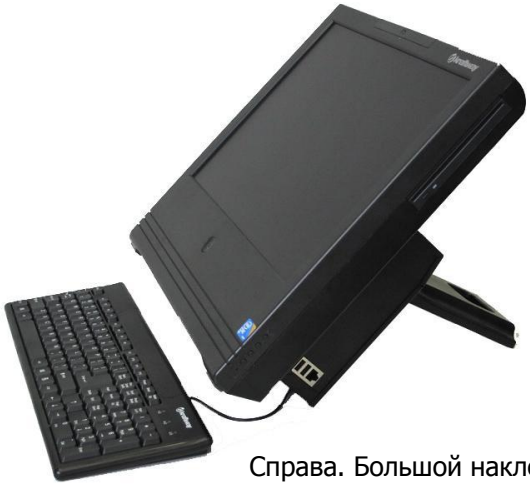
Решение "Kraftway Базальт ВД"

- Два независимых вычислительных модуля, монитор и мультимедийные устройства в одном корпусе
  - Незащищенный вычислительный модуль
    - построен по стандартной схеме компьютера
  - Защищенный вычислительный модуль имеет дополнительные элементы защиты
    - Гальванические развязки сигнальных линий
    - Экранирование питающих и сигнальных кабелей
    - Устранение паразитных перекрестных наводок
    - Развязывающий фильтр между землями

Внешний вид

Спереди

Справа



Справа. Большой наклон

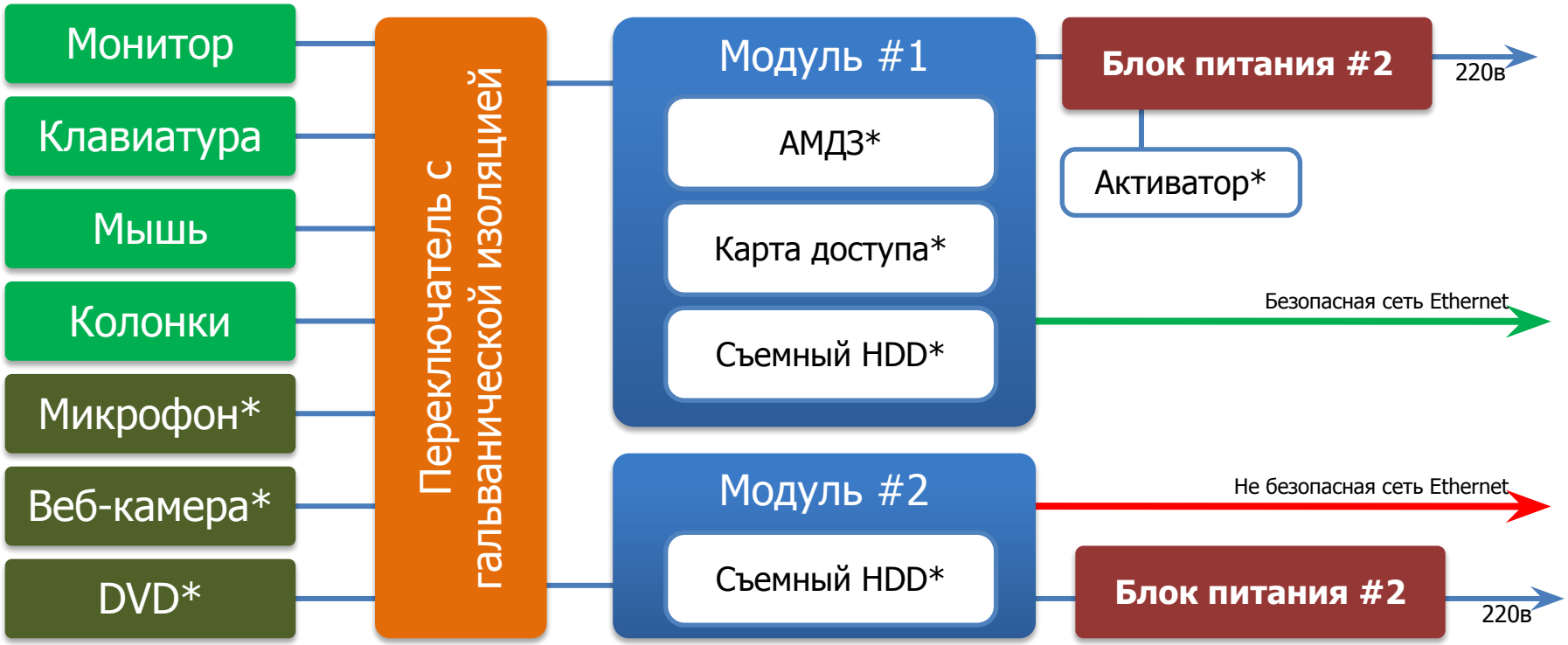
Сзади

Слева

Слева. Большой наклон

Функциональная схема устройства

Наследуя свойства серия моноблочных ПК Kraftway Studio модель Базальт BM представляет собой высокотехнологичный класс компьютерных персональных устройств. В едином стильном корпусе размерами немногим более обычного ЖК-монитора объединяются: высококачественная широкоэкранная TFT-матрица, два традиционных компьютера, один из которых оборудован средствами видеоконференций (веб-камера, акустическая система, микрофон), DVD, считывателем карт памяти, средствами аппаратной аутентификации. Второй ПК представляет из себя платформу для создания терминальной станции или ПК начального уровня.



* опция

Платформа

- Компания Kraftway разработала универсальную платформу для создания продуктов для оснащения рабочих мест.
- Накопленный опыт разработки и целый ряд уникальных решений позволяют в короткий срок создавать продукт под конкретную задачу заказчика.
- Большой набор опций.
- Изоляция электрических цепей ПК при переключении.
- Цветовая индикация состояния.

Улучшенная эргономика

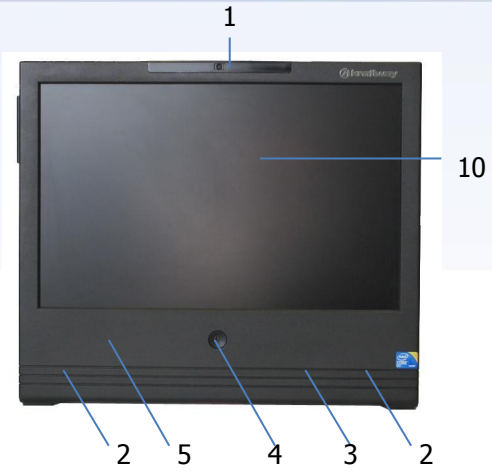
Моноблочный ПК даже при комплектации двумя вычислительными модулями занимает место одного монитора, что позволяет значительно увеличить свободное пространство и уменьшить количество проводов на рабочем месте.

Технические характеристики	
Форм-фактор	Моноблочное настольное исполнение, Два независимых вычислительных модуля в одном шасси с дисплеем Встроен KVM коммутатор с переключением на герконах
Монитор	высококонтрастный 19" дисплей с максимальным разрешением 1440x900 пик
Модуль #1	Intel® Core™ 2 Duo, Pentium D, Celeron, До 8 GB DDR2 2.5" SATA HDD объемом от 250 ГБ сеть Ethernet 10/100/1000 Гб
Модуль #2	Atom 230 До 2GB DDR2 2.5" SATA HDD объемом от 250 ГБ сеть Ethernet 10/100/1000 Гб
Уровень шума	менее 28 Дб
Операционная система	Kraftway Terminal Linux ОС Microsoft® Windows® 7 ОС Microsoft® Windows Vista® ОС Microsoft® Windows® XP Linux ASP Linux, Alt Linux, SUSE Linux, Fedora
Габариты корпуса шасси	высота 311 мм, ширина 480 мм, глубина 740 мм
Мультимедиа устройства	Модуль #1 комплектуется оптическим накопителем DVD+/-RW, считывателем карт памяти, веб-камерой, микрофоном и акустической системой
Вес	11 кг (со всеми опциями и установленными модулями в максимальной комплектации)
Напряжение питания	100-240 В, 50-60 Гц , внешние блоки питания, раздельное для модулей
Гарантия	3 года

Дополнительные элементы защиты

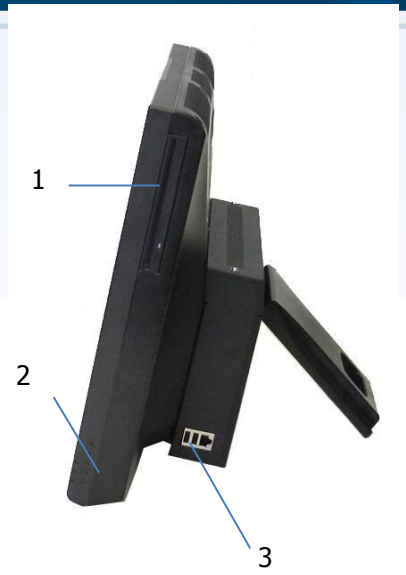
- Фильтр электромагнитных излучений монитора
- Радиочастотный идентификатор пользователя
- Гальваническая развязка блоков питания
- Электронный замок, интегрированный в BIOS.

Назначение элементов



1. Встроенная камера
2. Встроенные динамики
3. Встроенный микрофон
4. Кнопка включения питания и переключения между вычислительными модулями
5. Встроенный бесконтактный считыватель RFID карт
6. Вентиляторы принудительного охлаждения
7. Наклейка с серийным номером
8. Опорная подставка
9. Гнездо замка KengsingtonLock
10. 19” LCD экран
11. Маркер контроля вскрытия корпуса

Назначение элементов (продолжение)



1. DVDRW привод
2. Кнопки управления настройками монитора
3. Разъемы подключения клавиатуры, мыши и порты Ethernet
4. Модуль сменных жестких дисков
5. Разъемы для наушников и внешнего микрофона

Спасибо за внимание

- Вопросы
- Демонстрация на стенде