БлокХост АМДЗ

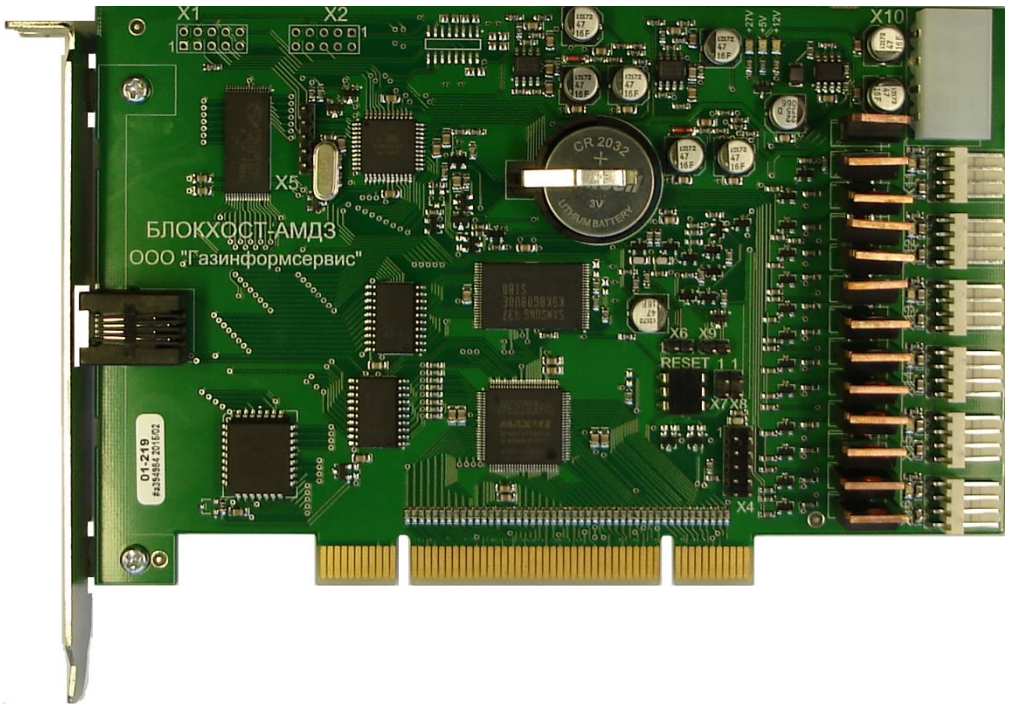
Аппаратно-программный комплекс доверенной загрузки (АПК) «БЛОКХОСТ-АМДЗ» предназначен для обеспечения доверенной загрузки операционных систем семейств Windows/Unix/Linux (в т.ч. систем виртуализации ESX/ESXi) на персональных электронно-вычислительных машинах (ПЭВМ) типа IBM PC.

Преимущества

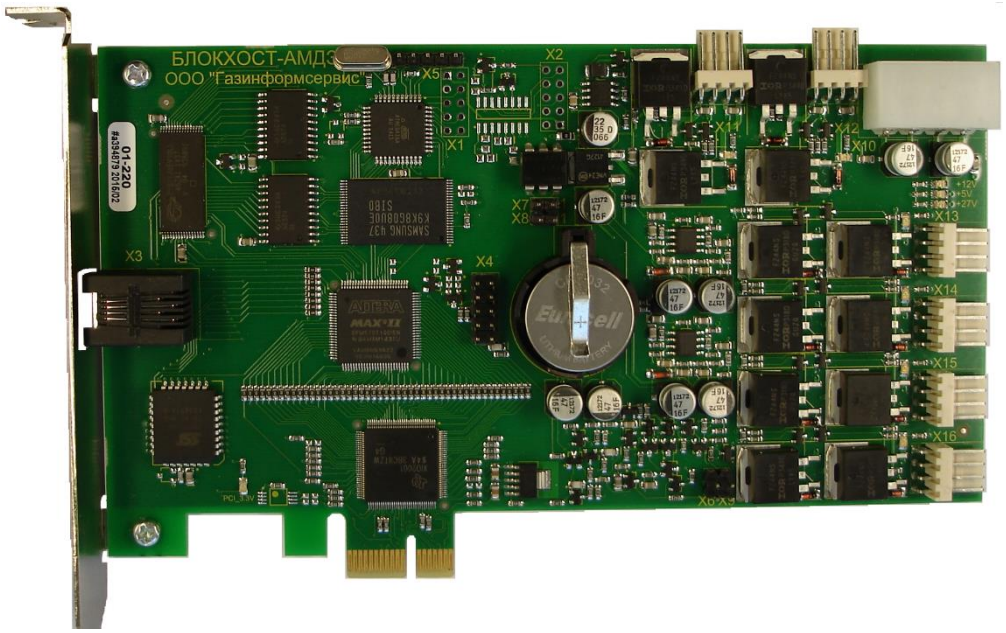
1. Поддержка загрузки ОС на ПЭВМ с Legacy BIOS и EFI/UEFI.
2. Поддержка загрузки ОС с MBR и GPT-разделов.
3. Доверенная загрузка ОС Microsoft Windows 2000/XP/2003/Vista/7/2008/8/8.1/2012.
4. Доверенная загрузка ОС семейств Linux/Unix, поддерживающих стандарт Linux Standard Base (LSB) версий 3.x/4.x, в т.ч. систем виртуализации VMware ESX 3.x/4.x, VMware ESXi 5.x.
5. Широкий спектр поддерживаемых загрузчиков ОС (GRUB, LILO, NTLDR и пр.).
6. Широкий спектр поддерживаемых файловых систем (ext2/ext3/ext4, MS-DOS, FAT, NTFS, UFS, UFS2 и пр.).
7. Возможность аппаратного управления внешними устройствами (FDD, CD, DVD), до 6 устройств.
8. Подключение по принципу Plug and Play – не требуется установки дополнительного ПО на ПЭВМ.
9. Индивидуальные параметры аутентификации для каждого зарегистрированного пользователя.

Варианты исполнения

1) PCI;



2) PCI-E.



Технические характеристики

1. Варианты исполнения комплекса: PCI, PCI-E
2. Тип датчика случайных чисел (ДСЧ): программный и аппаратный
3. Количество аппаратных ДСЧ: 2 (основной и резервный)
4. Поддерживаемые персональные электронные идентификаторы: iButton, eToken, SafeNet eToken, ESMART Token, ESMART Token SC, JaCarta PRO, Rutoken-ЭЦП, USB-накопители
5. Интерфейсы аппаратно отключаемых внешних устройств: IDE, SATA
6. Количество подключаемых внешних устройств: 6

Функциональные возможности

1. Аутентификация с использованием пароля и/или персонального идентификатора с PIN-кодом:

1. длина пароля: от 8 до 32 символов;
2. возможность генерации паролей и PIN-кодов с использованием ДСЧ;
3. срок действия парольной информации: от 1 до 45 дней;
4. возможность смены пароля пользователями без привлечения администратора безопасности;
5. ограничения на количество попыток аутентификации пользователей;
6. ограничения на время аутентификации пользователей;

2. Контроль целостности системы:

1. контроль целостности программной части (в т.ч. загрузочной записи и реестра ОС Windows);
2. контроль целостности аппаратной части (в т.ч. сменных носителей);
3. блокировка загрузки ОС при нарушении целостности программной и/или аппаратной частей ПЭВМ.