OKBSAPR.RU
okbsapr@okbsapr.ru

ПЕРСПЕКТИВНЫЕ РЕШЕНИЯ РАЗВИТИЯ ОБЪЕКТОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В УСЛОВИЯХ НОВЫХ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ

Смоленск, 2017

По сложившейся в мире практике задача защиты информации при ее обработке в информационных системах решается посредством включения в их состав аппаратных СЗИ – средств защиты информации.

Основными задачами этих средств являются:

обеспечение доверенной загрузки;

создание изолированной программной среды;

защита от несанкционированного доступа;

защита от разрушающих программных воздействий и вредоносных программ.

Традиционный подход к реализации требований по защите информации приводит к значительному увеличению стоимости разработки и эксплуатации информационных систем.

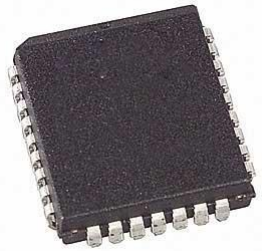
ОКБ САПР удалось обеспечить решение этих задач новым, нетрадиционным методом

Защищенные микрокомпьютеры

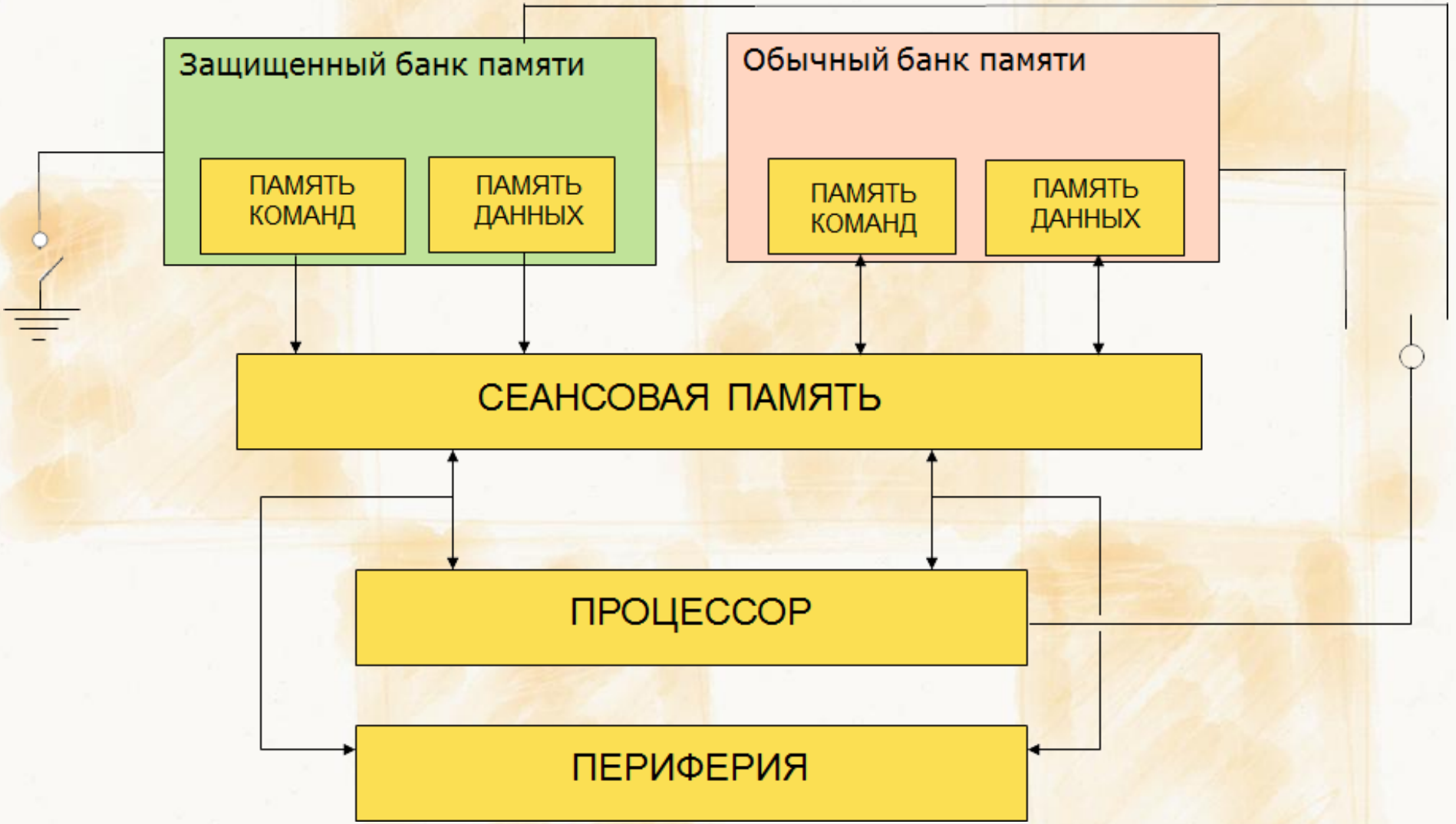
По мере движения информационных технологий в сторону облачных инфраструктур естественные требования к клиентским компьютерам дополнились еще одним – требованием сочетания мобильности с защищенностью.

Современные, в том числе планшетные компьютеры создаются на основе «гарвардской» архитектуры, что создает возможность намного более простого и дешевого решения поставленной задачи. В этом случае достаточно микросхему банка памяти, в которой размещается ОС, перевести в режим «только чтение», read only.

Read only



НОВАЯ ГАРВАРДСКАЯ АРХИТЕКТУРА



ОСОБЕННОСТИ АРХИТЕКТУРЫ

1. Динамическая изменяемость
2. Неизменность (целостность) ОС и СПО в защищенном режиме
3. Защищенность от «вирусов»
4. Возможность адаптации стандартных ОС и СПО

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

1. Выбор сертифицированной ОС, в том числе «Astra Linux Special Edition»
2. Возможность использования в выделенных помещениях
3. Корректность установки СКЗИ и использования ключевых носителей с неизвлекаемым ключом
4. Возможность исполнения в защищенном корпусе
5. Отсутствие отечественных и зарубежных аналогов

Решение защищено 12 патентами с 32 пунктами патентных формул, разработка выполнена полностью на отечественной базе и элементах «восточных» производителей.

Линейка включает в себя варианты как с одной (только защищенной) ОС (подтип МКТ), так и с двумя ОС (защищенной и незащищенной) и переключателем (подтип МКTrusT).

Защищенный режим

- ✓ Включение обозначается специальным индикатором;
- ✓ При каждом новом включении загружается предустановленный образ ОС в режиме Read only;
- ✓ Возможна установка VPN;
- ✓ Совместим с сертифицированным СЗИ НСД «Аккорд Х К»;
- ✓ Совместим с защищенным средствами хранения данных семейства «Секрет».

Почему МК?

- ✓ Стоимость ≈ 15 000 руб. (розничная цена)
- ✓ Мобильность, сравните:  и 
- ✓ Защищенность   
- ✓ Энергоэффективность   

✓100шт. ≈ 1шт.
✓3Вт(W) 300 Вт(W)

- ✓ МК может использоваться как локальное рабочее место наряду с другими СВТ.
- ✓ МК обладает ощутимыми преимуществами при использовании в качестве облачного рабочего места.

Вариант МК с одной ОС подходит для сценариев применения, предполагающих работу только в защищенной среде, и ни в какой другой.

МКТ – это микрокомпьютер в форм-факторе донгла (внешне похож на большую флешку), в котором есть только одна ОС – защищенная ОС Linux, расположенная в RO памяти устройства.

МКТ+ чуть больше по размеру, но зато может обновляться в удаленном режиме по специально разработанной защищенной процедуре.

MKTrusT – микрокомпьютер, позволяющий работать в одном из двух режимов – защищенном или незащищенном, без ограничения возможностей.

МКТ-card и **МКТ-card long** – это доверенный облачный микрокомпьютер с динамически изменяемой архитектурой. Конструктивно он оформлен как док-станция с отчуждаемым компьютером.

TrusTPad – это планшет, построенный на «гарвардской» архитектуре, так же работающий в 2-х режимах.

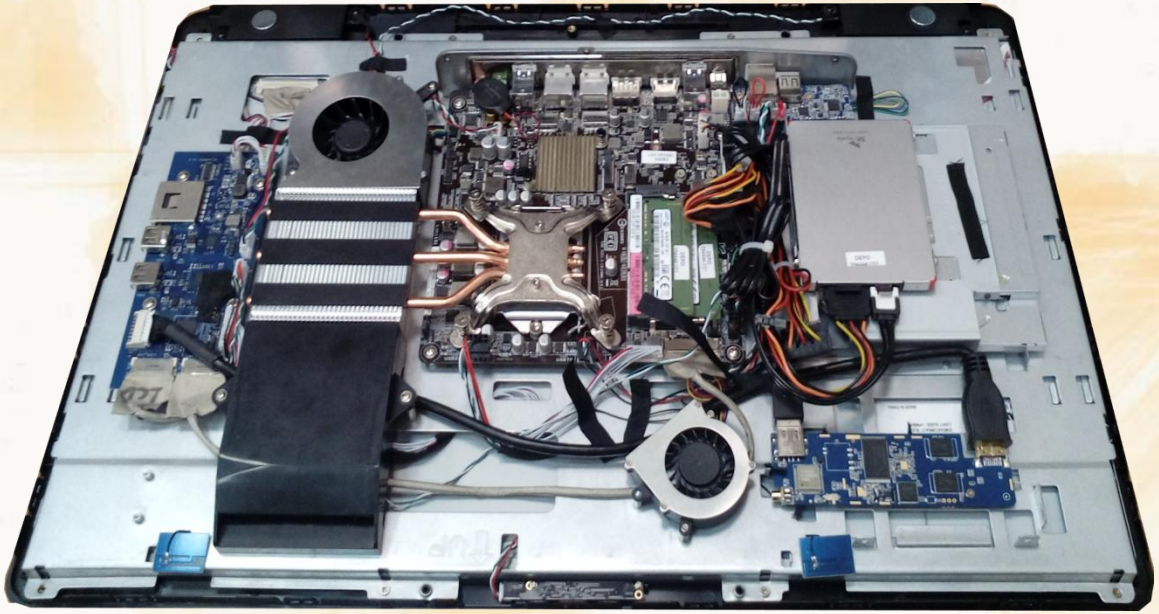
Защищенный двухконтурный моноблок

МК + DEPO представляет собой АРМ, предназначенный для работы как в "открытом" сегменте ЛВС с доступом к Интернет (на базе моноблока DEPO), так и в "закрытом" сегменте ЛВС (на базе защищенных микрокомпьютеров линейки МК).

- Удобная организация рабочего пространства
- Решение «2 рабочих мест в одном» – один моноблок для работы в двух контурах
- Соответствие требованиям по защите информации

Состав моноблока:

- Моноблок DEPO;
- Встроенный микрокомпьютер МК;
- Встроенный KVM-переключатель, обеспечивает удобное переключение рабочего сеанса между моноблоком и встроенным микрокомпьютером (переключение между устройствами осуществляется посредством клавиатуры);
- Средства защиты информации



Преимущества

- **Полностью российский продукт.**
В решении применены и интегрированы продукты российского производства: моноблок, микрокомпьютер, возможна установка СЗИ НСД «Аккорд», антивирусного ПО.

- **Удаленное централизованное управление.**
Возможность развертывания системы централизованного управления с функциями обновления, выключения и перезагрузки, аудита ИБ.

- **Эргономика рабочего места**.
Уникальный двухконтурный моноблок в едином корпусе, без внешних KVM, эргономичен удобен для установки (минимум времени на развёртывание АРМ работника) и транспортировки.

НОУТБУК РУКОВОДИТЕЛЯ
с предустановленными и настроенными СЗИ

Ноутбук руководителя – идеальное решение для удаленной работы с защищаемой информацией.

Изделие представляет собой ноутбук со встроенным СЗИ НСД «Аккорд» и считывающим устройством смарт-карт или биометрии. Работа ноутбука возможна в 2- х режимах, один из которых – защищенный. Загрузка компьютера контролируется встроенным модулем СЗИ НСД «Аккорд», который проверяет наличие уникального идентификатора.

- контроллер Аккорд-GXM

- контроллер Аккорд-GXMH

- контроллер Аккорд-M.2

В случае успешной идентефикации пользователя, дальнейшая загрузка выполняется из встроенной памяти «Аккорда», а штатный накопитель HDD отключается. Целостность загрузочного образа обеспечивается функционалом СЗИ НСД. Основной и единственной задачей образа является создание защищенного VPN соединения с терминальным сервером или веб-порталом. Параметры соединения записываются на смарт-карту, которая одновременно является идентификатором пользователя.

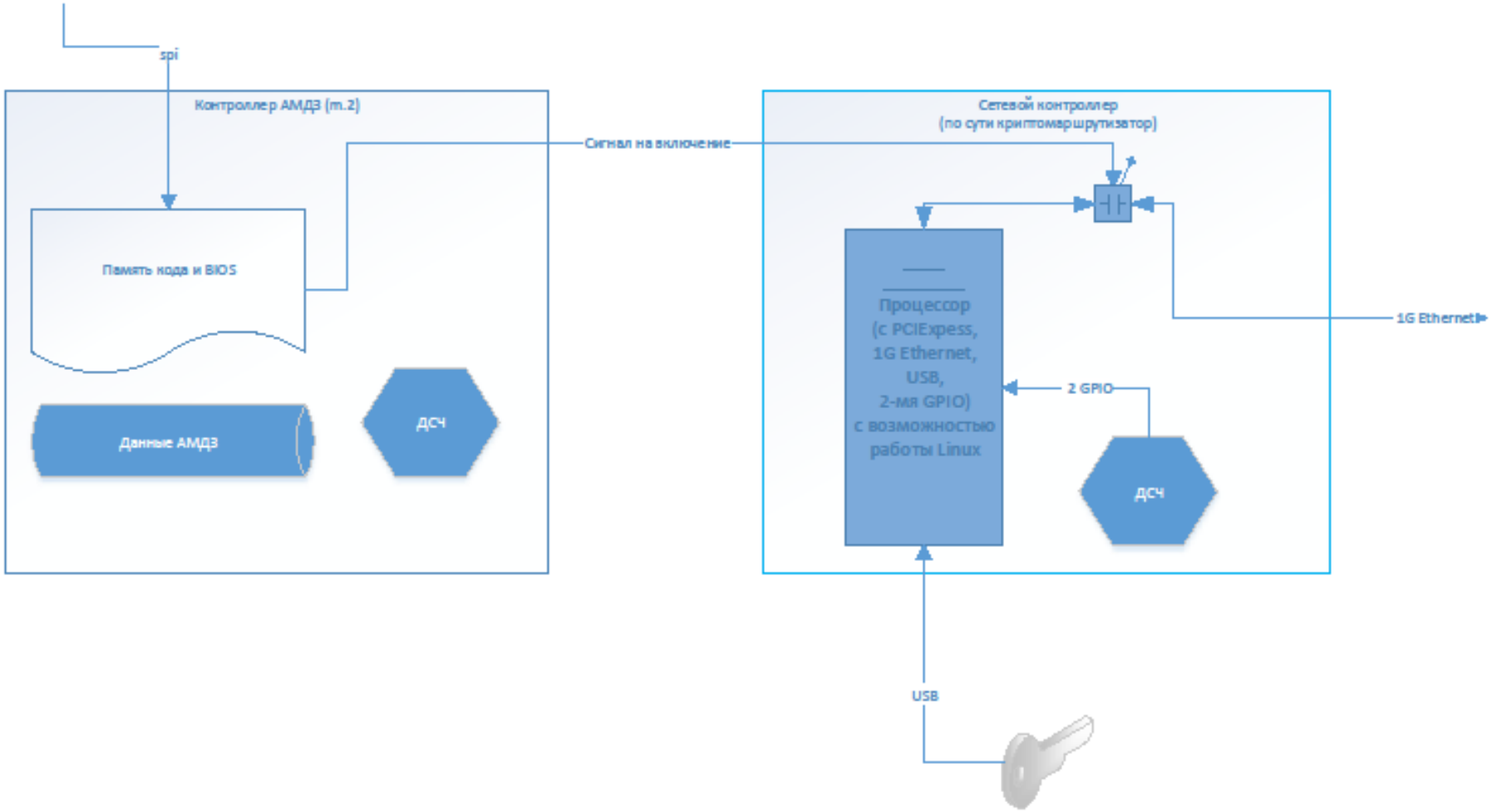
Таким образом «Ноутбук руководителя» служит еще защищенным тонким клиентом, который поможет владельцу работать с необходимыми документами, находясь дома, в командировке, отпуске и т.д. Поэтому именно для этого решения актуально использование в комплекте служебных носителей семейства «Секрет», выступающих в этой схеме в качестве защищенного локального хранилища.

Специальный USB-носитель,

который можно использовать только на разрешенных администратором СВТ

- Личный Секрет;
- Секрет Особого Назначения
- **Состав:**
- «Секрет» – это USB-носитель, который можно использовать только на том СВТ, на который установлен «Секретный агент»
- «Секретный агент» - специальное ПО, предназначенное для безопасной работы с «Секретами»
- «Секретный агент» узнает только зарегистрированные «Секреты», а зарегистрировать свой «Секрет» может только владелец или администратор «Секрета».

Схема
системы защиты ноутбуков
(защита от IME)



Смоленск, 2017

OKBSAPR.RU
okbsapr@okbsapr.ru

Спасибо за внимание!