СРЕДСТВО ОБЕСПЕЧЕНИЯ ДОВЕРЕННОГО СЕАНСА СВЯЗИ

СОДС «МАРШ!»

ОКБ САПР
2022

Среда доверенная, если

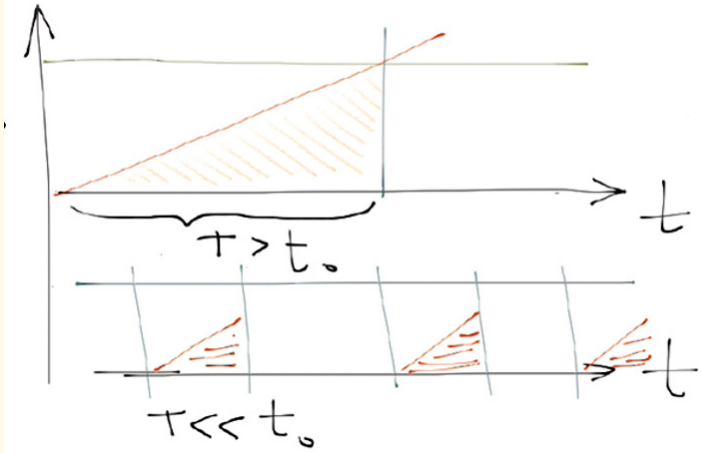
На проверенном компьютере используются

- проверенная ОС,
- проверенные программы,
- проверенные данные.

Доверенную среду обеспечивают

- контроль запуска задач и процессов;
- взаимное невлияние задач;
- защита от перехвата управления;
- защита ИТ как последовательности операций.

Обеспечить все это тем сложнее и дороже, чем дольше потенциальное время проведения атаки.



Там, где доверенная среда нужна постоянно, необходимо обеспечивать ДВС, доверенную вычислительную среду.

А там, где не постоянно?

Проблемы применения ДВС

Организация доверенной вычислительной среды (ДВС) на компьютерах пользователей, которые работают с удалённой защищённой системой непродолжительное время, не всегда уместна – стоимость ДВС высока, а организация сложна.

Для кратковременного соединения с защищённой корпоративной сетью рациональнее использовать средства доверенного сеанса связи (ДСС), которые организуют доверенную среду на некоторое время.

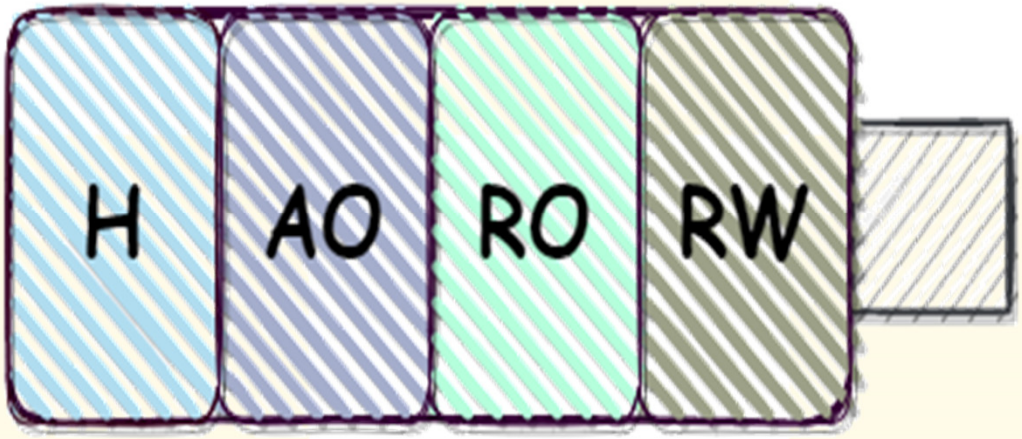
СОДС «МАРШ!»

СОДС «МАРШ!» организует с удаленной системой ДСС, в рамках которого поддерживается доверенная среда.

Устройство подключается к незащищенному компьютеру, загружает на него ОС из защищенной от перезаписи памяти и устанавливает защищенное соединение с удаленной информационной системой.

Особенности архитектуры «МАРШ!»

H - Hidden
AO - AddOnly
RO - ReadOnly
RW - ReadWrite



На этапе производства память СОДС «МАРШ!» разбивается на разделы и к ним устанавливаются различные права доступа, которые контролируются микроконтроллером и пользователем изменены быть не могут.

Особенности архитектуры «МАРШ!»

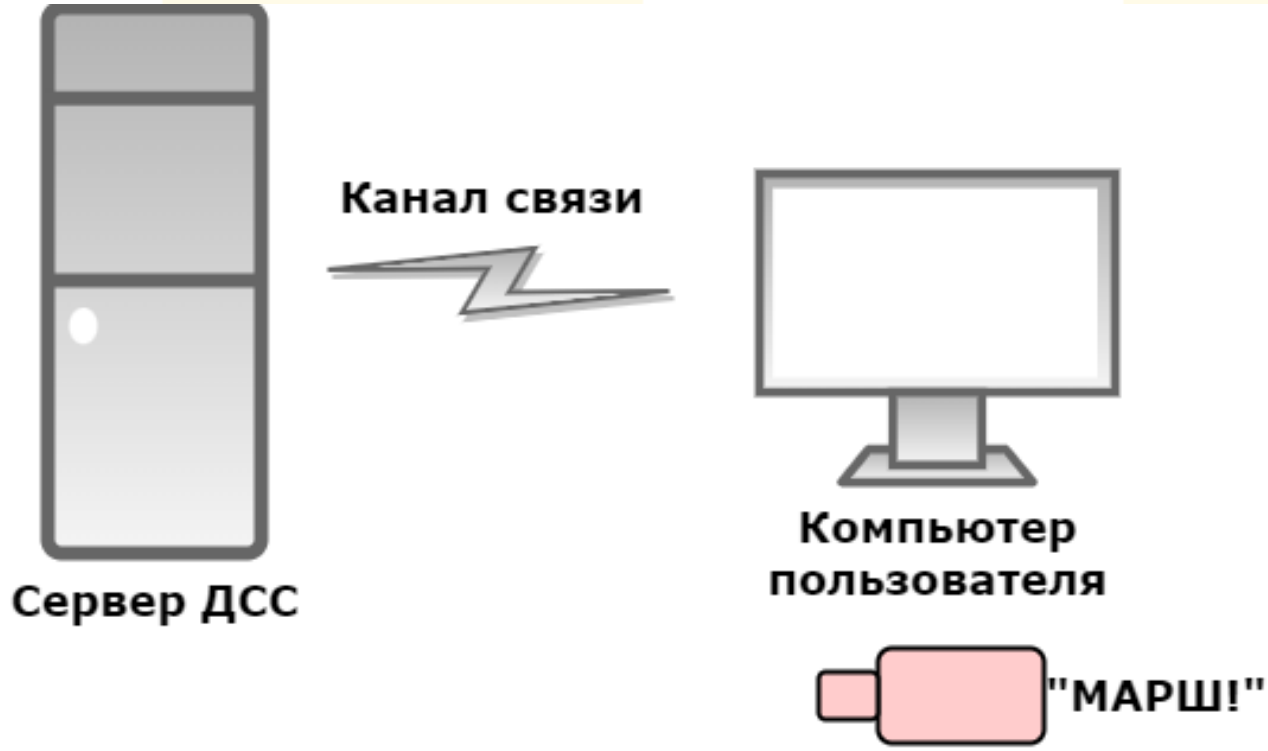
Память СОДС «МАРШ!» содержит

- хотя бы один раздел ReadOnly (RO),
- хотя бы один раздел ReadWriteHidden (RWH),
- могут быть разделы AddOnly (AO) и разделы с общим доступом RW.

В RO разделе размещаются ОС и другое ПО, которое не должно изменяться длительное время. Обновления и дополнения ПО «МАРШ!» размещаются в одном из разделов RWH, в другом размещается ключевая информация VPN, а раздел AO используется для ведения аппаратных журналов событий безопасности.

Принцип работы «МАРШ!»

В рамках ДСС между собой взаимодействуют Клиент ДСС и Сервер ДСС. В качестве Клиента ДСС выступает компьютер пользователя, загруженный с СОДС «МАРШ!».



Функции «МАРШ!»

- ✓ доверенная загрузка ОС;
- ✓ защищённое на основе асимметричных криптографических алгоритмов соединение с Сервером ДСС;
- ✓ возможность использования устройства «МАРШ!» в качестве средства И/А пользователя для доступа к сервисам РИС (в т. ч. хранение ключей и сертификатов);
- ✓ среда функционирования прикладного ПО сторонних производителей.

Особенности «МАРШ!»

«МАРШ!» – это «серебряная пуля» для хакера, поскольку

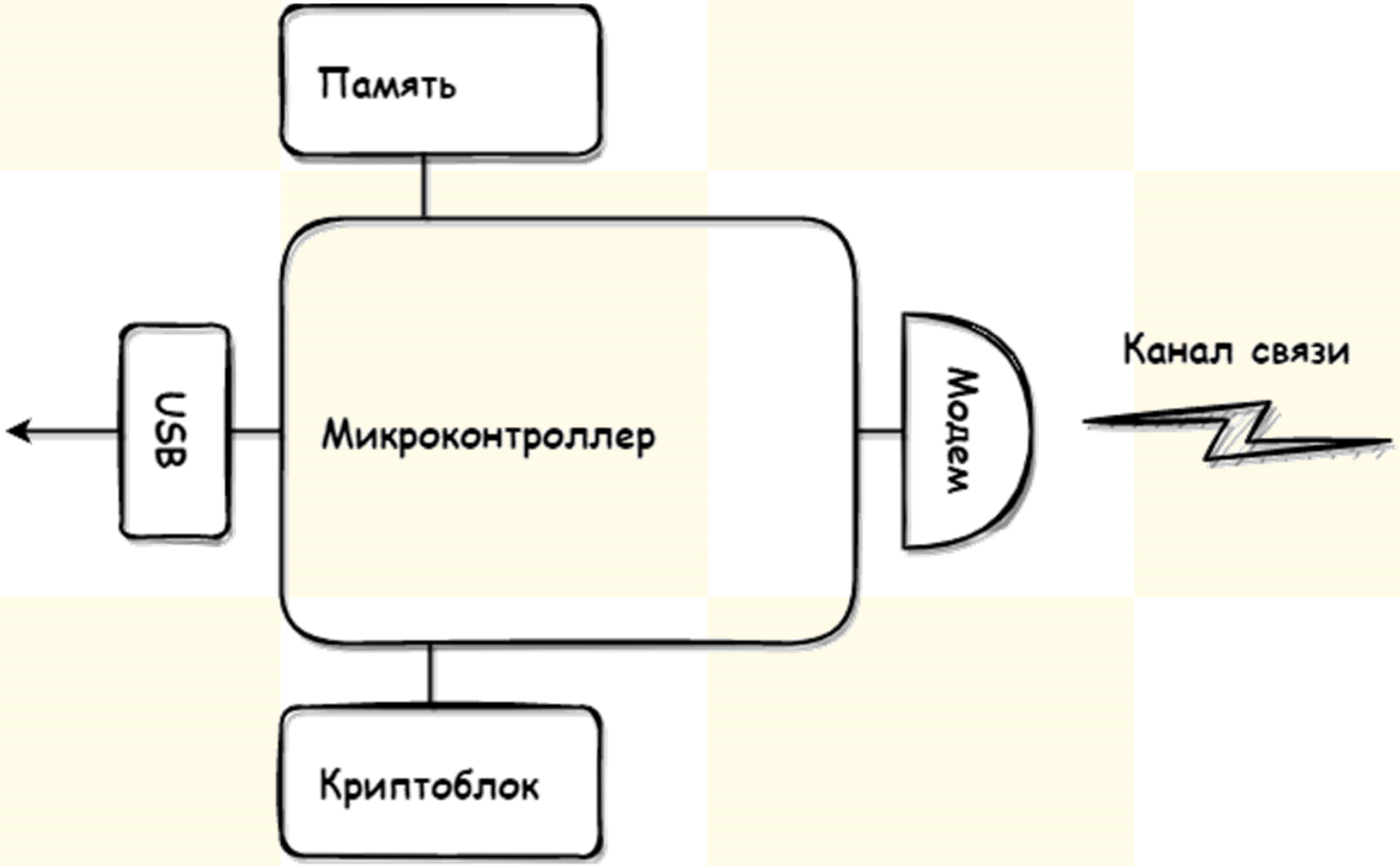
- ✓ состояние критичных компонентов зафиксировано,
- ✓ вирусы блокированы,
- ✓ ключи неизвлекаемы,
- ✓ перехват управления невозможен,
- ✓ управление отчуждено от клиента (пользователь не может ничего напортить).

«M!&M»

Вариант «M!&M» отличается от СОДС «МАРШ!» наличием модуля связи (модема) в качестве встроенного аппаратного компонента.

При необходимости организации ДСС с рабочего мобильного места, у которого нет собственных средств связи, более предпочтительным вариантом является использование модема.

Особенности архитектуры «M!&M»



Применение «M!&M»

«M!&M» подходит, например, для удаленной работы сотрудника банка, оформляющего банковские карты. Многие банки предлагают оформление карты в любом удобном для клиента месте, а иногда этот способ оформления карты – единственно возможный (для интернет-банков).

При использовании «M!&M» можно быть уверенным в том, что никакое несанкционированное воздействие не сможет изменить программное обеспечение устройства, а значит, и повлиять на прием и передачу данных.

Спасибо за внимание!

Если у вас возникли вопросы, то **напишите нам**.

Наш сайт в интернете:
www.okbsapr.ru