Программно-аппаратные средства обеспечения информационной безопасности

Лекция № 10

Современные программно-аппаратные средства обеспечения информационной безопасности (ч.3)

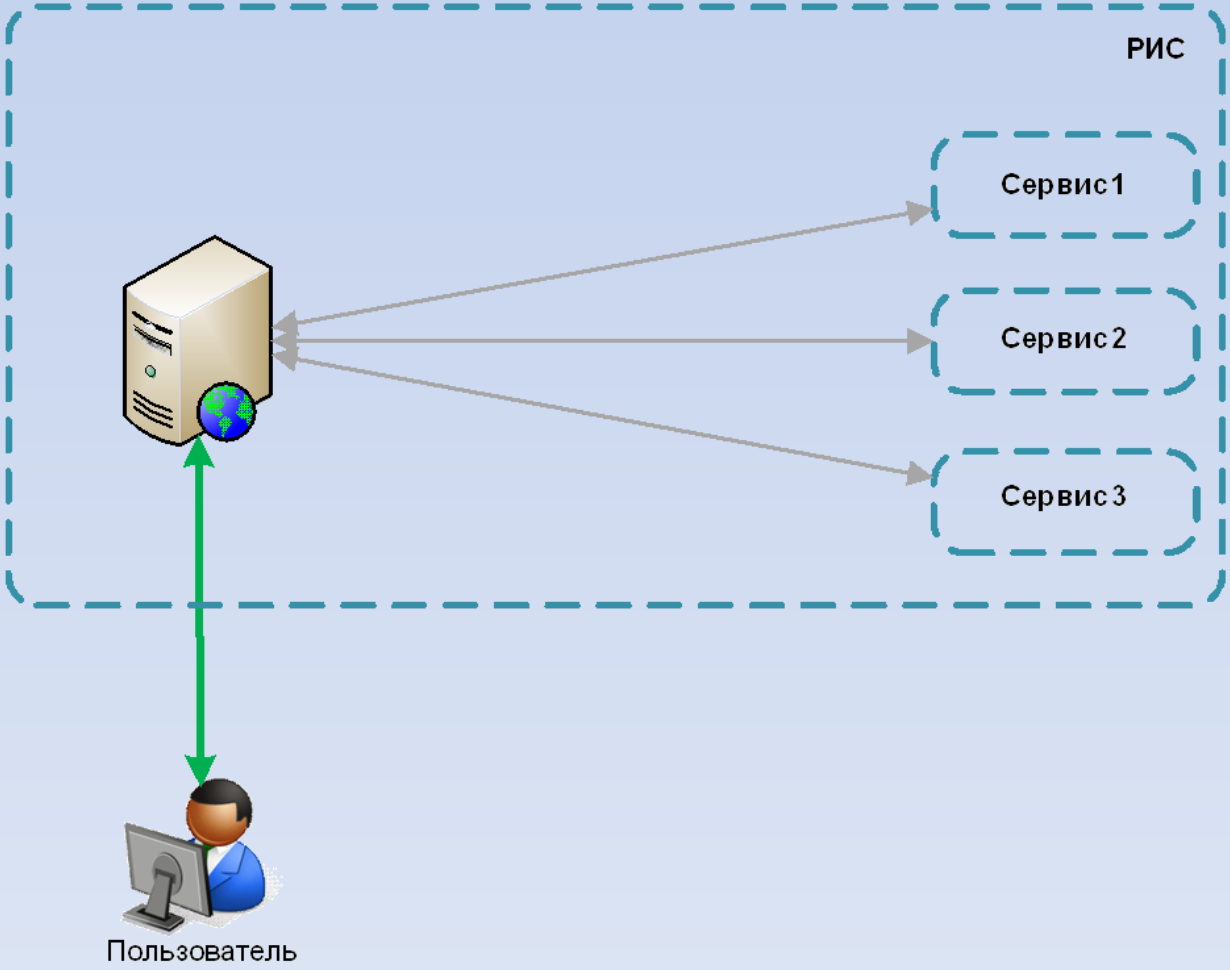
Рахманенко И.А.

План

- Доверенные сеансы связи МАРШ!
- Защищенные микрокомпьютеры «МКТ»
- Защищенные носители «Секрет»

ДОВЕРЕННЫЕ СЕАНСЫ СВЯЗИ МАРШ!

Распределенные информационные системы



- Сервис-ориентированная архитектура
- Виртуализация
- ЦОД

Особенности защиты удалённого доступа к ИР

- Сложность контроля выполнения требований политики ИБ на удалённых АРМ пользователей
- Необходимость использования сертифицированных ОС, СЗИ НСД и СКЗИ для шифрованием и работы с ЭЦП
- Необходимость аттестации АРМ пользователей
- Ограничение функционала сертифицированных ОС и прикладного ПО (в т.ч. сложность процедуры обновлений)
- Высокая стоимость комплекта сертифицированных ОС, СЗИ НСД и СКЗИ, а также процедуры аттестации

Концепция ДСС

Обеспечение достаточных условий для защищённой работы удалённых пользователей с сервисами защищаемых ИР на определённый период времени без построения ИПС и без снижения класса защиты ИР.

Два режима работы компьютера:

- Открытый режим (без доступа к сервисам защищаемым ИР)
- Режим ДСС (доверенный сеанс работы с сервисами защищаемых ИР)

Концепция ДСС

Доверенный сеанс связи (ДСС) – период работы компьютера, в рамках которого:

- обеспечивается доверенная загрузка ОС
- организуется защищённое сетевое соединение
- поддерживаются достаточные условия для работы СКЗИ

Клиенты РИС

- в общем случае заранее неизвестно, с какого компьютера будет инициировано соединение с сервером;
- один и тот же пользователь может осуществлять подключение к серверу с разных компьютеров (например, один раз с рабочего компьютера, второй — с домашнего);
- тип компьютера пользователя не подлежит контролю (стационарный компьютер, планшет, ноутбук);
- количество пользователей, желающих обратиться к удаленному сервису, а значит, и количество компьютеров, подлежащих защите, заранее может быть неизвестно.

Комплекс «МАРШ!»

- Клиент ДСС
- Сервер ДСС

Комплекс «МАРШ!»

Клиент ДСС

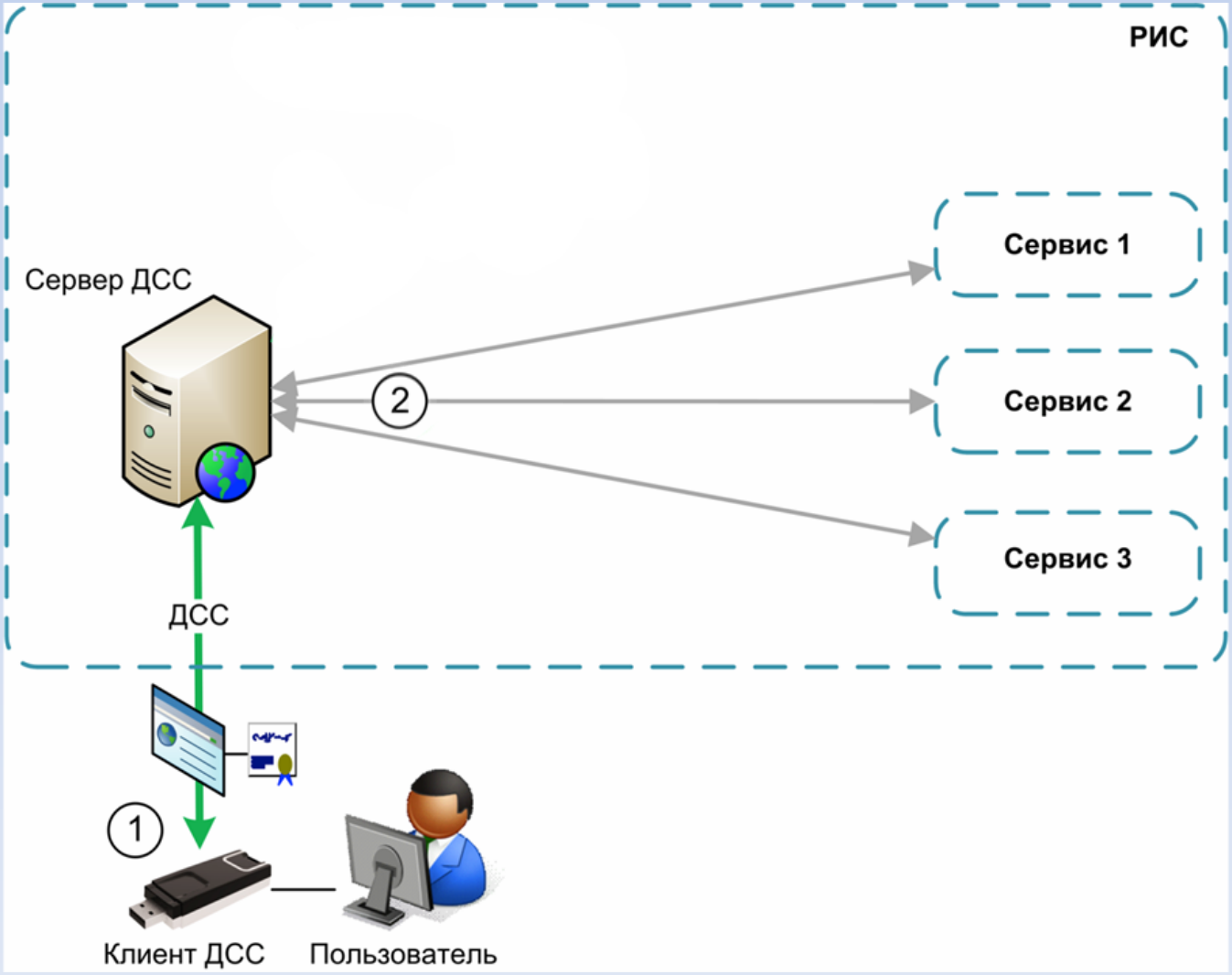
- Загрузочное USB-устройство с собственным микропроцессором
- Аппаратно разделённые области памяти с однократно назначаемыми атрибутами доступа
- Загрузочная ОС, СКЗИ и набор прикладного ПО в защищённой от записи области памяти

Комплекс «МАРШ!»

Сервер ДСС

- Доверенный сервер
- Создание и работа защищённых сетевых соединений с Клиентами ДСС
- Переключение Клиентов ДСС на сервисы защищаемых ИР в соответствии с правами пользователей

Схема работы



Преимущества «МАРШ!»

- Необходимый функционал и достаточный уровень защиты доступа пользователя к защищаемым информационным ресурсам
- Мобильность, готовность к работе на произвольном (в т.ч. недоверенном) компьютере
- Отсутствие ограничений на работу пользователя с компьютером вне режима доверенного сеанса связи
- Приемлемая стоимость

Доверенная среда

Режим доверенной среды обеспечивает защищённый ввод данных поставщиками данных, а также защищённое получение данных потребителями

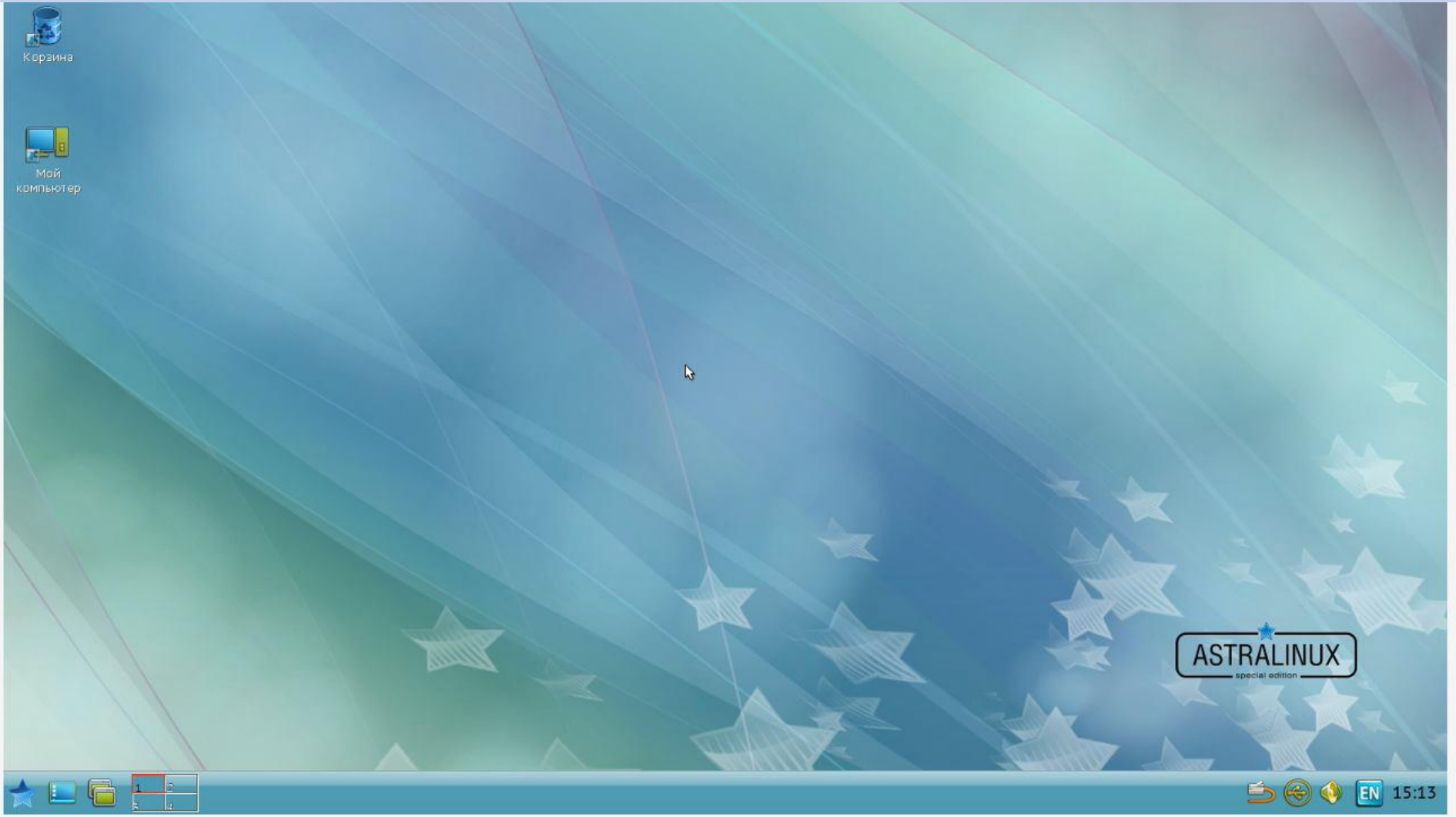
ДСС «МАРШ!»

Требования

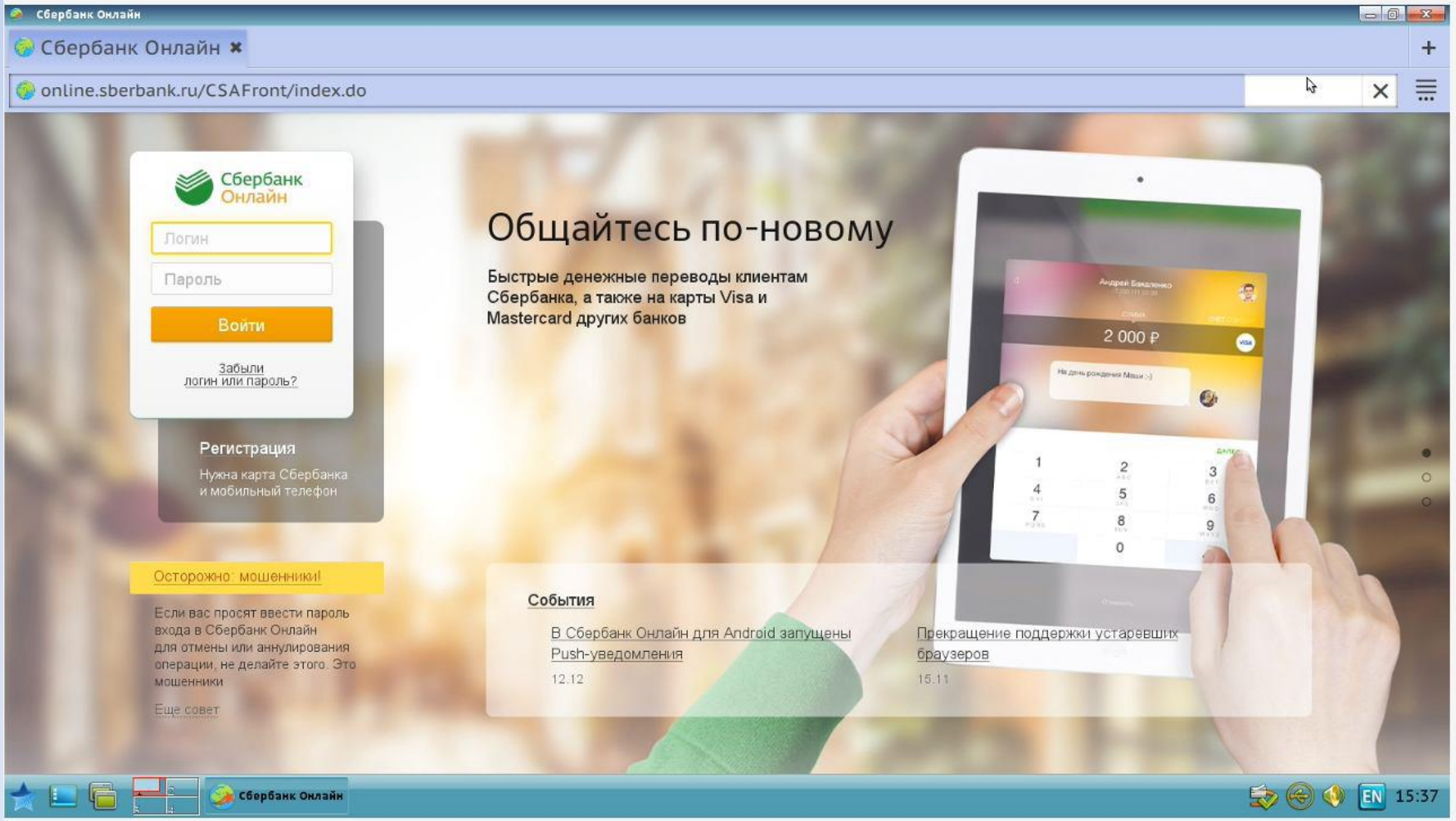
Требования к компьютерам:

- бездисковая рабочая станция с центральным процессором архитектуры x86 (IA-32) или AMD64 (x86-64)
- объем оперативной памяти не менее 128 Мб,
- свободный USB-порт (стандарта 1.1. или 2.0);
- BIOS с возможностью осуществлять загрузку с USB-устройств.

После загрузки



Браузер

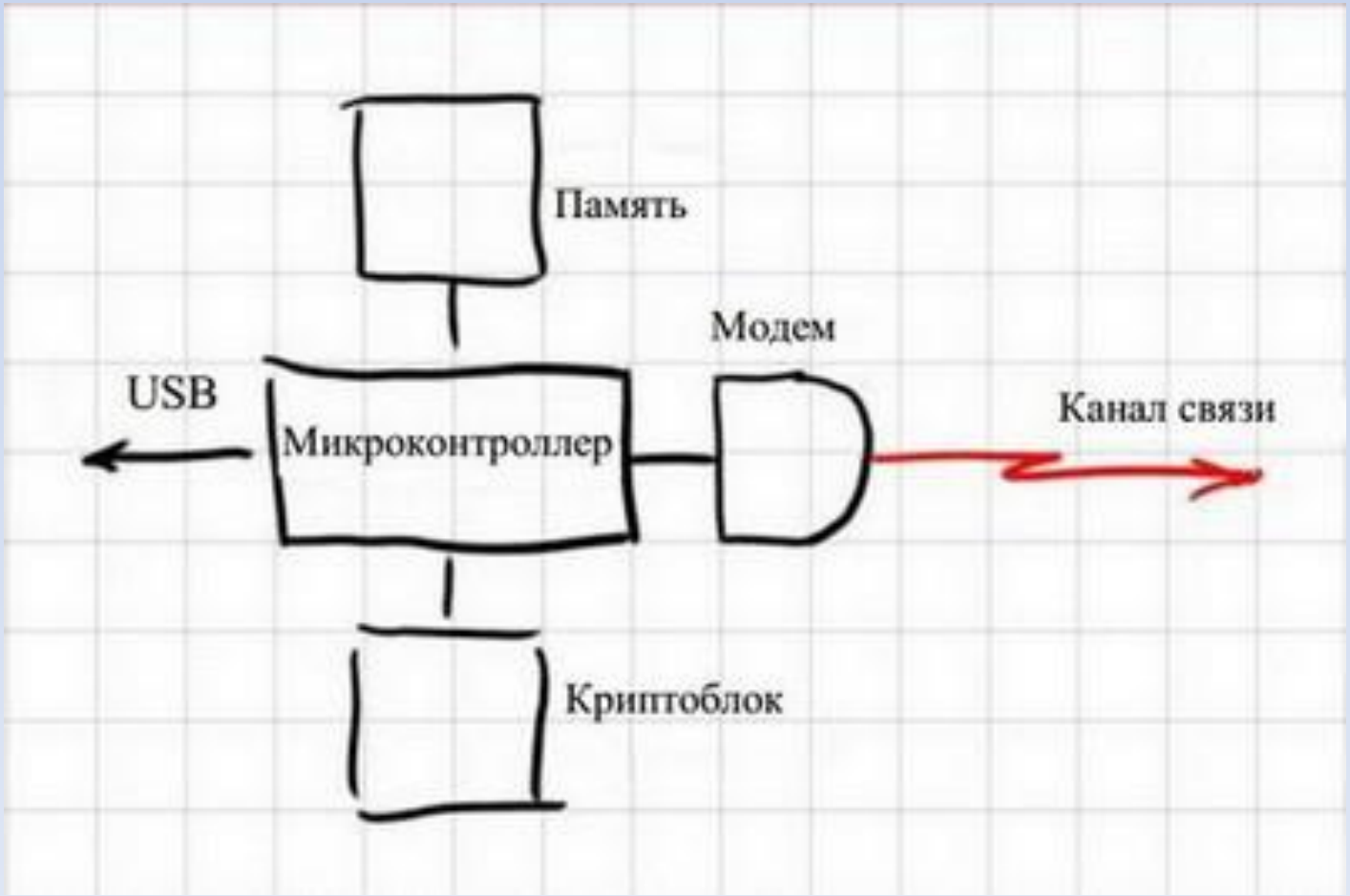

Сбербанк Онлайн
Сбербанк Онлайн
online.sberbank.ru/CSAFront/index.do
Сбербанк Онлайн
Логин
Пароль
Войти
Забыли логин или пароль?
Регистрация
Нужна карта Сбербанка и мобильный телефон
Осторожно: мошенники!
Если вас просят ввести пароль входа в Сбербанк Онлайн для отмены или аннулирования операции, не делайте этого. Это мошенники
Еще совет
Общайтесь по-новому
Быстрые денежные переводы клиентам Сбербанка, а также на карты Visa и Mastercard других банков
2 000 ₽
События
В Сбербанк Онлайн для Android запущены Push-уведомления
12.12
Прекращение поддержки устаревших браузеров
15.11
Сбербанк Онлайн
EN
15:37

ДСС «МАРШ!»

- Сертификат – по классу КС2
- Стоимость Клиента ДСС – 5 т.р.
- Стоимость Сервера ДСС – 250 т.р.*

M!&M

- Добавлен модем



M!&M

- Используется мобильная рабочая станция;
- Используется PC, для которой политикой безопасности запрещено подключение к сети;
- Рабочая станция эксплуатируется в условиях, в которых уровень развития сетевой инфраструктуры не позволяет иметь собственные средства связи.

ЗАЩИЩЕННЫЕ МИКРОКОМПЬЮТЕРЫ «МКТ» (ОКБ САПР)

Технология

- Память, в которой размещается ОС, переводится в режим «только чтение»
- Этот обеспечивает неизменность ОС аппаратным способом, никакие программные действия злоумышленника не могут нарушить целостность, а, следовательно, доверенность программной среды.

Технология

- Из доверенной среды нельзя выходить в недоверенную
- Для этого применяются отдельные ОС
- Взаимовлияние защищенной и незащищенной ОС друг на друга исключено, так как они размещены в физически разделенным банках памяти и ни при каких обстоятельствах не могут быть запущены одновременно.

Линейка устройств

- МКТ –предназначен только для работы в защищенном режиме.
- МКTrusT – предназначен для работы в одном из двух режимов на выбор – защищенном или обычном, без ограничений. Выбор осуществляется пользователем: он устанавливает физический переключатель в одну или вторую позицию. При этом загружается одна из двух разных ОС, расположенных в независимых одна от другой банках памяти устройства.

MKT

MKTrusT

Линейка устройств

- МКТ-card – терминал, состоящий из стационарной док-станции, к которой подключается периферия, и отчуждаемого мобильного устройства, которое является носителем всей персонифицированной части информационной среды клиентского рабочего места.

MKT-card

MKT-card long

Линейка устройств

- TrusTPad – планшетный компьютер, работающий аналогично MKTrusT – с возможностью выбора одного из режимов с помощью переключателя.

Линейка устройств

- TrusTPhone – IP-телефон, также построенный на «гарвардской» архитектуре по логике MKTrusT. Фактически, это TrusTPad функцией IP-телефонии, выполненный в виде стационарного телефона с ЖК-дисплеем и сенсорным номеронабирателем.

Характеристики

- Процессор: 4-ядерный, 1,6 ГГц, Cortex A9.
- Графический процессор: Mali400, 2D/ 3D OpenGL ES2.0/ OpenVG1.1.
- ОЗУ: 2GB DRR3.
- WiFi: IEEE 802.11 b/g/n.
- Bluetooth: V4.2.
- Считыватель карт: MICRO SD (TF card) до 32GB.
- Порт HDMI: как минимум 1.
- Порт USB: как минимум 1 (OTG).

MKTrusT

- Позволяет работать в одном из двух режимов – защищенном (например, работа с ДБО или иными критичными к защищенности сервисами) или незащищенном, без ограничения возможностей.
- Защищенная ОС – Linux собственной сборки, незащищенная ОС – Android.

MKTrusT

- MKTrusT требует для работы только телевизор (монитор или проектор) через HDMI порт, питание от USB порта (не менее 1 Ампер), сеть – WiFi.

Характеристики MKTrusT

- Защищенный диск: 1, 8 ГБ
- Незащищенный диск: 1, 8 ГБ
- Диск для обновлений: 1, 8 ГБ
- Порт USB: 1 (host)
- Порт питания: 1 USB
- Питание: DC 5V, 1A

Характеристики MKTrusT

- Световой индикатор режима работы: 1 (зеленый цвет – защищенный режим, красный – незащищенный)
- Звуковой индикатор режима работы: 1 (доступен в защищенном режиме)
- Переключатель режима.

- *Размеры и вес:*
- Размер без колпачка (с колпачком) – 10 (11.5) x 5 (6) x 1.3 см
- Вес –62 гр.

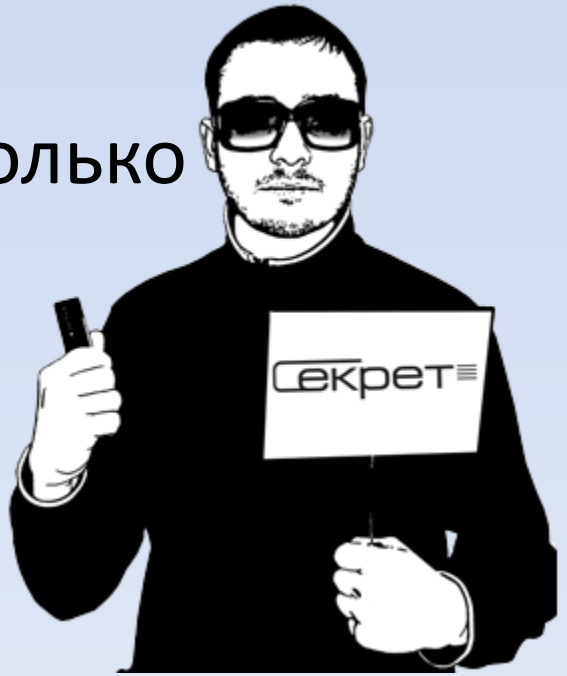
ЗАЩИЩЕННЫЕ НОСИТЕЛИ «СЕКРЕТ» (ОКБ САПР)

Защищенные носители «Секрет»

- «Секрет» — это специальный носитель информации, который имеет независимые от компьютера, к которому он будет подключаться, механизмы принятия решения о том, на каких компьютерах с ним можно работать

Линейка устройств «Секрет»

- «Личный секрет» — это самое недорогое устройство в линейке, предназначенное для защиты личных данных пользователя, хранимых им в «Секрете», в том числе и при утрате этого носителя. Типовое использование — один или несколько домашних компьютеров.



Линейка устройств «Секрет»

«Личный секрет»

- Необходимо установить ПО «Секретный агент» для того, чтобы ОС обнаружила устройство.
- Возможна установка PIN-кода.

Линейка устройств «Секрет»

- «Секрет фирмы» — это корпоративное решение, включающее в себя помимо необходимого числа «Секретов» также сервера аутентификации и регистрации, оборудованные средствами защиты информации обеспечивающими адекватный масштабу сети уровень защищенности.

Линейка устройств «Секрет»

«Секрет фирмы»

- ПО сервера аутентификации выполняется на обычном ПК, выделенном для этой цели, поэтому для обеспечения доверенной среды вычислений нужно установить на этот ПК ПАК Аккорд, который будет обеспечивать доверенную загрузку ОС и контролировать доступ к серверу аутентификации.

Линейка устройств «Секрет»

- «Секрет особого назначения» - предназначен для сотрудников, в сферу ответственности которых входит работа с данным, конфиденциальность которых критична, но которые, вместе с тем, должны храниться на служебном носителе и переноситься сотрудником в рамках его должностных обязанностей на различные компьютеры (а не только между зафиксированными администратором системы в списке разрешенных рабочих мест).

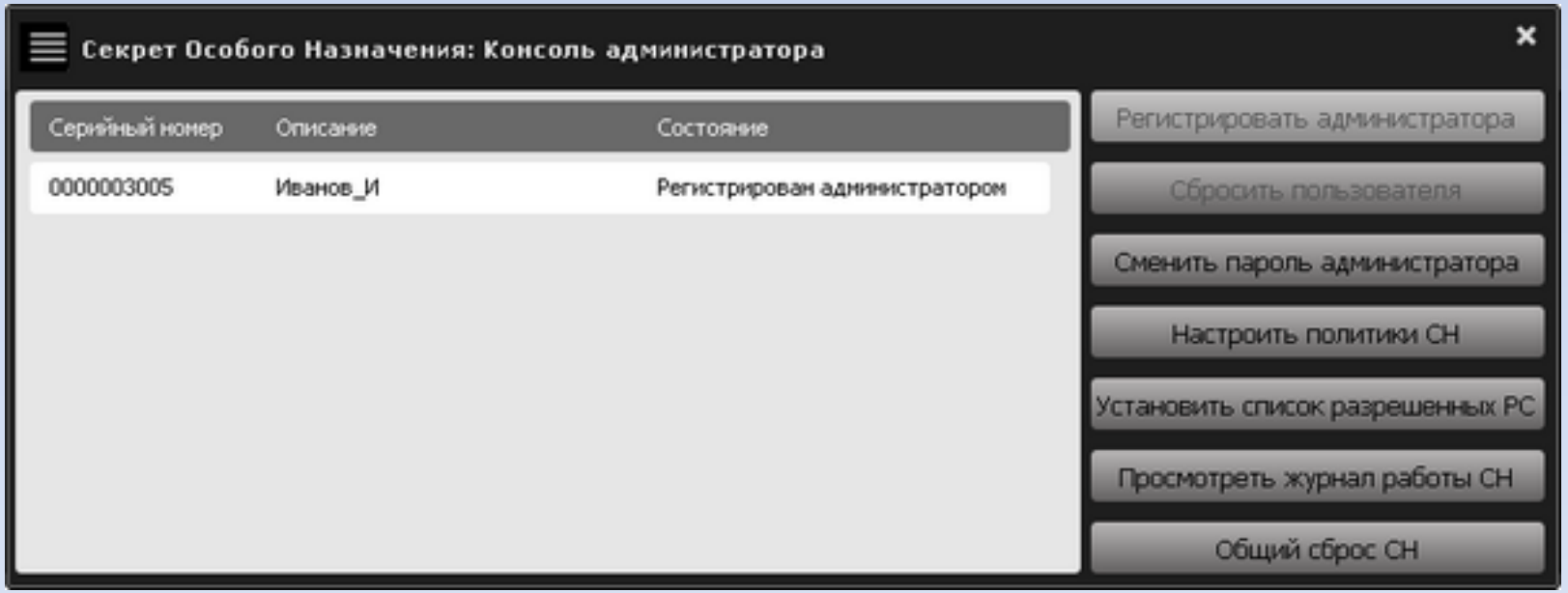
Линейка устройств «Секрет»

«Секрет особого назначения»

- В аппаратном журнале фиксируются все попытки работы с ним на различных ПК, вне зависимости от того, была ли попытка успешной.
- Отредактировать журнал нельзя.

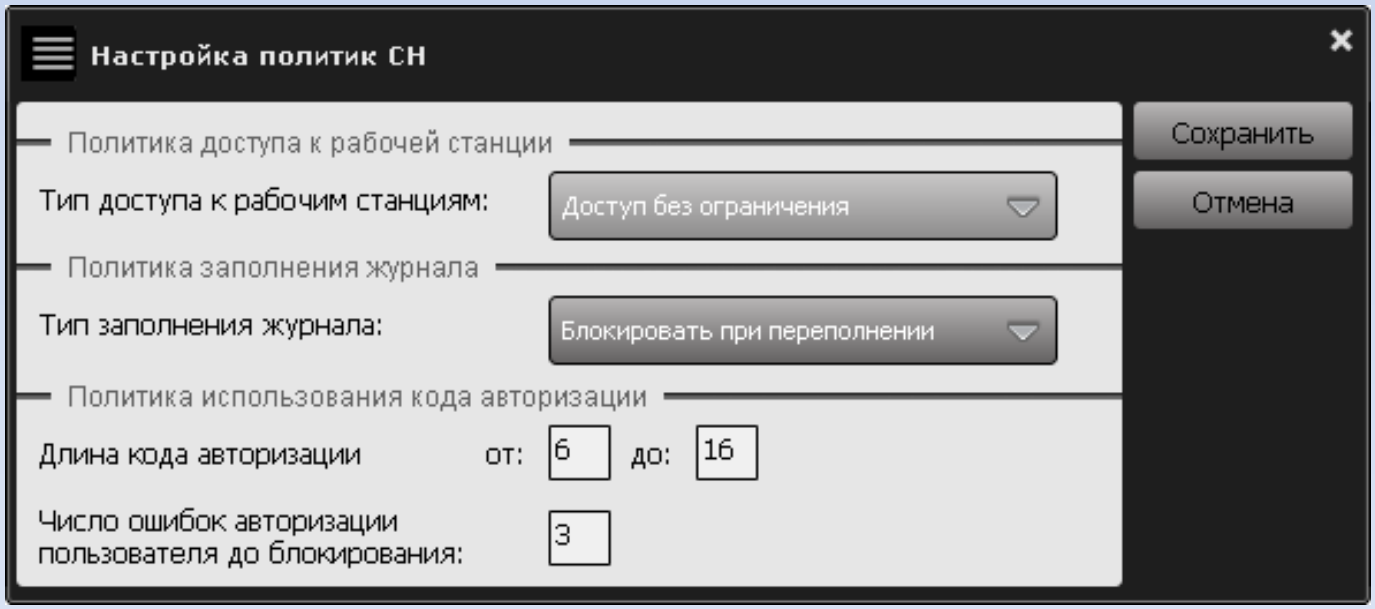
Линейка устройств «Секрет»

«Секрет особого назначения»



Линейка устройств «Секрет»

«Секрет особого назначения»

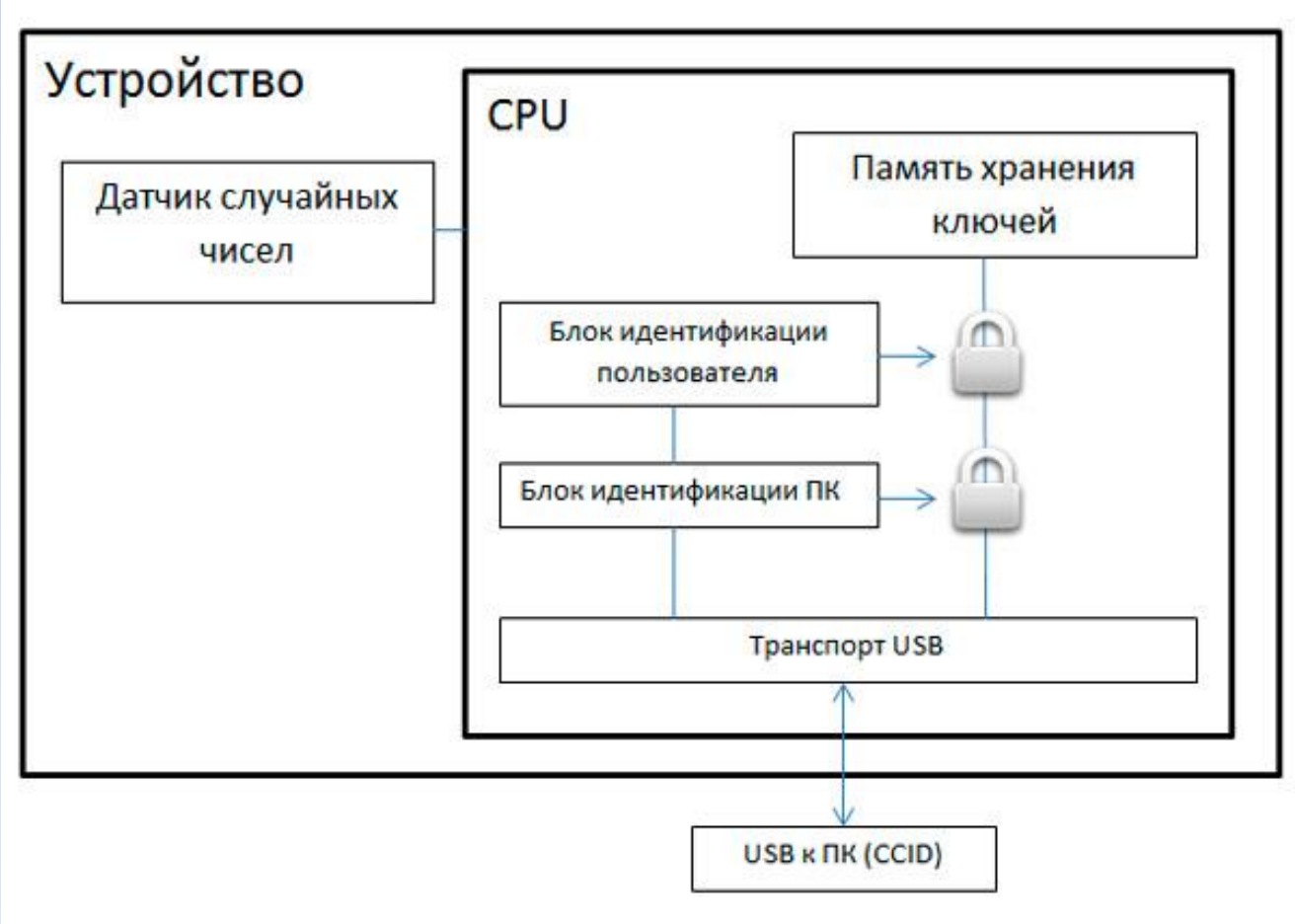


Линейка устройств «Секрет»

- «Идеальный токен» - предназначен для хранения ключевой информации.
- Производится контроль подключения только с рабочего места.

Линейка устройств «Секрет»

- «Идеальный токен»



Линейка устройств «Секрет»

«ПАЖ» - средство архивирования журналов событий

- Запрещает редактирование журналов.
- Данные можно только добавлять (Add Only), и настроить на работу с одним или несколькими конкретными ПК, чтобы журналы не путались.
- Можно настроить сбор журналов из разных источников.

Рассмотренные вопросы

- Доверенные сеансы связи МАРШ!
- Защищенные микрокомпьютеры «МКТ»
- Защищенные носители «Секрет»

СПАСИБО ЗА ВНИМАНИЕ!