Новая Гарвардская архитектура

ОКБ САПР
2022

Новая гарвардская архитектура

Новая гарвардская архитектура – это архитектура компьютера, лишенная базовой уязвимости классических архитектур.

Атака на перехват управления состоит из ряда шагов, один из которых – запись в долговременную память вредоносного ПО и обработчика прерываний.

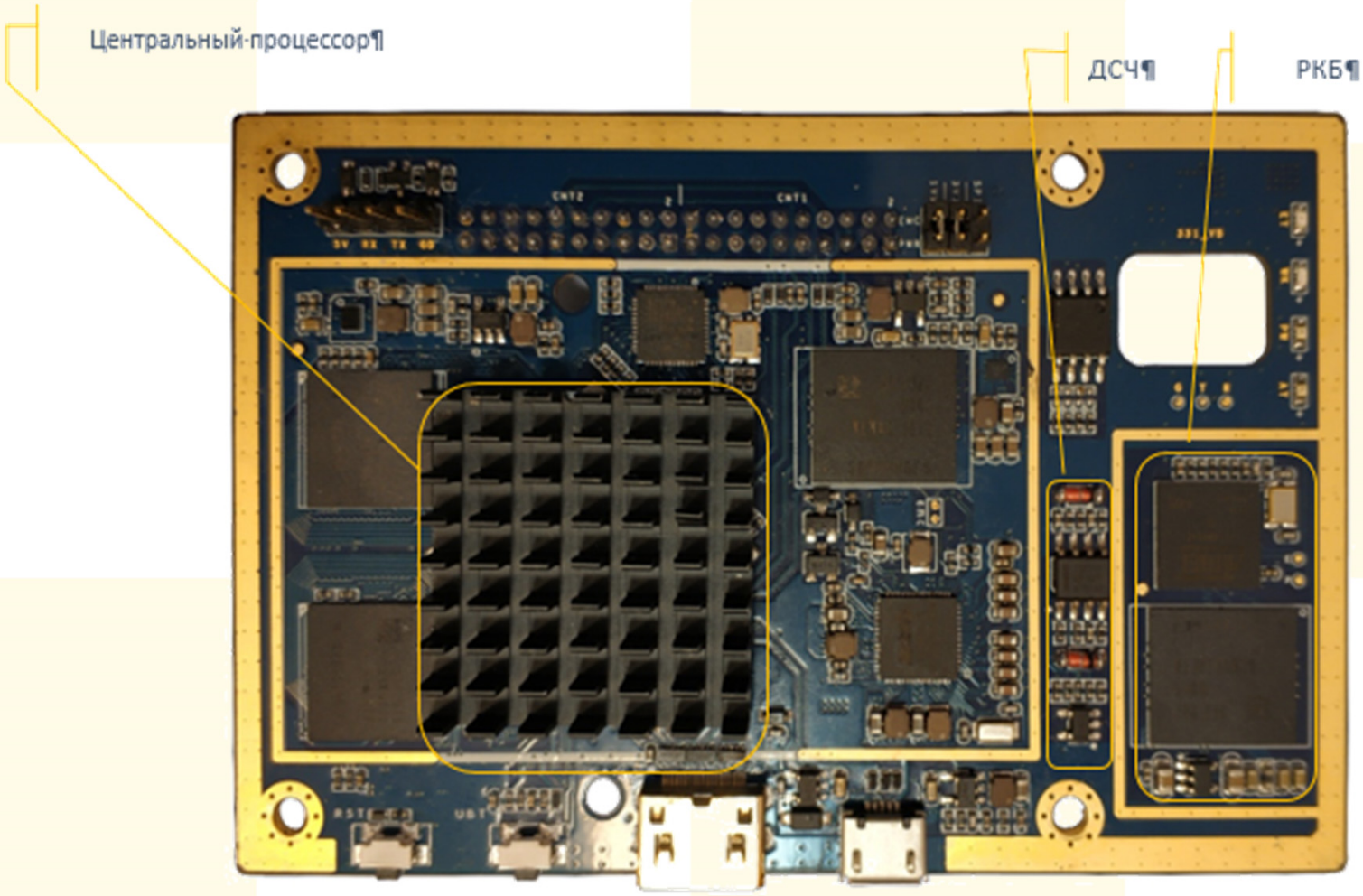
Новая гарвардская архитектура построена таким образом, чтобы этот шаг осуществить было невозможно, но операции записи, необходимые для работы ОС и прикладного ПО могли выполняться в сеансовой памяти.

Микрокомпьютеры m-TrusT

Защищённые микрокомпьютеры m-TrusT – это одноплатные компьютеры Новой гарвардской архитектуры.

Их общее назначение – защищенная сетевая коммуникация.

Микрокомпьютеры m-TrusT



«Вирусный иммунитет»

ОС микрокомпьютера хранится в банке памяти, физически переведенном в режим «только чтение».

Это значит, что, даже если в оперативной памяти окажется вирус, записаться в долговременную память он не сможет.

При следующем включении будет загружена эталонная ОС в своем неизменном виде.

Это и есть своего рода «вирусный иммунитет».

Возможности m-TrusT

- ✓ обеспечение среды функционирования криптографии, позволяющей сертифицировать вариант исполнения СКЗИ на m-TrusT на класс КС3;
- ✓ обеспечение защиты платформы благодаря РКБ, встроенному в основной аппаратный блок компьютера, и СДЗ, сертифицированному ФСТЭК России;

Достоинства m-TrusT

- ✓ работа в автоматическом режиме – существенно снижает нагрузку на организационно-технические меры при эксплуатации СКЗИ;
- ✓ изменение форм-фактора без повторной сертификации изделия – значительно сокращает сроки работ по защите КИИ;
- ✓ работа с любыми каналами связи, используемыми в КИИ – нет необходимости разводить «зоопарк» решений;
- ✓ защита КИИ без глубокой переработки ее структуры – сильно сокращает затраты на проведение мероприятий.

Решения на базе m-TrusT

- ✓ криптошлюз fin-TrusT;
- ✓ ССВТ УД TrusT Удалёнка;
- ✓ двухконтруный моноблок;
- ✓ защищённые терминалы m-TrusT Терминал и Центр-TrusT;
- ✓ канальный шифратор TrusT-in-Motion;
- ✓ межсетевой экран МЭ-TrusT;
- ✓ АРМ защищенного хранения и сетевой загрузки….

Список постоянно пополняется.

Криптошлюзы fin-TrusT

fin-TrusT – это криптошлюз для защиты сетевого взаимодействия технических средств финансовой организации.

С помощью fin-TrusT защищаются коммуникации между

- подразделениями и офисами банков,
- банком и процессинговым центром,
- процессинговым центром и банкоматами.

Выполняются требования законодательства, блокируются уязвимости во взаимодействии в финансовой сфере.

Криптошлюзы fin-TrusT

Встроенное в fin-TrusT СКЗИ DCrypt от компании ТСС сертифицировано ФСБ России России в исполнениях на m-TrusT на классы КС2 и КС3.

Собственная ОС и вычислительные ресурсы обеспечивают достаточную для защиты сетевого взаимодействия производительность и высокий уровень защищенности.

Датчик случайных чисел и размещение ПО в памяти с доступом «только чтение» исключают вредоносное воздействие на ПО и обеспечивают неизменность среды функционирования СКЗИ.

Линейка fin-TrusT

- ✓ fin-TrusT банкомат – криптошлюз в технологическом корпусе для установки в банкоматы с возможностью поддержки двух и более операторов мобильного Интернета;
- ✓ fin-TrusT офис – криптошлюз в корпусе одноюнитового сервера для установки в бэк- или фронт-офис до пятидесяти абонентских устройств;
- ✓ fin-TrusT центр – сервер VPN для установки в центр обработки данных (ЦОД) или серверную стойку головного отделения.

Важные нюансы

fin-TrusT поддерживает одновременную работу нескольких независимых каналов связи.

Например, могут быть подключены 2 Ethernet от разных провайдеров и/или 2 LTE-модема разных операторов связи.

Это повышает отказоустойчивость.

fin-TrusT может использоваться совместно с ПАК КриптоПро NGate, есть Акт совместимости.

fin-TrusT: выполнение требований регуляторов

Базовые меры Приказа ФСТЭК России № 239:
ИАФ: 1, 2, 3, 4, 5, 7;
УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, 14;
ОПС: 1;
АУД: 2, 3, 4, 5, 6, 7, 8, 9;
АВЗ: 1;
ОЦЛ: 1, 3, 4, 5;
ОДТ: 1, 3, 4, 5, 6;
ЗТС: 3;
ЗИС: 1, 2, 6, 13, 16, 19, 20, 21, 27, 32, 33, 34, 35, 38;
ИНЦ: 1, 2;
ОПО: 2, 4;
ДНС: 4, 5.

fin-TrusT: выполнение требований регуляторов

Дополнительные (не включенные в базовый набор) меры Приказа ФСТЭК России № 239:

ОЦЛ: 2;

ОДТ: 7;

ЗТС: 1;

ЗИС: 10, 12, 17, 25, 31.

TrusT Удалёнка

TrusT Удалёнка – это специальное средство вычислительной техники, предназначенное для организации защищённого контролируемого удалённого доступа.

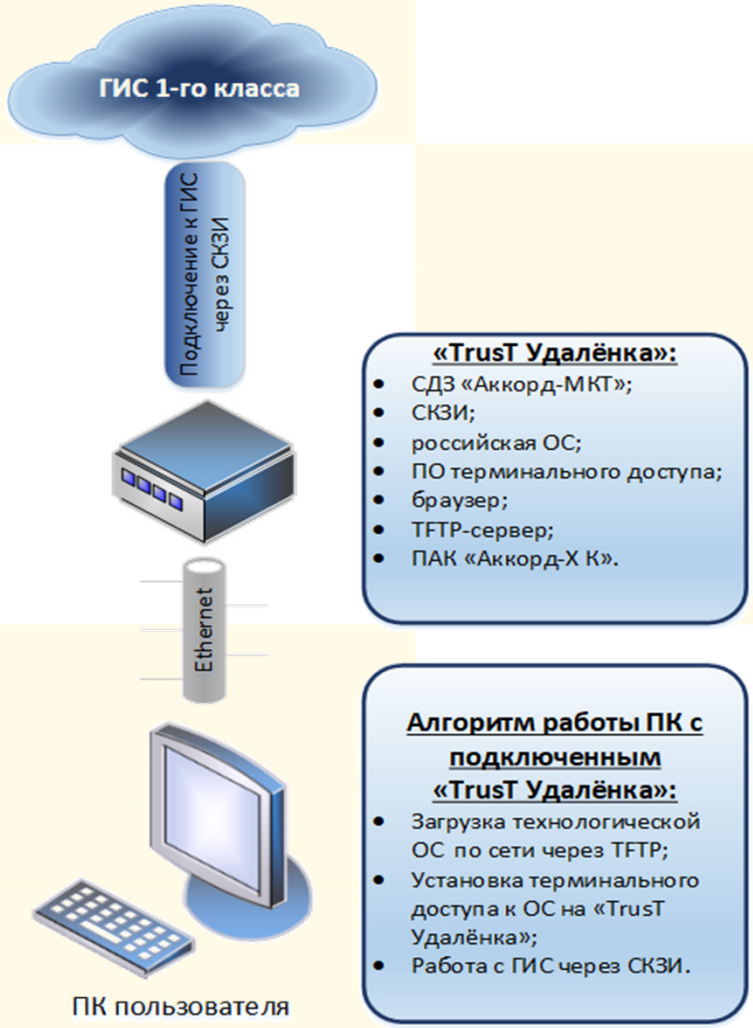
Иными словами, для защищенной работы на удалёнке.

Выполняются требования к защищенности государственных информационных систем (ГИС) 1 класса.

Состав TrusT Удалёнки

- защищенный микрокомпьютер с аппаратной защитой данных m-TrusT;
- СДЗ уровня BIOS Аккорд-МКТ;
- СКЗИ, сертифицированное ФСБ по классу КС3;
- ПАК Аккорд-Х К (средство разграничения доступа).

Схема работы TrusT Удалёнки



«TrusT Удалёнка»:

- СДЗ «Аккорд-МКТ»;
- СКЗИ;
- российская ОС;
- ПО терминального доступа;
- браузер;
- TFTP-сервер;
- ПАК «Аккорд-Х К».

Алгоритм работы ПК с подключенным «TrusT Удалёнка»:

- Загрузка технологической ОС по сети через TFTP;
- Установка терминального доступа к ОС на «TrusT Удалёнка»;
- Работа с ГИС через СКЗИ.

К компьютеру пользователя в разрыв сети подключено устройство TrusT Удалёнка, оно не мешает пользователю работать на своем компьютере, как ему нравится.

Когда нужно подключиться к ГИС, пользователь перезагружается, и с TrusT Удалёнки на его компьютер загружается технологическая ОС с терминальным клиентом, и TrusT Удалёнка становится

- для компьютера пользователя терминальным сервером,
- а для ГИС – терминальным клиентом.

Достоинства TrusT Удалёнки

1. Выполняется требование **УПД.17** 17-21 Приказов ФСТЭК России: ПО исполняется не на компьютере пользователя, а на m-TrusT, целостность которого проверена СДЗ.
2. Обеспечивается целостность исполняемой ОС: встроенное средство разграничения доступа – Аккорд-Х К.
3. Криптографические ключи можно использовать до 3-х лет без дополнительных ключевых носителей и мер по их контролю: в m-TrusT реализована функция неизвлекаемого ключа.

Двухконтурный моноблок

Двухконтурный моноблок – это, собственно, моноблок, в который установлен защищенный микрокомпьютер m-TrusT.

Такая конструкция позволяет пользователю работать в одной из двух защищенных ОС (в общем случае одна из них Windows, а вторая – Linux).

Двухконтурный моноблок

ОС Windows загружается с жесткого диска моноблока. Пользователь может устанавливать любое ПО и инициировать любые подключения в рамках заданных для него правил разграничения доступа.

ОС Linux загружается из защищенного от записи раздела памяти m-TrusT, то есть не просто с другого жесткого диска, а с другого компьютера.

Из ОС Linux пользователь может только получить доступ к терминальному серверу.

Достоинства двухконтурного моноблока

1. работа в стационарной ОС и с терминальным сервером может вестись параллельно, а не последовательно, для переключения не требуется ни перезагрузка, ни смена сеанса, все процессы продолжаются в каждой ОС своим чередом;

2. архитектура m-TrusT обеспечивает «вирусный иммунитет»;

Достоинства двухконтурного моноблока

3. СДЗ уровня BIOS (СПО Аккорд-МКТ) обеспечивает доверенную загрузку ОС;

4. СЗИ НСД (СПО Аккорд X K) обеспечивает разграничение доступа пользователей, а также регистрацию событий, контроль целостности и контроль подключения машинных носителей.

Защищённые терминалы

Если поставить m-TrusT с необходимыми для офисной периферии портами в привычный для офисного терминала корпус – получится защищенный терминал на базе микрокомпьютера m-TrusT.

Варианты защищённых терминалов

- ✓ «m-TrusT Терминал»: ОС полностью хранится в памяти микрокомпьютера, доступной в режиме «только чтение»;

- ✓ «Центр-TrusT»: в неперезаписываемой памяти хранится только постоянная часть ОС, а набор функционального ПО, которое не может располагаться в неизменяемой памяти, загружается по технологии защищенной сетевой загрузки «Центр-Т» с сервера хранения и сетевой загрузки.

Функции m-TrusT Терминала

- ✓ И/А пользователя;
- ✓ контроль целостности ПО;
- ✓ доверенная загрузка ОС;
- ✓ защита от модификации программ и данных;
- ✓ «вирусный иммунитет»;
- ✓ защита информации при ее передаче по каналам связи;
- ✓ исключение доступа через общие ресурсы;
- ✓ ДСС пользователя с удаленными ресурсами;
- ✓ регистрация действий пользователя.

Функции Центр-TrusT

- ✓ И/А пользователя;
- ✓ защищенная загрузка ПО по сети;
- ✓ защита от модификации программ и данных;
- ✓ удаленное администрирование загружаемых образов;
- ✓ «вирусный иммунитет»;
- ✓ защита информации при ее передаче по каналам связи (опционально);
- ✓ исключение доступа через общие ресурсы;
- ✓ ДСС пользователя с удаленными ресурсами;
- ✓ регистрация действий пользователя.

m-TrusT Терминал: требования регуляторов

Базовые меры 17-21 Приказов ФСТЭК России:

ИАФ: 1, 2, 3, 4, 5, 6;

УПД: 1, 2, 4, 5, 6, 9, 10, 11, 13, 15, 17;

ОПС: 1, 2, 3;

ЗНИ: 2, 5, 8;

РСБ: 1, 2, 3, 4, 5, 6, 7;

АВЗ: 1;

АНЗ: 1, 2, 3, 4, 5;

ОЦЛ: 1, 3, 6;

ОДТ: 3, 4, 5;

ЗИС: 1, 3, 5, 11, 15, 20, 21, 22, 30;

ИНЦ: 2; УКФ: 2.

m-TrusT Терминал: требования регуляторов

Дополнительные (не включенные в базовый набор) меры 17-21 Приказов ФСТЭК России:

ИАФ: 7;

ЗНИ: 4, 6, 7;

РСБ: 8;

ОЦЛ: 2, 5, 8;

ЗИС: 4, 14, 16, 19, 26, 29.

TrusT-in-Motion

TrusT-in-Motion – это канальный шифратор для подвижных объектов КИИ (маршрутизатор) на базе защищенного микрокомпьютера m-TrusT, обеспечивающий непрерывное защищённое сетевое взаимодействие в системах с подвижными объектами в условиях интенсивных вибрационных воздействий и экстремальных показателей температур.

Функции TrusT-in-Motion

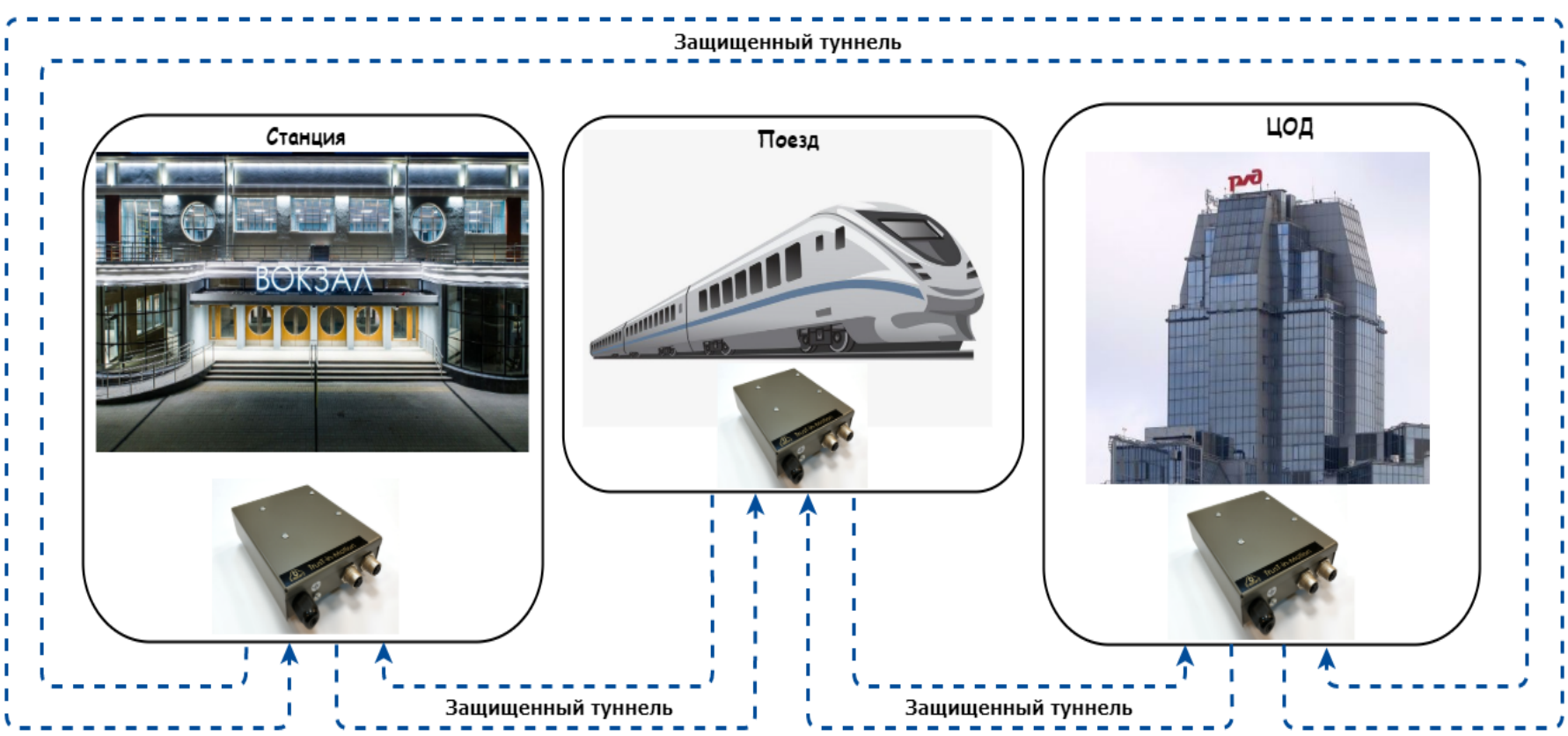
- ✓ защита сетевого взаимодействия в условиях функционирования без участия персонала;
- ✓ стойкость к интенсивным внешним воздействиям;
- ✓ гибкое управление трафиком и криптографическую защиту сети;
- ✓ бесперебойное функционирование в условиях вибрационных воздействий и изменений температуры окружающей среды;
- ✓ доверенная среда функционирования криптографии.

Примеры применения TrusT-in-Motion

- ✓ наземный транспорт;
- ✓ банковская транспортная инфраструктура;
- ✓ инфраструктура медицинских учреждений;
- ✓ инфраструктура авиационного транспорта.

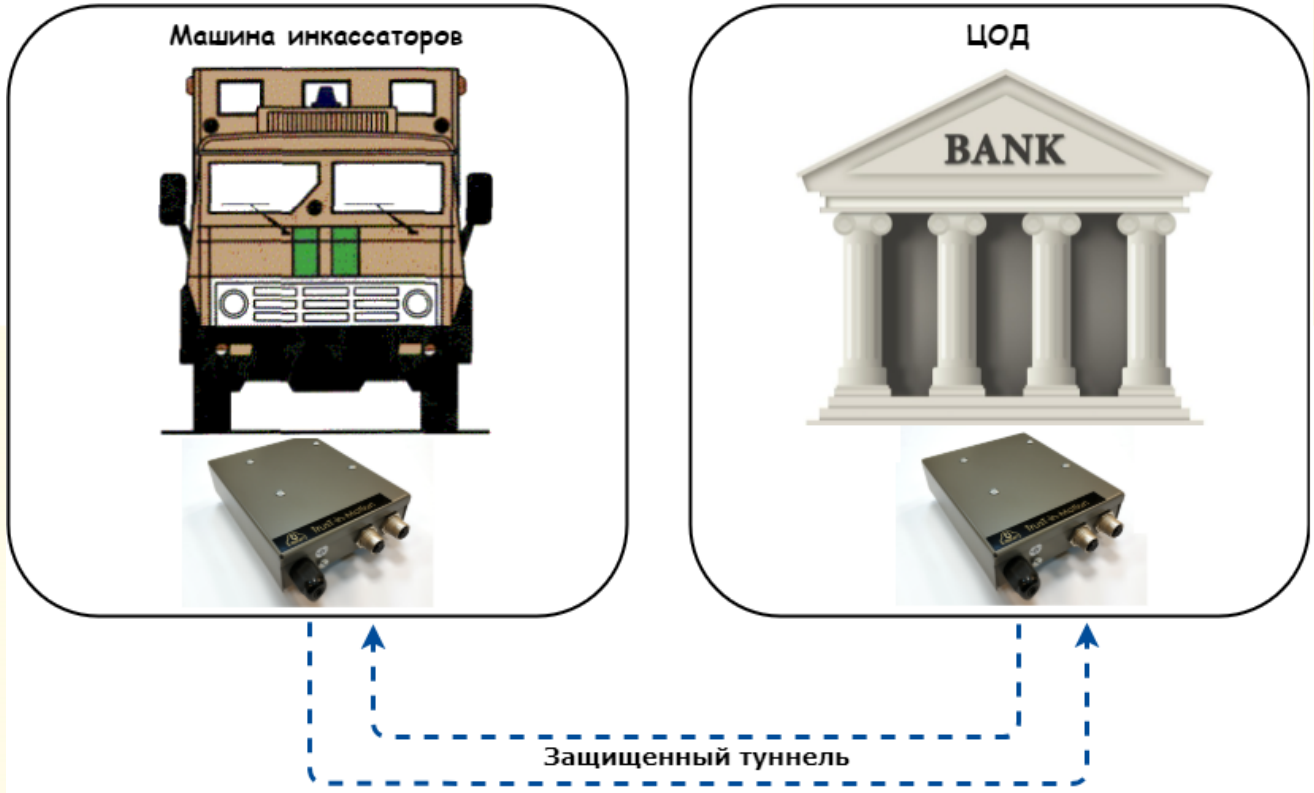
Примеры применения TrusT-in-Motion

Обеспечение защиты сетевого взаимодействия объектов наземного транспорта.



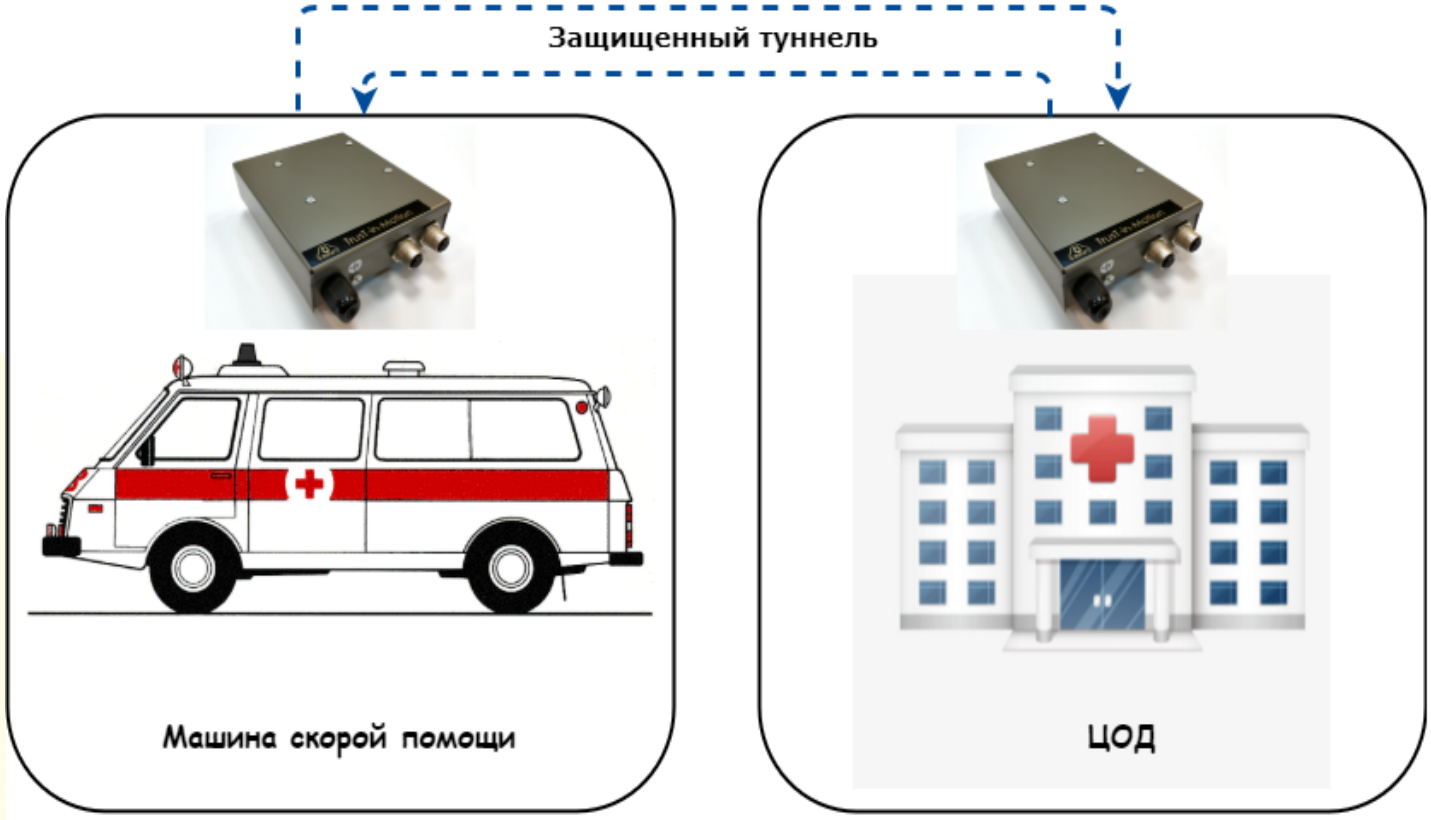
Примеры применения TrusT-in-Motion

Обеспечение защиты сетевого взаимодействия объектов банковской транспортной инфраструктуры.



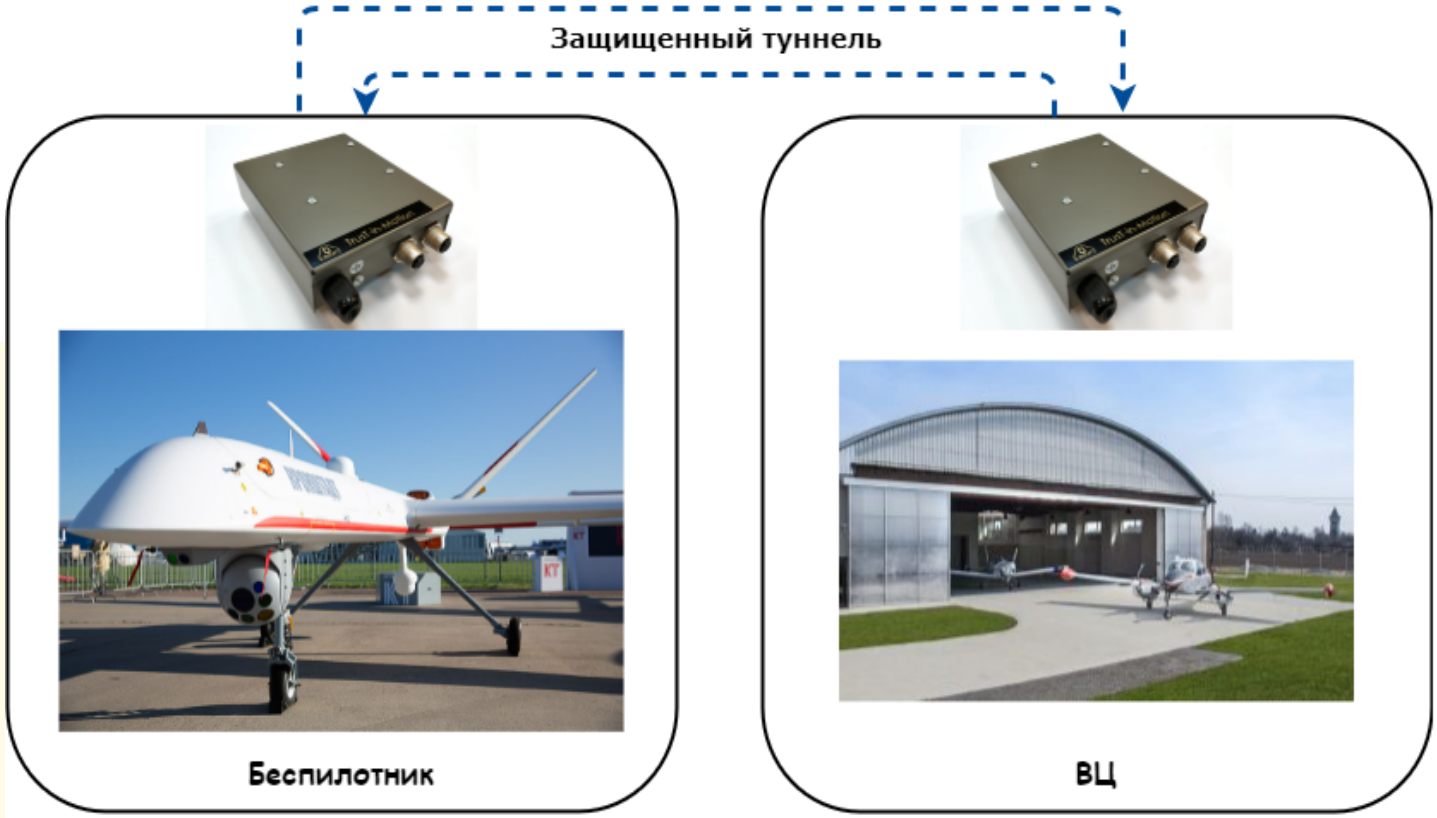
Примеры применения TrusT-in-Motion

Обеспечение защиты сетевого взаимодействия объектов инфраструктуры медицинских учреждений.



Примеры применения TrusT-in-Motion

Обеспечение защиты сетевого взаимодействия объектов инфраструктуры авиационного транспорта.



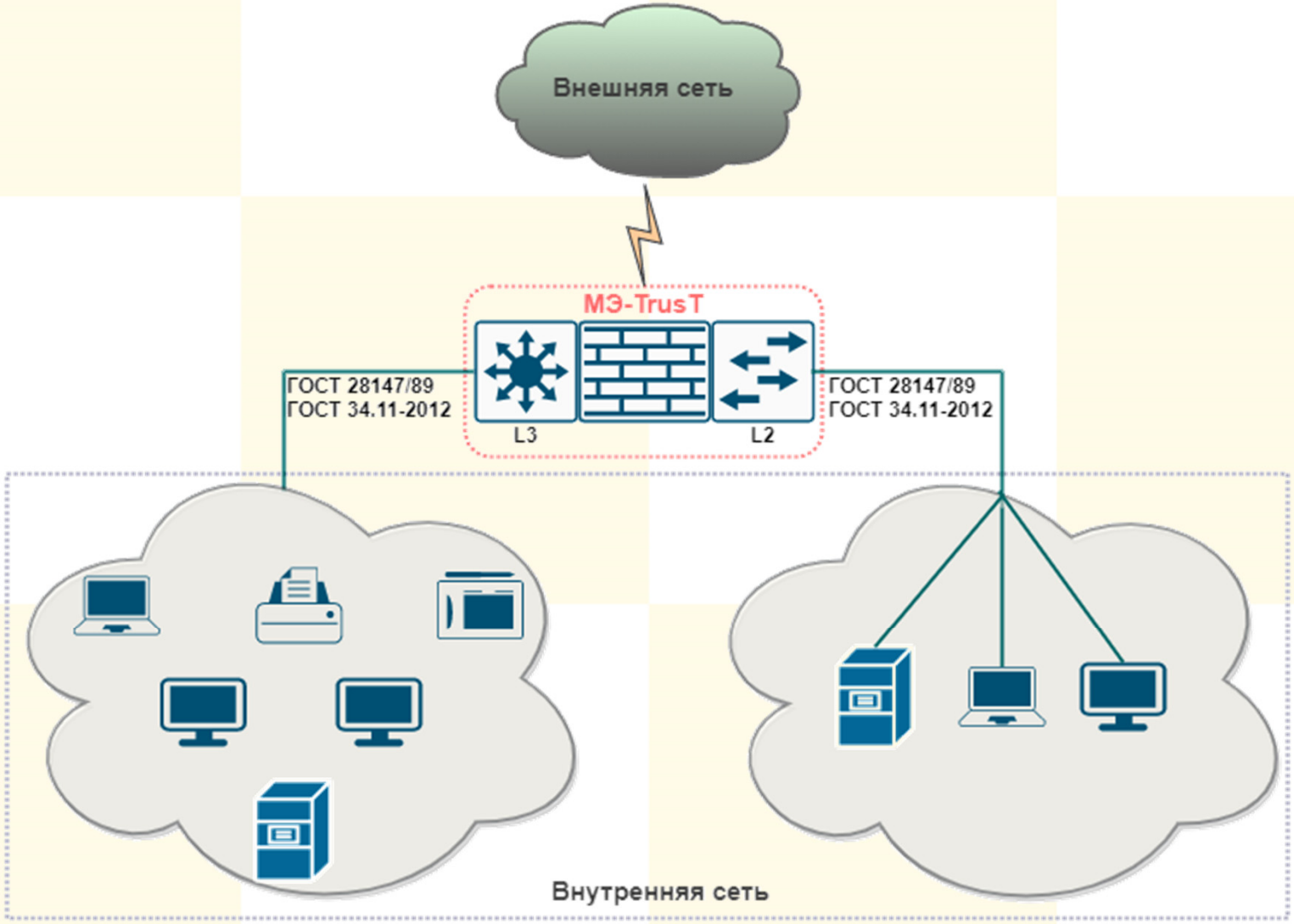
МЭ-TrusT

МЭ-TrusT – это межсетевой экран на базе специализированного компьютера m-TrusT.

МЭ-TrusT позволяет эффективно решать задачи по обеспечению сетевой защиты, поддерживая работу одновременно

- в режиме фильтрации сетевого трафика на уровне L2 в режиме коммутатора
- на уровне L3 в режиме маршрутизатора.

Схема работы МЭ-TrusT



Функции МЭ-TrusT

- ✓ безопасное и надежное соединение между филиалами предприятия или дата-центрами;
- ✓ возможность подключения большого количества уделанных внешних пользователей к внутренней сети;
- ✓ высокую скорость шифрования (до 20 Гбит/с);
- ✓ журналирование событий (отображаются созданные правила фильтрации).

АРМ защищенного хранения и сетевой загрузки

АРМ защищенного хранения и сетевой загрузки (АРМ ЗХСЗ) – это инфраструктурный элемент решения Центр-Т, предназначенного для управления загрузкой терминальных станций. О нем можно прочитать в презентации «Инфраструктурные решения».

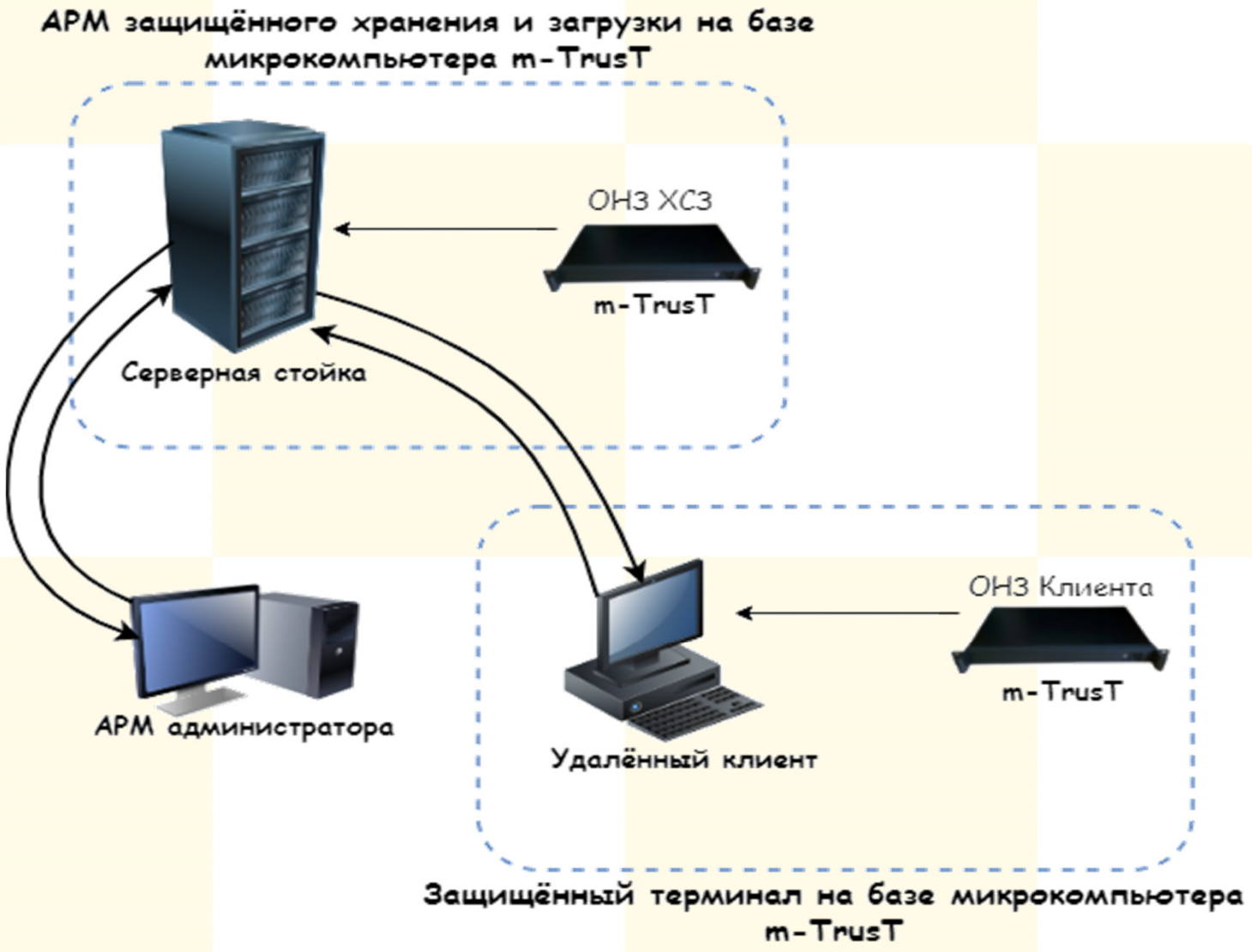
АРМ ЗХСЗ на базе m-TrusT имеет следующие преимущества перед СХСЗ на базе обычного сервера:

- ✓ низкая стоимость;
- ✓ техническая защита от модификации ПО сервера.

АРМ ЗХСЗ предпочтительнее, в следующих случаях

- ✓ производится проектирование или модернизация системы терминального доступа;
- ✓ имеет значение размер оборудования (например, предполагается установка СХСЗ в телекоммуникационный шкаф);
- ✓ нет возможности выделения отдельного СВТ для развертывания СХСЗ;
- ✓ желательно упрощение технической поддержки оборудования;
- ✓ запрещена загрузка сервера сетевой загрузки с внешнего носителя.

На базе M-TrusT может быть и терминал, и сервер загрузки



Спасибо за внимание!

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

Наш сайт в интернете:
www.okbsapr.ru