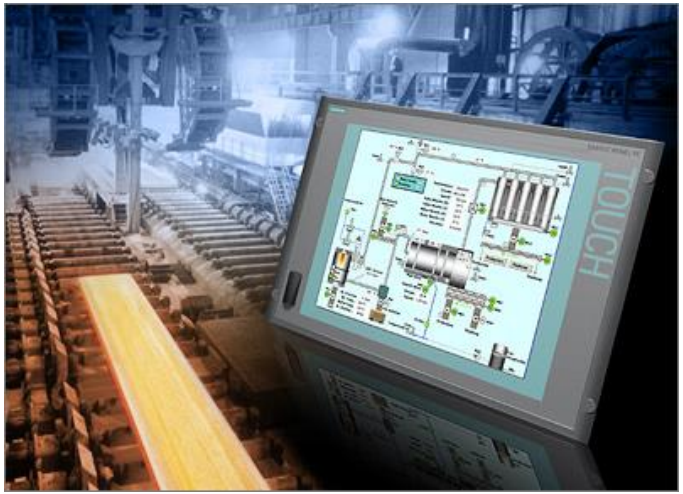
ITSF XII ВСЕРОССИЙСКАЯ КОНФЕРЕНЦИЯ

Как организовать безопасный удалённый доступ к АСУ ТП для сервисных организаций в режиме мониторинга?

Денис Бубнов
Компания ICL Системные технологии

Удаленный доступ к промышленным сетям. Зачем?

- АСУ ТП являются важнейшими компонентами инфраструктуры предприятия и требуют высокого уровня конфигурации, контроля, обслуживания и мониторинга
- Данные задачи невозможно выполнить без участия экспертов сервисных организаций



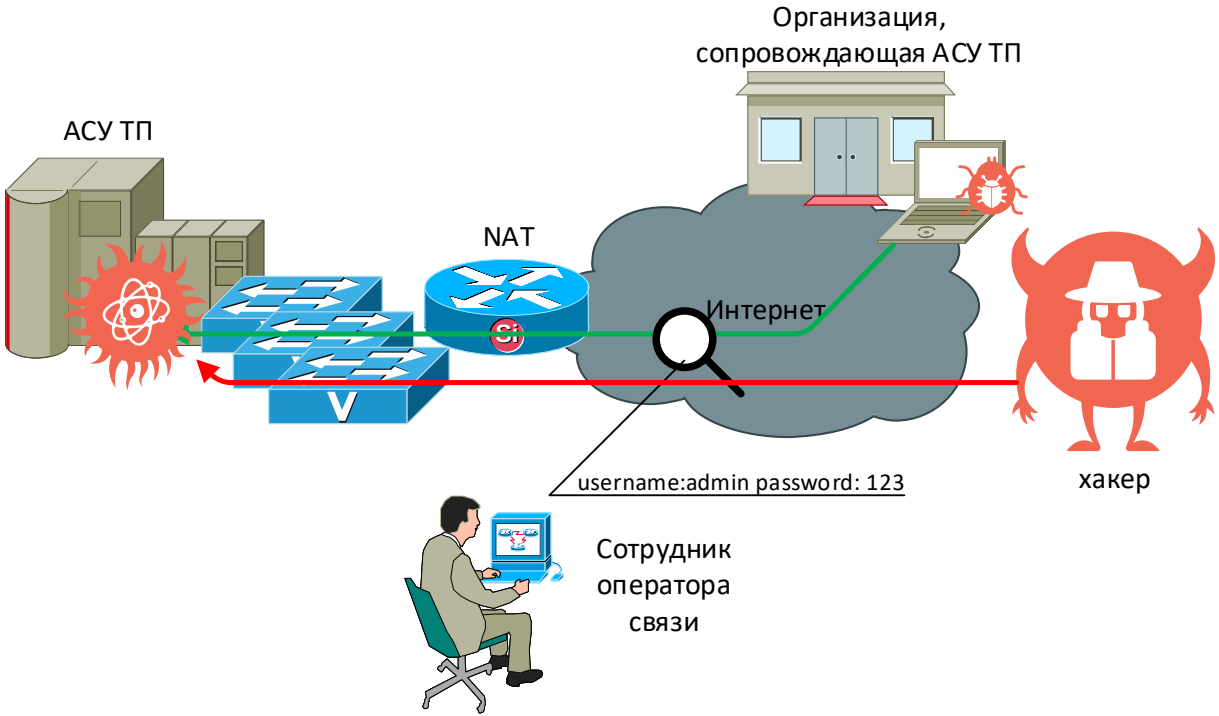
Удаленный доступ к промышленным сетям. Зачем?

- Зачастую требования УД являются частью сервисного контракта компании-разработчика.
- Полноценная поддержка решений АСУ ТП невозможна без обеспечения УД

Удаленный доступ к АСУ ТП. Проблемы

- Насколько удаленный доступ соответствует внутренним регламентам предприятия?
- Как контролировать подключения?
- Как контролировать действия по конфигурации, обслуживанию, мониторингу?
- Как защитить от несанкционированного доступа?
- Как выполнить требования законодательства?

Удаленный доступ к промышленным сетям. Как делать НЕ правильно



Удаленный доступ – вопросы безопасности

- Знаете ли вы, кто подключается к АСУ ТП?
- Как обеспечивается криптографическая защита подключений?
- Как производится аутентификация?
- Как контролируется защищенность удаленной АРМ?
- Как контролируется действия удаленного пользователя?

Удаленный доступ – требования законодательства

- 187 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- Приказ ФСТЭК №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
- Реализация защиты удаленного доступа требуется для объектов КИИ любой категории значимости.

Что такое защищенный удаленный доступ?

Управляемость.

- Активация и деактивация удаленного доступа, изменение уровня доступа по необходимости

Контроль.

- Каждый пользователь удаленного доступа должен пройти надежную аутентификацию, все его действия должны журналироваться

Что такое защищенный удаленный доступ?

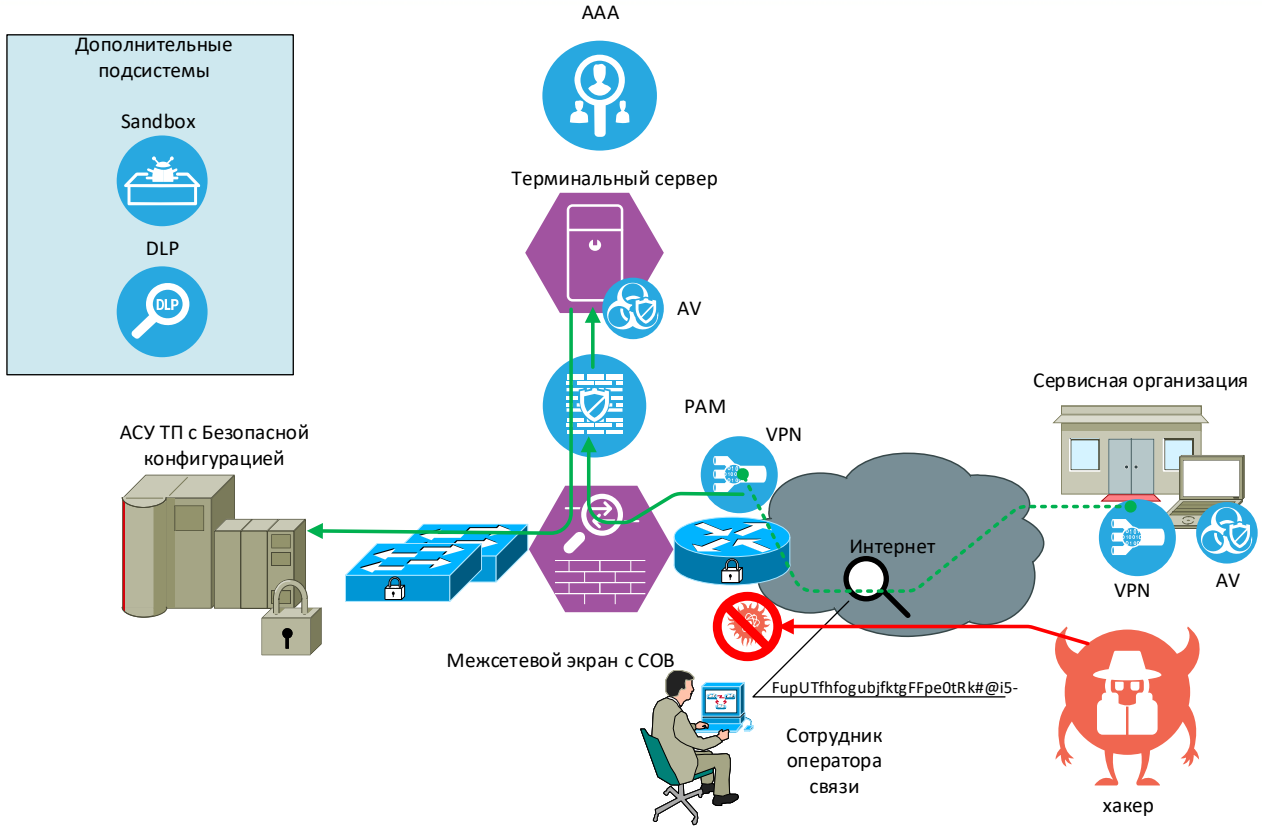
Безопасность

- Доступ к серверам АСУ ТП должен осуществляться через доверенного посредника;
- Учетные данные (логины/пароли) не должны передаваться сервисным организациям;
- Для сетевых взаимодействий в рамках защищенного удаленного доступа должна быть предусмотрена криптографическая защита;

Что такое защищенный удаленный доступ?

- Должны использоваться только разрешенные и безопасные протоколы удаленного управления и мониторинга;
- Доверенный посредник должен быть защищен от вредоносного ПО;
- Должен соблюдаться принцип минимума привилегий для обеспечения задач сервисной организации.

Архитектура защищенного удаленного доступа?



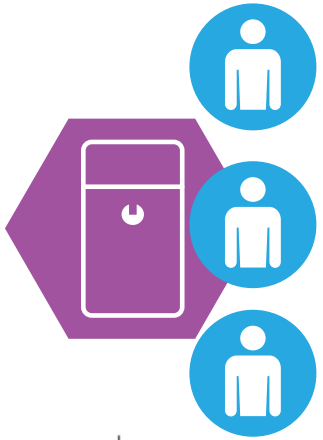
Архитектура удаленного доступа: состав основных подсистем

- Подсистема контроля действий администраторов;
- Подсистема встроенных СрЗИ АСУ ТП
- Подсистема криптографической защиты каналов связи;
- Подсистема межсетевого экранирования и СОВ
- Подсистема антивирусной защиты.

Подсистема контроля действий администраторов

Терминальный сервер

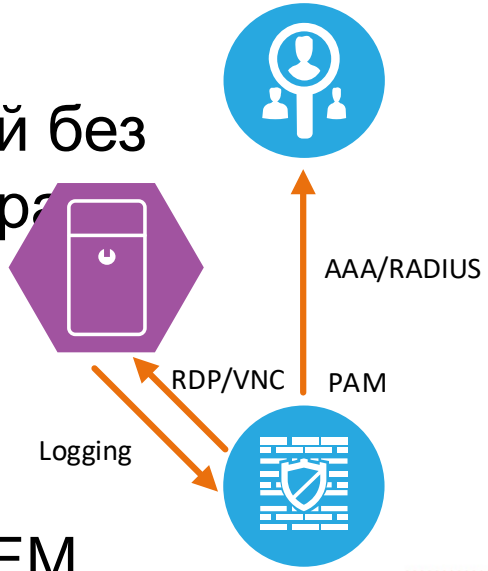
- Единая точка входа и доверенный посредник, контролируемый предприятием;
- Может быть использован для поддержки множества систем;
- Определяет набор разрешенных приложений.



Подсистема контроля действий администраторов

Комплекс контроля за действием администраторов

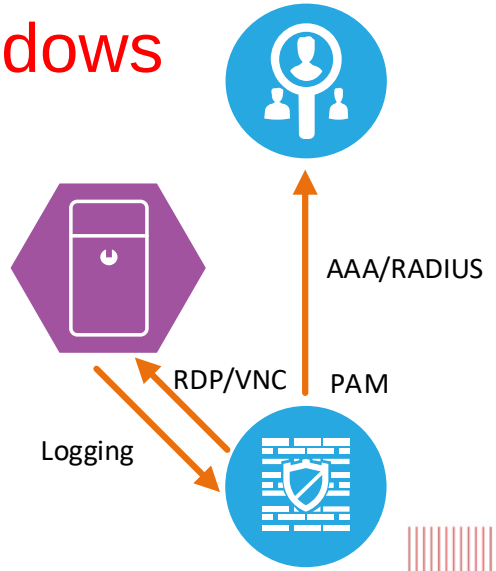
- Аутентификация удаленных пользователей без использования базы терминального сервера
- Журналирование терминальных сессий
- Интеллектуальный анализ действий администраторов;
- Генерация событий для корпоративной SIEM.



Подсистема контроля действий администраторов

Технические решения:

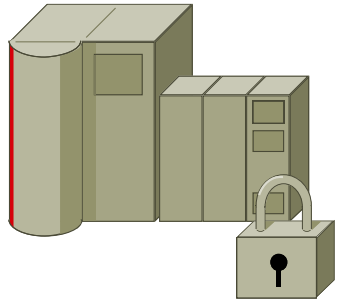
- Терминальный сервер – Microsoft Windows Server Terminal Services;
- Комплекс контроля действий администраторов – Wallix, CyberArc, Balabit.



Подсистема встроенных средств АСУ ТП

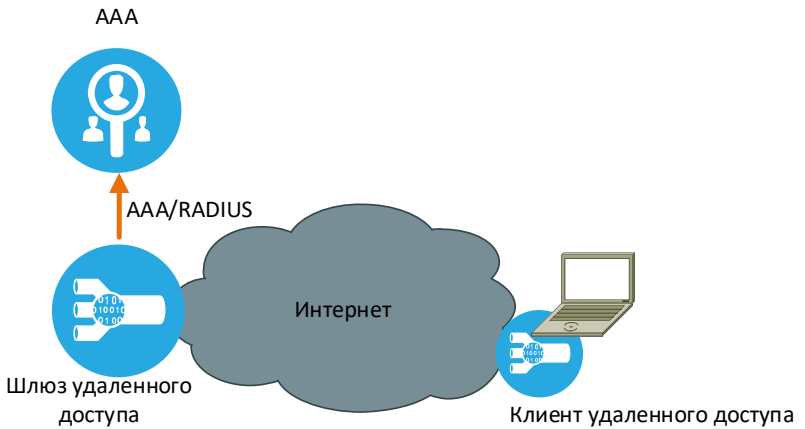
Технические решения:

- Безопасная конфигурация интерфейсов управления (ACL, политика паролей, безопасных протоколов управления/мониторинга);
- Управление учетными записями, привилегиями и журналированием (AAA);
- Усиленная конфигурация безопасности поддерживающего сетевого оборудования.



Подсистема криптографической защиты каналов связи

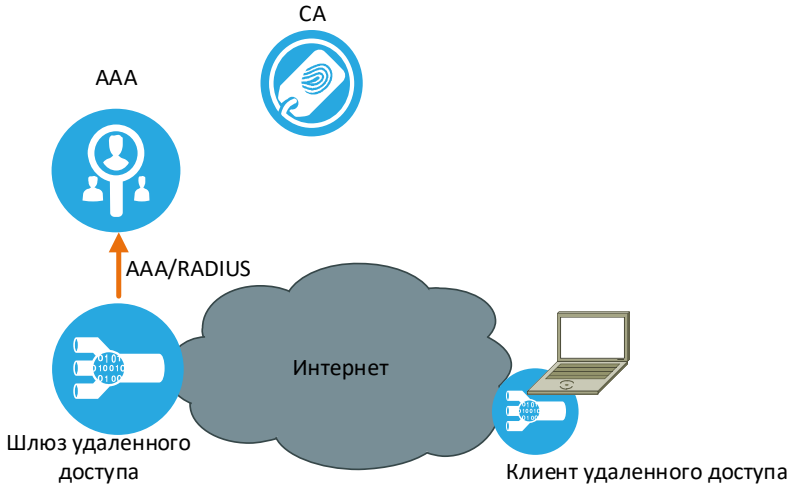
- Криптографически защищенный канал связи между предприятием и сервисной организацией;
- На стороне сервисной организации устанавливается клиент удаленного доступа;
- Реализует надежную аутентификацию.



Подсистема криптографической защиты каналов связи

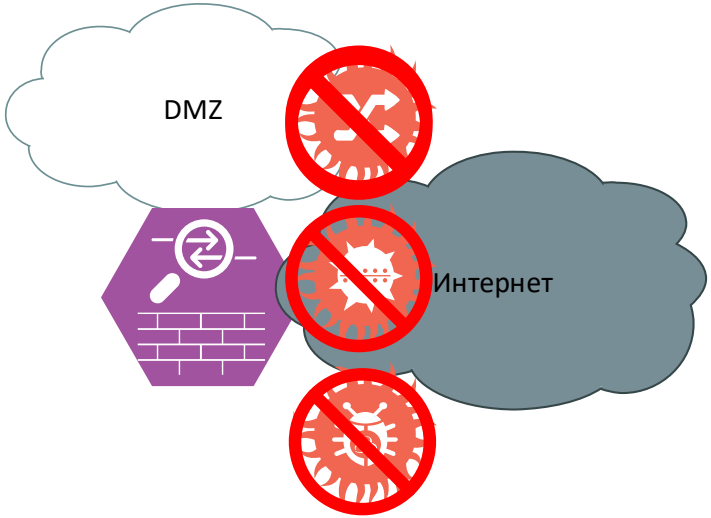
Технические решения:

- Криптошлюзы и клиенты удаленного доступа S-Terra, VIPNet, Континент;
- Опционально – центр сертификации Крипто ПРО.



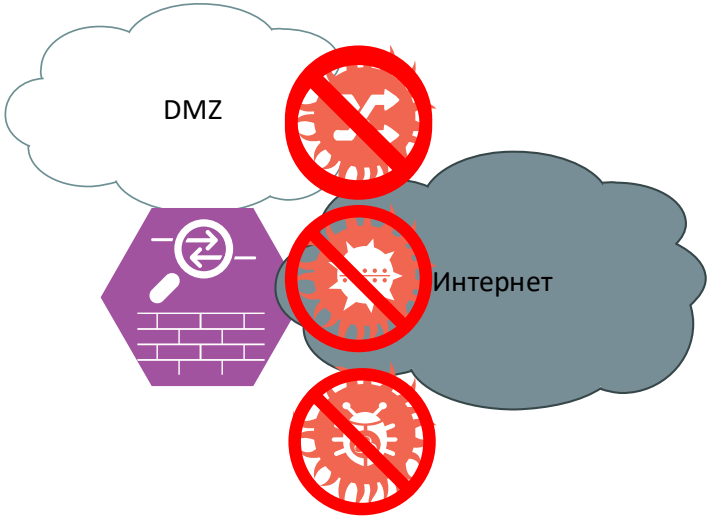
Подсистема МЭ и СОВ

- Реализация корпоративных политик безопасности;
- Формирование ДМЗ для защищенного удаленного доступа;
- Блокировка сетевых атак до уровня L7.



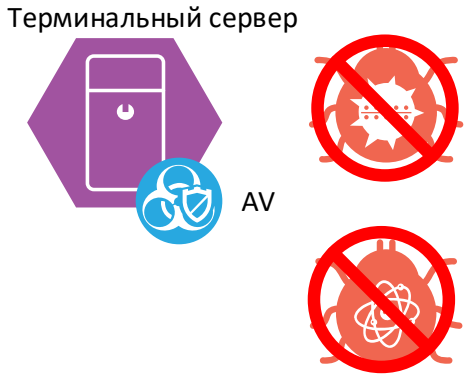
Подсистема МЭ и СОВ

- Рекомендуются решения от компаний Check Point, FortiNet;
- Подсистема может быть дополнена корпоративными средствами централизованного управления, мониторинга, анализа конфигураций.



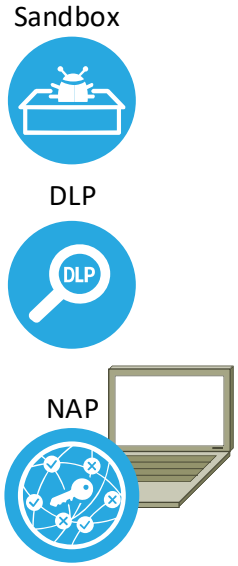
Подсистема антивирусной защиты

- Терминальный сервер должен быть подключен к корпоративной антивирусной системе;
- Должно производиться регулярное обновление сигнатур и ПО, сканирование дисков и ОЗУ терминального сервера.



Дополнительные подсистемы

- Подсистема контроля утечек информации (DLP);
- Подсистема защиты от атак «нулевого дня»
- Подсистема контроля соответствия удаленных АРМ требованиям ИБ.



Итог: выполнение требований

Требование	подсистема	Примечание
Активация и деактивация удаленного доступа, изменение уровня доступа по необходимости	Контроля действия администраторов	**Терминальный сервер и Privilege Access Management (PAM)**
Каждый пользователь удаленного доступа должен проходить надежную аутентификацию, все его действия должны журналироваться	Контроля действия администраторов; встроенных СрЗИ АСУ ТП; криптографической защиты каналов связи	**Терминальный сервер, Privilege Access Management (PAM), клиент удаленного доступа**

Итог: выполнение требований

Требование	подсистема	Примечание
Доступ к серверам АСУ ТП должен осуществляться через доверенного посредника	Контроля действия администраторов	**Терминальный сервер**
Учетные данные (логины/пароли) не должны передаваться сервисным организациям	Контроля действия администраторов	**Privilege Access Management (PAM)**

Итог: выполнение требований

Требование	подсистема	Примечание
Для сетевых взаимодействий в рамках защищенного удаленного доступа должна быть предусмотрена криптографическая защита	Криптографической защиты каналов связи	**Шлюзы криптографической защиты и клиент удаленного доступа**
Должны использоваться только разрешенные и безопасные протоколы удаленного управления и мониторинга	Межсетевого экранирования и СОВ	**Межсетевой экран**

Итог: выполнение требований

Требование	подсистема	Примечание
Доверенный посредник должен быть защищен от вредоносного ПО	Антивирусной защиты	**Корпоративная система антивирусной защиты**
Должен соблюдаться принцип минимума привилегий для обеспечения задач сервисной организации	Встроенных СрЗИ АСУ ТП; Контроля действия администраторов	**Privilege Access Management (PAM)**

Итог: выводы

Решение по защищенному удаленному доступу позволяет обеспечить:

- выполнение требований сервисной организации по необходимому доступу к АСУ ТП;
- выполнение требований законодательства;
- защиту АСУ ТП от угроз безопасности, связанных с удаленным доступом

ВОПРОСЫ