КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

25 октября 2018 г.
г. Казань

#CODEIB

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ БЕЗОПАСНОГО УДАЛЕННОГО ДОСТУПА

КОТ ИБ corporation

КОТ ИБ

Денис Бубнов
Независимый эксперт

ТЕЛЕФОН: +7 (961) 335-49-09

EMAIL: dvbubnov@gmail.com

Безопасный удаленный доступ? Зачем?

Хочу работать удаленно!

Сервер снова завис…ну не ехать же на работу!

У нас серьезные системы, которые обслуживают подрядчики

У меня система мониторинга, хочу ее видеть везде!

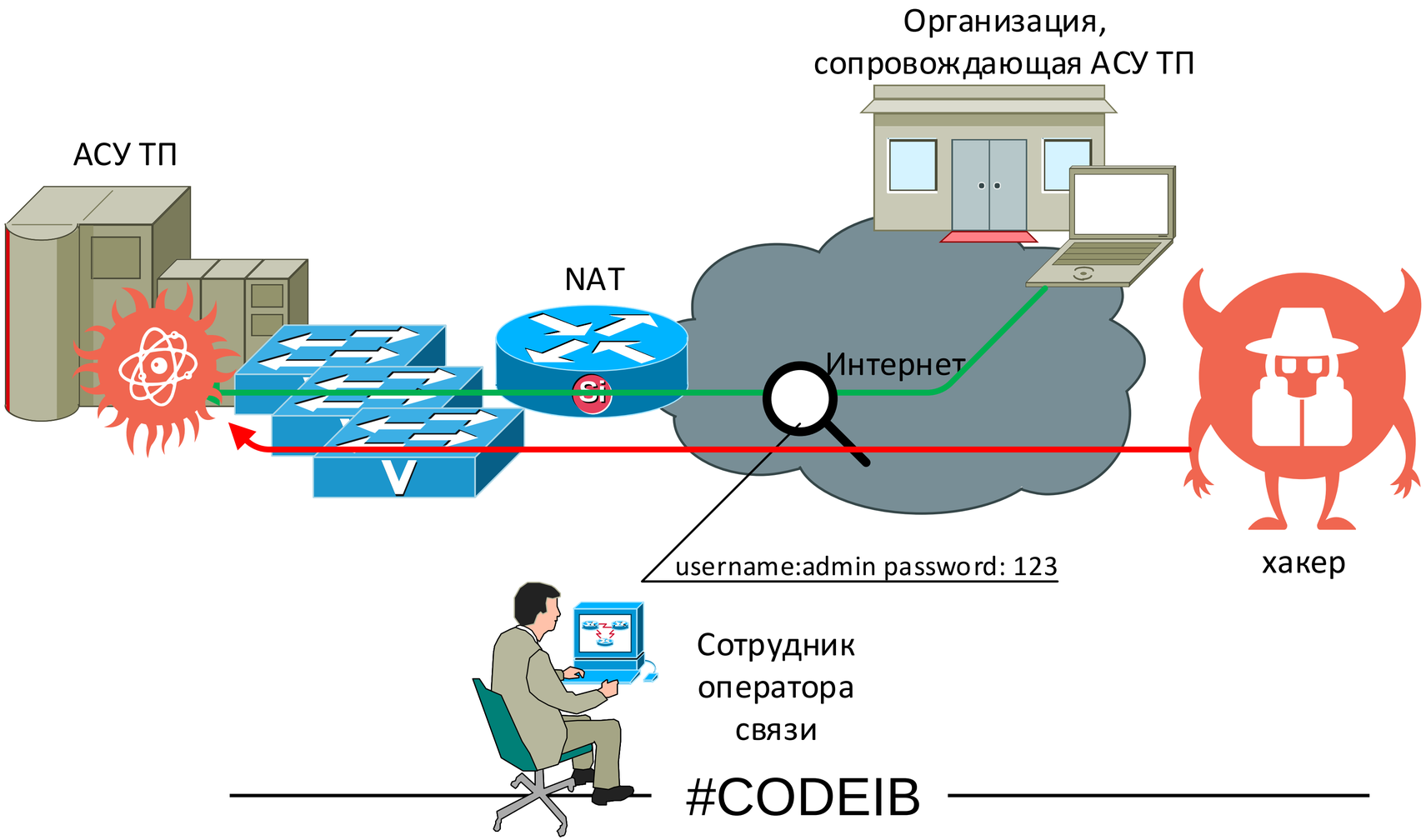
с 1С из дома

Анна Васильевна – главный бухгалтер, хочет работать с 1С с домашнего компьютера

Безопасный удаленный доступ – что говорит законодательство?

- **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.

Удаленный доступ. Как обычно бывает (на примере АСУ ТП)



Удаленный доступ. Немного цифр

Служб безопасности предприятий это запрещают

Систем удаленного доступа защищены только VPN

Систем удаленного доступа не защищены (сделаны через NAT)

Какое количество систем доступны в Интернет по SSH/RDP?...Страшно представить

* По данным из сети

БЕЗОПАСНЫЙ УДАЛЕННЫЙ ДОСТУП

УПРАВЛЯЕМОСТЬ

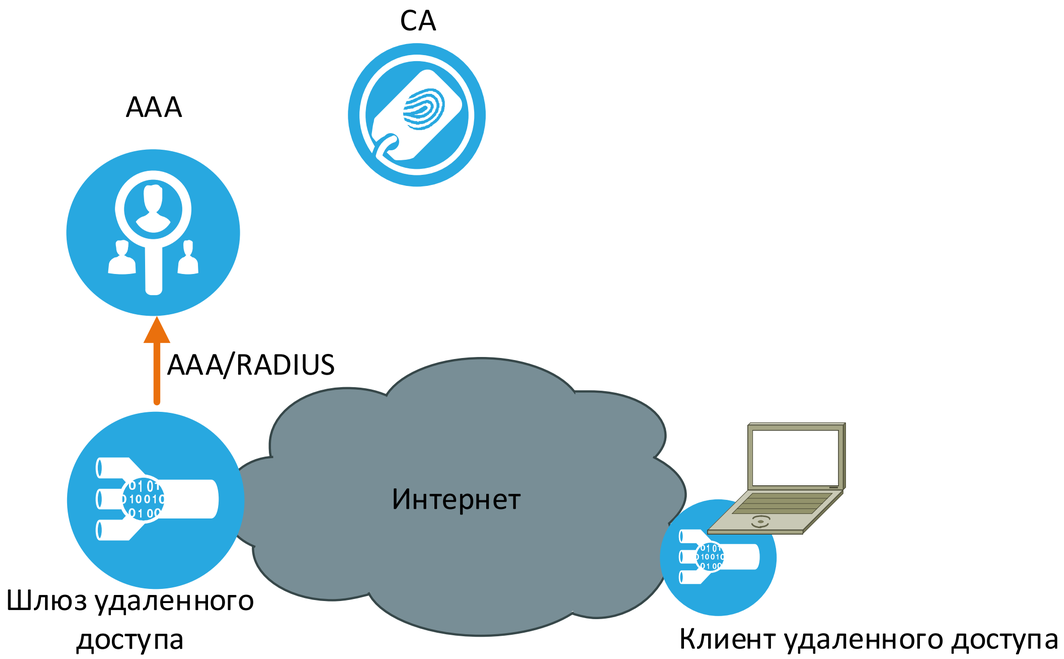
КОНТРОЛЬ

БЕЗОПАСНОСТЬ

Удаленный доступ. Как сделать правильно?

Компоненты решения: подсистема VPN

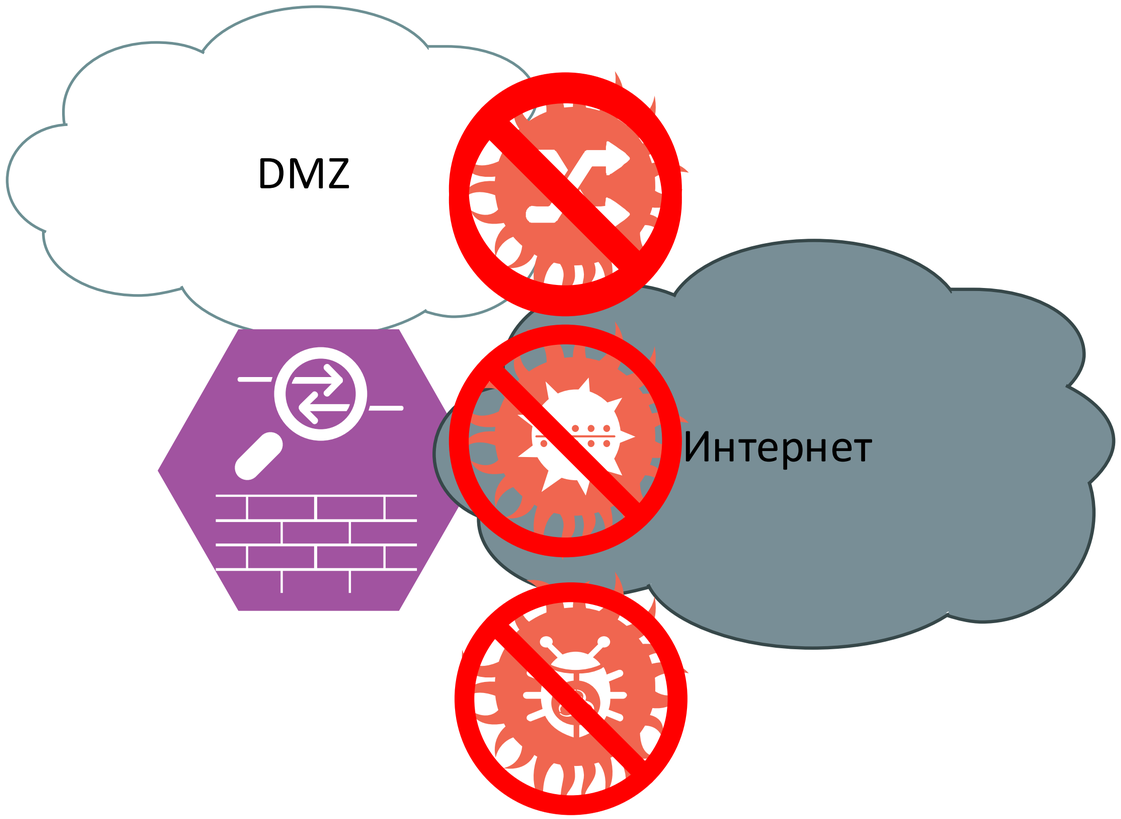
- Криптографическая защита передаваемых данных;
- Надежная аутентификация (PKI, RADIUS);
- Широкий спектр решений, как Open Source, так и коммерческих. Наличие сертифицированных продуктов



Компоненты решения: подсистема FW&IPS

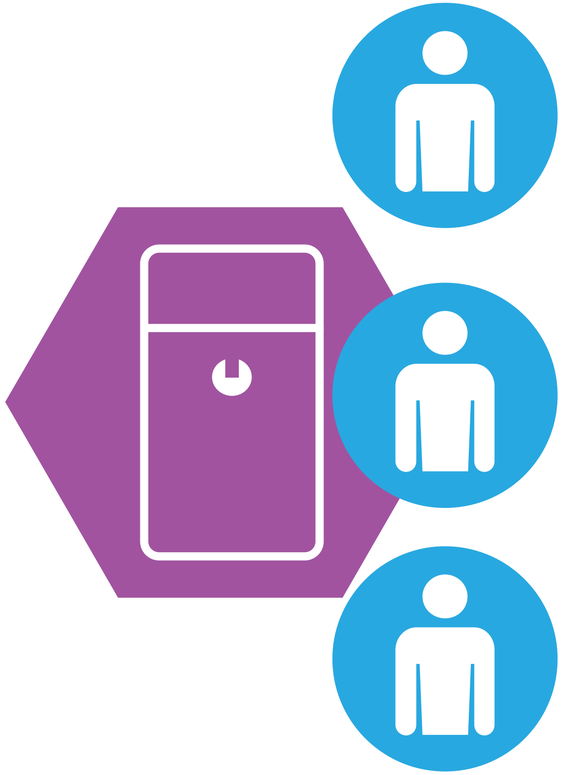
- Реализация корпоративных политик безопасности;
- Формирование ДМЗ для защищенного удаленного доступа;
- Блокировка сетевых атак до уровня L7.

- Наличие сертифицированных продуктов



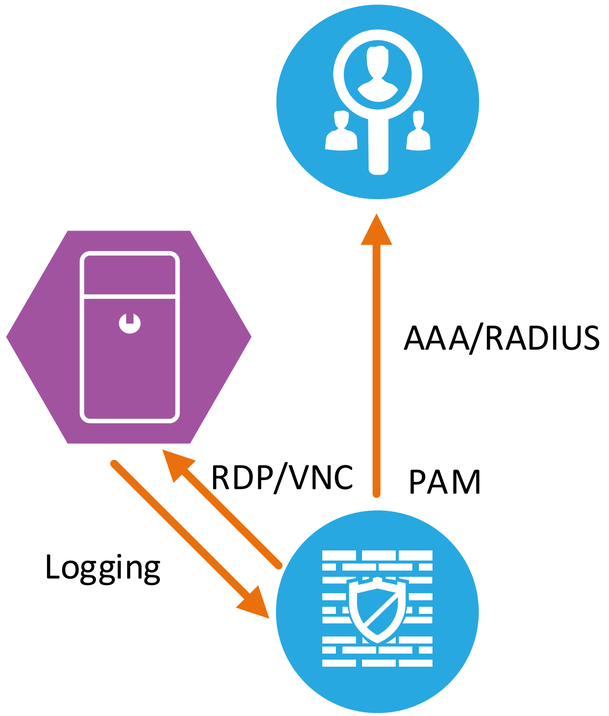
Компоненты решения: терминальный сервер

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



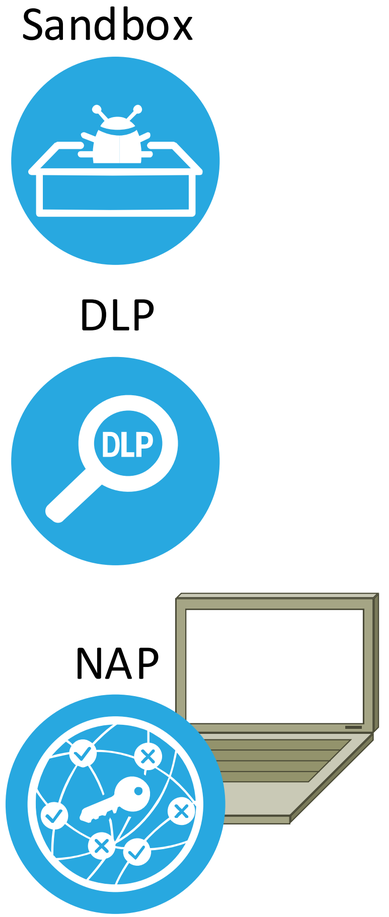
Компоненты решения: PAM

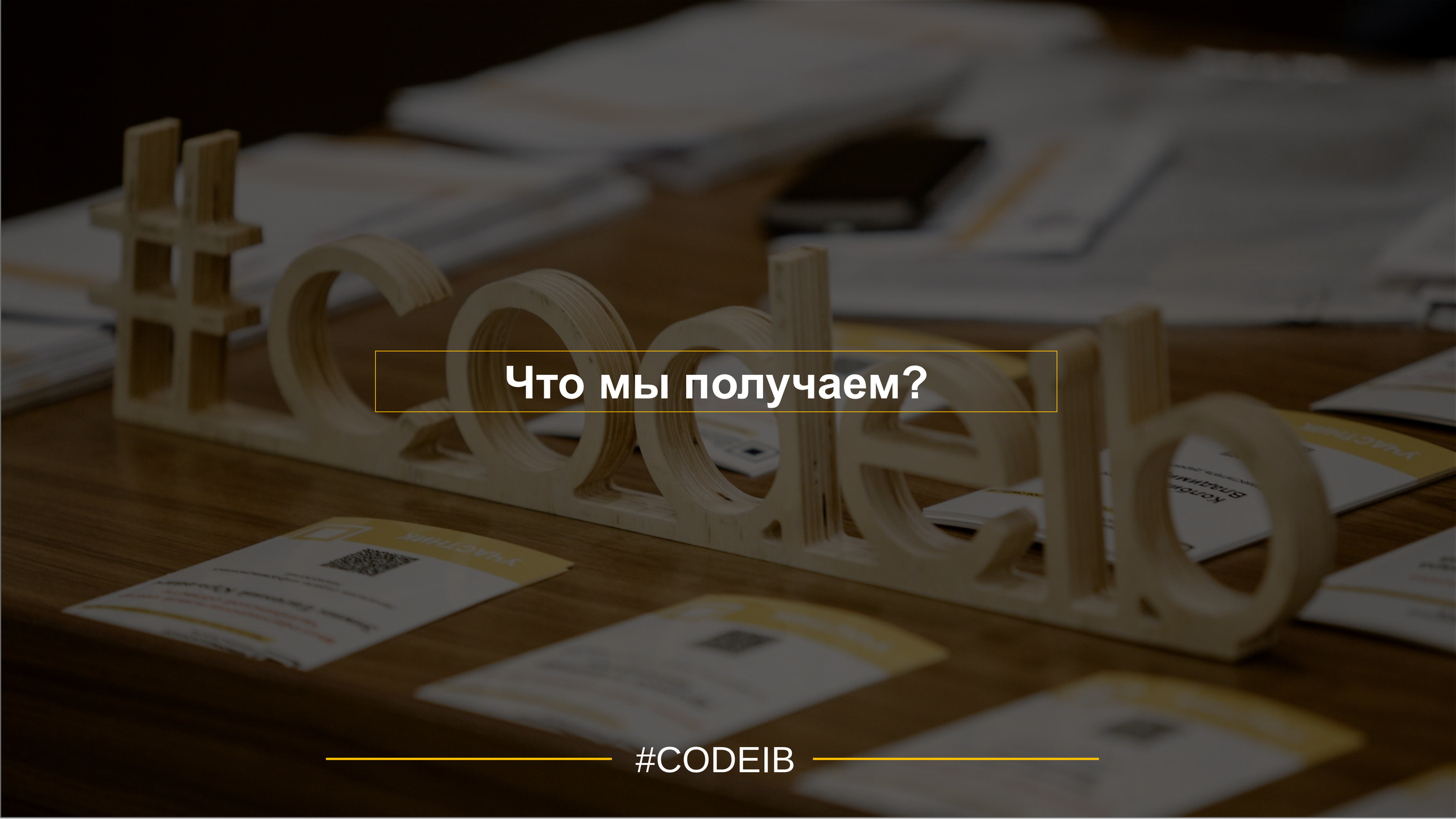
- Аутентификация удаленных пользователей без использования базы терминального сервера;
- Журналирование терминальных сессий
- Интеллектуальный анализ действий администраторов;
- Поддержка популярных протоколов управления (RDP, SSH, VNC)



Компоненты решения: что добавить?

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





Что мы получаем?

Безопасный удаленный доступ

Полный контроль внешних подключений

Защита передаваемых данных по сетям операторов связи

Контролируемая программная среда (нет возможности использовать сомнительный софт)

fff

Запись всех действий (стереть журналы невозможно)

Изоляция сервисов корпоративной сети

Удобство доступа из любой точки мира

Открытые стандарты, нет Vendor Lock, дорогих подписок и лицензий (но это не точно)

Защита от вредоносного софта, утечек информации

Соответствие законодательству

СПАСИБО ЗА ВНИМАНИЕ!