Актуальные вопросы централизованного управления информационной безопасностью

СЕРГЕЙ ОВЧИННИКОВ

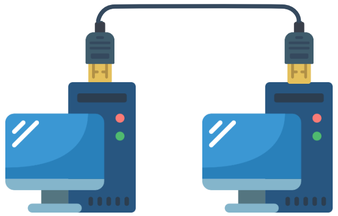
ДИРЕКТОР ПО МАРКЕТИНГУ
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: OSV@CONFIDENT.RU

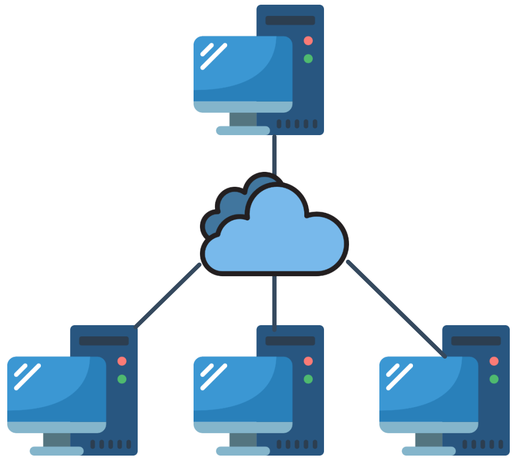
WEB: WWW.DALLASLOCK.RU

Развитие подходов к управлению ИБ

Локальные ПК

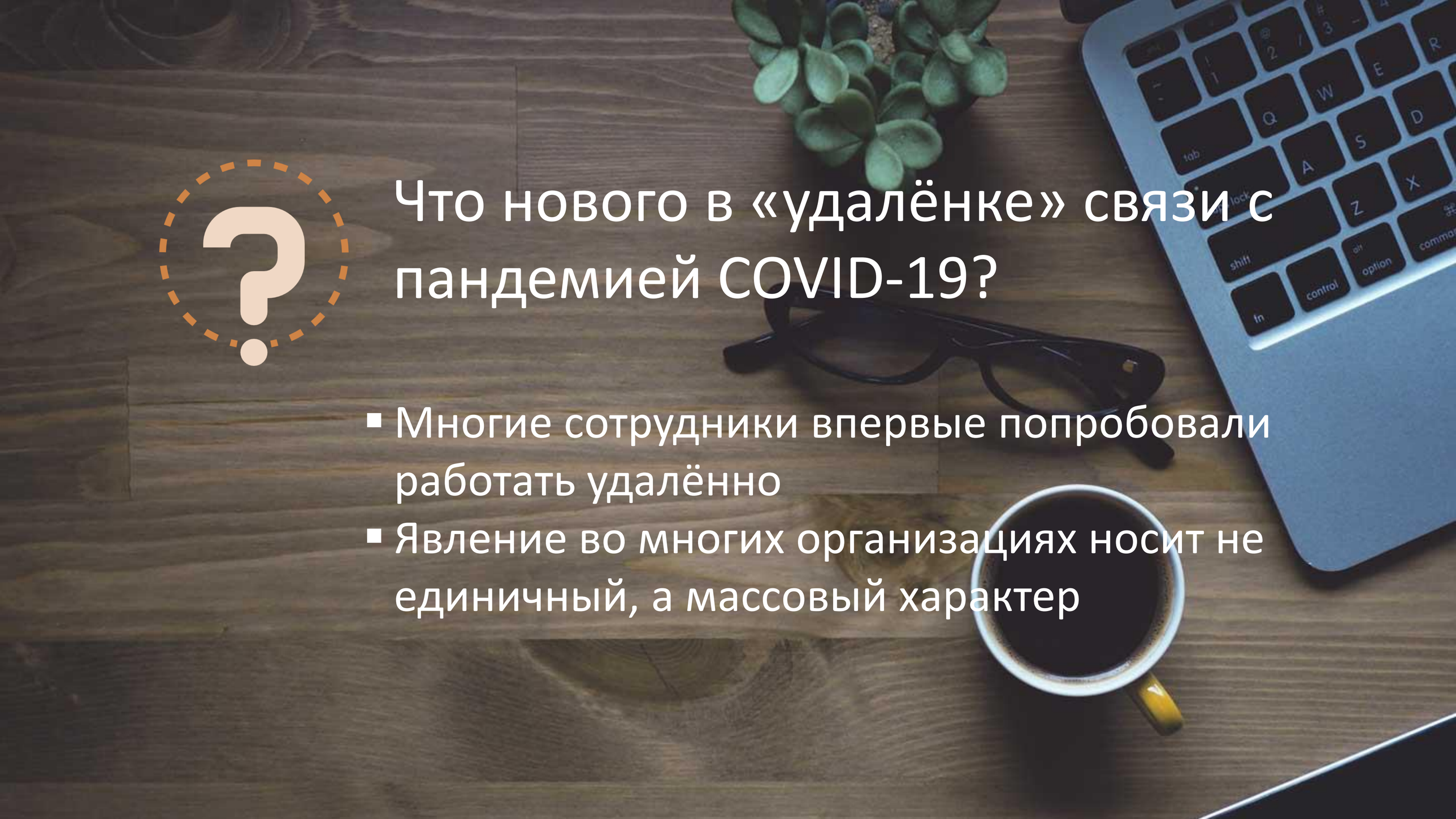


Удалённое администрирование



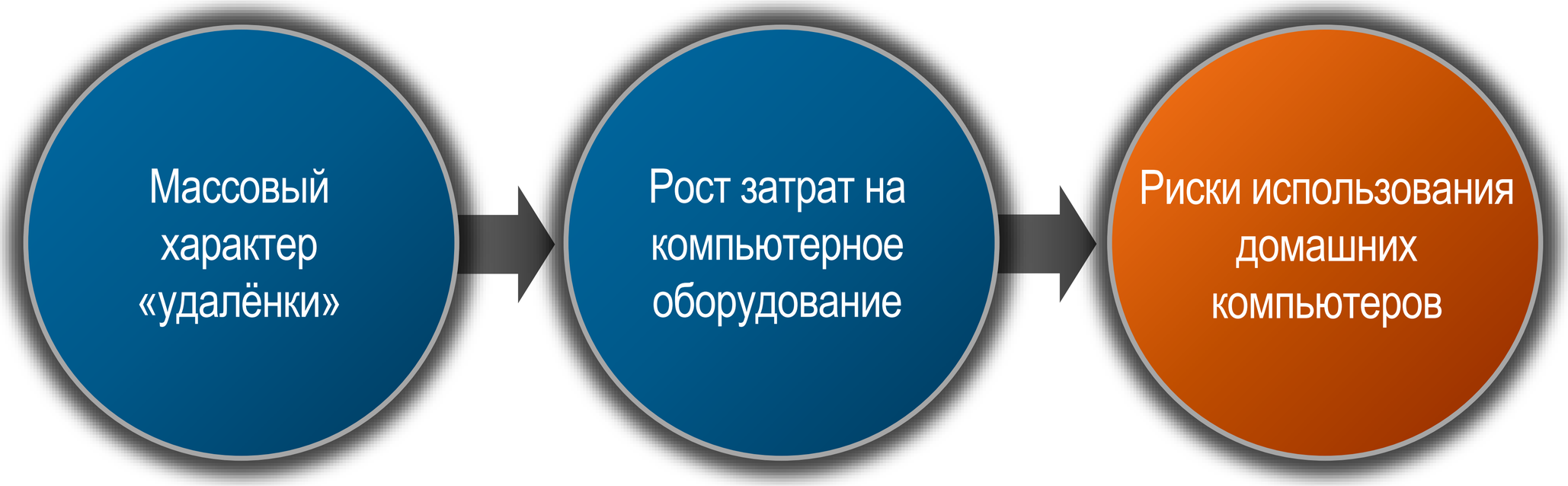
Централизованное управление:

- однотипными агентами
- разнотипными агентами
- сторонними решениями



Что нового в «удалёнке» связи с пандемией COVID-19?

- Многие сотрудники впервые попробовали работать удалённо
- Явление во многих организациях носит не единичный, а массовый характер



Сотрудники чаще используют домашние компьютеры для работы:

- для пользователя это удобнее
- для организации это дешевле

Вопросы

Какое количество пользователей находится у государственных заказчиков на «удалёнке»?

Используют ли они домашние компьютеры для доступа к ресурсам организации?

Какими СЗИ защищены эти компьютеры и есть ли возможность управлять этими СЗИ?

На конец 2020 года*:

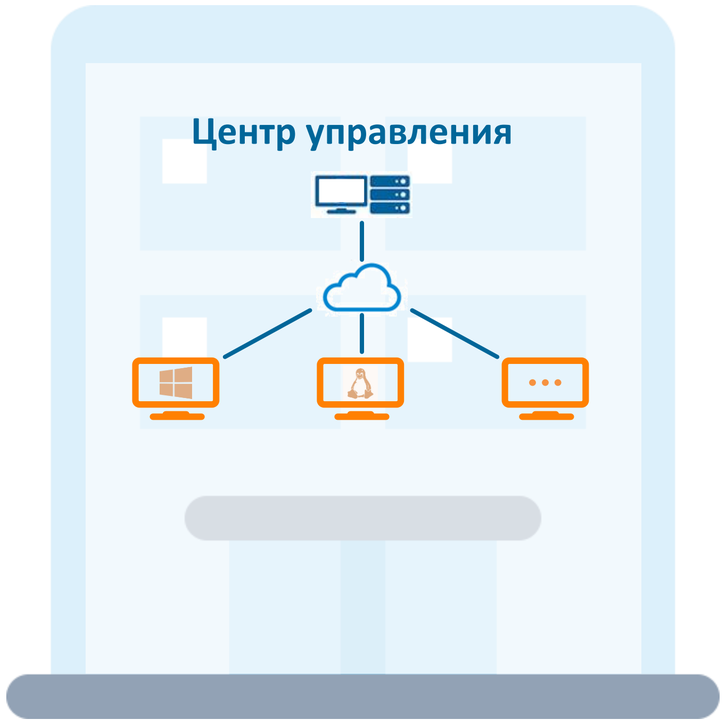
*В среднем **32%** пользователей государственных заказчиков находится на «удалёнке»*

*Более **90%** из них используют домашние компьютеры для доступа к ресурсам организации*

На домашних ПК применяются VPN-клиенты и иногда антивирусы. Полноценное централизованное управление этими СЗИ не осуществляется.

* По результатам опроса партнёров Центра защиты информации ООО «Конфидент», январь-февраль 2021 г.

IT-инфраструктура до COVID-19

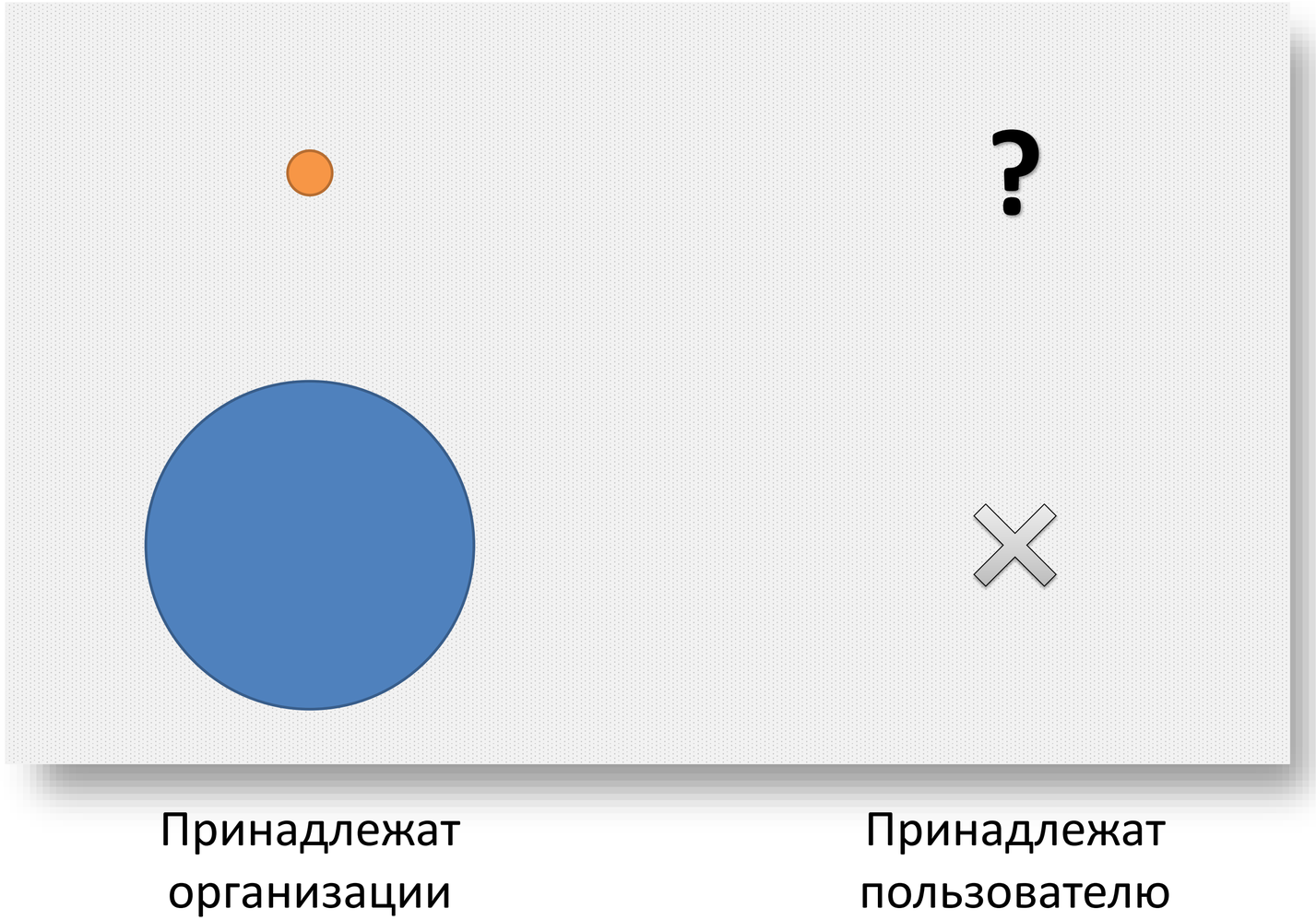


- Конечные точки защищены большим набором сертифицированных СЗИ
- АРМ доступны по IP для средств централизованного управления
- Относительно хорошие каналы связи внутри периметра

IT-инфраструктура сейчас

- У пользователя есть домашний ПК для работы, который почти не защищён и часто находится за NAT (Network Address Translation)
- Канал связи далеко не всегда хороший, но всегда нагружен
- Сложный учёт СВТ, ПО и СЗИ

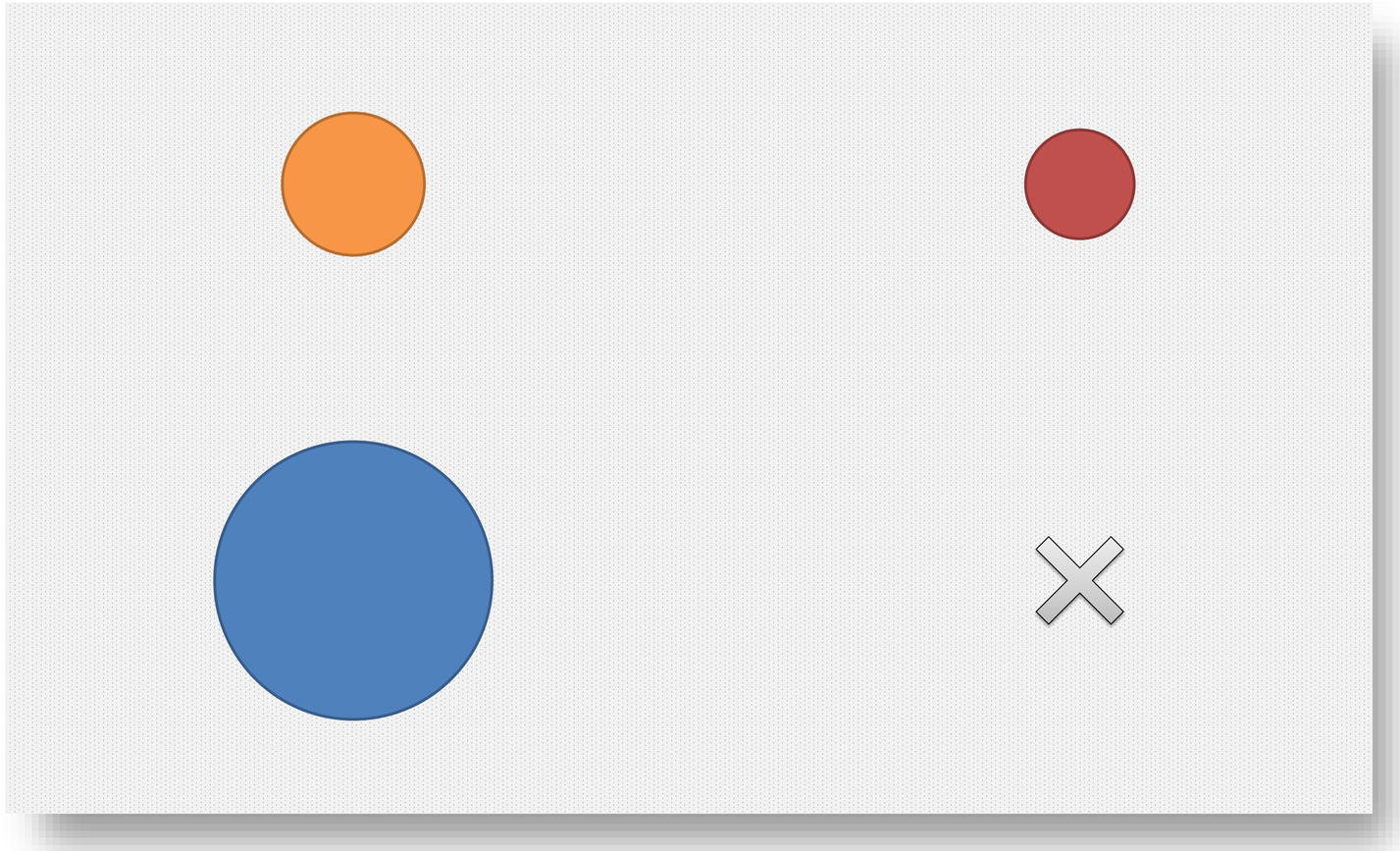
Количество компьютеров до COVID-19



Количество компьютеров сейчас

Вне офиса

Внутри офиса



Принадлежат организации

Принадлежат пользователю

Что делать с домашними компьютерами?

Что делать с домашними компьютерами?

- Решения на основе Bootable USB Drive (Live USB)
- VPN-клиенты
- Антивирусы
- Прочие решения: СЗИ от НСД, МЭ, СОВ, DLP и т.д.

Этими компьютерами надо заниматься

Выводы:

1. Неизбежность использования домашних ПК для обработки информации.
2. Требования к центру управления информационной безопасностью должны включать:
   - работа в сложных сетевых инфраструктурах;
   - управление клиентскими частями под Windows и Linux, поддержка российских ОС;
   - функциональность для инвентаризации;
   - бесперебойная работа в больших инфраструктурах и при «слабом» сетевом соединении.

Единый центр управления

- Управление СЗИ Dallas Lock (Windows/Linux)
- Работа за NAT
- Контроль настроек сетевого оборудования
- Инвентаризация
- VNC-клиент

Разработано

- Сбор и анализ инцидентов ИБ
- Автоматическая геолокация АРМ
- Интегральные показатели защищённости для компьютеров внутри/ вне офиса, принадлежащих организации/ пользователям
- Анализ сценариев «что если» для улучшения показателей ИБ и планирования расходов на СЗИ

Перспективы

Спасибо за внимание!

СЕРГЕЙ ОВЧИННИКОВ

ДИРЕКТОР ПО МАРКЕТИНГУ
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: OSV@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU