

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СЗИ ОТ НСД В СОВРЕМЕННЫХ УСЛОВИЯХ

Сергей Овчинников

Директор по маркетингу,
Центр защиты информации «Конфидент»



Распространённое мнение

«СЗИ от НСД обладают только той функциональностью, которую определяют требования Регулятора»

- Авторизация до загрузки ОС
- Контроль целостности до и после загрузки ОС
- Защита от НСД
- Контроль подключения носителей и переноса информации
- Персональный межсетевой экран
- Обнаружение и предотвращение вторжений
- Безопасная среда («песочница»)
- Инвентаризация ПО
- Защита виртуализованных сред
- Резервное копирование и восстановление
- Интеграция с другими системами (SIEM, контроль защищённости)
- Журналирование всех событий

Примерно так воспринимают СЗИ от НСД

Централизованное управление,
профессиональные сервисы

- Авторизация до загрузки ОС
- Контроль целостности до и после загрузки ОС
- Защита от НСД
- Контроль подключения носителей и переноса информации
- Персональный межсетевой экран
- Обнаружение и предотвращение вторжений
- Безопасная среда («песочница»)
- Инвентаризация ПО
- Защита виртуализованных сред
- Резервное копирование и восстановление
- Интеграция с другими системами (SIEM, контроль защищённости)
- Журналирование всех событий

Примерно так обстоят дела на самом деле

Продуктовая линейка Dallas Lock



Dallas Lock 8.0



Dallas Lock Linux



СДЗ Dallas Lock



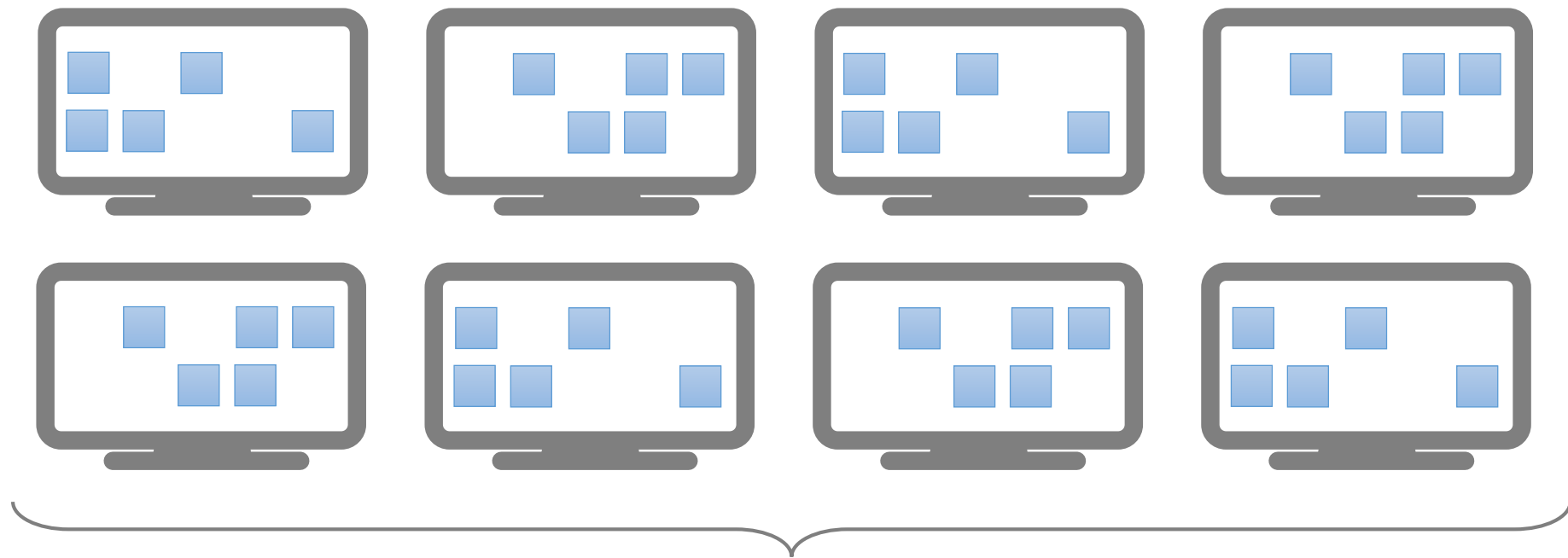
СЗИ ВИ Dallas Lock

Набор решений для защиты конечных точек в физических и виртуализованных средах с централизованным управлением

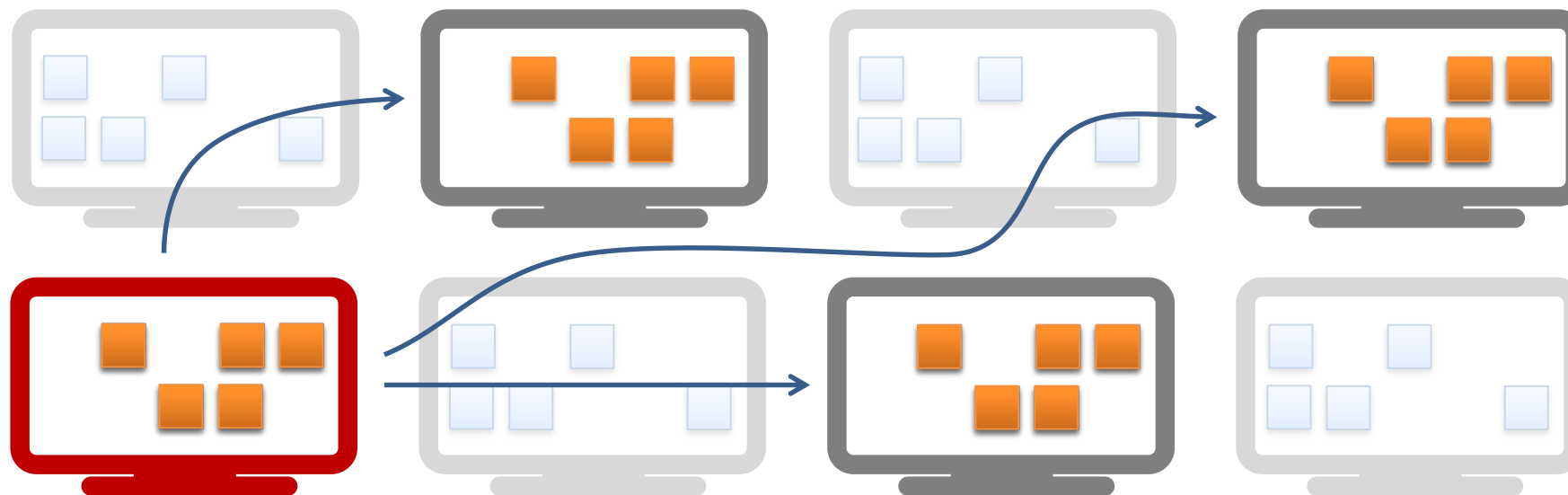


Кейс:

Контроль целостности в
больших инфраструктурах



Необходимо контролировать целостность объектов (ресурсов): файлы, реестр, программно-аппаратная среда. Компьютеров много и они разные (x32, x64), а объекты размещаются в разных местах.



Выбираем компьютер и ставим на контроль целостности объекты.
Dallas Lock сам находит похожие компьютеры и ставит объекты на контроль.

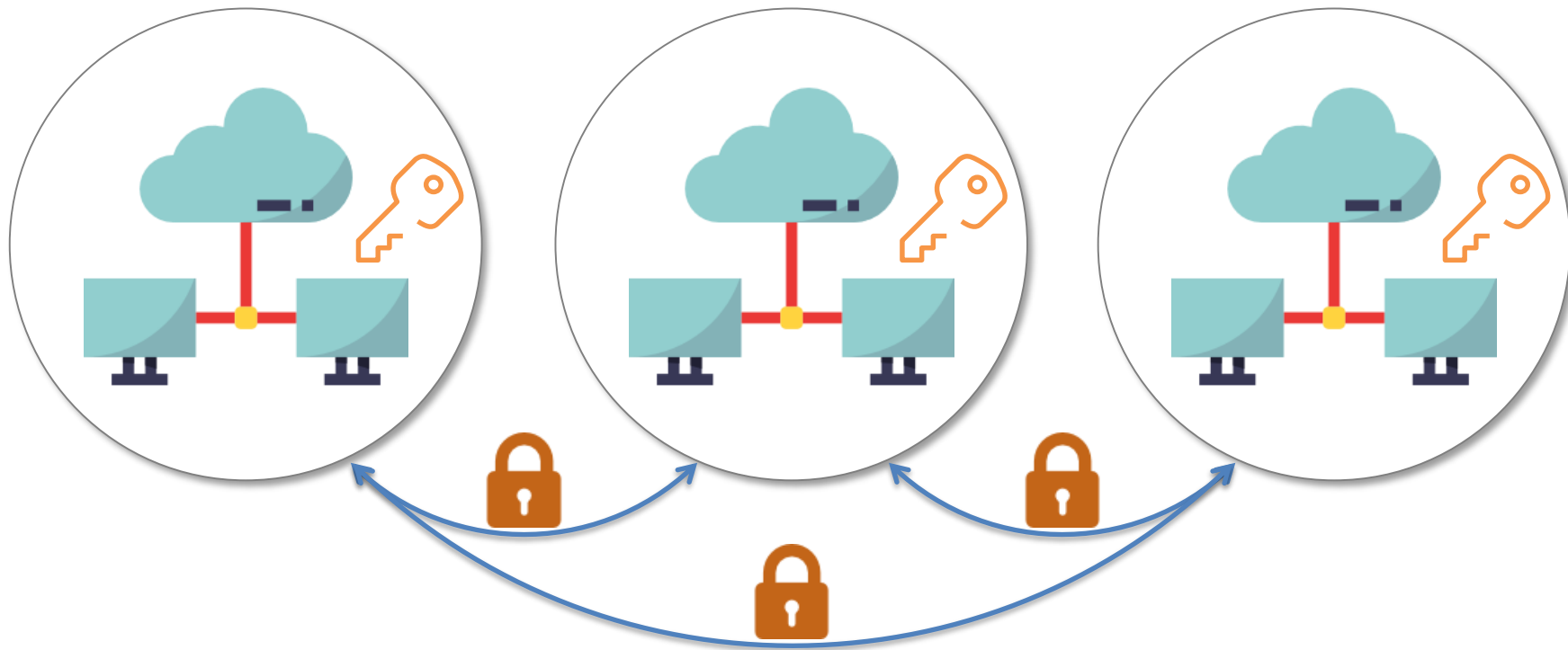


Все остальные объекты также легко
обнаруживаются в сети



Кейс:

Контроль переноса информации
на внешние накопители



Dallas Lock позволяет полностью исключить утечки информации через сменные накопители.

1

КЛЮЧИ

ПРЕОБРАЗОВАНИЯ
ДОСТУПНЫ ТОЛЬКО
АДМИНИСТРАТОРУ



2

ПАРОЛЬ

ПОЛЬЗОВАТЕЛЯ ДЛЯ
ДОСТУПА
К НОСИТЕЛЮ



3

DALLAS LOCK

БЕЗ «ДАЛЛАСА»
ЗДЕСЬ ТОЧНО НЕ
ОБОЙТИСЬ



Злоумышленнику придётся постараться



Кейс:

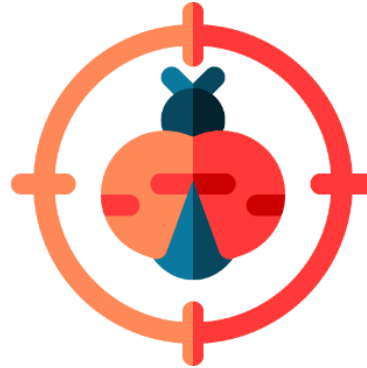
От замкнутой программной среды
к безопасной среде



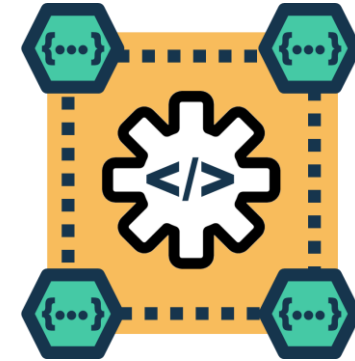
У любого пользователя есть множество идей на тему:
«почему бы не запустить эту программу»



**ЗАПРЕТ
АДМИНИСТРАТИВНЫХ
ПРИВИЛЕГИЙ**

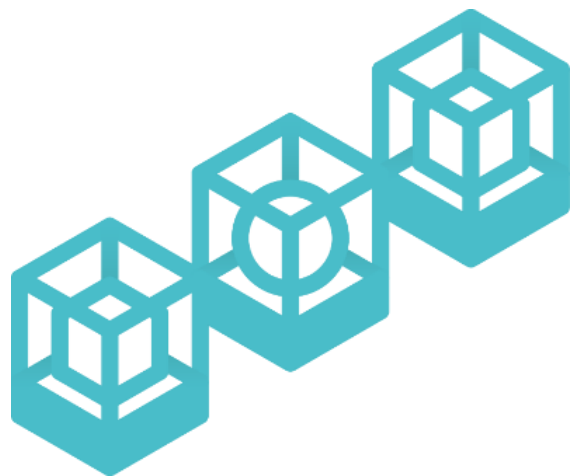


**УСТАНОВКА И
ОБНОВЛЕНИЕ
АНТИВИРУСА**



**НАСТРОЙКА
ЗАМКНУТОЙ
ПРОГРАММНОЙ СРЕДЫ**

Инструменты администратора ИБ, которые иногда не срабатывают или не совсем удобны



**Централизованное
управление**



БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX



потенциально опасные приложения можно запускать в частично виртуализованной безопасной среде



настройки включают: контроль приложений, эвристический анализ, доступ к файловой системе и реестру



в журнале фиксируются принудительное завершение приложения с указанием нарушенных правил



Кейс:

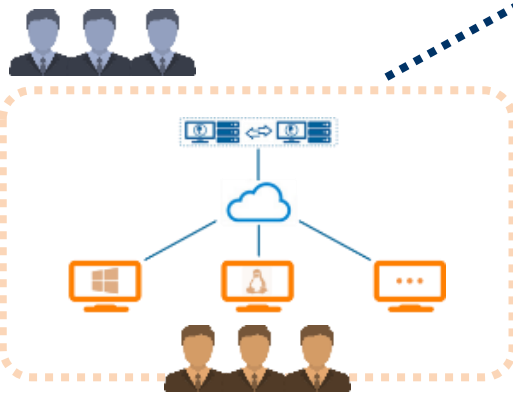
Управление пользователями
с повышенными привилегиями



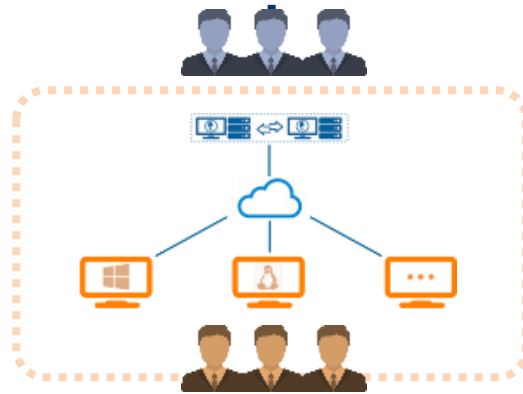
Задачи привилегированных пользователей:

- ★ Установка и обновление средств защиты информации.
- ★ Разграничение доступа к информационным ресурсам.
- ★ Контроль целостности программно-аппаратной среды.
- ★ Управление сменными накопителями.
- ★ Управление межсетевым экранированием.
- ★ Обнаружение и предотвращение вторжений.
- ★ Реагирование на инциденты.
- ★ Прочее...

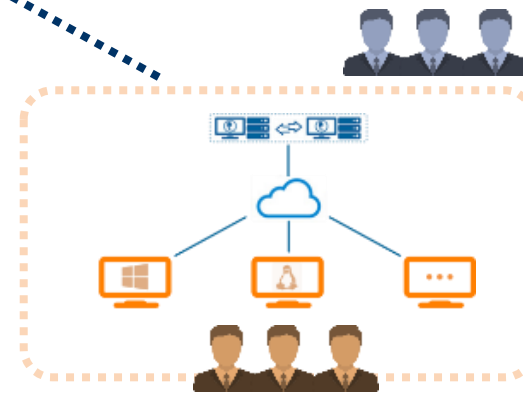
**Менеджер
серверов безопасности**



Домен безопасности



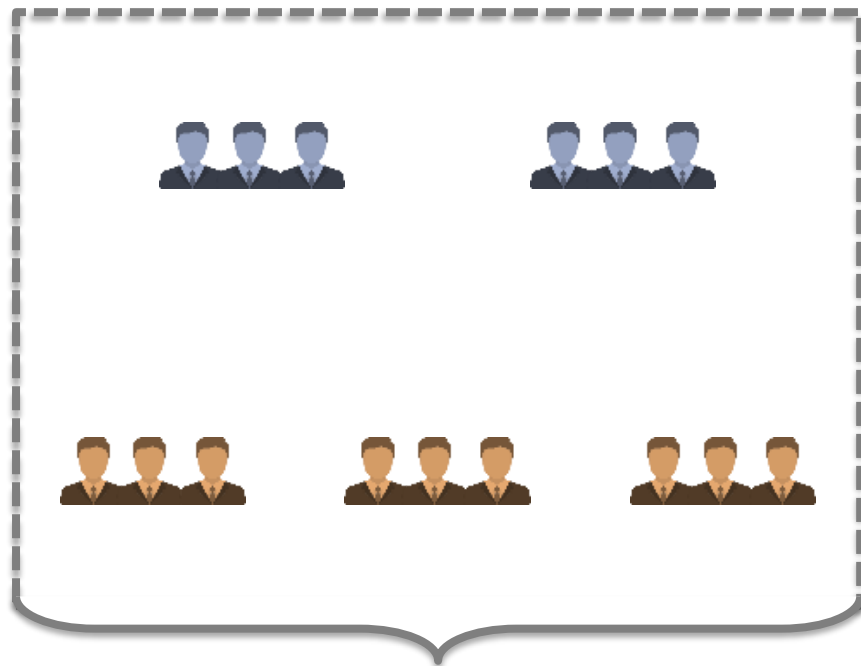
Домен безопасности



Домен безопасности



Главный администратор
информационной безопасности



Функциональное
распределение обязанностей

Администраторы домена имеют полномочия
только в рамках своего **домена безопасности**

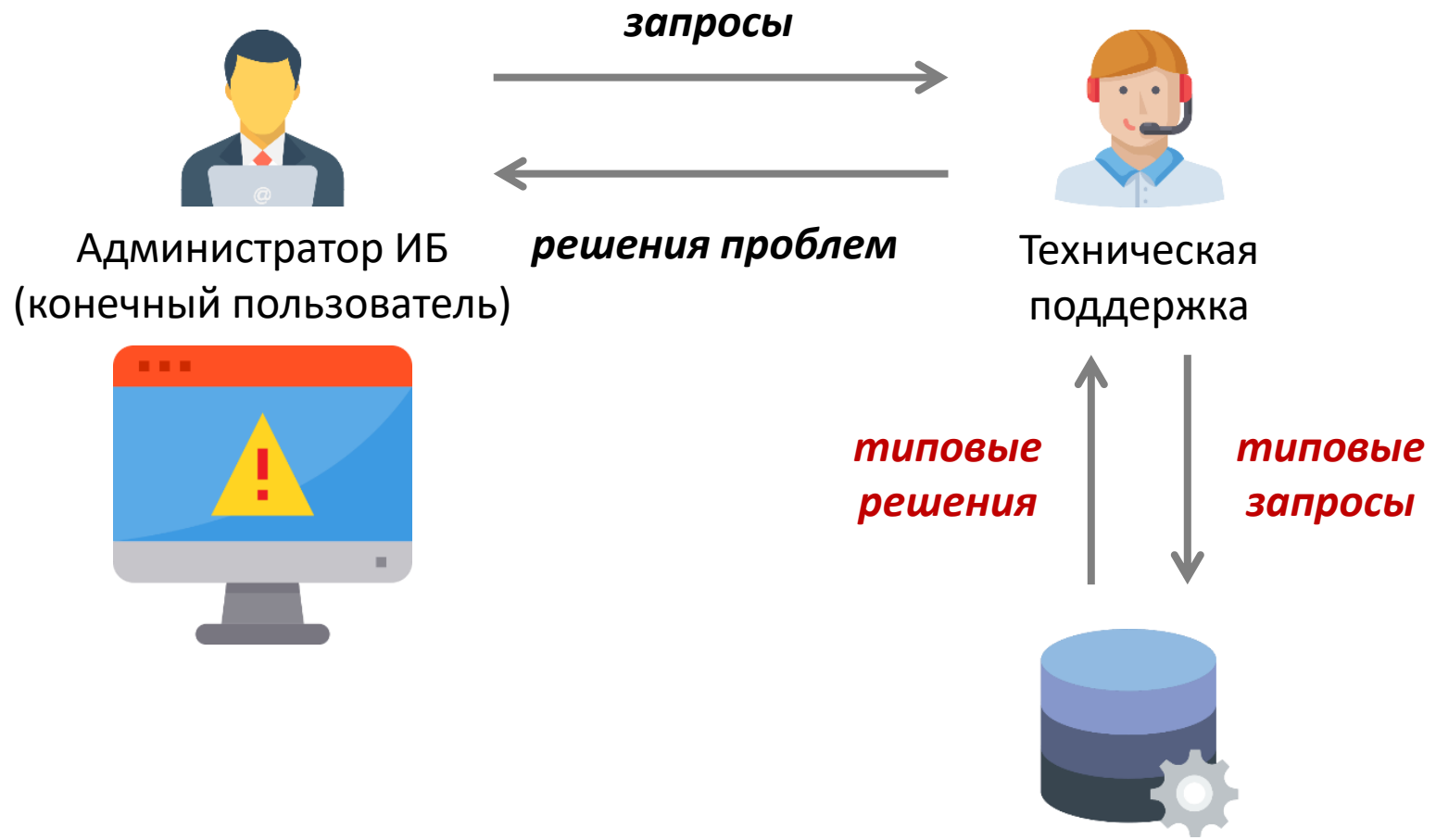
Администраторы группы имеют полномочия
только в рамках своей **группы компьютеров**

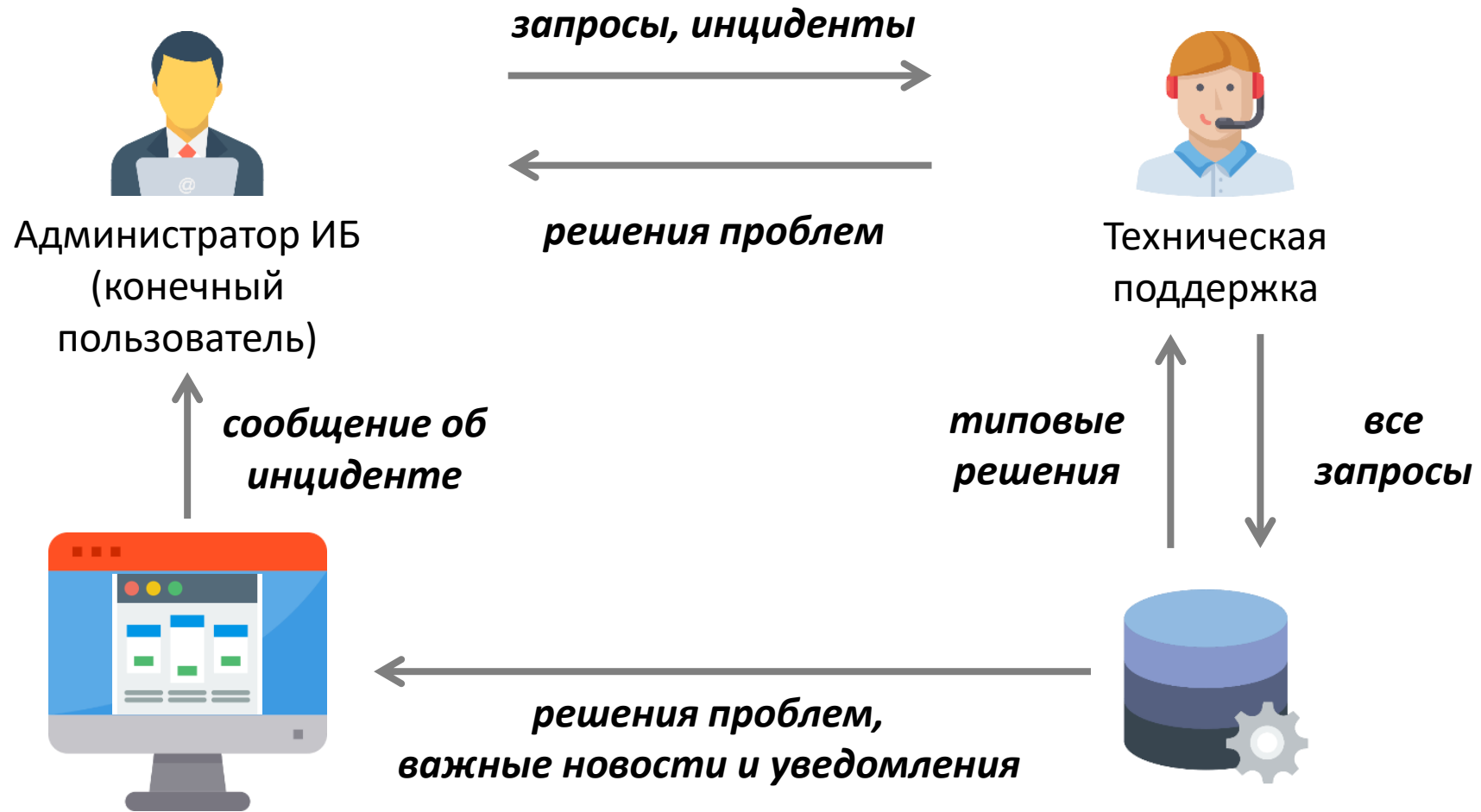
**НСД, СКН, МЭ, СОВ,
паспортизация ПО и т.п.**



Кейс:

Организация технической
поддержки

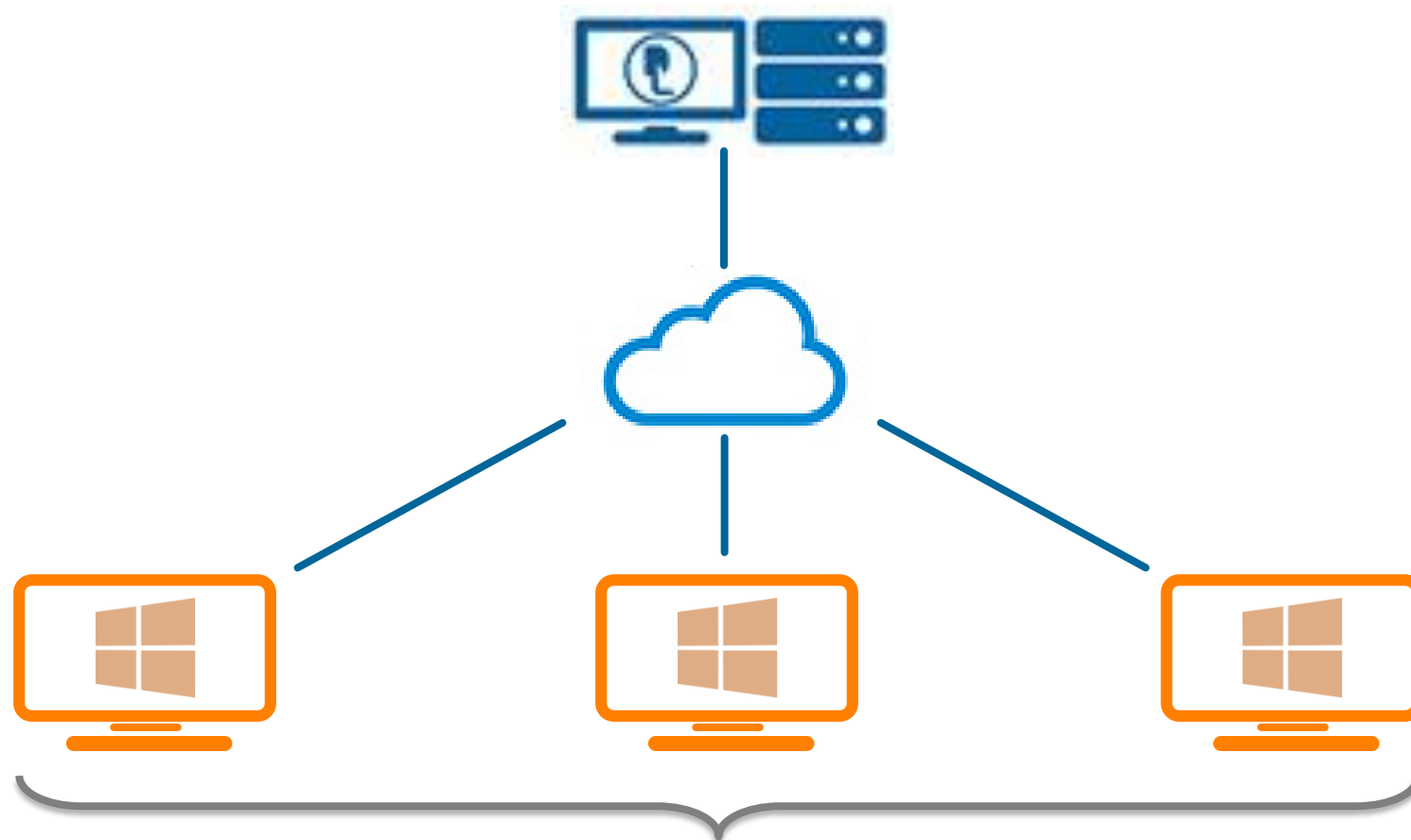




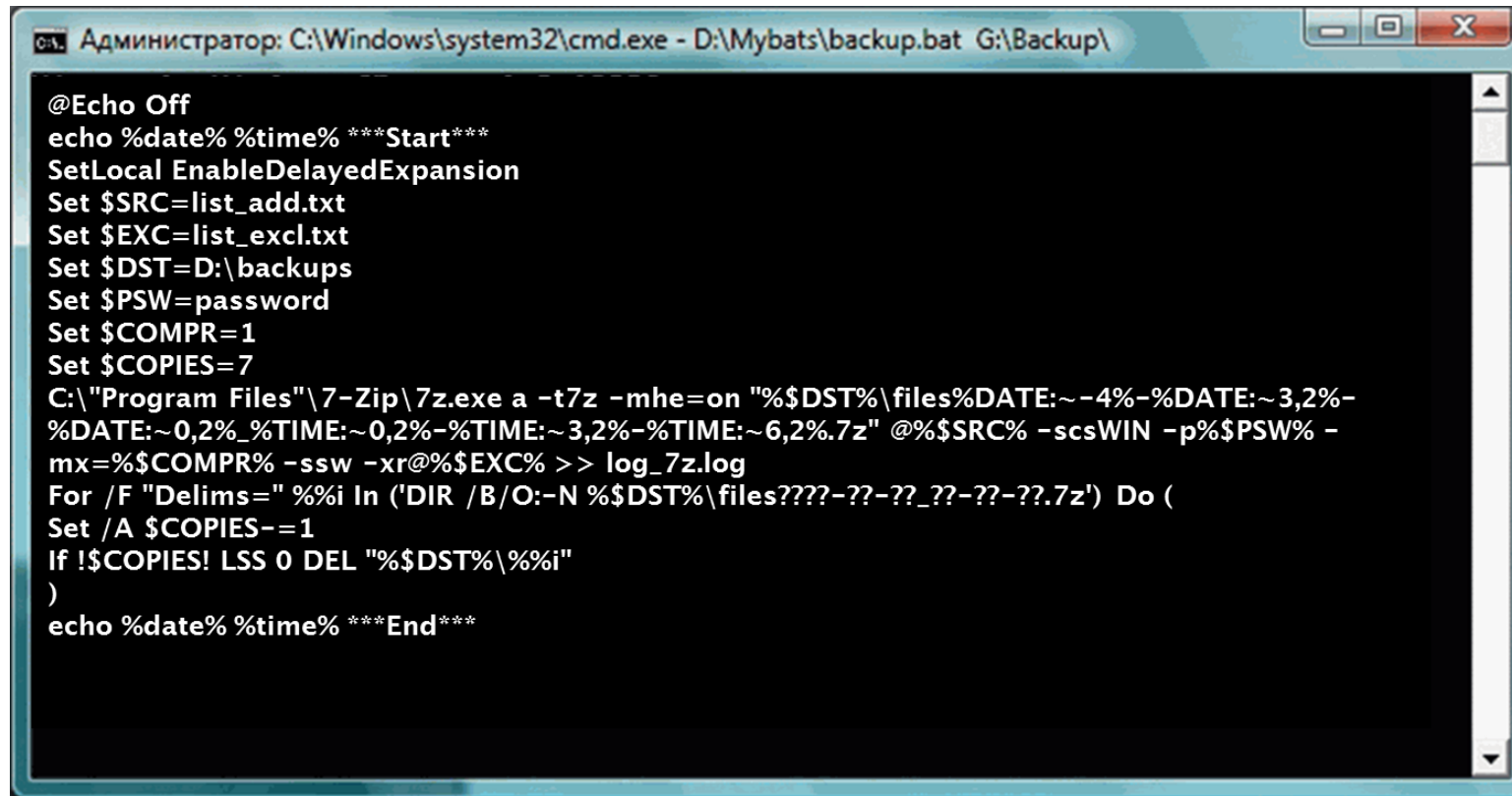


Кейс:

Резервное копирование и
восстановление



На компьютерах пользователей и серверах есть файлы, которые с определённой периодичностью необходимо резервировать



```
Администратор: C:\Windows\system32\cmd.exe - D:\Mybats\backup.bat G:\Backup\  
  
@Echo Off  
echo %date% %time% ***Start***  
SetLocal EnableDelayedExpansion  
Set $SRC=list_add.txt  
Set $EXC=list_excl.txt  
Set $DST=D:\backups  
Set $PSW=password  
Set $COMPR=1  
Set $COPIES=7  
C:"Program Files"\7-Zip\7z.exe a -t7z -mhe=on "%$DST%\files%DATE:~-4%-DATE:~3,2%-  
%DATE:~0,2%_TIME:~0,2%-TIME:~3,2%-TIME:~6,2%.7z" @$SRC% -scsWIN -p$PSW -  
mx=%COMPR% -ssw -xr@$EXC% >> log_7z.log  
For /F "Delims=" %i In ('DIR /B/O:-N %DST%\files????-??-??_??-??-???.7z') Do (  
Set /A $COPIES-=1  
If !$COPIES! LSS 0 DEL "%DST%\%i"  
)  
echo %date% %time% ***End***
```

Знакомая история?

Мастер создания задания

Параметры

Объекты ФС

Имя задания:

Активировать расписание запуска

Каждый день

Каждую неделю

Каждый месяц Числа

Запустить задание после загрузки ОС, если компьютер был недоступен

Резервная копия

Максимальное количество резервных копий

Время хранения резервных копий

Место хранения резервных копий:

«Как тебе такое,
Илон Маск?»

Dallas Lock 8.0-C, admin, 0 (Открытые данные), метка не выбрана (СБ: WIN-FRQQ8TURTKB) Демо-версия.

Состояние Учетные записи Параметры безо Контроль ресурс СХД РК МЭ СОВ Журнал СБ Администрировк

Задания Категории Действия

- Создать
- Свойства
- Активировать
- Копировать
- Обновить
- Деактивировать
- Удалить
- Запустить

Объекты DL

Windows Linux СДЗ Общее

Сервер безопасности (WIN-FRQQ8TURTKB)

- Default
 - Client_10
 - Client_11
 - Client_12
 - Client_4
 - Client_5
 - Client_6
 - Client_7
 - Client_8
 - Client_9
 - WIN-FRQQ8TURTKB

Имя	Запуск	Время запуска	Выполнение	Клиент
<input checked="" type="checkbox"/> Задание 1	Пн	9:00	В процессе	Client_10
<input type="checkbox"/> Задание 2	Каждый день	9:00		Client_11
<input type="checkbox"/> Задание 3	Каждый день	9:00		Client_12
<input checked="" type="checkbox"/> Задание 4	20 числа	08:00	Успешно	Client_6
<input checked="" type="checkbox"/> Задание 5	31 числа	12:00	Ошибка	Client_9

Централизованное управление
резервным копированием и восстановлением

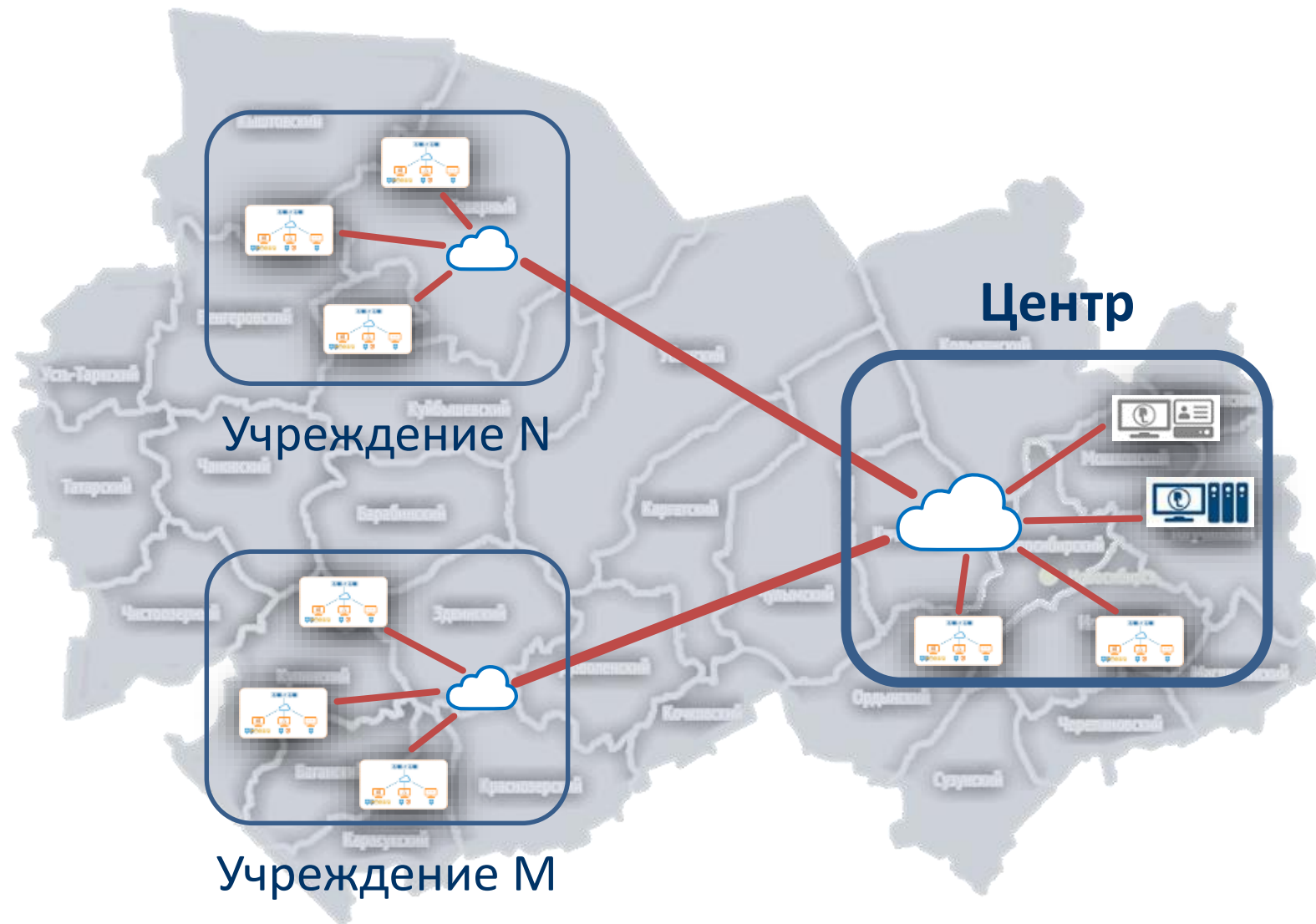
IX. Обеспечение доступности (ОДТ)				
ОДТ.0	Разработка политики обеспечения доступности	+	+	+
ОДТ.1	Использование отказоустойчивых технических средств		+	+
ОДТ.2	Резервирование средств и систем		+	+
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+
ОДТ.4	Резервное копирование информации	+	+	+
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+
ОДТ.7	Кластеризация информационной (автоматизированной) системы			
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+	+	+

В нормативных документах ФСТЭК России есть соответствующие меры защиты информации в базовом наборе мер

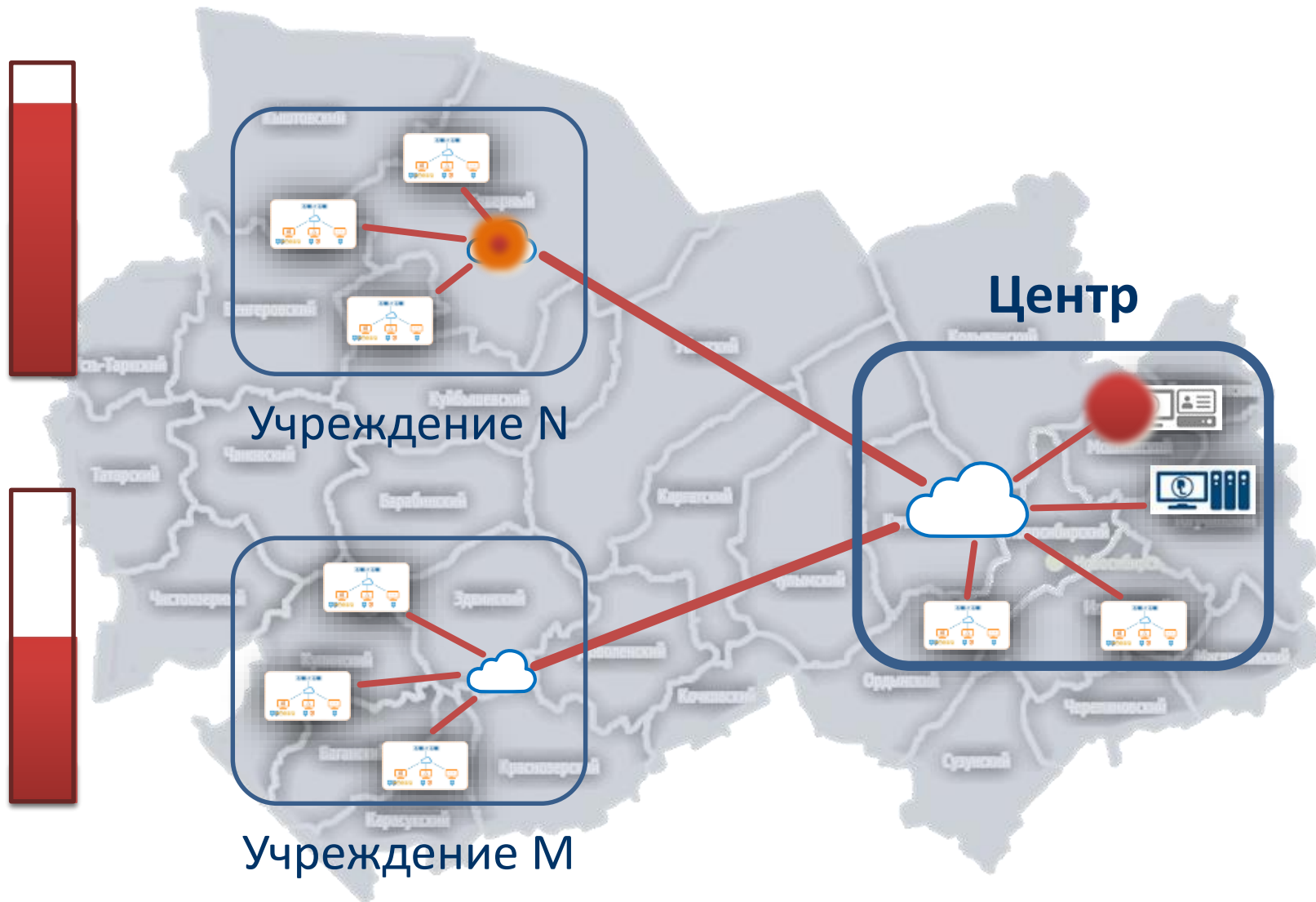


Кейс:

Управление лицензиями
на средства защиты информации



Количество лицензий на СЗИ



РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ ИНСТРУМЕНТОВ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ В ЗАВИСИМОСТИ ОТ КОЛИЧЕСТВА КЛИЕНТСКИХ АРМ

КОЛИЧЕСТВО КЛИЕНТСКИХ АРМ	СЕРВЕР БЕЗОПАСНОСТИ (СБ)	РЕПЛИКАЦИЯ СБ	СУБД ДЛЯ ХРАНЕНИЯ ЖУРНАЛОВ СБ	МЕНЕДЖЕР СБ	СЕРВЕР ЛИЦЕНЗИЙ	ВЫГРУЗКА СОБЫТИЙ В SIEM-СИСТЕМУ
< 10	○	—	—	—	—	—
10 – 500	●	—	—	—	—	—
500 – 5 000	●	●	●	—	—	●
5 000 – 50 000+	● (несколько доменов безопасности)	●	●	●	●	●

○ - опционально

● - рекомендуется применять



Опрос компаний-интеграторов, специализирующихся на защите информации в госсекторе и входящих в партнёрскую сеть Центра защиты информации ООО «Конфидент», которая насчитывает более 500 компаний.

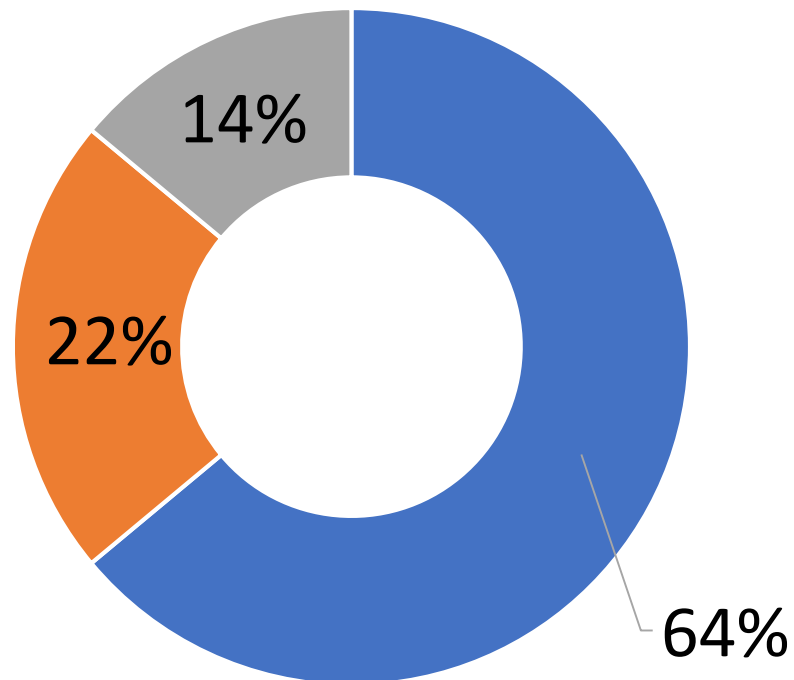
Аудитория: менеджеры и руководители отделов продаж, руководители отделов и специалисты по защите информации, руководители компаний.

Цель исследования: выяснить, каким образом изменилась работа партнёров в условиях пандемии нового коронавируса, и влияет ли данная ситуация на проекты 2020 года.

Дата: 23.04.2020 г.



Как изменился режим работы?



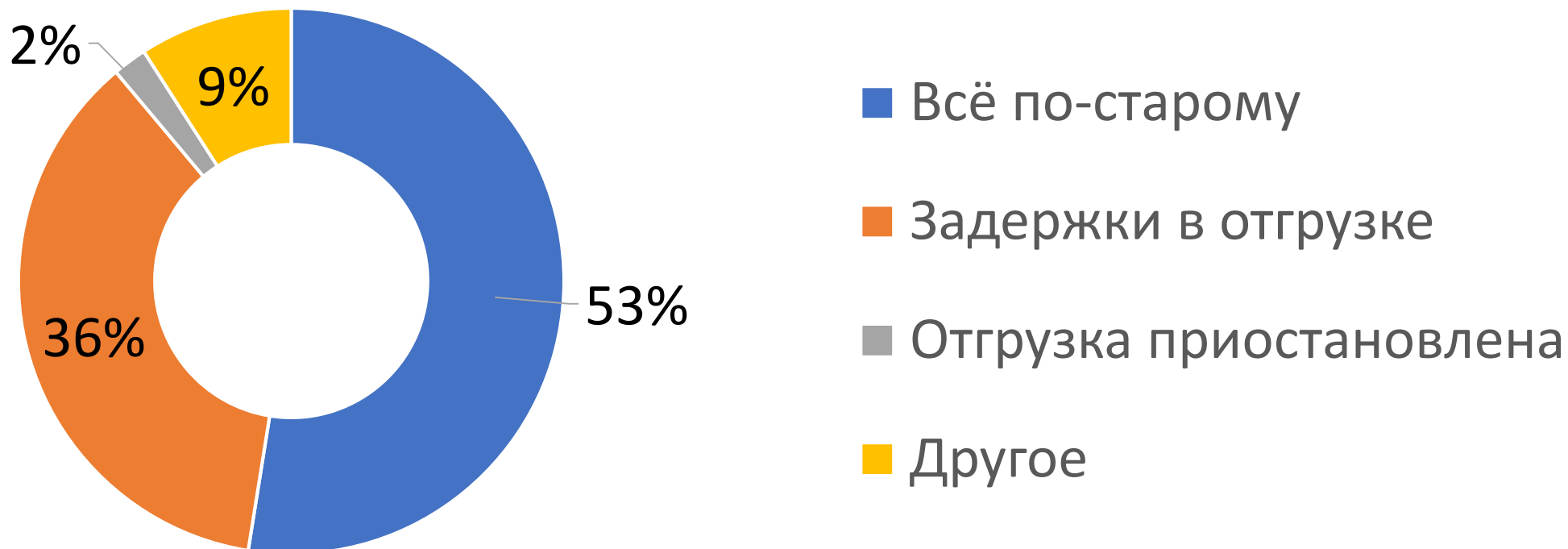
■ Переход на удалённую работу

■ Часть сотрудников на "удалёнке"

■ Всё по-старому

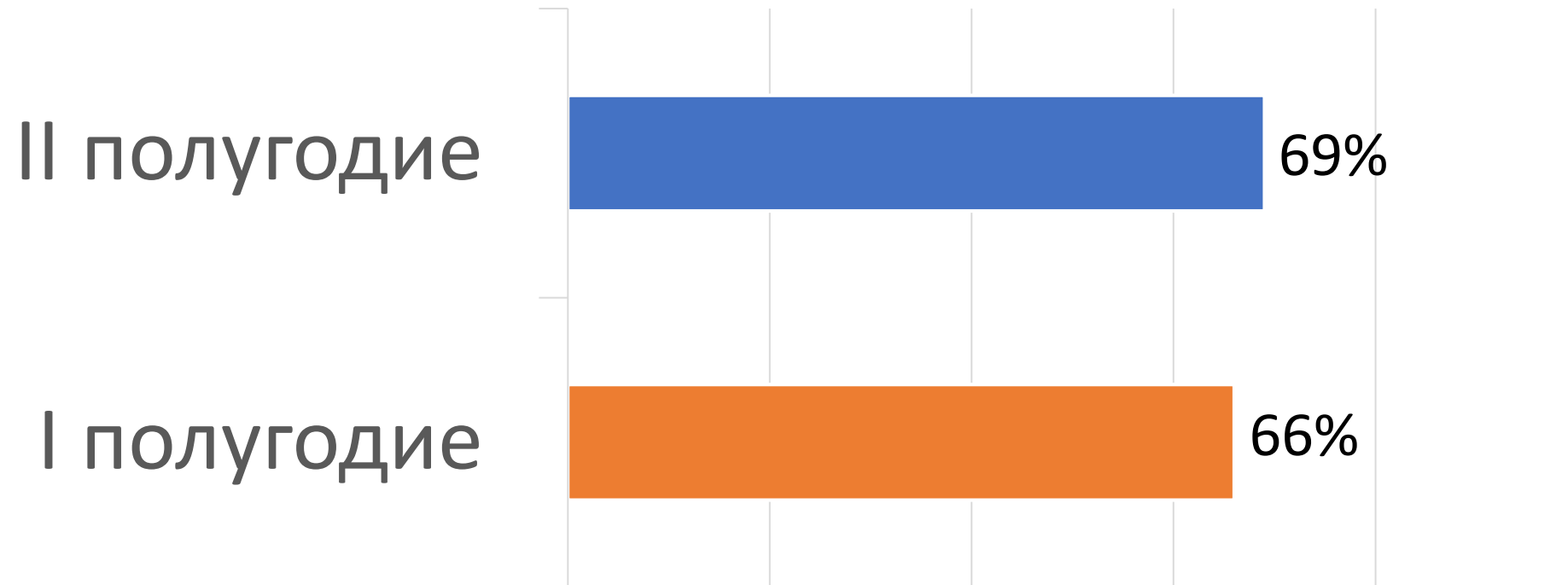


Как осуществляется отгрузка продукции?



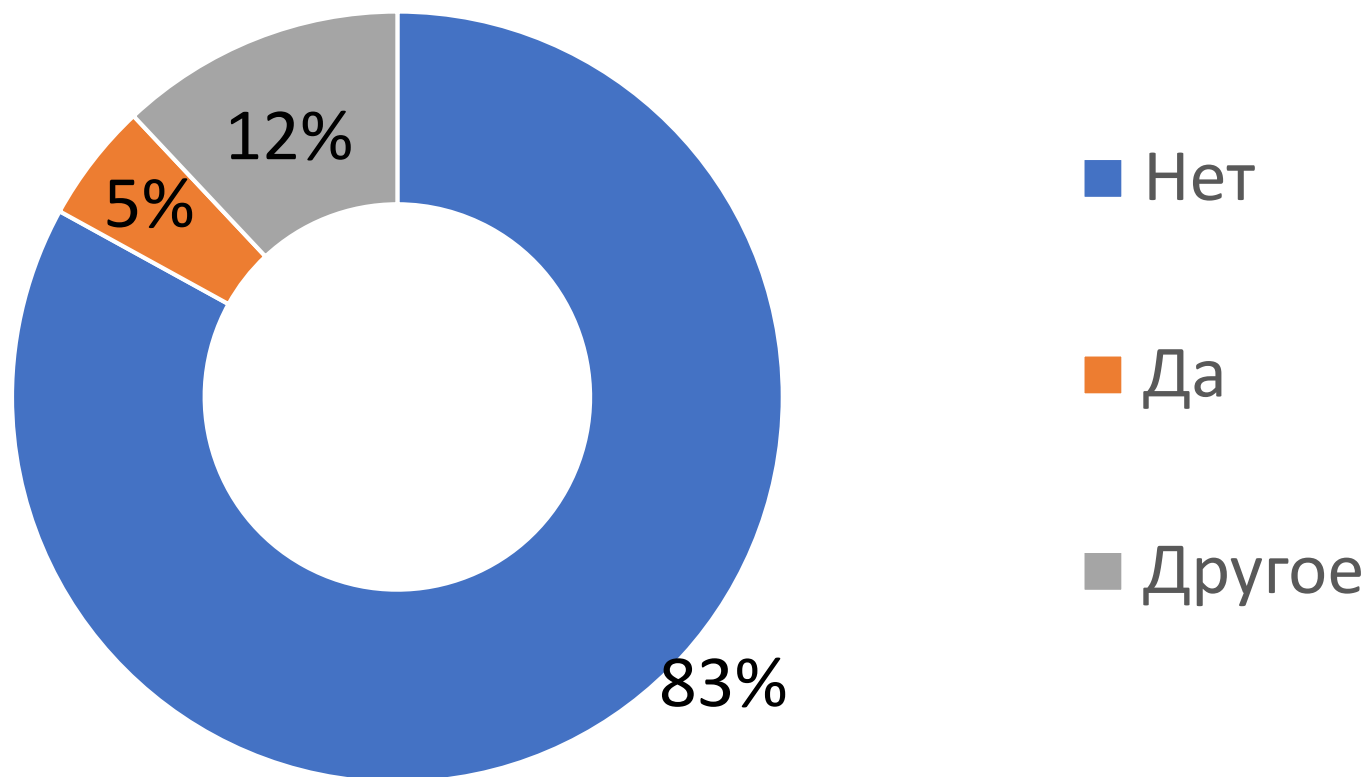


Доля проектов, которые точно состоятся






Столкнулись ли вы с сокращением зарплат, увольнениями, неоплачиваемыми отпусками?





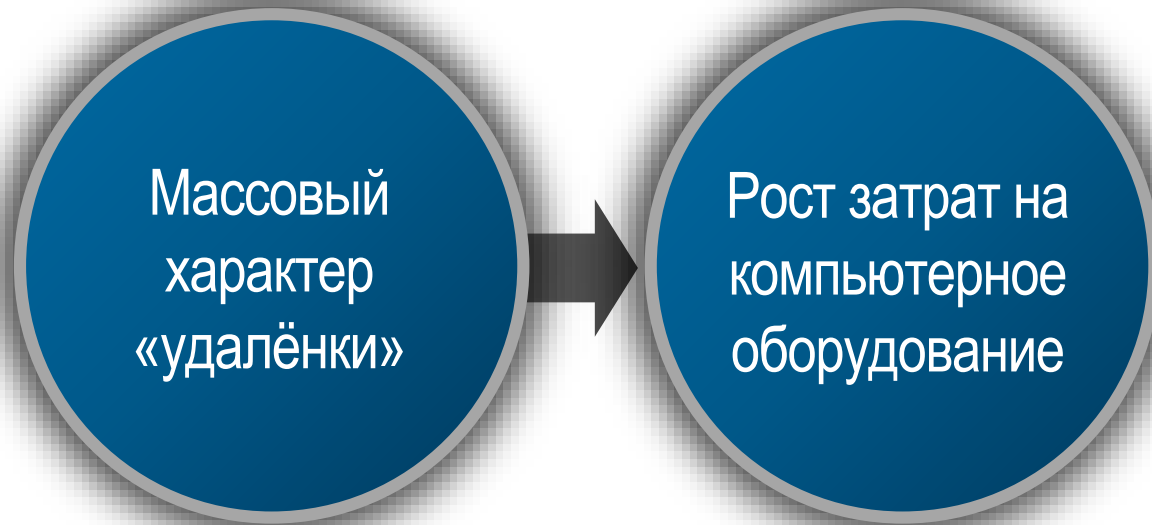
Что нового в «удалёнке» связи с пандемией COVID-19?

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

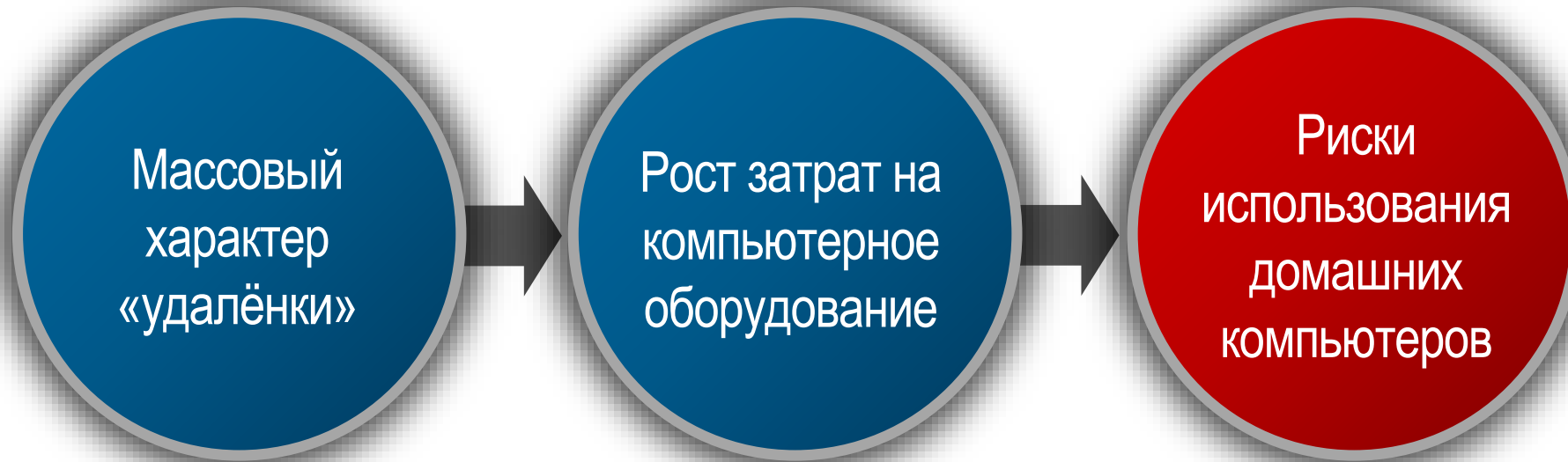


Массовый
характер
«удалёнки»

Переход на удалённую работу
произошёл во многих отраслях



Затраты предприятий на обеспечение удалённой работы значительно выросли



Сотрудники чаще используют домашние компьютеры для работы:

- для пользователя это **удобнее**
- для предприятия это **дешевле**

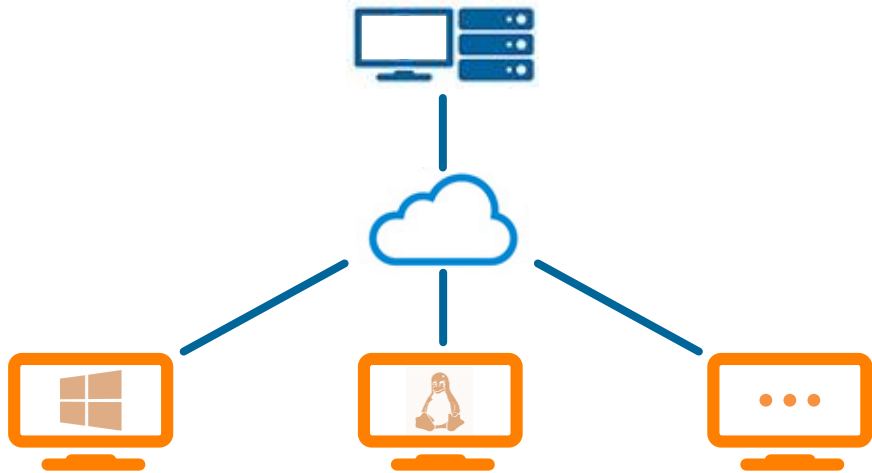


Каким образом пользователи переносят информацию между домашним и рабочим ПК?



Допустимо ли устанавливать СЗИ на домашние компьютеры сотрудников? Как управлять такими СЗИ?

Центр управления



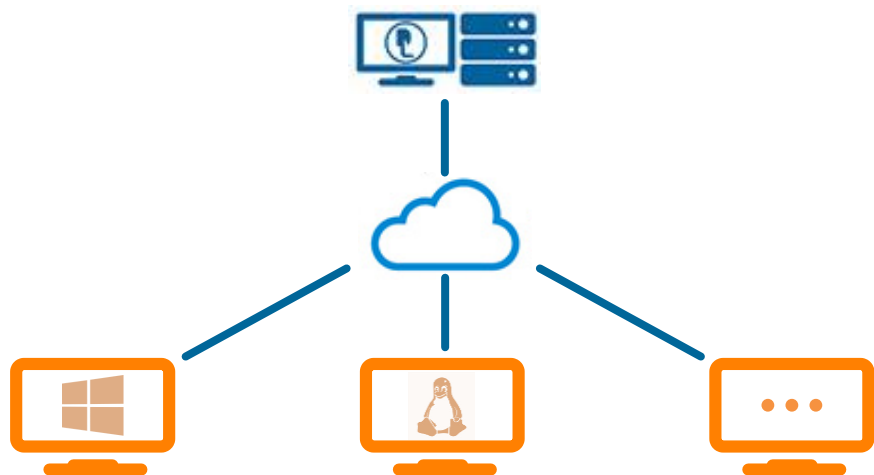
Современные требования к Центру управления информационной безопасностью:

- Работа за NAT (Network Address Translation)
- Управление клиентскими частями под Windows и Linux, поддержка российских ОС
- Обеспечивать бесперебойную работу в больших инфраструктурах и при «слабом» сетевом соединении

Система защиты информации
обязана отвечать новым вызовам

Единый центр управления Dallas Lock

Единый центр управления Dallas Lock



Новое кросс-платформенное решение для централизованного управления ИБ предприятия:







- Работа за NAT
- Управление клиентскими частями под Windows (СЗИ от НСД, МЭ, СОВ, СКН) и Linux (СЗИ от НСД, СКН, МЭ), включая российские ОС
- Не требователен к ресурсам, поддержка работы более 100 тыс. АРМ одновременно

Отвечает новым вызовам

СЗИ от НСД отличаются

УРОВЕНЬ ЗРЕЛОСТИ СЗИ

низкий ←————→ *высокий*

Базовые функции защиты информации от несанкционированного доступа				
Централизованное управление, включая развёртывание				
Наличие сертифицированных модулей в составе системы защиты: СКН, МЭ, СОВ, ...				
Развитые сервисы производителя, включая круглосуточную техническую поддержку				
Дополнительные функции, не входящие в «базовый» набор мер				

СПАСИБО ЗА ВНИМАНИЕ!

Сергей Овчинников

Директор по маркетингу,
Центр защиты информации «Конфидент»

