ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ ДИСТАНЦИОННОЙ РАБОТЫ

Егор Кожемяка

Директор Центра защиты информации «Конфидент»

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

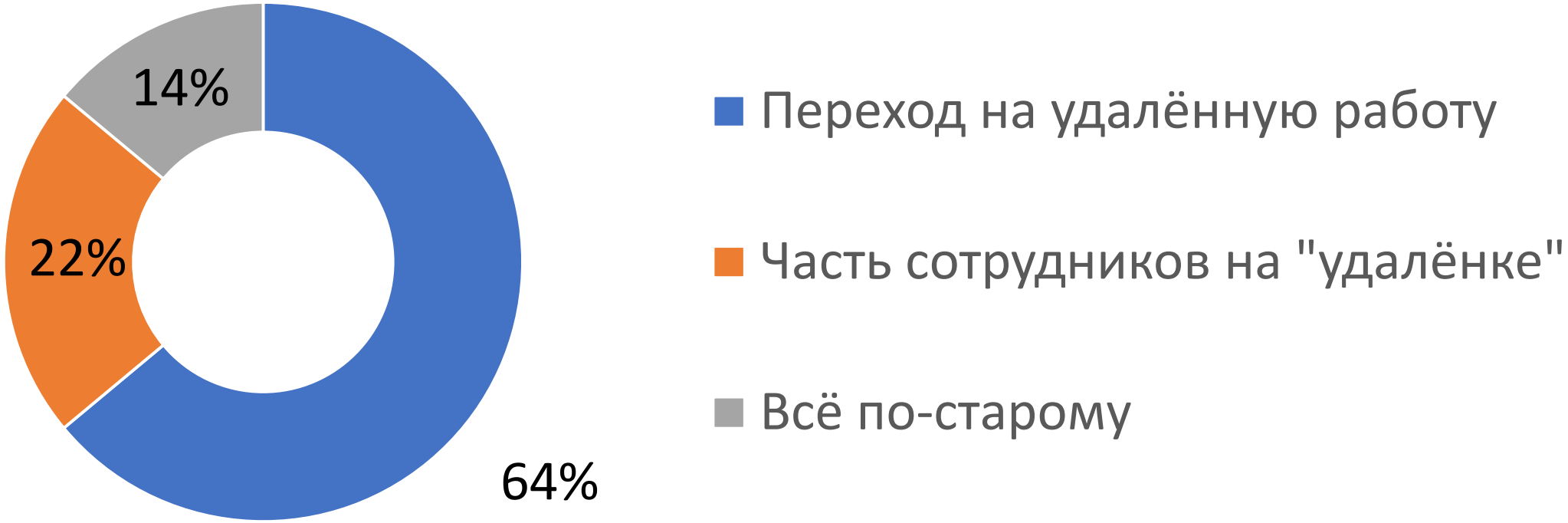
Опросы компаний-интеграторов, специализирующихся на защите информации в госсекторе и входящих в партнёрскую сеть Центра защиты информации ООО «Конфидент», которая насчитывает более 500 компаний.

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

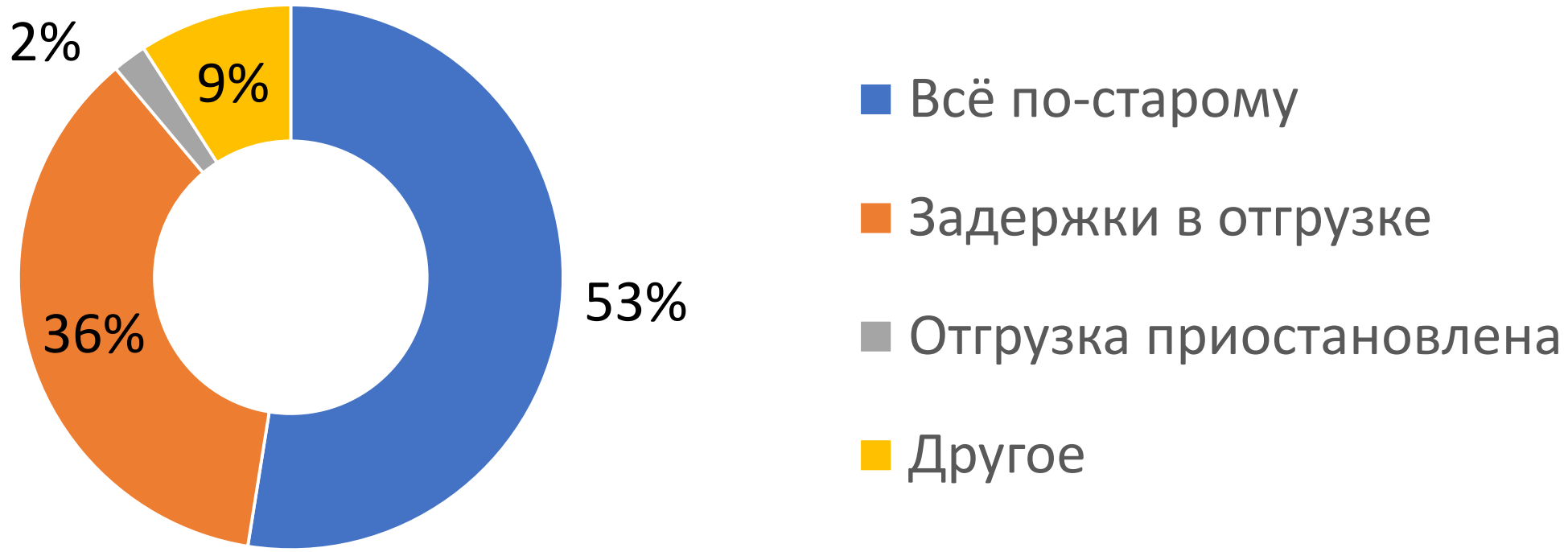
Весна 2020

Январь-февраль 2021

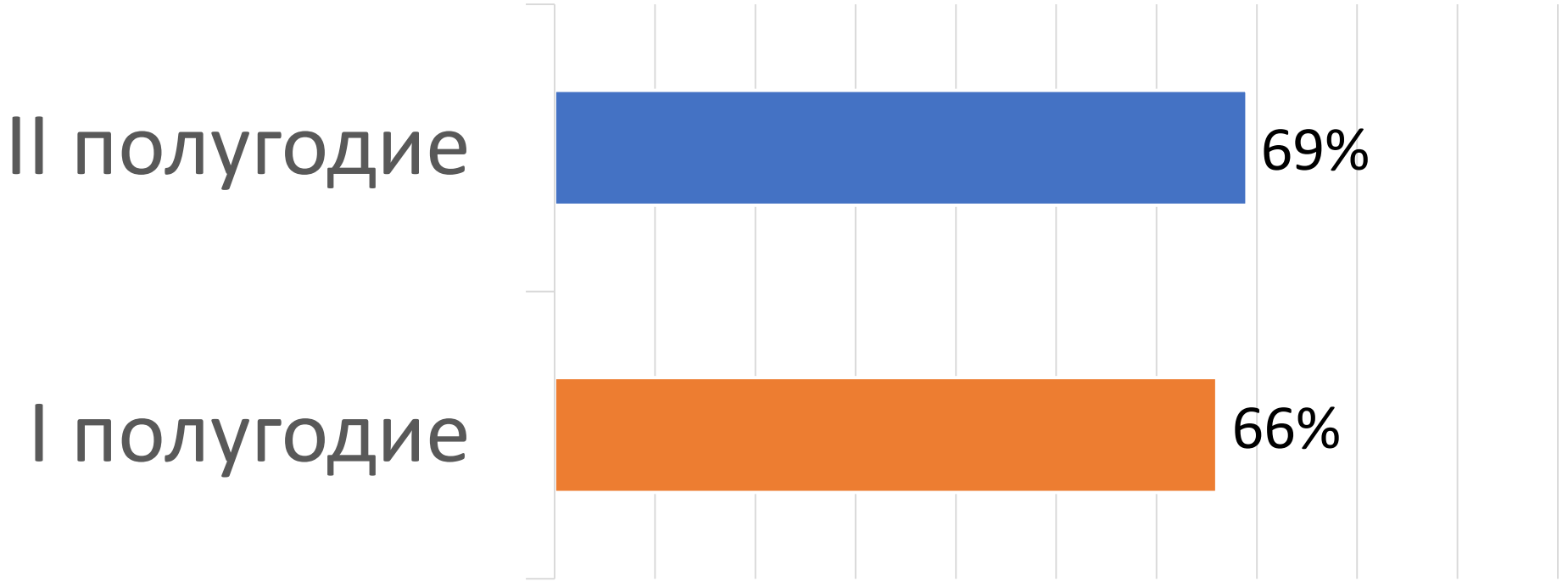
Как изменился режим работы?



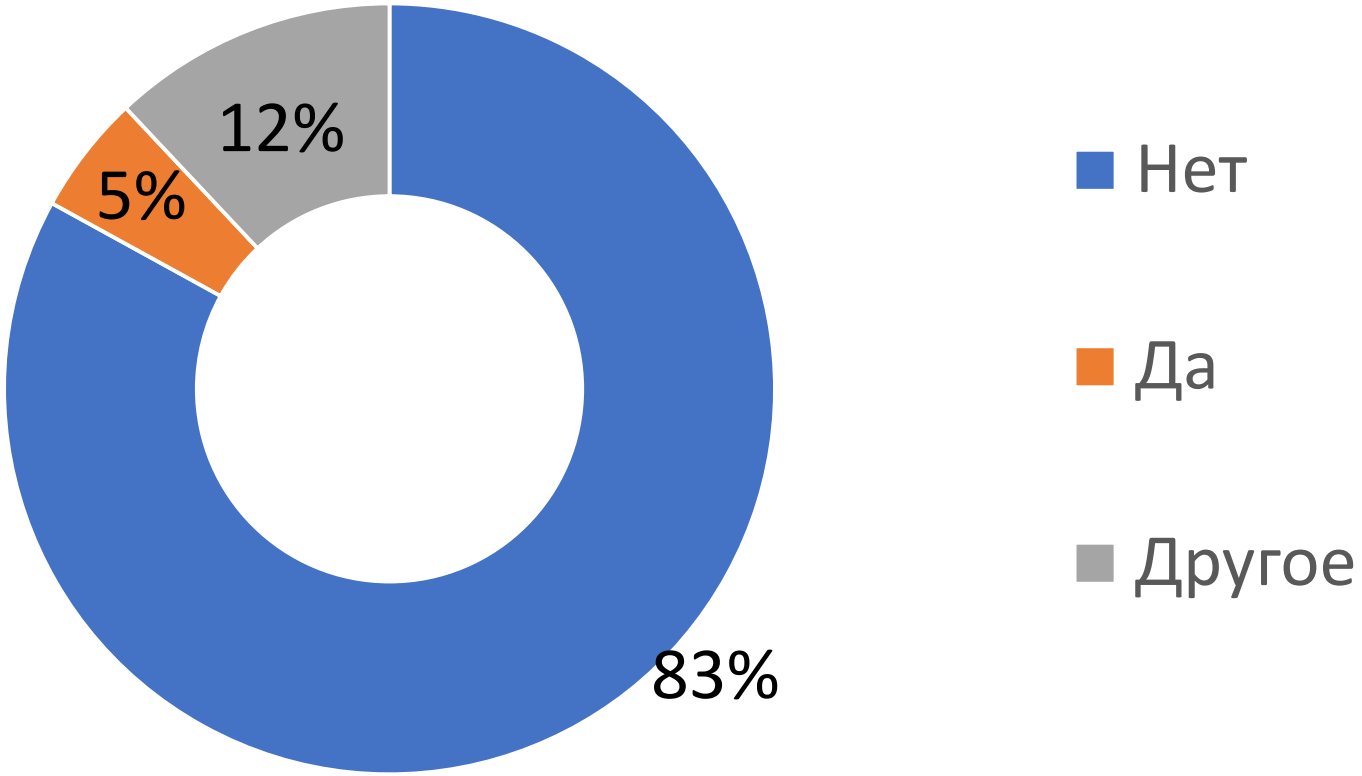
Как осуществляется отгрузка СЗИ?

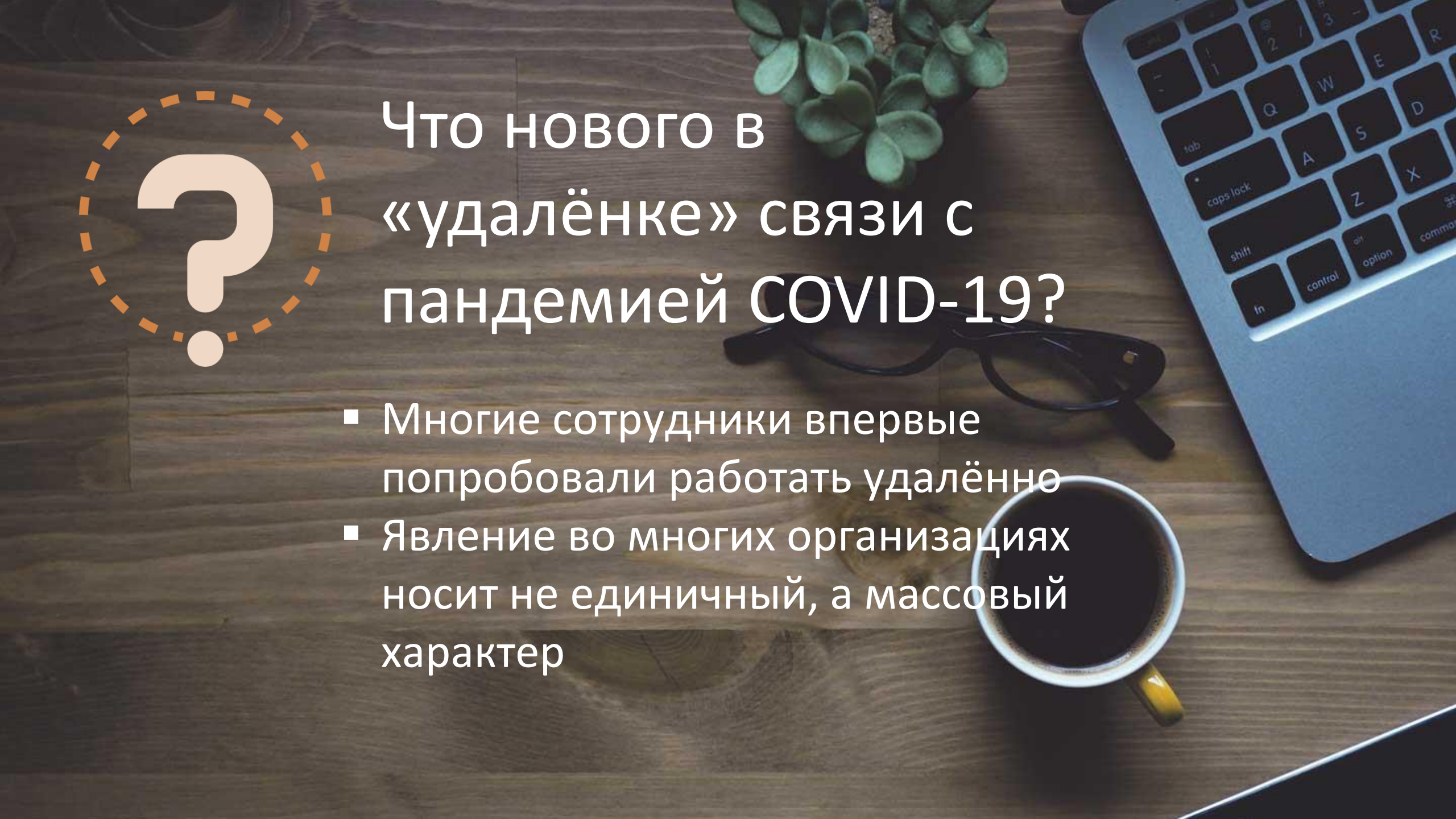


Доля проектов, которые точно состоятся



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



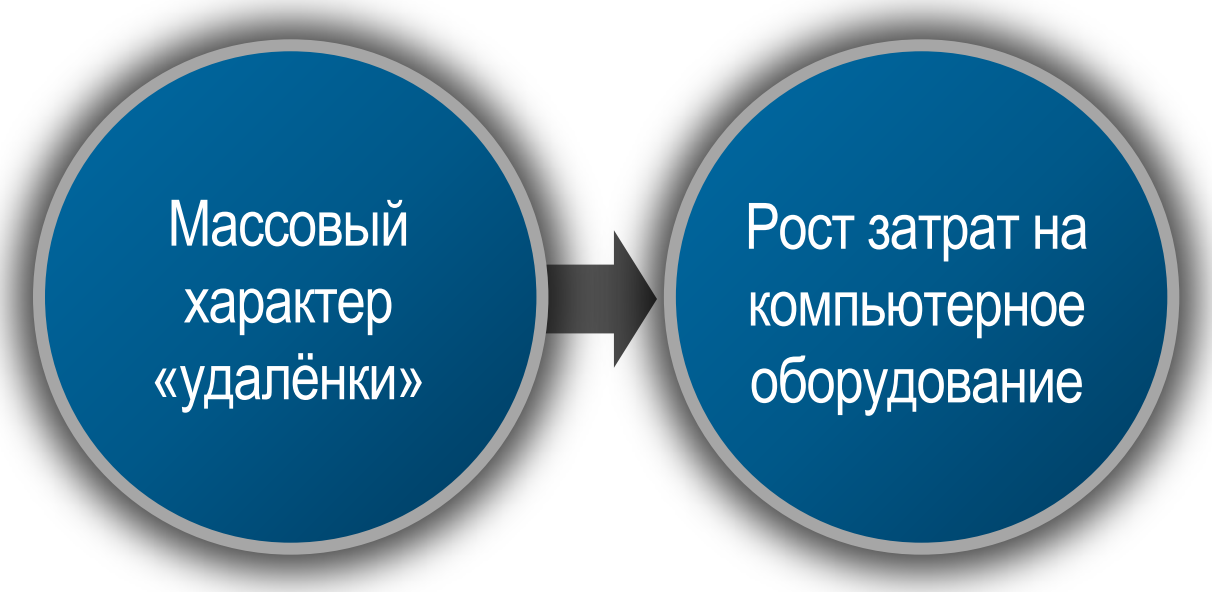


Что нового в «удалёнке» связи с пандемией COVID-19?

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

Массовый характер «удалёнки»

Переход на удалённую работу произошёл во многих отраслях



Затраты организаций на обеспечение удалённой работы значительно выросли

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.

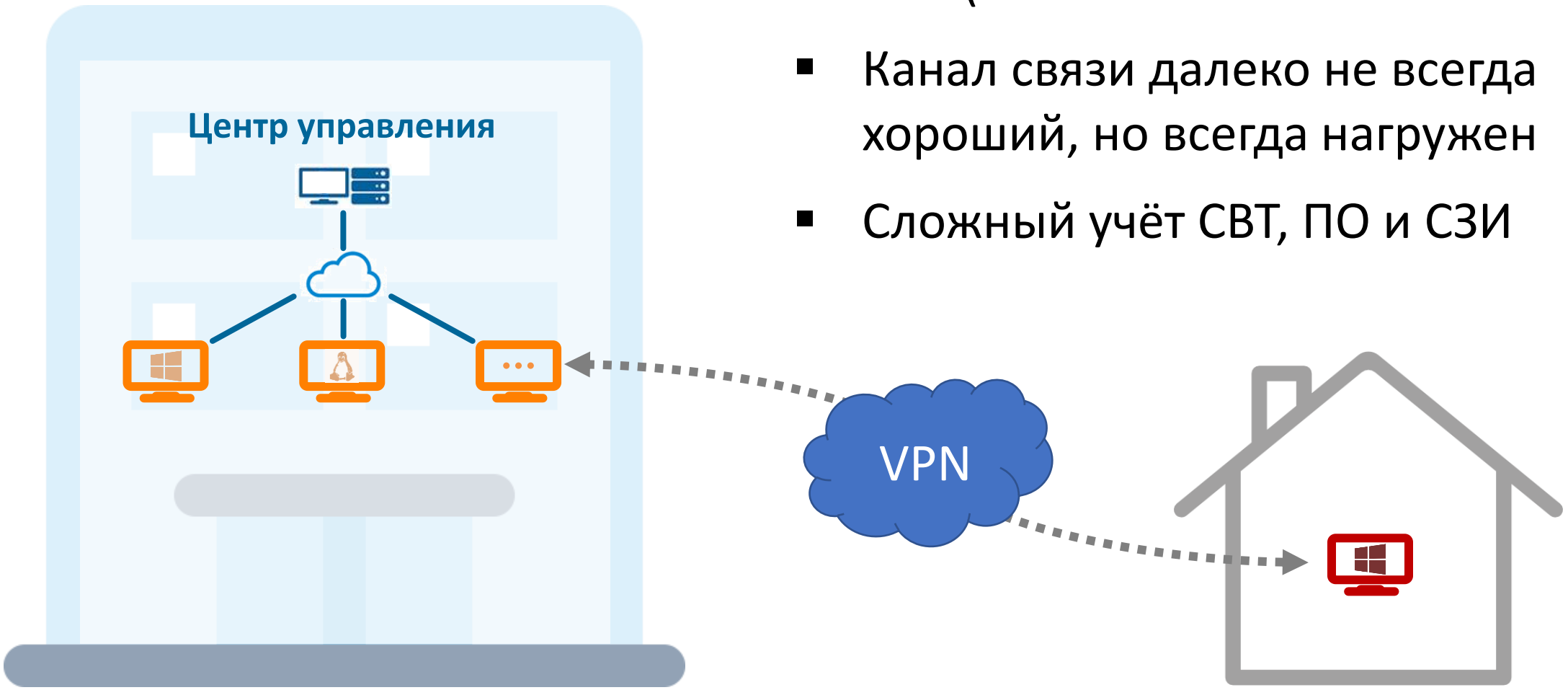
* По результатам опроса партнёров Центра защиты информации ООО «Конфидент», январь-февраль 2021 г.

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

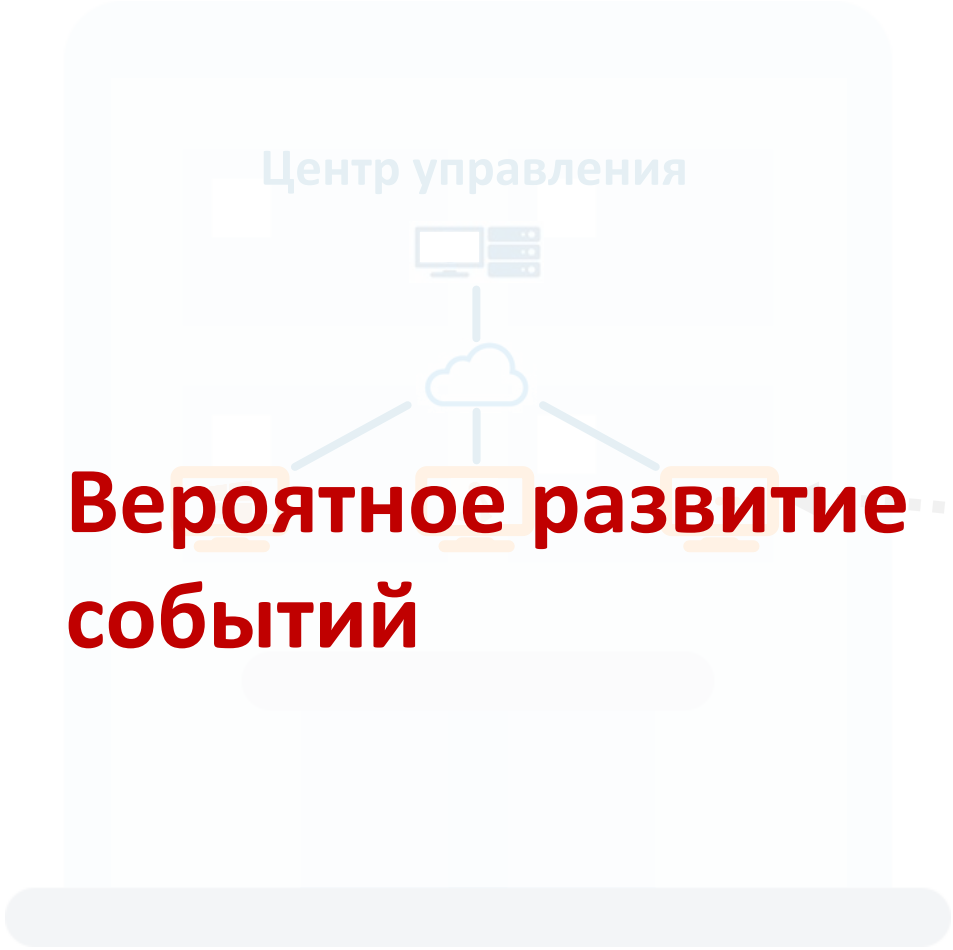
IT-инфраструктура сейчас

- 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



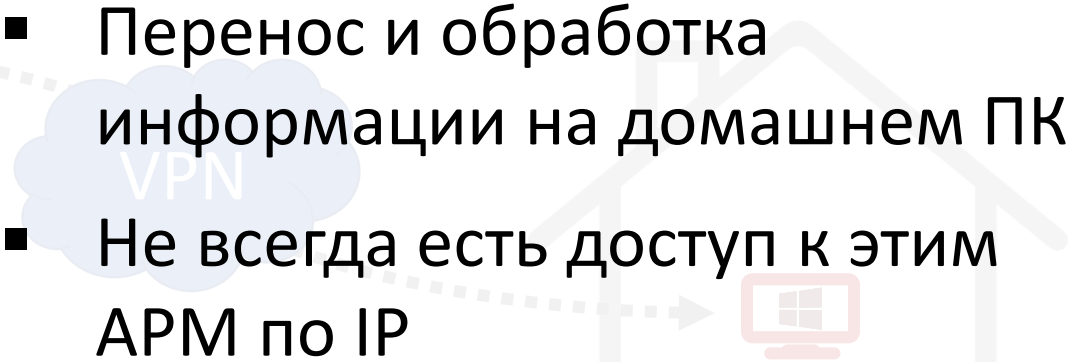
IT-инфраструктура сейчас

- 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

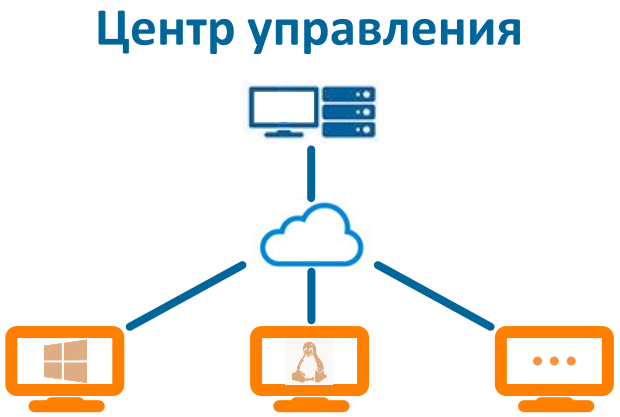


Вероятное развитие событий

- Перенос и обработка информации на домашнем ПК
- Не всегда есть доступ к этим АРМ по IP
- Рост затрат на эксплуатацию ИС



Выводы



1. Неизбежность использования домашних ПК для обработки информации. Правовые основания для работодателей и работников в т.ч. в части установки СЗИ на домашние ПК существуют и описаны в 407-ФЗ.
2. Требования к центру управления информационной безопасностью должны включать:
   - работа в сложных сетевых инфраструктурах
   - управление клиентскими частями под Windows и Linux, поддержка российских ОС
   - бесперебойная работа в больших инфраструктурах и при «слабом» сетевом соединении

СПАСИБО ЗА ВНИМАНИЕ!

Егор Кожемяка

Директор Центра защиты информации «Конфидент»

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ