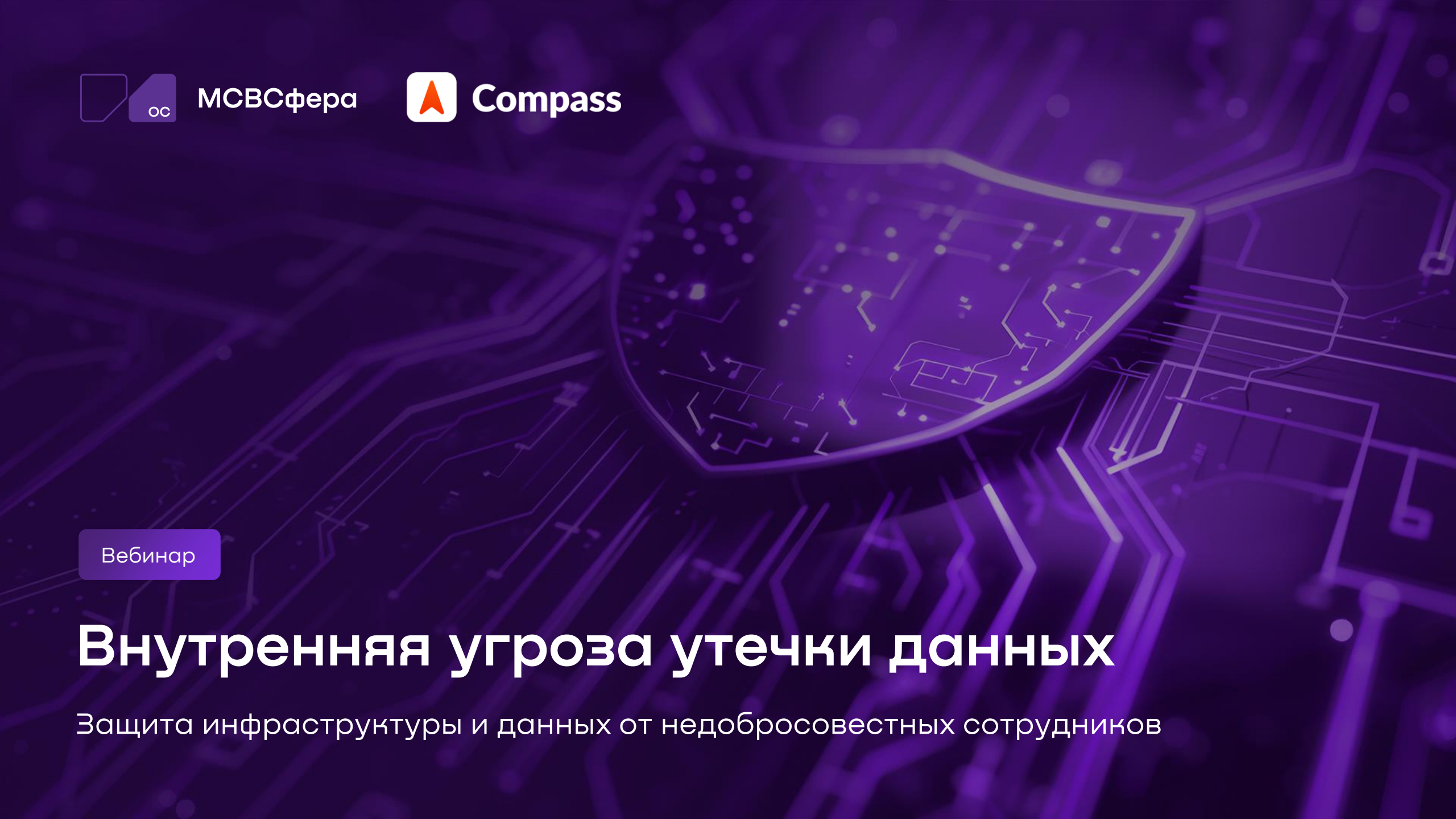

МСВСфера
Compass
Вебинар
Внутренняя угроза утечки данных
Защита инфраструктуры и данных от недобросовестных сотрудников

Спикеры

МСВСфера

Максим Фокин
Директор департамента сертификации
и безопасной разработки «Инферит ОС»

Леонид Кантер
Архитектор ОС «МСВСфера», «Инферит ОС»

Станислав Бондарчук
Руководитель отдела интеграций
корпоративного мессенджера Compass

Угрозы ИБ для бизнеса

Фокин Максим

Директор департамента сертификации и безопасной разработки

Основные риски для бизнеса

МСВСфера

Финансовые риски

Операционные риски

Риски, связанные с ИБ
и утечками данных

Репутационные риски

Юридические
и регуляторные риски

Кадровые риски

Риски, связанные
с конкуренцией

Риски, связанные
с форс-мажорными
обстоятельствами

Основные причины утечки данных

МСВСфера

Человеческий фактор

До 60% инцидентов

Неосторожность сотрудников

Отправка данных не тем адресатам, потеря устройств

Социальная инженерия

Фишинг, мошенничество

Умышленные действия

Кража данных уходящими сотрудниками, саботаж

Основные причины утечки данных

МСВСфера

Внутренние угрозы

30–40% случаев

Злоупотребление доступом

Сотрудники копируют или передают конфиденциальную информацию

Недостаточный контроль доступа

Бывшие сотрудники сохраняют доступ к системам

Основные причины утечки данных

МСВСфера

Внешние кибератаки

20–30% утечек

Взлом корпоративных систем

Через уязвимости в ПО

Компрометация учетных записей

Перехват логинов / паролей

Основные причины утечки данных

МСВСфера

Слабые меры защиты

- Отсутствие шифрования данных
- Неправильная настройка облачных хранилищ
- Отсутствие или недостаточное количество средств защиты информации
- Неправильная конфигурация средств защиты информации
- Отсутствие мониторинга событий безопасности

Статистика утечек

МСВСфера

74%

утечек связаны с человеческим фактором

Verizon DBIR 2023

$4,45 млн (+15% за 3 года).

средняя стоимость утечки

IBM Cost of a Data Breach 2023

54%

компаний сталкивались с утечками из-за действий сотрудников

Ponemon Institute

43%

кибератак направлены на малый и средний бизнес

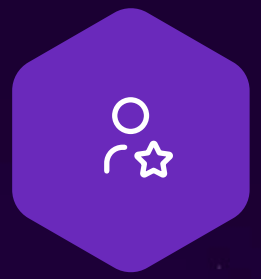
Accenture

МСВСфера

Последствия для бизнеса

Финансовые потери

Штрафы, компенсации, downtime



Репутационный ущерб

Потеря клиентов и партнеров

Юридические риски

152-ФЗ — штрафы от 1% до 3% годового оборота

Общие рекомендации по безопасности

МСВСфера

01. Постоянно проводить обучение сотрудников.

02. Внедрить практику киберучений в компании

03. Внедрить защиту от фишинга и социальной инженерии

04. Организовать принцип минимальных привилегий в информационных системах компании

05. Внедрить практики менеджмента уязвимостей в ПО

Общие рекомендации по безопасности

МСВСфера

06. Организовать постоянный мониторинг событий безопасности

07. Внедрить различные средства защиты информации, направленные на контроль утечек информации

08. Применять в инфраструктуре ПО только от надежных вендоров, обеспечивающих постоянное устранение уязвимостей в ПО, выпуск и доставку до пользователей обновлений

09. Периодически проводить аудиты информационной безопасности

Дополнительные возможности ОС «МСВСфера» для защиты информации

Леонид Кантер

Архитектор ОС «МСВСфера», «Инферит ОС»

МСВСфера

Контроль целостности в Linux

AIDE vs IMA/EVM, Сравнение методов защиты

МСВСфера

Контроль целостности: нормативные требования

01. Стандарт требует обеспечение целостности ОС и ПО (выявление и предотвращение изменений)

02. Контрольная мера А.12.5.1 (ГОСТ Р ИСО/МЭК 27002-2021): контроль системных файлов и библиотек

03. Приказ ФСТЭК №239 (2017), п. 13–14: применение средств контроля целостности в ГИС

04. Приказ ФСТЭК №31 (2014), ЗНИ.6: контроль целостности ПО и данных объектов КИИ

05. Приказ ФСТЭК №17 (2013): выявление нарушений целостности информации и регистрация инцидентов

06. Несоблюдение = риск внедрения вредоносного ПО, подмена сервисов (sshd, systemd), несоответствие требованиям аудита

Контроль целостности: AIDE

МСВСфера

Advanced Intrusion Detection Environment (AIDE)

Утилита для проверки целостности файловой системы

Работает постфактум: сравнение с эталонной базой

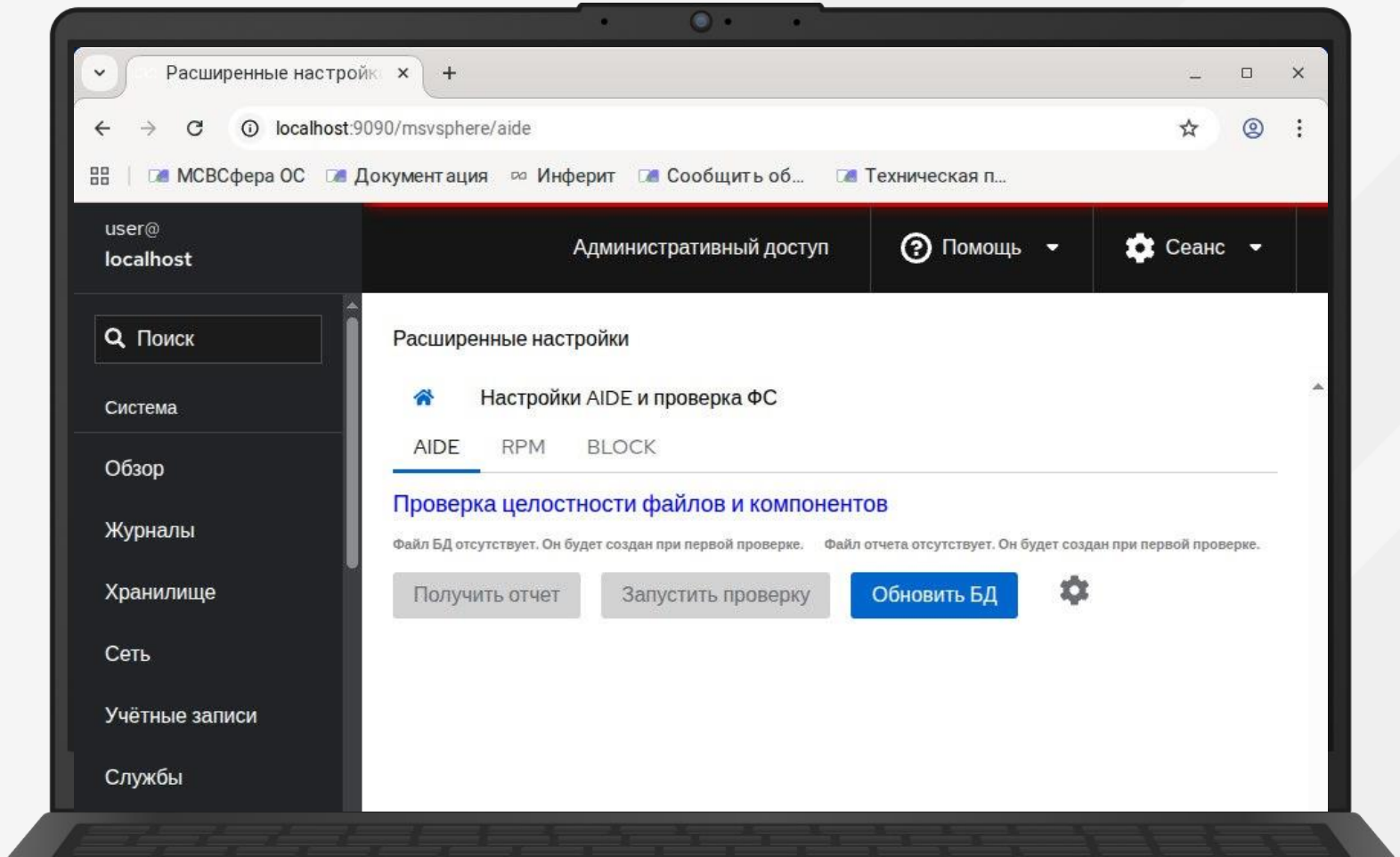
Простая установка и использование (dnf install aide)

Широко применяется в аудитах и расследованиях

Расширение Cockpit для работы с AIDE

МСВСфера

Установка:
dnf install cockpit-msvsphere-security-audit



Ограничения AIDE

МСВСфера

01. Проверки выполняются по расписанию, а не в реальном времени

02. Возможна задержка между атакой и её обнаружением

03. Злоумышленник может изменить базу AIDE

04. Не предотвращает запуск изменённых бинарников

Integrity Measurement Architecture (IMA)

МСВСфера

Вычисляет хеш файлов при каждом обращении

Хранит эталонные значения в расширенных атрибутах (xattr)

Запрещает выполнение при несовпадении

Записывает результаты в журнал ядра

Extended Verification Module (EVM)

МСВСфера

Подписывает метаданные файлов (права, SELinux-метки, владельцы)

Проверяет неизменность метаданных при доступе

Защищает систему от обхода IMA через изменение атрибутов

МСВСфера

Как работают вместе?

IMA

проверяет содержимое файлов

EVM

контролирует метаданные

Вместе блокируют запуск подменённых бинарников и изменение критичных атрибутов

МСВСфера

Практическое применение

Предотвращает запуск подменённых сервисов (например, sshd)

Защита от модификации системных библиотек

Основа доверенной загрузки вместе с Secure Boot и TPM

Используется в банках, госструктурах, ЦОД

Особенности использования IMA/EVM

МСВСфера

Настройка политики (/etc/ima/policy)

Требует поддержки в ядре и файловой системе (ext4, XFS)

Возможны накладные расходы на производительность

Обычно включается в «жёстких» профилях безопасности

Сравнение AIDE vs IMA/EVM

МСВСфера

AIDE

- Уровень: пользовательское приложение
- Проверка: по расписанию (постфактум)
- Простая установка и настройка
- Подходит для аудита и расследований

IMA/EVM

- Уровень: ядро ОС
- Проверка: в реальном времени
- Более сложная настройка
- Используется в системах с высокими требованиями безопасности

МСВСфера

Обновления в Linux

Почему, как и когда обновлять систему

Почему обновления критичны

МСВСфера

В среднем исправляется

60–100 CVE ежемесячно

Из них 5-10 критические

(ядро, glibc, OpenSSL, sudo, polkit)

Примеры громких уязвимостей

- Polkit (CVE-2021-3560) — root без пароля
- Sudo (CVE-2021-3156, Baron Samedit)
- glibc GHOST (CVE-2015-0235) — RCE
- Dirty COW (CVE-2016-5195) — привилегии
- Shellshock (CVE-2014-6271) — массовые атаки

МСВСфера

Требования ГОСТ Р ИСО/МЭК 27001-2021

01. Стандарт требует своевременной установки обновлений безопасности

02. Контрольная мера A.12.6.1: управление техническими уязвимостями

03. Контрольная мера A.12.6.2: использование только поддерживаемого ПО

04. Конкретные сроки (обычно 10–30 дней для критических уязвимостей)

05. Несоблюдение = риск компрометации и несоответствия требованиям аудита

Автоматические обновления

МСВСфера

Каждый компьютер обновляется из каналов вендора

PackageKit (GUI) или dnf-automatic (CLI)

Плюсы

Быстро закрываются уязвимости

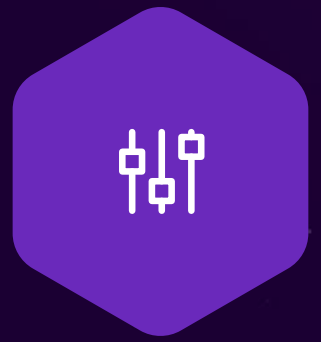
Минусы

- Риск внезапной перезагрузки
- Нет тестирования совместимости
- Не подходит для критичных сервисов

Контролируемые обновления

МСВСфера

Создание локального зеркала репозиториев (reposync + createrepo)



Тестирование обновлений на стенде

Распространение через HTTP/NFS

Массовая установка средствами Ansible (модуль dnf/yum)

Сравнение подходов

МСВСфера

Автоматические обновления

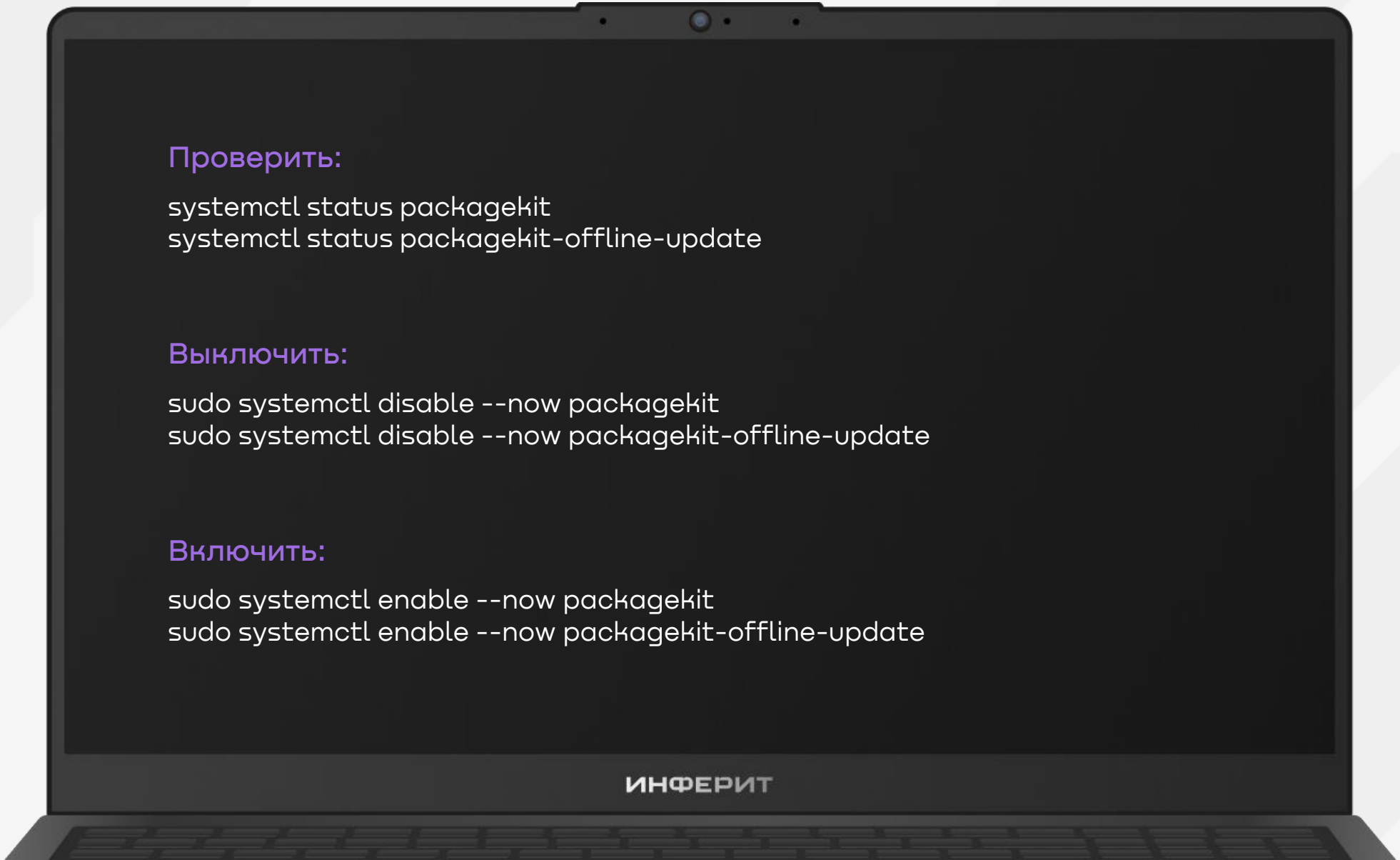
- Самостоятельная установка на каждом хосте
- Быстрая реакция на уязвимости
- Выше риск поломки ПО

Контролируемые обновления

- Централизованное управление (локальный репо + Ansible)
- Тестирование снижает риск сбоев
- С задержкой по сравнению с автообновлением

Управление через PackageKit

МСВСфера



Проверить:

systemctl status packagekit
systemctl status packagekit-offline-update

Выключить:

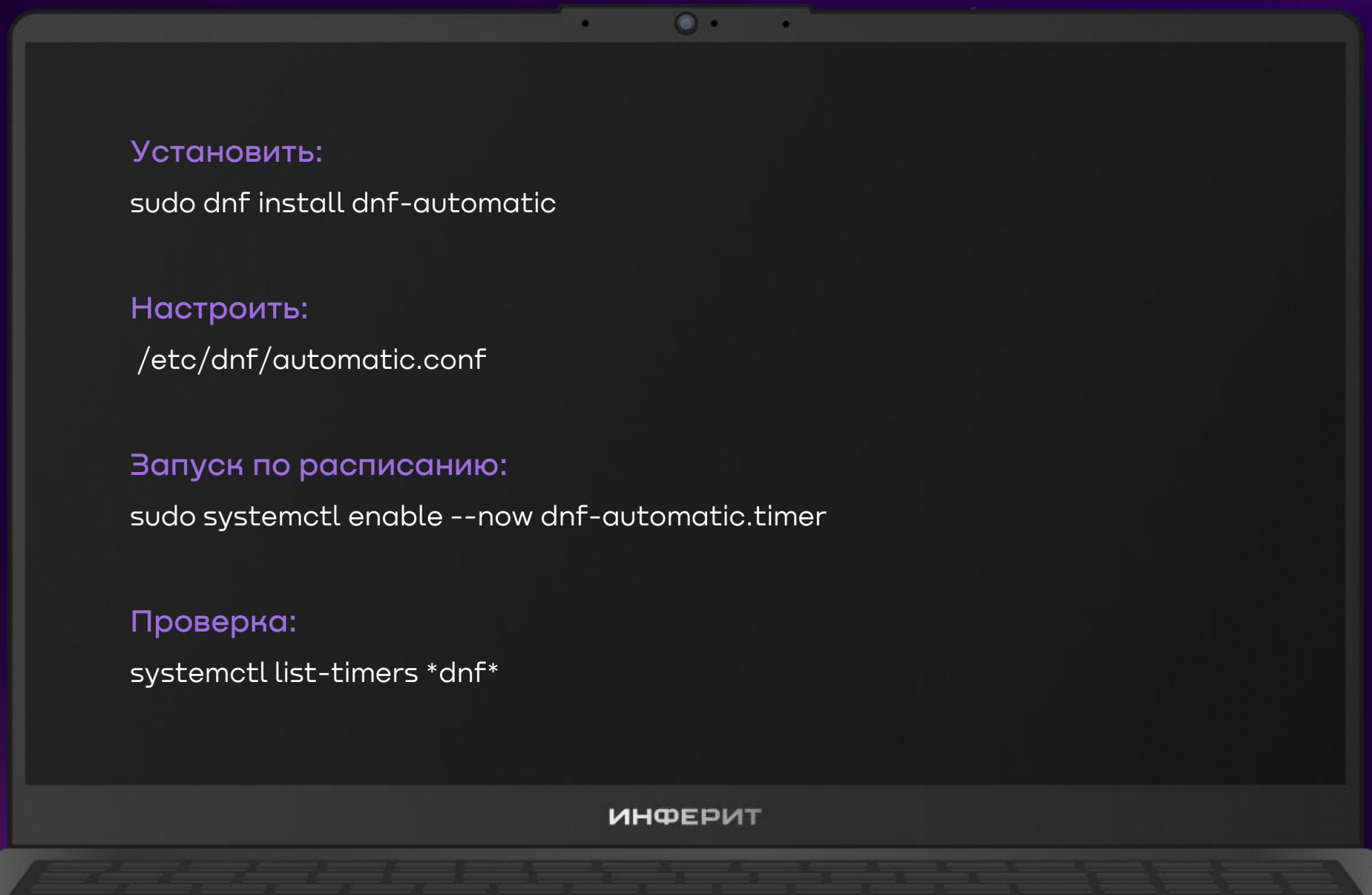
sudo systemctl disable --now packagekit
sudo systemctl disable --now packagekit-offline-update

Включить:

sudo systemctl enable --now packagekit
sudo systemctl enable --now packagekit-offline-update

Управление через dnf-automatic

МСВСфера



Установить:

sudo dnf install dnf-automatic

Настроить:

/etc/dnf/automatic.conf

Запуск по расписанию:

sudo systemctl enable --now dnf-automatic.timer

Проверка:

systemctl list-timers *dnf*

Регуляторные требования к USB-устройствам

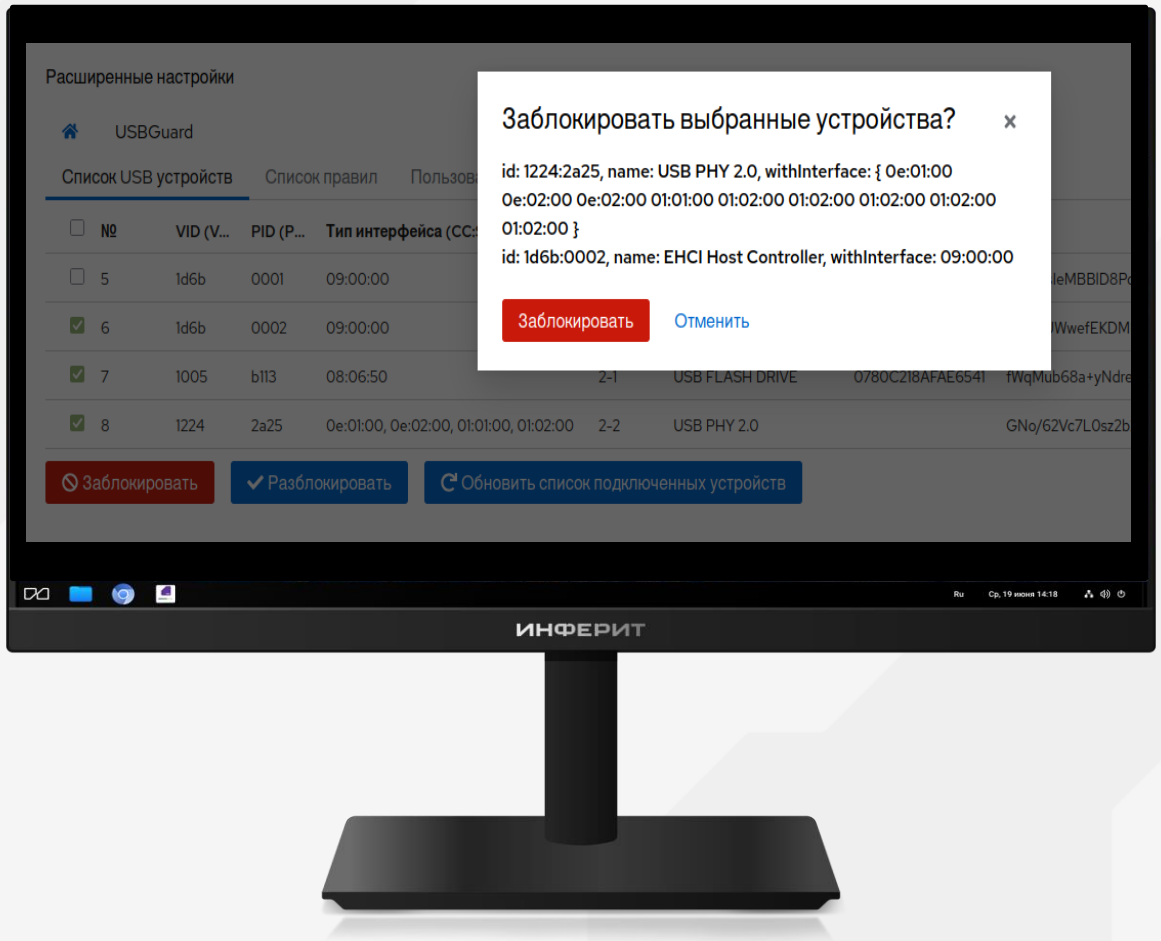
МСВСфера

ФСТЭК (Приказ №31, раздел ЗНИ.7): обязательный контроль съемных носителей, включая USB

ГОСТ Р ИСО/МЭК 27002: управление и ограничение использования внешних носителей, пункт 8.3.1 "Управление съемными носителями информации":

"Съемные диски разрешается использовать только в случаях, обусловленных потребностями бизнеса"

Практическая реализация: USBGuard (МСВСфера ОС + Cockpit)



- USBGuard через Cockpit управляет доступом по белым/чёрным спискам
- Установка: sudo dnf install cockpit-msvsphere-usbguard
- Запуск: sudo systemctl enable --now usbguard.service

МСВСфера

Создание образов ОС

Image Builder (composer-cli) vs Kickstart

Что такое composer-cli (Image Builder)

МСВСфера

Инструмент для создания кастомных образов ОС

Поддерживает вывод в ISO, qcow2, raw, tar, AMI, VHD и др.

Включает пакеты, конфигурацию и учетные записи

Обеспечивает одинаковую среду на всех серверах и VM

Полностью поддерживается в RHEL и совместимых дистрибутивах

Kickstart vs Image Builder

МСВСфера

Kickstart

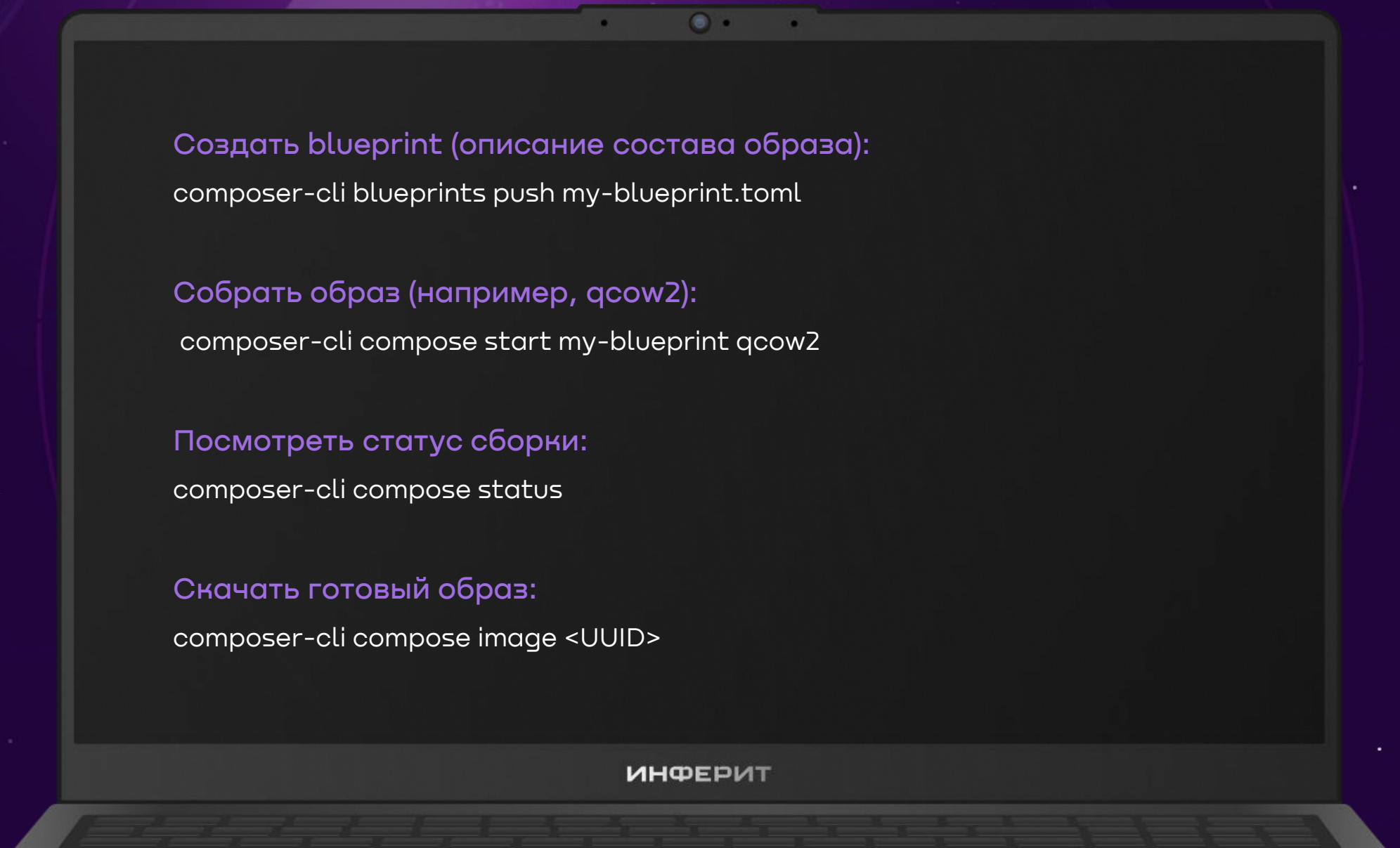
- Автоматизирует установку через Anaconda
- Скачивает пакеты из репозитория при установке
- Подходит для bare metal серверов

Image Builder (composer-cli)

- Создает готовый образ системы
- Запускается как есть, без отдельного процесса установки
- Быстрее и надежнее для облаков и массового развертывания

Пример использования composer-cli

МСВСфера



Создать blueprint (описание состава образа):

composer-cli blueprints push my-blueprint.toml

Собрать образ (например, qcow2):

composer-cli compose start my-blueprint qcow2

Посмотреть статус сборки:

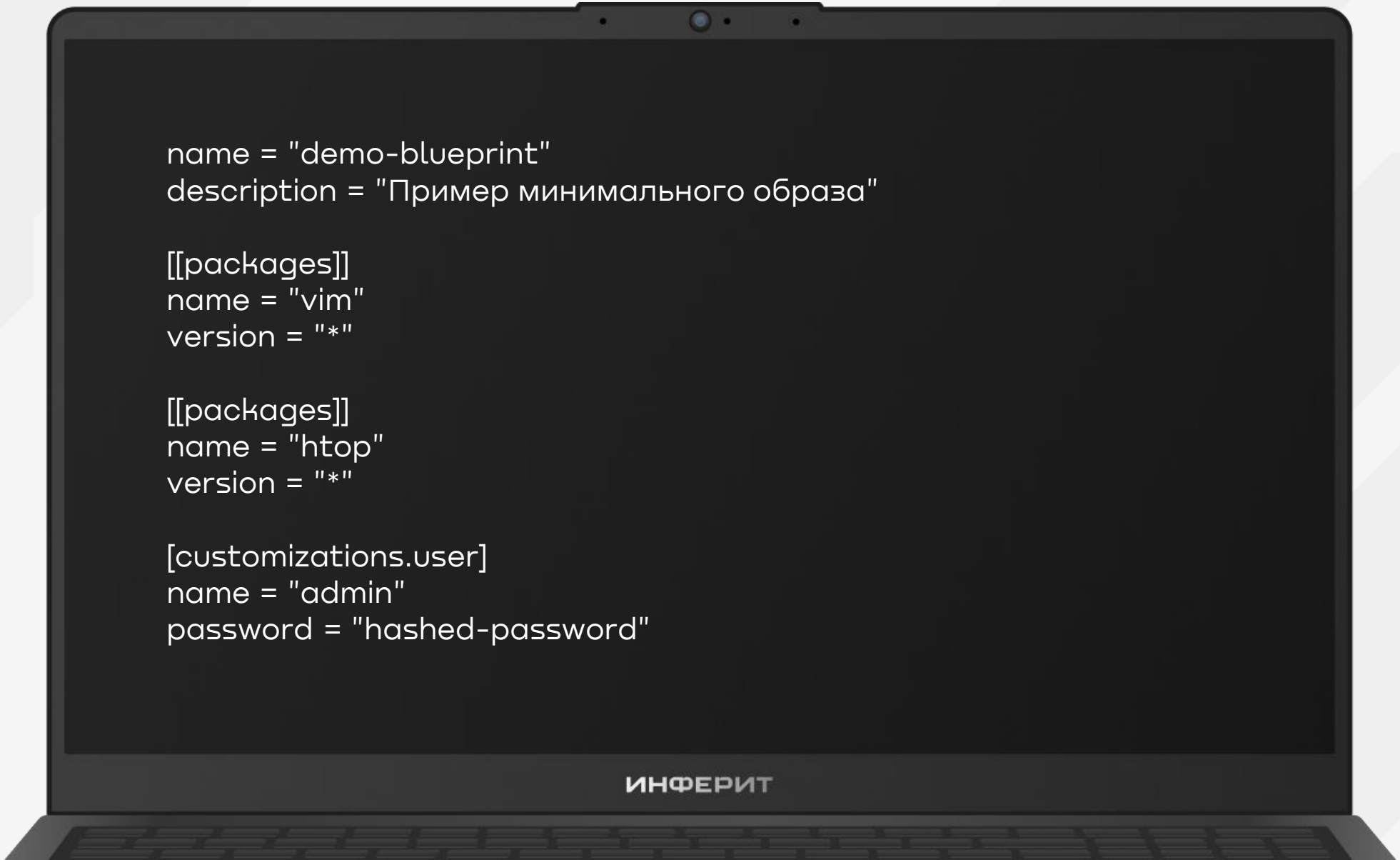
composer-cli compose status

Скачать готовый образ:

composer-cli compose image <UUID>

Пример blueprint TOML (минимальный)

МСВСфера



МСВСфера

Спасибо за внимание!

Если вы заинтересованы в сотрудничестве с «Инферит ОС», хотите обсудить проект и узнать больше о нашей операционной системе, мы будем рады помочь

msvsphere-os.ru

msvsphere@inferit.ru

8 800 707-85-53

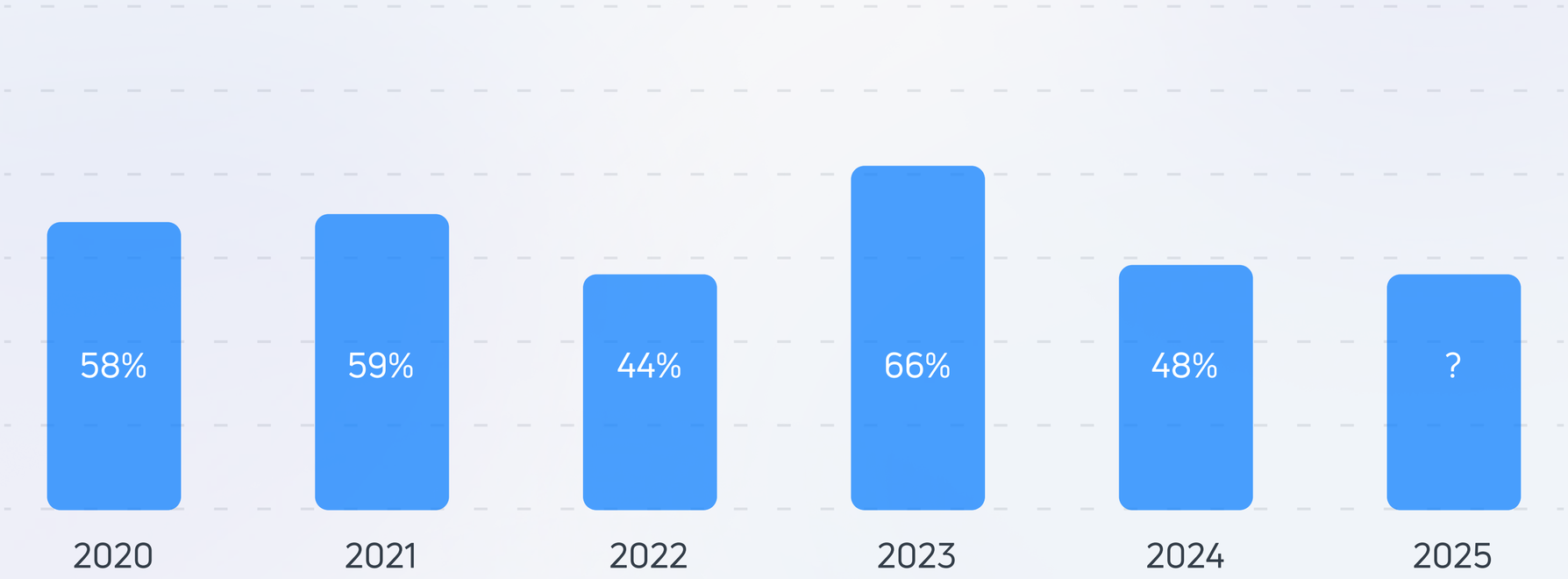
COMPASS

МСВСфера

Внутренняя угроза утечки данных: защита инфраструктуры и данных от недобросовестных сотрудников

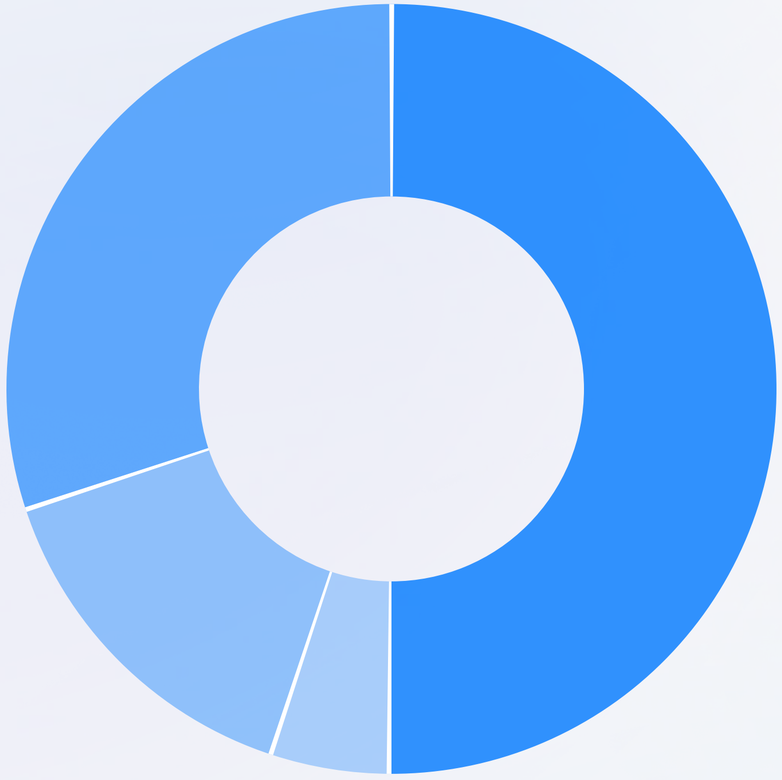
Статистика инцидентов, практические кейсы и инструменты защиты

Сколько компаний сталкиваются с утечками данных



Исследование SearchInform: из 1000 опрошенных компаний
половина фиксирует утечки по вине сотрудников

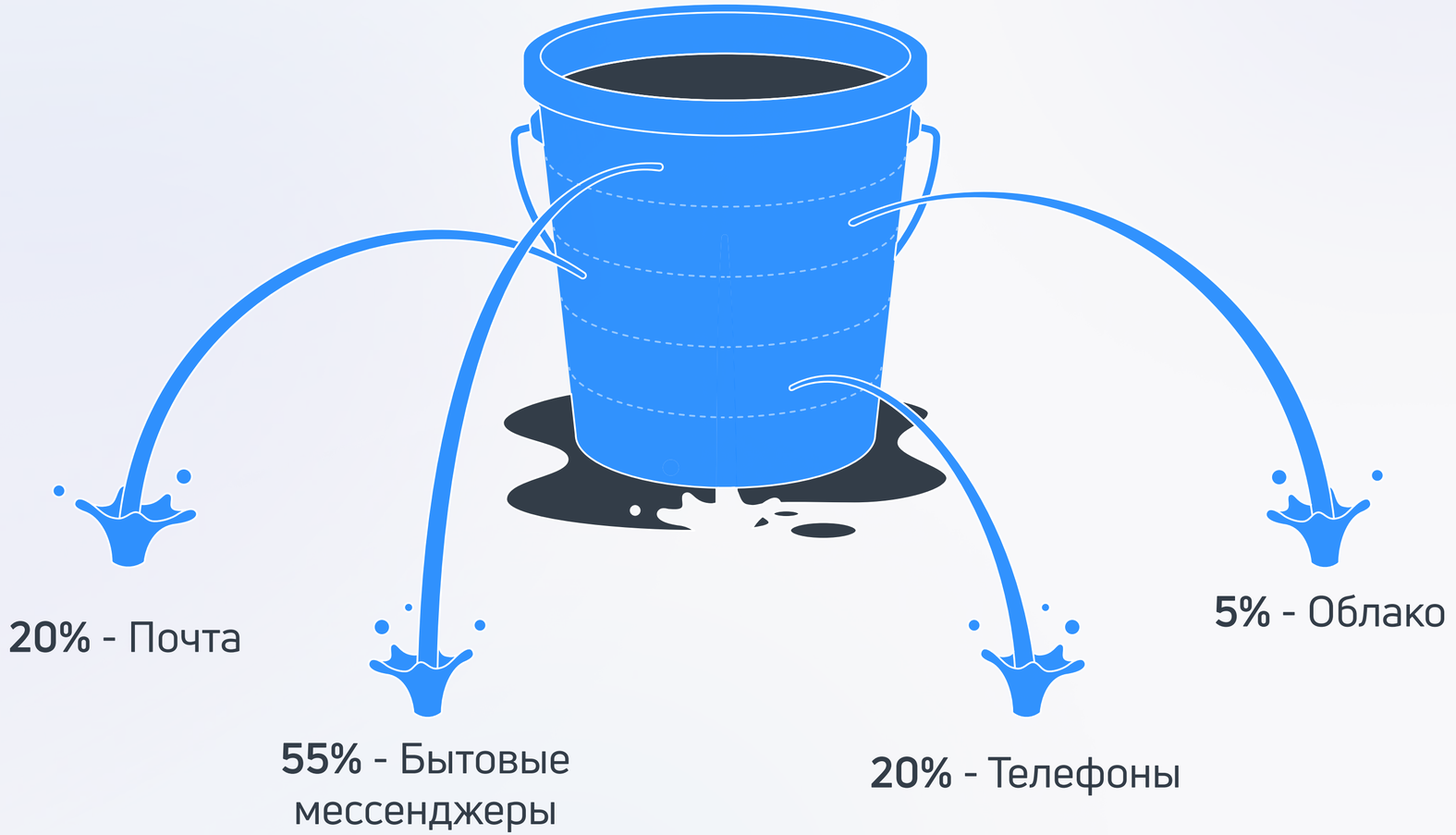
Какие данные утекают



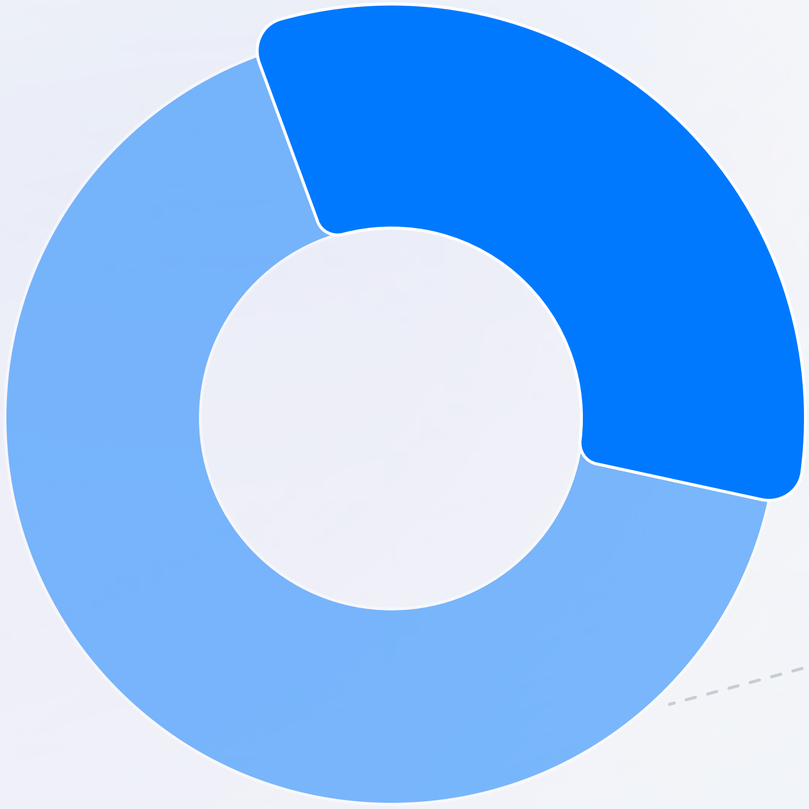
- **50%** – Клиенты и сделки
- **30%** – Персональные данные сотрудников
- **15%** – Техническая документация
- **1-5%** – Другие данные

Портрет нарушителя

Каналы утечек



Случайно или намеренно?



33% - умышленно

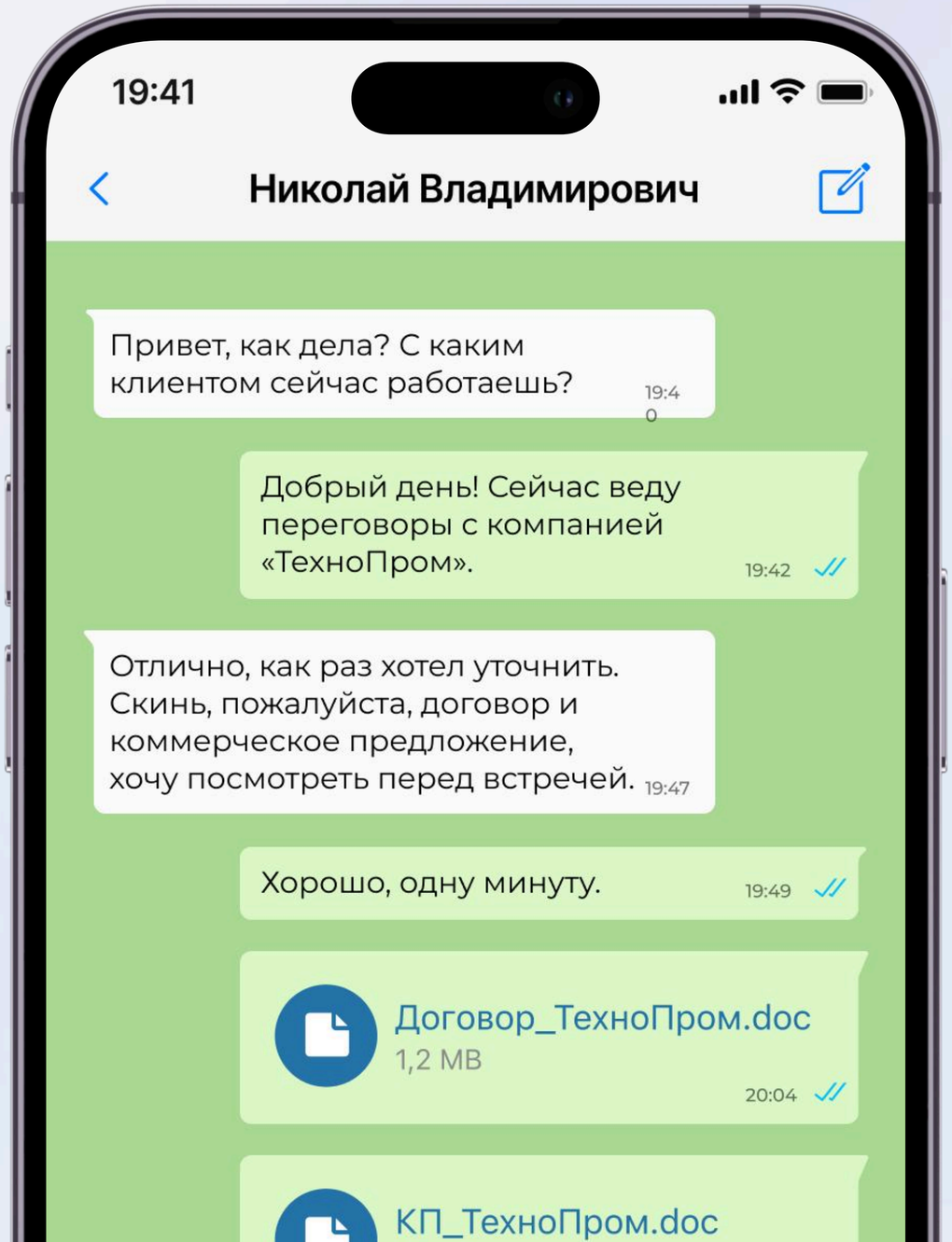
67% - случайно

В большинстве случаев сотрудники сами становятся жертвами злоумышленников и подставляют компанию

Как утекают данные бизнеса

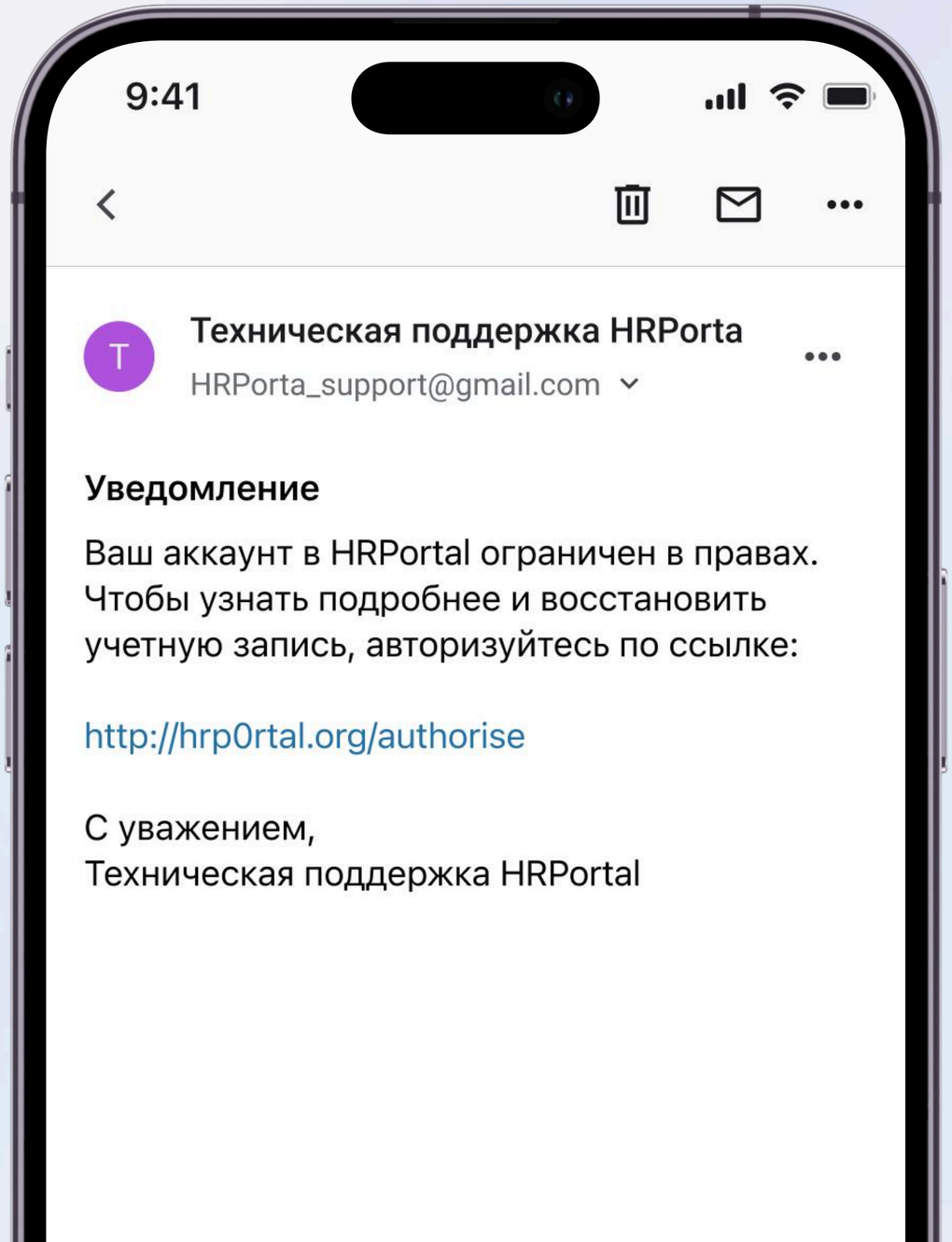
Fake Boss в WhatsApp и Telegram

1. Подделывают профиль руководителя, вплоть до фотографий и имени пользователя.
2. Находят сотрудника компании, который может «слить».
3. Пишут ему с фейкового профиля, убеждая в том, что сотрудник общается с руководителем.
4. С помощью поддельного кружочка или голосового могут вынудить отправить информацию или перевести деньги на левые реквизиты.



Spearfishing

1. Находят первых лиц, руководителей или сотрудников компании.
2. Изучают привычки, какими сервисами пользуется.
3. Вынуждают перейти по фишинговой ссылке.
4. Получают доступ к аккаунту и данным внутри него.



Как еще может утечь информация

Сотрудник **скачивает себе важные файлы** и они остаются у него навсегда

Сотрудник **продает данные** конкурентам за вознаграждение

Сотрудник **переходит по ненадежным ссылкам** и теряет доступ к аккаунтам

Сотрудник по ошибке отправляет файлы **«не в тот чат»**

Как с этим бороться

Общие методы

- ✓ Прописать правила поведения в цифровом пространстве и коммуникации в компании
- ✓ Регулярные тренинги и аудиты безопасности от офицеров ИБ

Технические

- ✓ Отказаться от Telegram и WhatsApp в пользу защищенных корпоративных сервисов
- ✓ Внедрить DLP-систему – она в реальном времени мониторит, как и куда двигается информация
- ✓ Обработка данных на собственном сервере и контроль доступов к информации

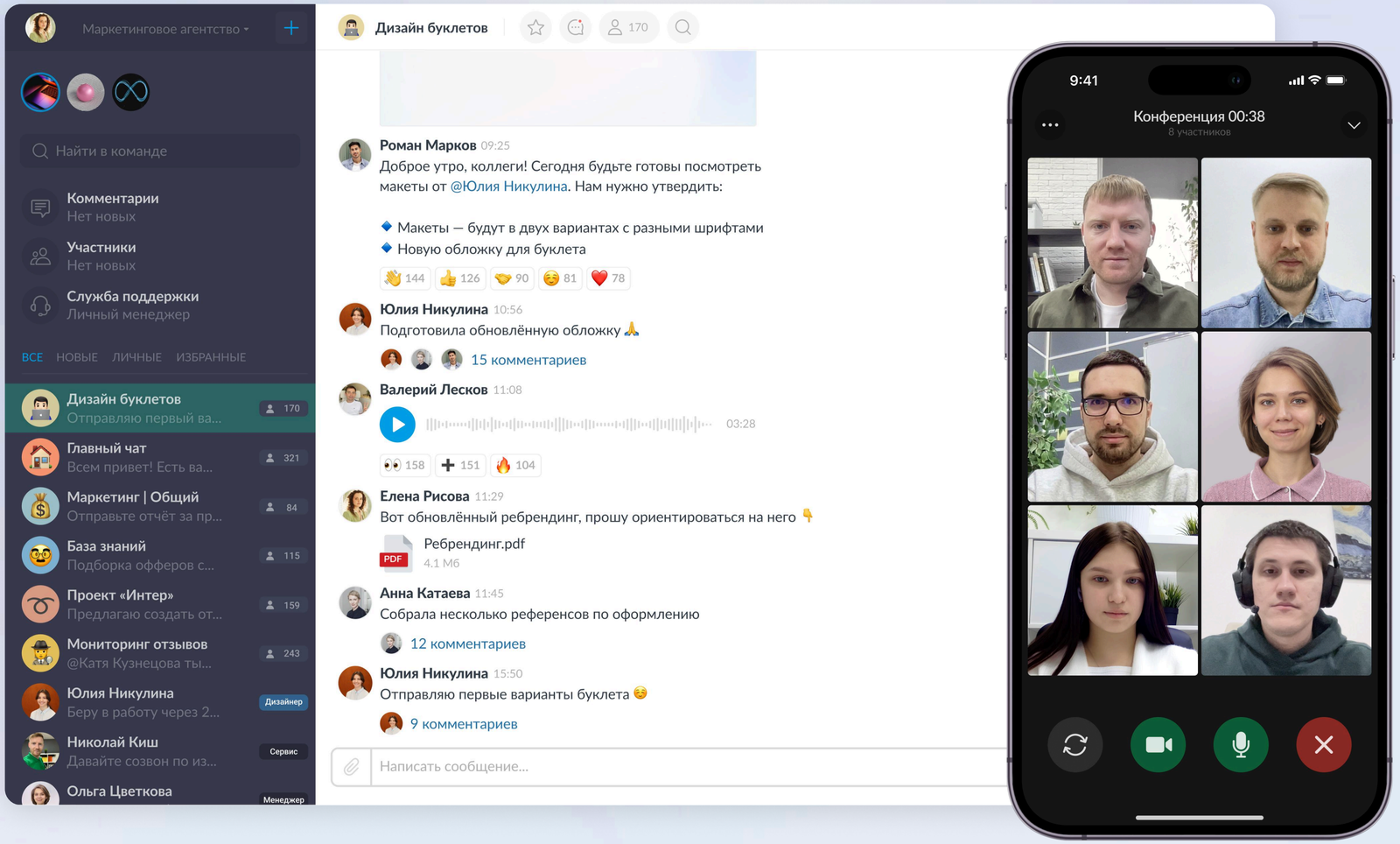
Защита информации, контроль доступов и обработка данных на собственном сервере

Compass — безопасный и быстрый корпоративный мессенджер

- В реестре российского ПО
- Интеграция с AD и LDAP
- Шифрование данных

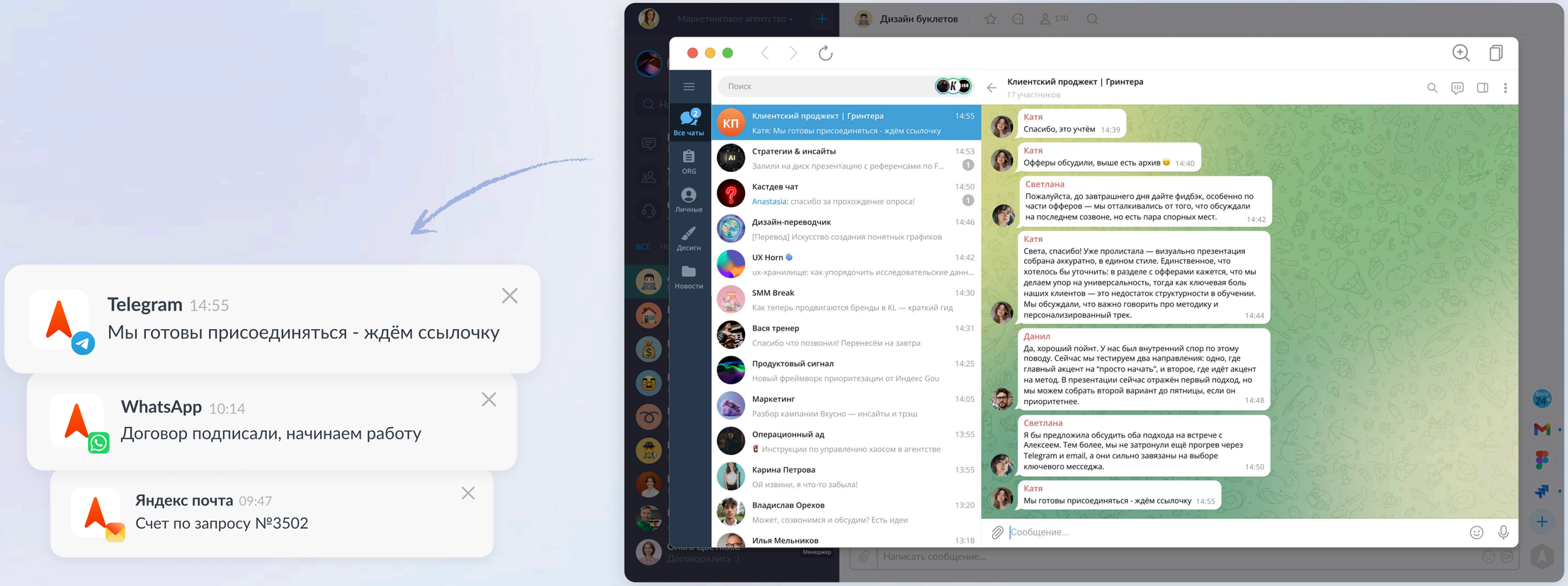
Корпоративный мессенджер и видеоконференции

iOS | Android | Windows | MacOS | Ubuntu | Debian | Astra Linux | RED OS | ALT Linux | МСВСфера | UBLinux | Manjaro



Compass Smart Apps

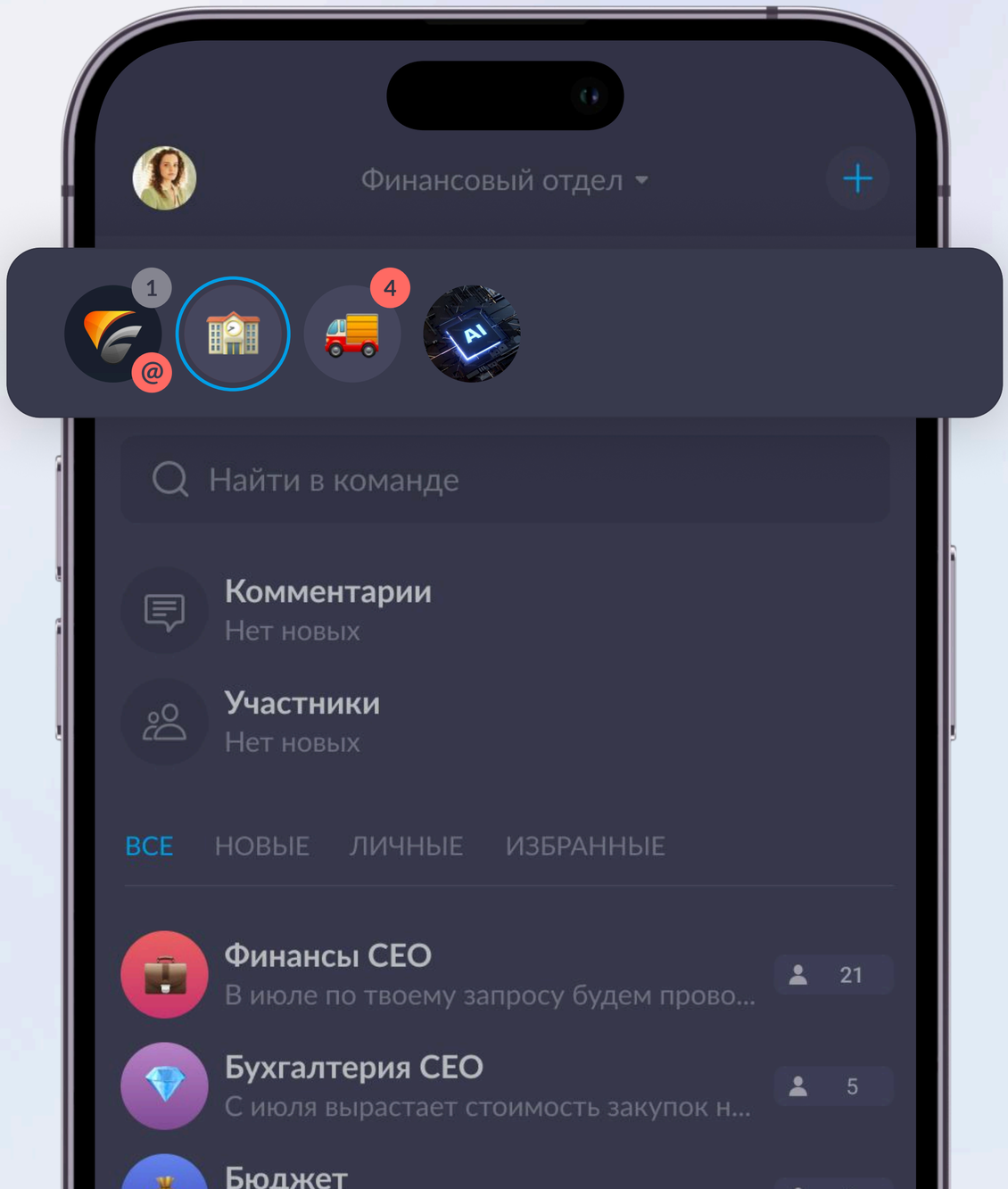
Быстрая и безопасная работа со сторонними сервисами в окне корпоративного мессенджера



Защищённые пространства

Создавайте безопасные пространства
для подразделений, проектов и команд.

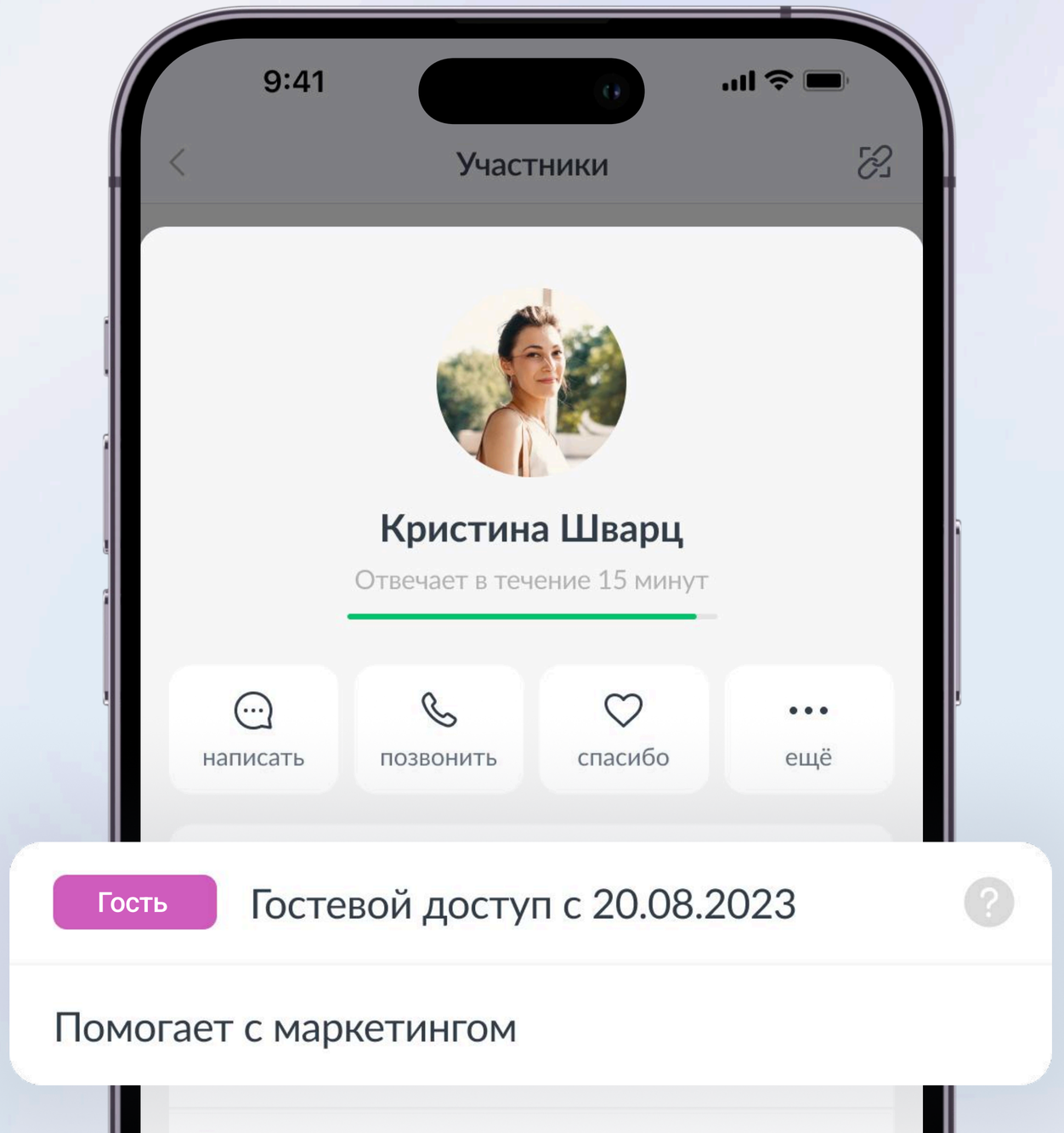
Каждое пространство - изолированная среда
с чатами и участниками для общения, которые
не пересекаются между собой.



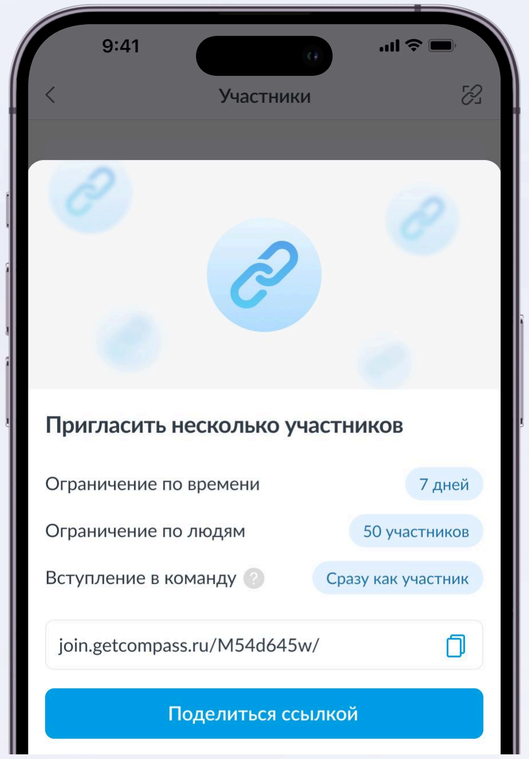
Гостевой доступ

Бесплатно добавляйте любое количество внешних пользователей в пространство по ссылке.

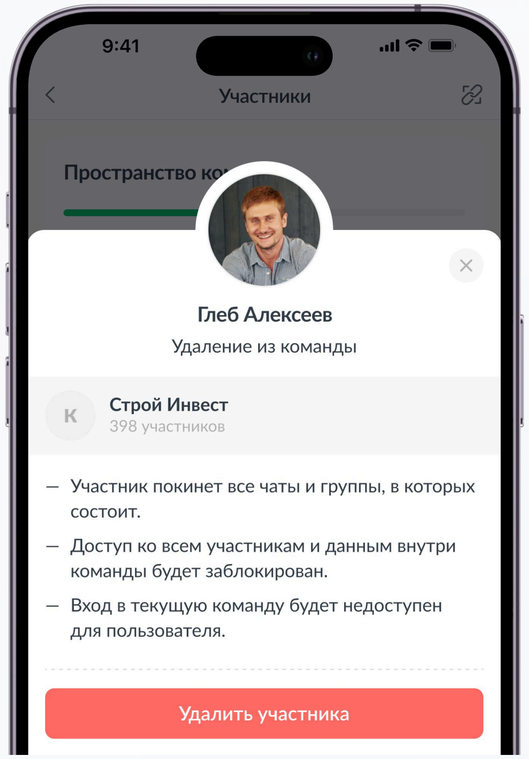
У гостя ограниченные права и доступы.
Он не видит список участников пространства и не может самостоятельно начинать с ними общение.



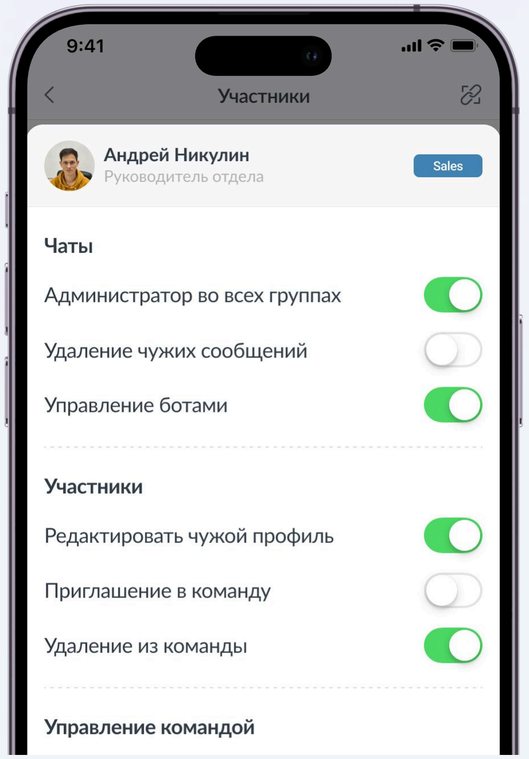
Управление сотрудниками



Мгновенно добавляйте сотрудников по ссылке



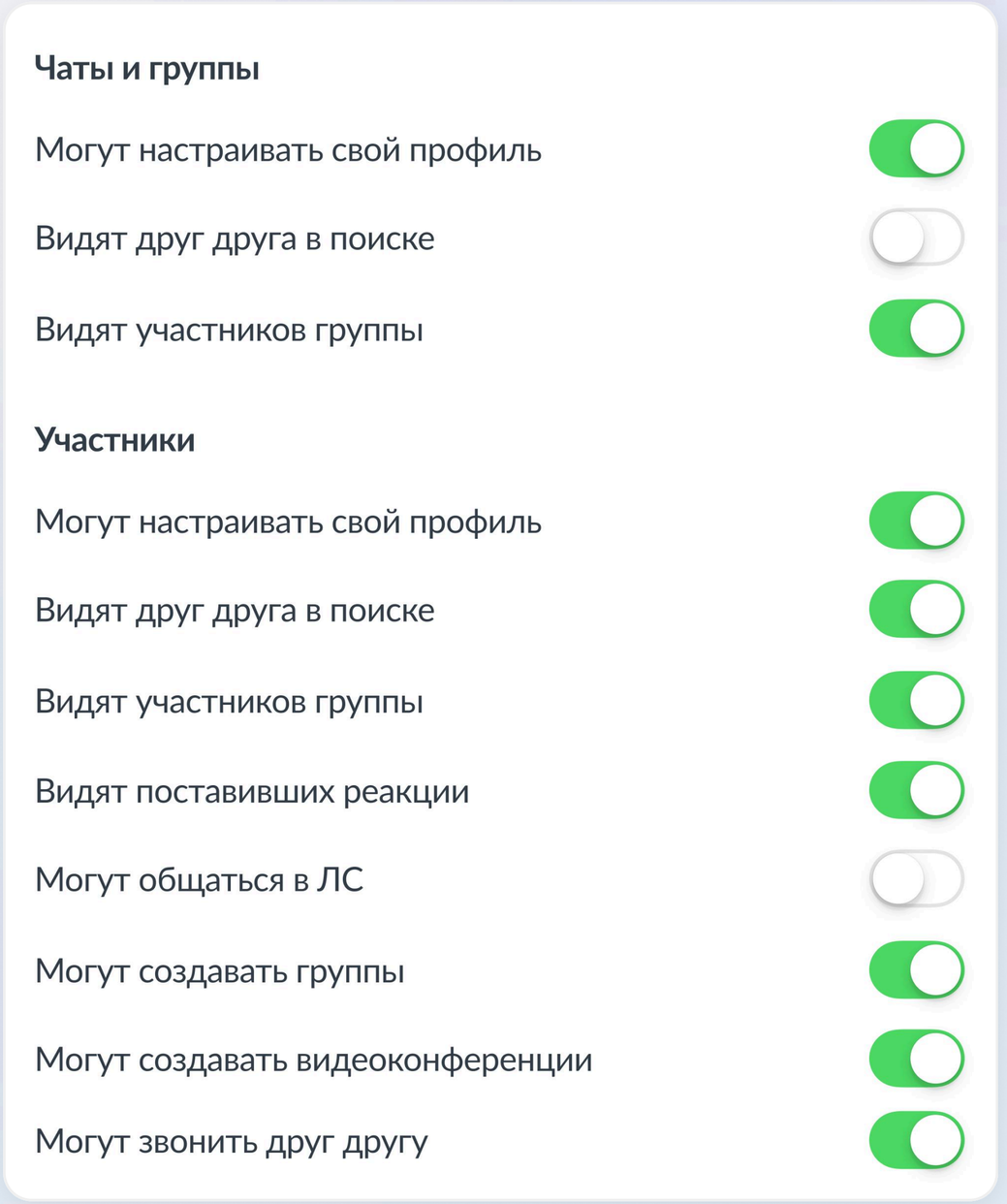
Закрывайте доступ к рабочей информации в 1 клик



Настраивайте права и назначайте администраторов

Ограничение действий

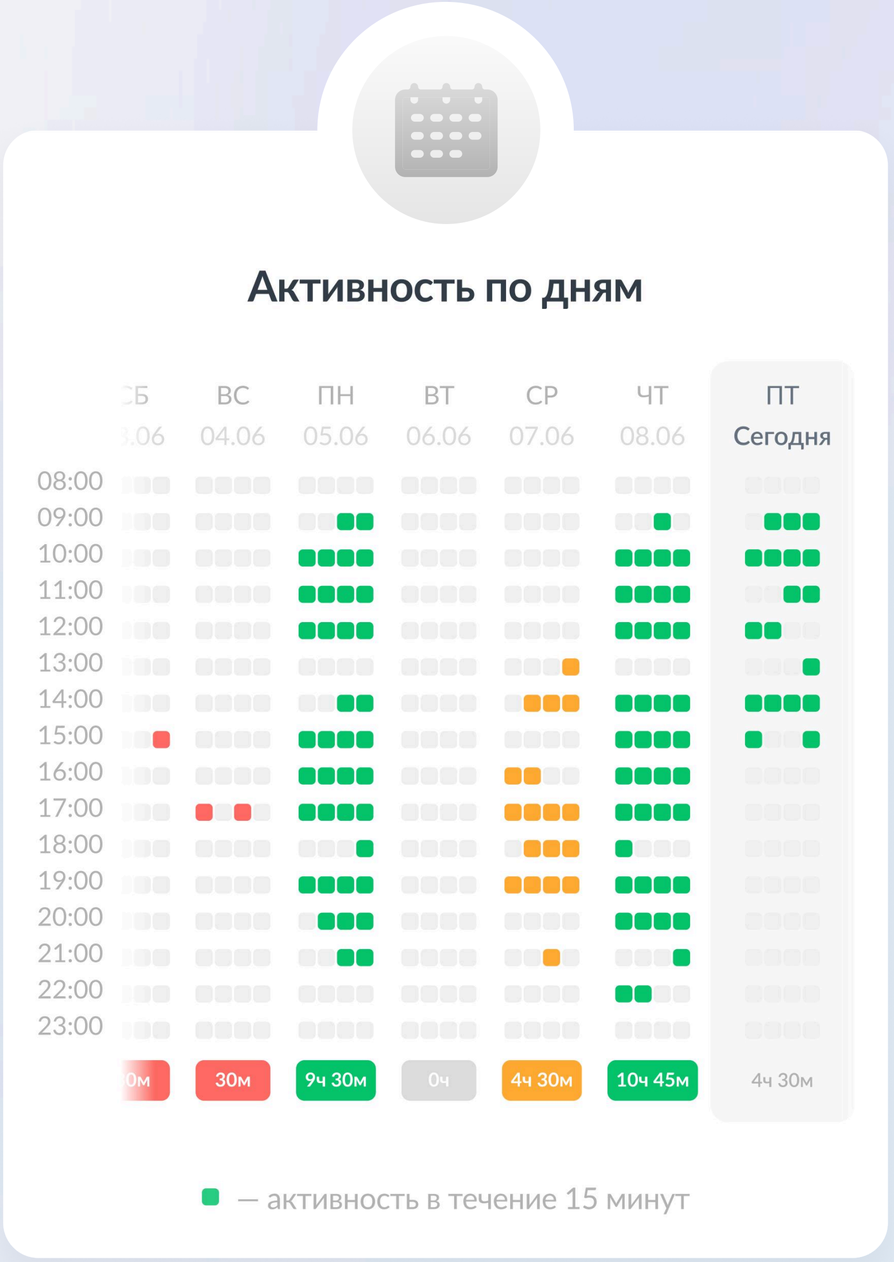
Настраивайте доступ к корпоративной информации. Контролируйте скачивание файлов, пересылку сообщений и общение сотрудников в личных и групповых чатах.



Статистика

Контролируйте работу каждого участника команды с помощью графика ежедневной активности.

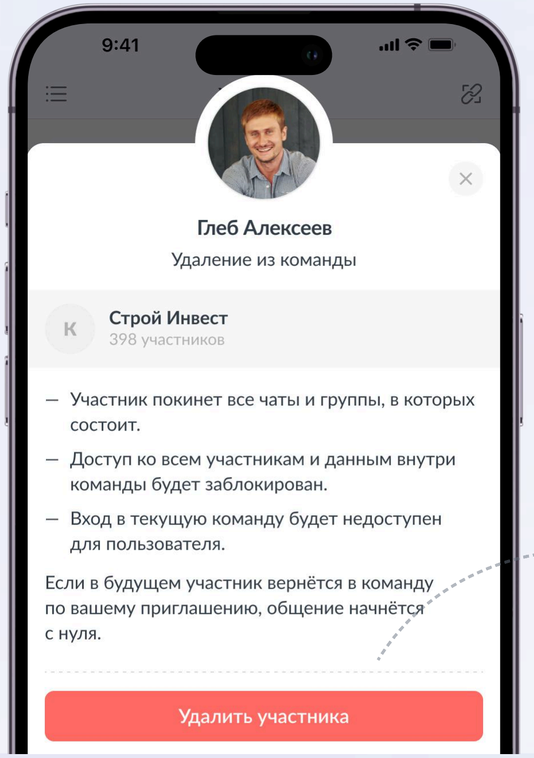
Если сотрудник общается по работе в других мессенджерах, это можно отследить с помощью графика активности и принять меры.

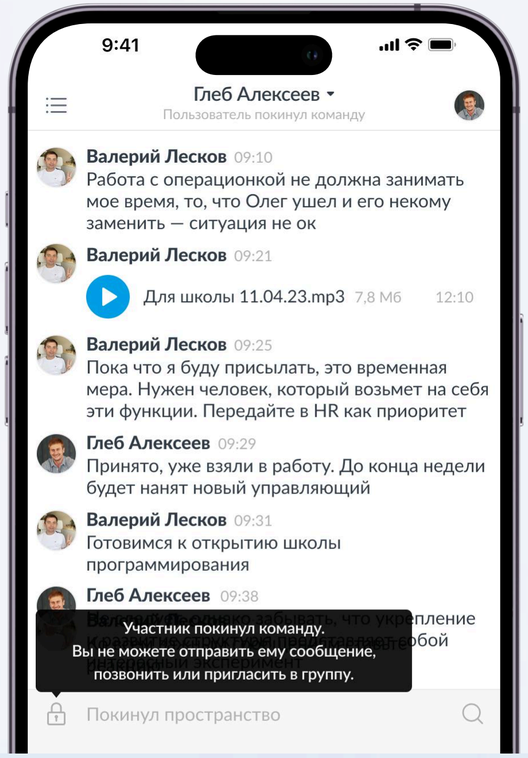


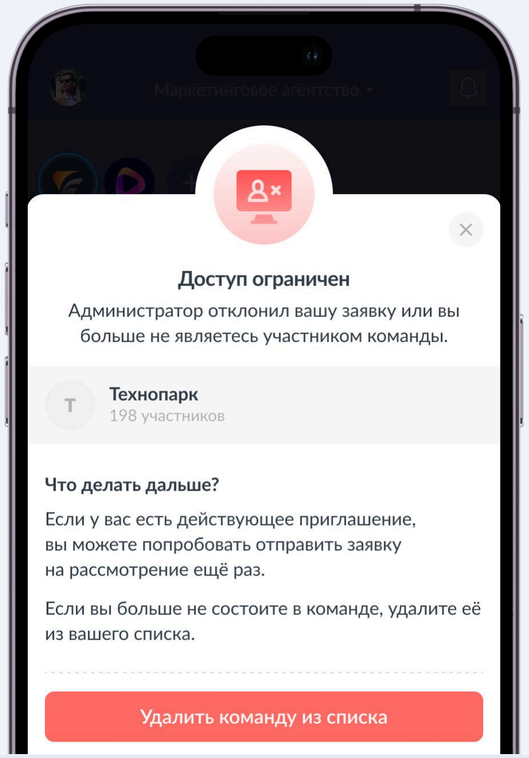
Активность в день **6 часов 30 минут**

Удаление сотрудников

Удаляйте уволенных сотрудников из всех чатов и рабочего пространства в 1 клик. После удаления сотрудник потеряет доступ к сообщениям, контактам, файлам и всей корпоративной информации.







Руководитель

Сотрудник

Спасибо за внимание

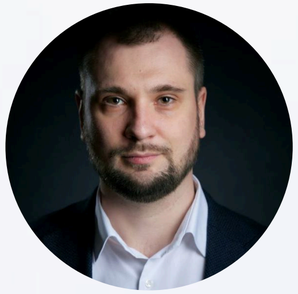
Звоните или пишите нам по любым вопросам – мы всегда на связи

Станислав Бондарчук

Руководитель интеграций

7 922 828-21-28

stas@getcompass.ru



Максим Фокин

Директор департамента сертификации

Maxim.Fokin@softline.com

Леонид Кантер

Архитектор ОС «МСВСфера»

Leonid.Kanter@softline.com

Переходите на сайт Compass
и скачивайте приложение

МСВСфера

Переходите на сайт МСВСфера
и узнавайте больше