

СТРАТЕГИЯ ИБ: 60+ ИНТЕРВЬЮ, 20 ИС И НЕ ТОЛЬКО...

Александр Морковчин

Эксперт по информационной безопасности, CISM, CISA, PCI DSS QSA
Morkovchin_ai@jet.su

НЕМНОГО ЦИФР ДЛЯ ПОНИМАНИЯ МАСШТАБА ПРОЕКТА



ИНТЕРВЬЮ

60

за 5 недель

Проведенных **очных и заочных интервью** с ответственными работниками:

- Специалисты информационной безопасности
- Представители бизнеса
- Прикладные администраторы ИС
- Администраторы ИТ-инфраструктуры и сетевого оборудования



АНАЛИЗ ИС

20

Информационных
систем различной
степени критичности

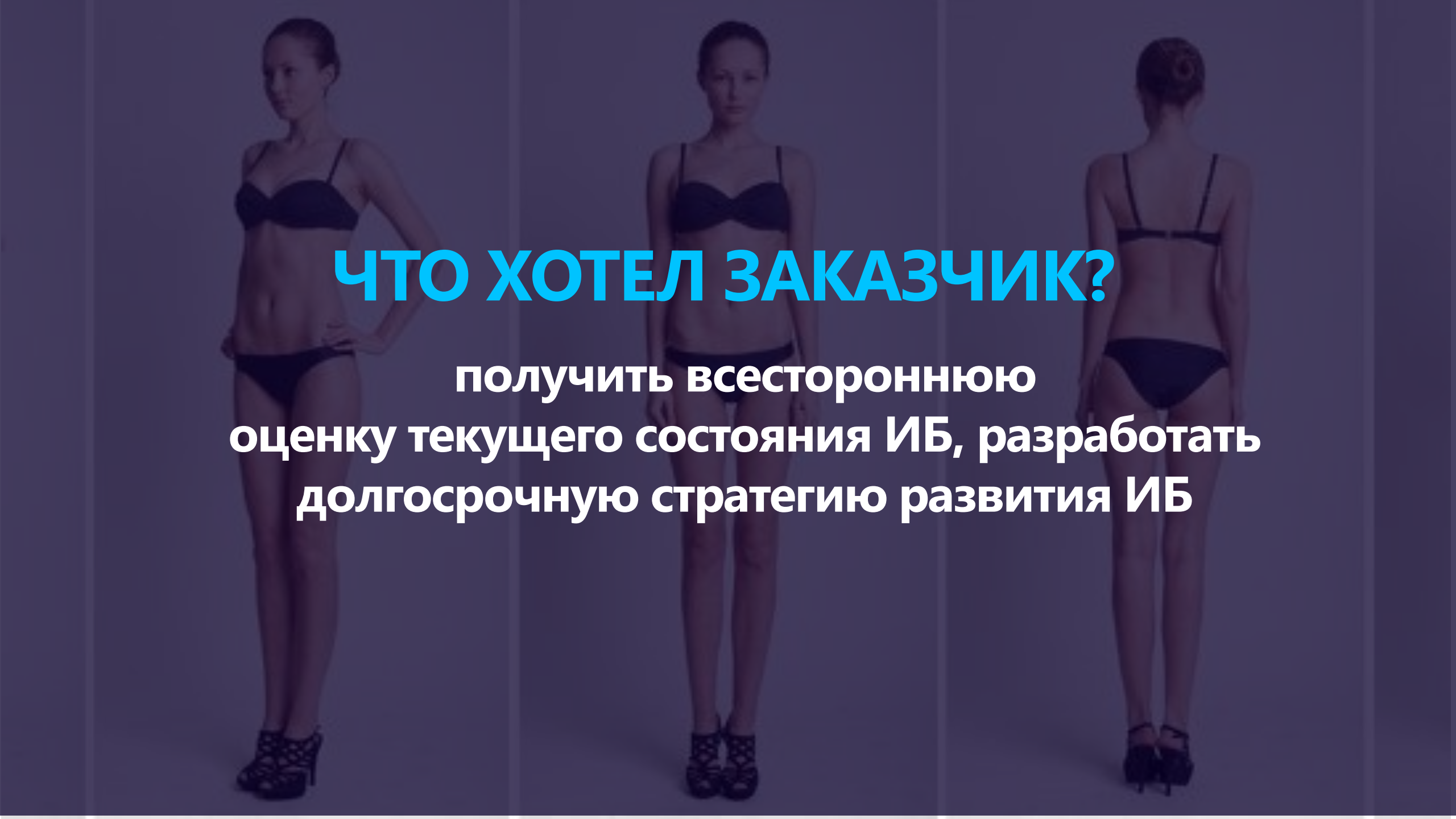


АНАЛИЗ DFS

70

ТБ объем
проанализированного
файлового хранилища

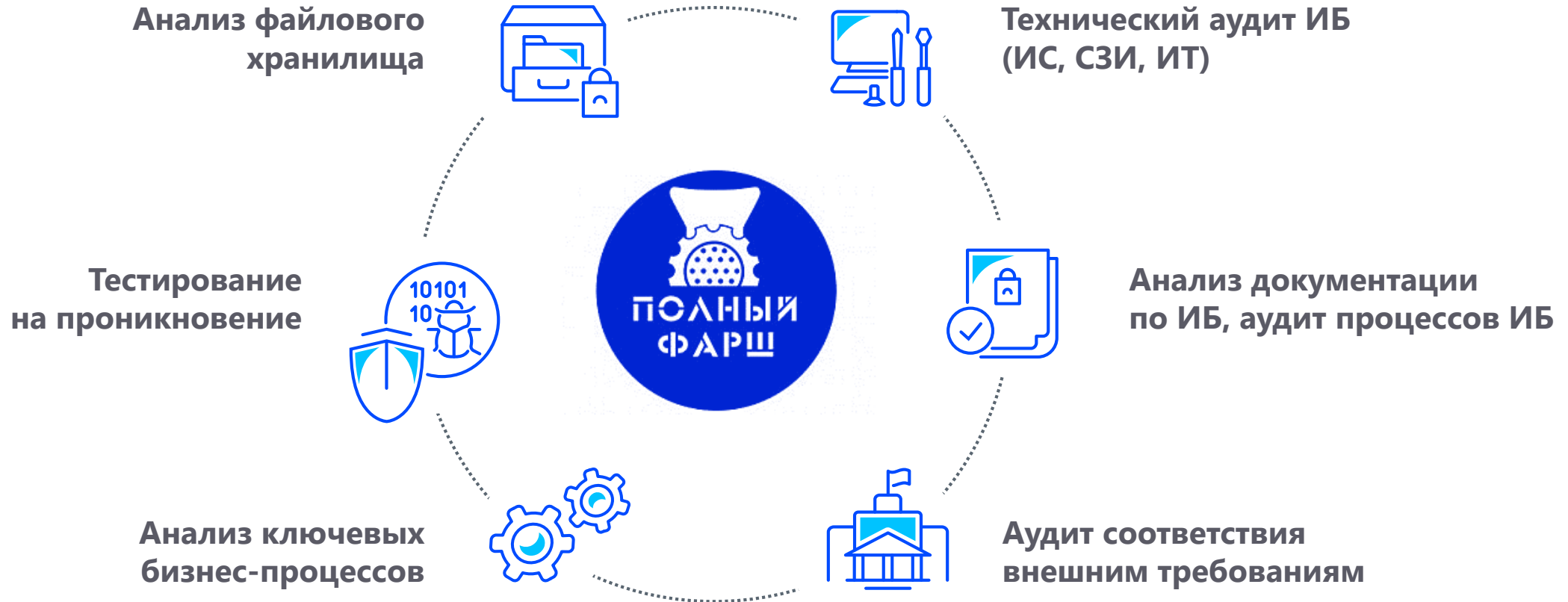


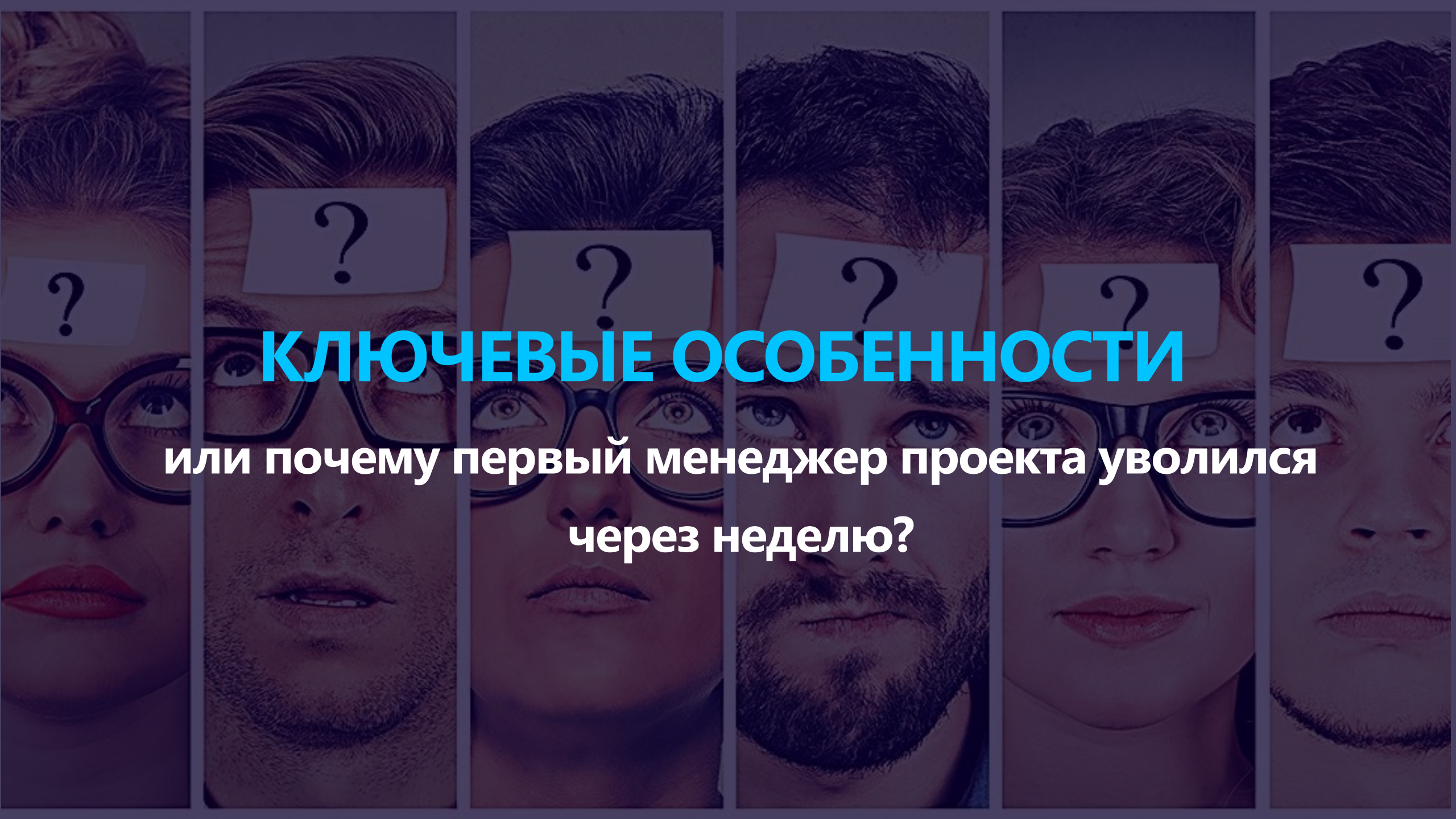


ЧТО ХОТЕЛ ЗАКАЗЧИК?

получить всестороннюю
оценку текущего состояния ИБ, разработать
долгосрочную стратегию развития ИБ

ПО КАКИМ НАПРАВЛЕНИЯМ МЫ РАБОТАЛИ





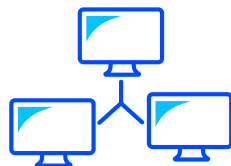
КЛЮЧЕВЫЕ ОСОБЕННОСТИ

или почему первый менеджер проекта уволился
через неделю?

А ЕЩЕ КОНСУЛЬТАНТЫ ОСТАЛИСЬ?



Compliance



Network



IS tools



Information
systems



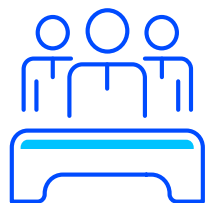
IT & IS



Pentest

← **6 отдельных проектных команд** →

Специалисты ИБ



16

Добровольцев-мазохистов
Центра информационной
безопасности

Выделенная роль: **Администратор ИБ**



- Работа с **#teamlead**
- Централизованный сбор информации
- Работа с проектной областью (наведение порядка)
- Работа с нормоконтролем

АНАЛИЗ 70ТБ ДАННЫХ ФАЙЛОВОГО ХРАНИЛИЩА

01

Разворачивание
решения в ИТ-
инфраструктуре

- ~40 отдельных вручную запускаемых заданий
- ~4 недели – время полного анализа файлового ресурса

» **02**

Сканирование отдельных
каталогов

- Отдельные отчеты-приложения со сводной статистикой
- Выделенный аналитик со стороны ОК и ОПЗС

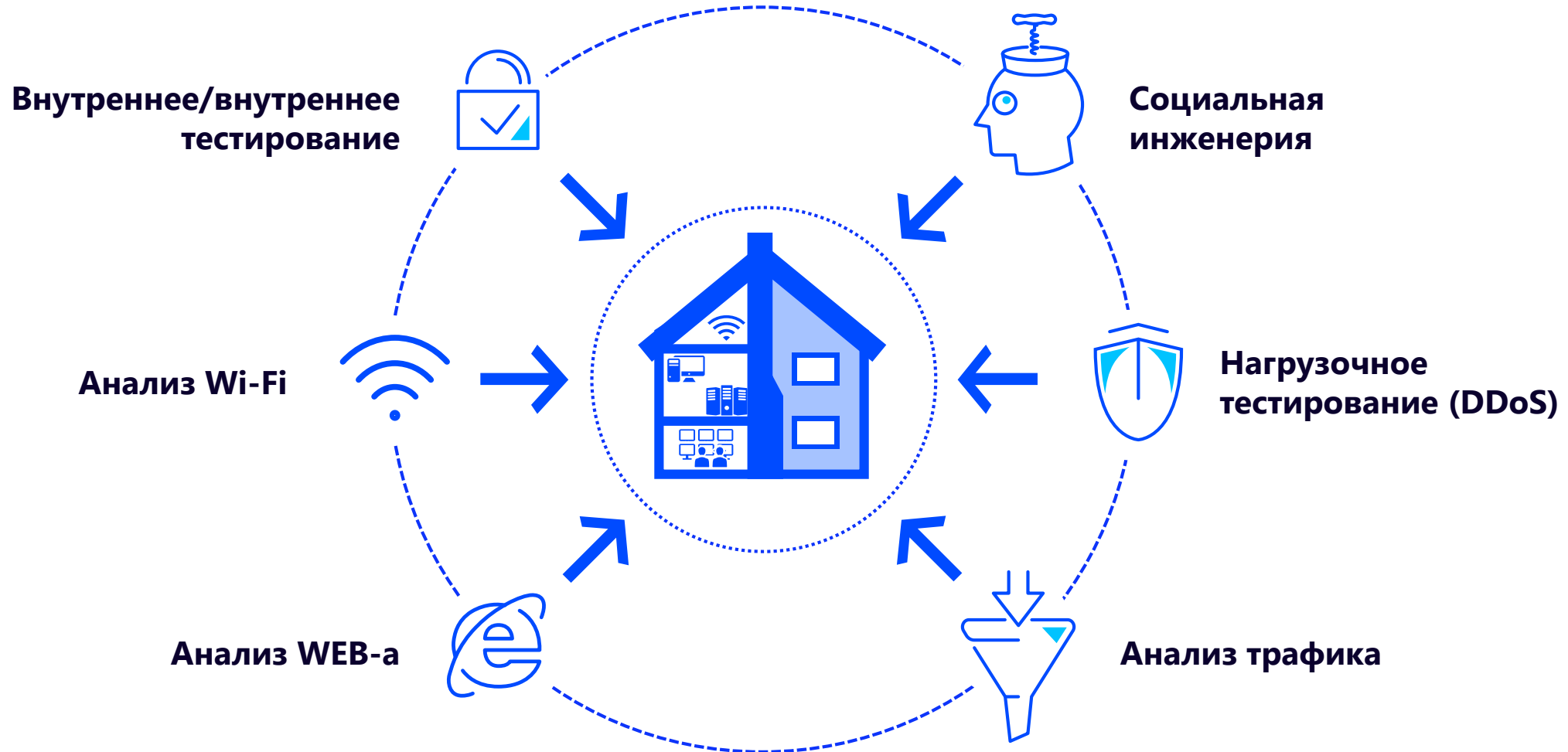
» **03**

Расширенная аналитика



Паспортные данные проектной команды и паспорта безопасников

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ НА ВСЕХ ПЛОЩАДКАХ



«С НОВЫМ ГОДОМ!» ИЛИ КАК МЫ ВРЕМЕННО ЗАМЕЩАЛИ РОЛЬ PR-МЕНЕДЖЕРА

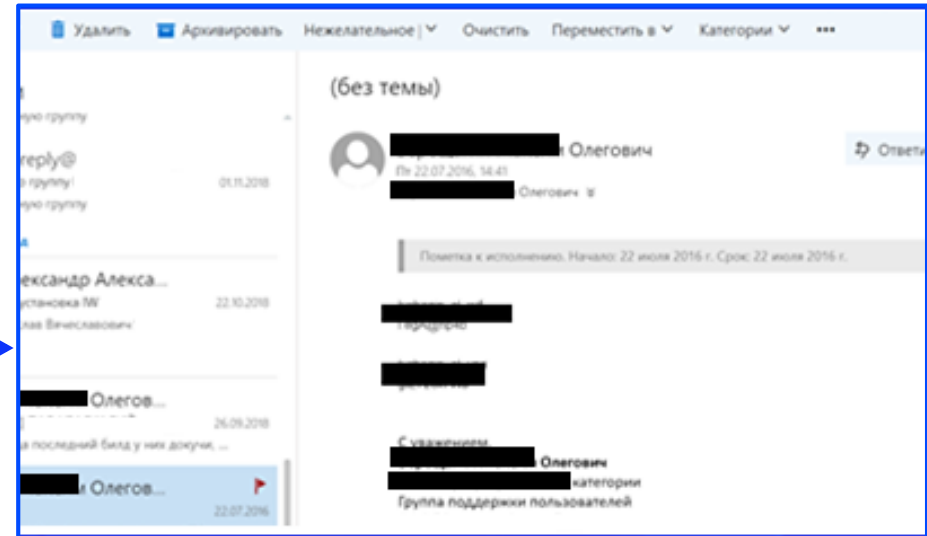


1

Новогодние плакаты размещаются в местах общего доступа, работники переходят по ссылке и оставляют свои данные

Доступ хакера в почтовый ящик «жертвы», поиск паролей и инструкции к подключению к VPN

2



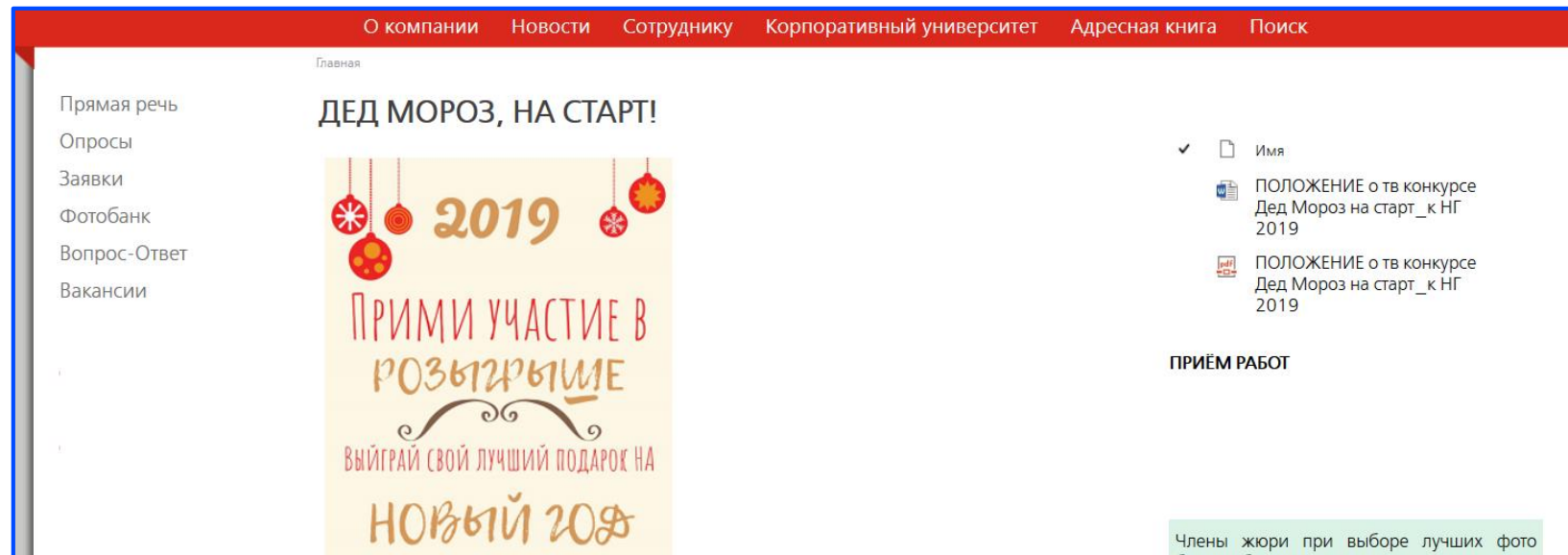
ВНУТРЕННИЙ ПОРТАЛ НАМ В ПОМОЩЬ



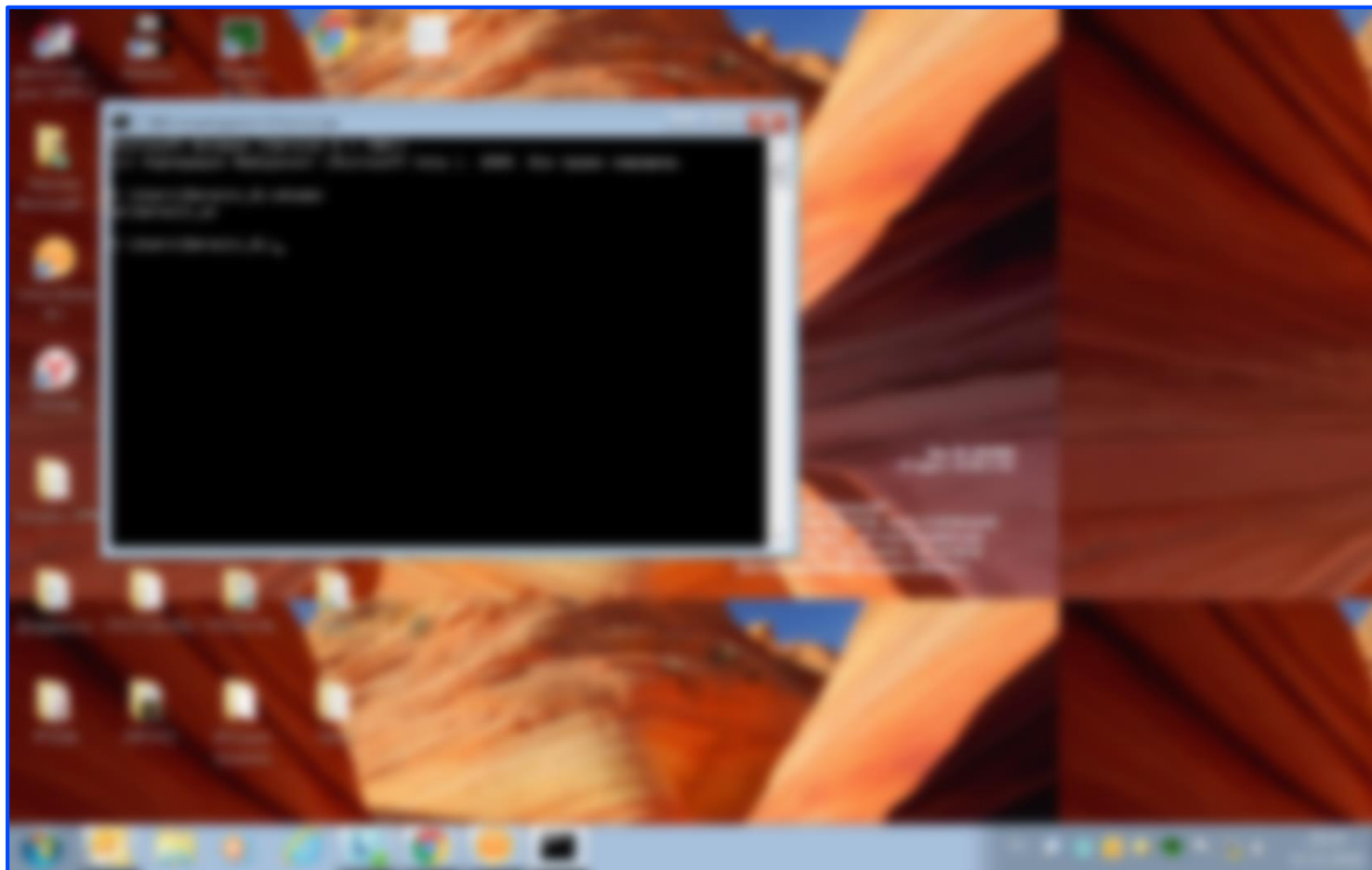
From: Елена Г
Sent: 2018 1:39 PM
To: Татьяна
Subject: уточнить

Добрый день!

Татьяна, в столовой лежит плакат. Написано подробности на -2019.ru.
При входе открывается страница, а какие домен/логин и **пароль** необходимо вводить?



ДОСТУП НА АРМ ТОП-МЕНЕДЖЕРА

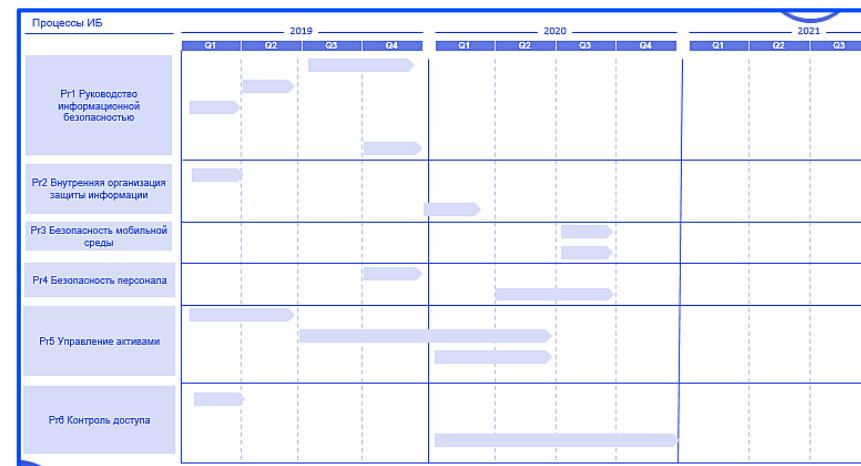
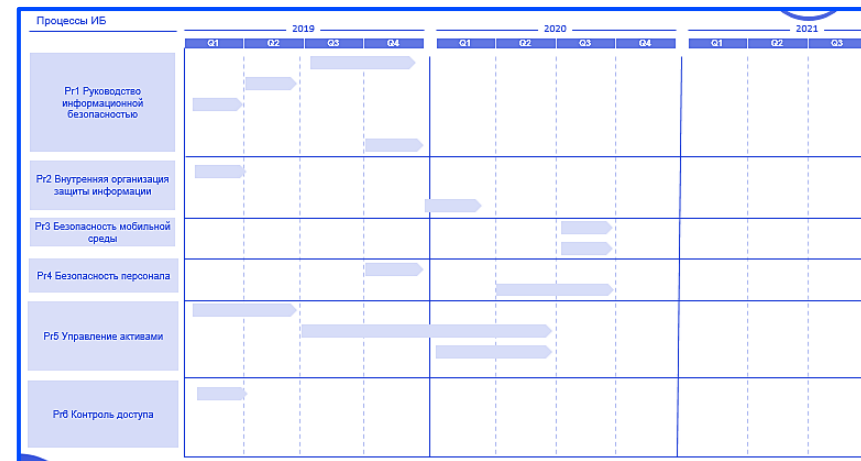


A hand holding a pen is shown writing the word "RESULTS" in a bold, hand-drawn style. The word is underlined with a single horizontal stroke. The background is a solid dark blue color.

RESULTS

ИЛИ ЧТО В ИТОГЕ ПОЛУЧИЛОСЬ

ДОЛГОСРОЧНАЯ СТРАТЕГИЯ РАЗВИТИЯ ИБ



* Road-map на три года

ВЫВЕДЕННАЯ ФОРМУЛА СЧАСТЬЯ ПРОЕКТА ИБ



IV

4 квартал
2018 года

+

∞

Размытые
границы
работ

+



5 недель
на все работы

=



Заявка
на провал

И НАПОСЛЕДОК... БРОНИРУЙТЕ САМИ 😊



СПАСИБО ЗА ВНИМАНИЕ!

Александр Морковчин

Эксперт по информационной безопасности, CISM, CISA, PCI DSS QSA

Morkovchin_ai@jet.su