ИНФОСИСТЕМЫ ДЖЕТ

ЛЕТ

ФОРМИРУЕМ ТРЕНДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИБ АСУ ТП: невозможное – возможно

Алексей Петухов,
руководитель направления по ИБ АСУ ТП
Центра информационной безопасности

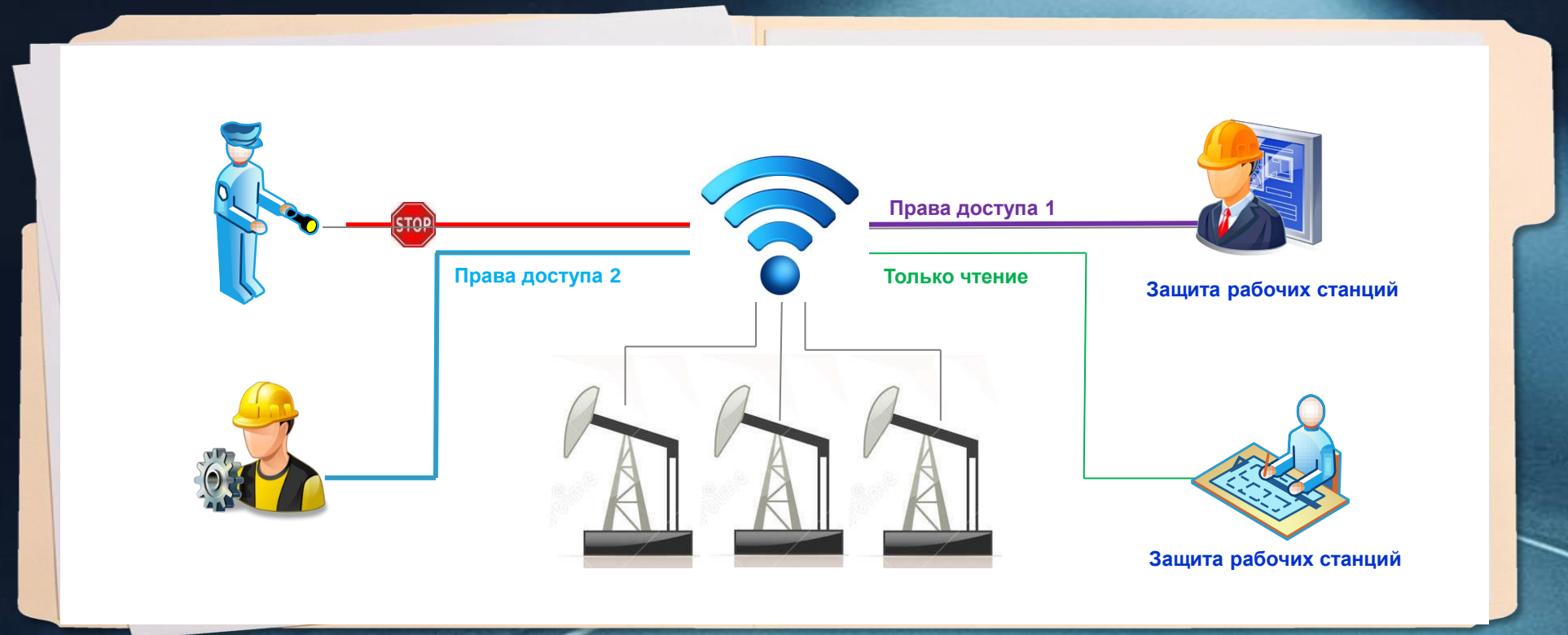
Современный подход к автоматизации

- ✓ Безопасный город
- ✓ Предприятие 4.0
- ✓ Умная энергетика
- ✓ Цифровое месторождение
- ✓ …

Пример: беспроводные сети

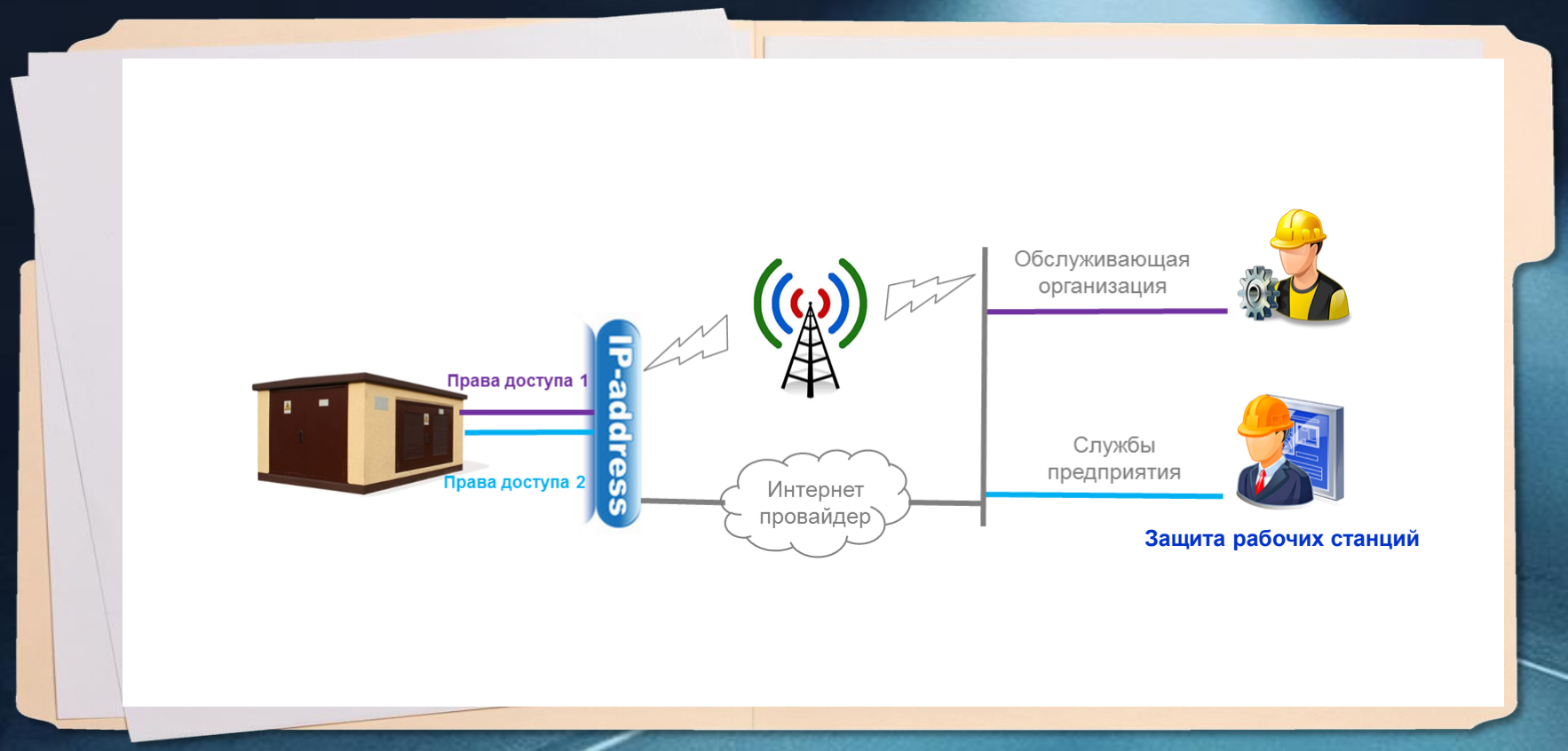
Цифровое месторождение

Вместо неустойчивых, «узких» радиоканалов и дорогостоящих решений с физической связью используются широкополосные физические и беспроводные технологии связи



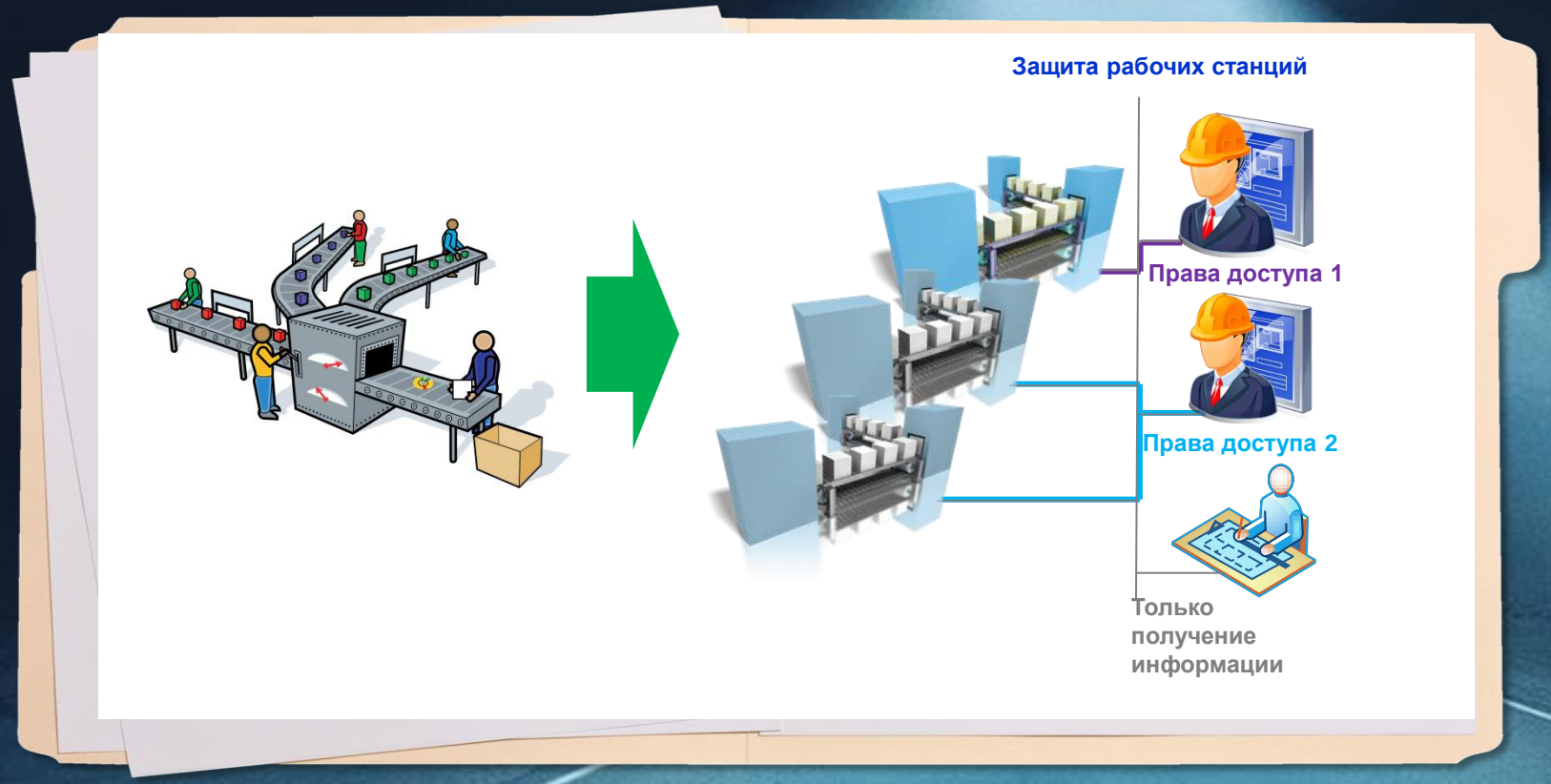
Пример: удалённое управление

«Поставщики» ресурсов (электричества, воды, газа и т.п.)



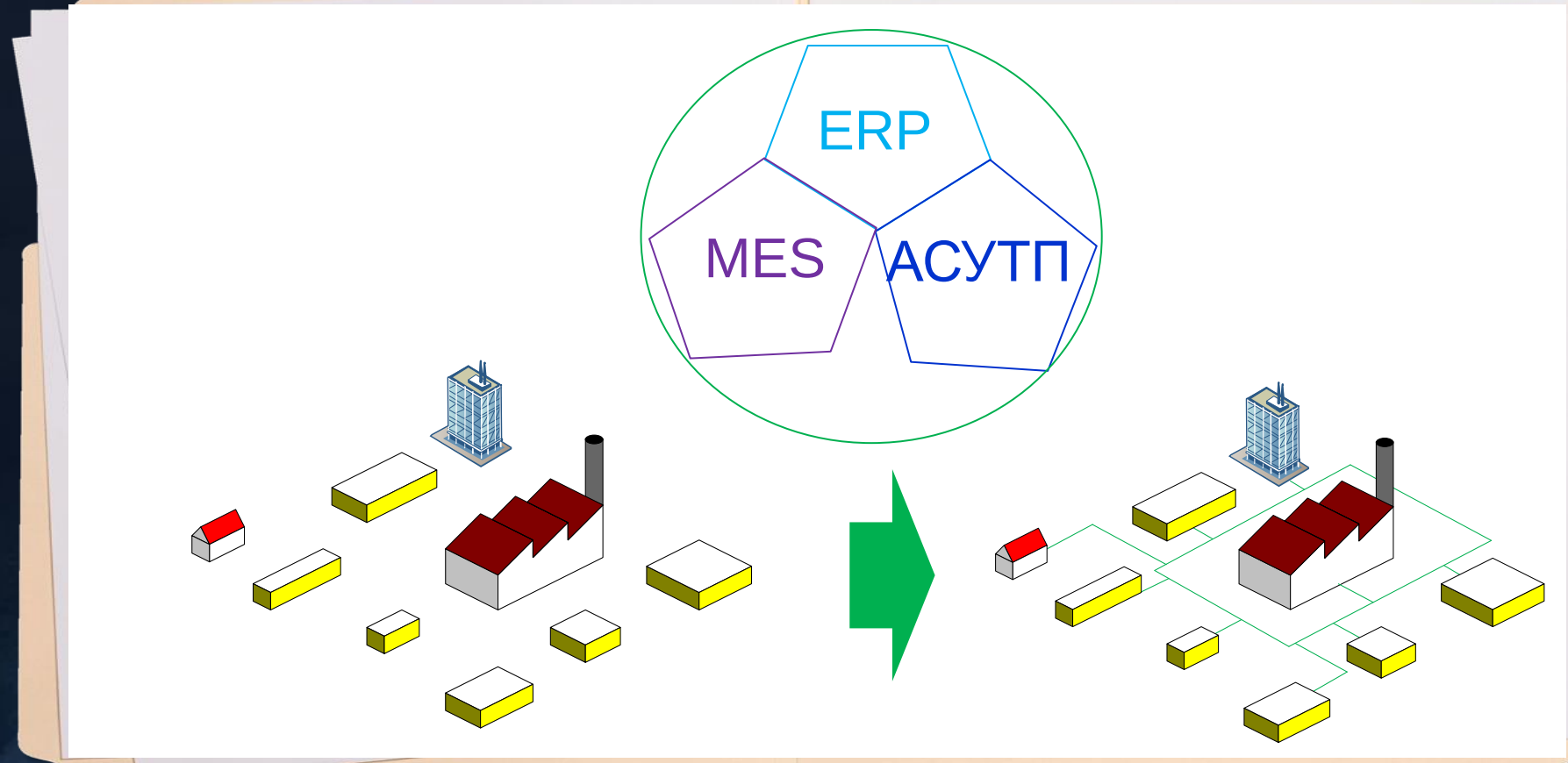
Пример: автоматизация производства

Автоматизация предприятия. Предприятие 4.0



Пример: интеграция систем

Автоматизация предприятия. Предприятие 4.0



В этих проектах есть безопасность

Обобщённый типовой подход к ИБ:

- ✓ *Штатные средства защиты* ***– иногда***
- ✓ *Сетевая защита (FW, IDS…)* ***– часто***
- ✓ *Антивирусы* ***–почти всегда***
- ✓ *Документы* ***– вроде бы***
- ✓ *Организационные меры* ***– какие-то***

(не)Решаемые проблемы

- Отсутствие квалифицированной настройки СЗИ
- Неконтролируемый сетевой периметр
- Отсутствие реальной защиты от человеческого фактора
- Отсутствие средств мониторинга состояния ИБ

ИТОГО:
Невозможность контроля состояния ИБ на предприятии

Точно целимся, метко стреляем

Необходимо:

- Защищаться от некомпетентных, «продвинутых» и недовольных сотрудников
- Контролировать «безупречных» подрядчиков
- Мониторить, разбирать и расследовать инциденты
- Отслеживать и поддерживать уровень ИБ в реальном времени

Техническая реализация

- Ограничение использования ресурсов рабочих станций:
  - Контроль целостности и listing
  - Контроль съемных носителей
- Контроль внутренних подключений и целостности периметра:
  - NAC и сканеры уязвимости
  - Мониторинг технологического трафика
- Контроль действий привилегированных пользователей (PIM)
- Разграничение полномочий (IDM)

Повышение эффективности

Для повышения эффективности применяемых решений необходимо:

- Обеспечить централизованный сбор событий ИБ
- Автоматизировать процессы формирования, анализа инцидентов и принятия решений по ним
- Визуализировать производственные процессы и инциденты

SOC - инструмент для служб ИБ и АСУТП

Больше чем безопасность

В сухом остатке

- С новыми технологиями приходят новые угрозы
- В проектах по автоматизации/модернизации уже есть ИБ
- Глубина проработки ИБ оставляет желать лучшего
- Диалог между представителями служб ИБ и АСУ ТП еще не налажен (в большинстве компаний)

Что делать службам ИБ

- Налаживать контакты со службами АСУ ТП, с компаниями «автоматизаторами» и «информатизаторами» предприятий
- Выстраивать полноценный процесс управления ИБ в технологическом сегменте:
  - Выдвигать требования (в т.ч. к типовым проектам)
  - Участвовать во внедрении и эксплуатации СЗИ
  - Обеспечивать должный уровень информационной безопасности

Поможем и подскажем

Компетенции и опыт нашей компании позволяют :

- Разработать стандарты и требования по ИБ АСУ ТП
- Провести обследование и аудит технологического сегмента
- Внедрить, настроить и поддержать базовые средства и меры защиты
- Выявить и устранить ключевые уязвимые места в ИБ предприятия
- Выстроить процессы обеспечения ИБ технологического сегмента с целью обеспечения непрерывности бизнеса

Надёжный партнёр

2011 г. – первый проект по обеспечению ИБ АСУ ТП в крупной энергетической компании

8 успешно завершенных проектов в энергетических и промышленных компаниях России и СНГ

7 успешно завершенных проектов в нефтяных компаниях

Объектами защиты были системы, построенные на базе решений: *Emerson, Siemens, Converge, Yokogawa, Bentley, Honeywell, Allen Bradley, ABB-Bailey, Wonderware, SAAB, GE, OMRON, Hirschmann,Телескоп+, АДКУ-2000,ТЕКОН, Квинт и др.*

ИНФОСИСТЕМЫ ДЖЕТ

Jet infosystems

Л Е Т

ФОРМИРУЕМ ТРЕНДЫ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Спасибо за внимание!