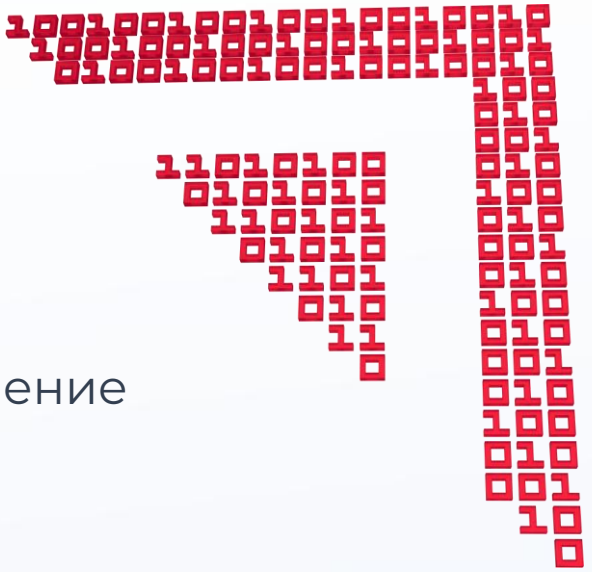
ИТ-аудит как вакцина от кибермошенничества. Как бизнесу защитить себя до атаки

АЦРКК

2025

Ситуация



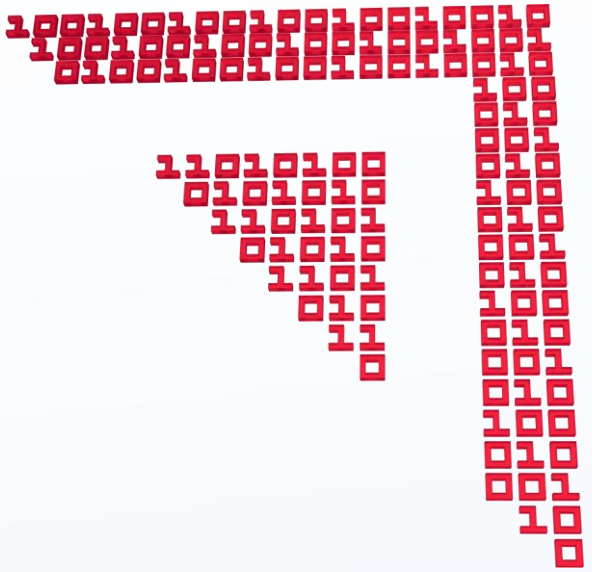
- В 2024 г. ~130 000 инцидентов.

- 710 млн записей о гражданах в 135 случаях попали в распространение

- За 8 месяцев 2025 года количество кибератак в РФ выросло в 3 раза к аналогичному периоду 2024 года.

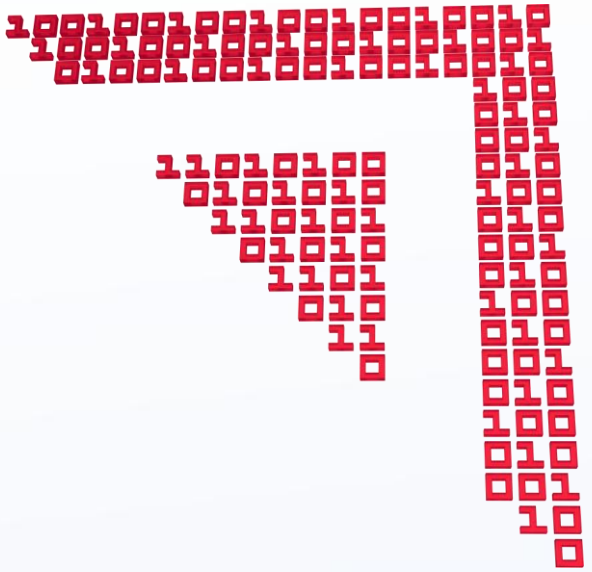
- Совокупный ущерб, причинённый российской экономике за период 2023 – 2024 годов, может составлять не менее 1 трлн руб. за 8 месяцев 2025 года уже 1,5 трлн руб.

Сценарии



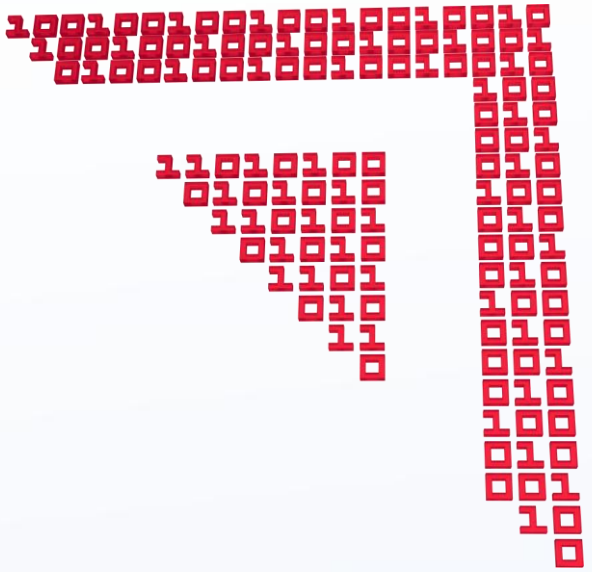
- Подмена реквизитов при оплате поставщику
- Взлом аккаунтов директора или бухгалтера
- Внедрение вируса через подрядчика
- Утечка базы клиентов
- Манипуляции через поддельные тендеры и документы

Последствия



- Потеря финансов
- Остановка работы предприятия
- Закрытие предприятия
- Обман физических лиц посредством украденных персональных данных

Основные причины проникновений



- Ошибки в проектировании ИТ ландшафта
- Использование неверных ИТ продуктов
- Пренебрежение базовыми правилами защиты
- Отсутствие корректной стратегии ИБ
- Некомпетентность штатных специалистов, не имеющих опыта и навыков построения безопасного ИТ ландшафта и тренирующихся на текущей компании
- Излишняя уверенность руководства в том, что у них в ИТ все под контролем

Шаги

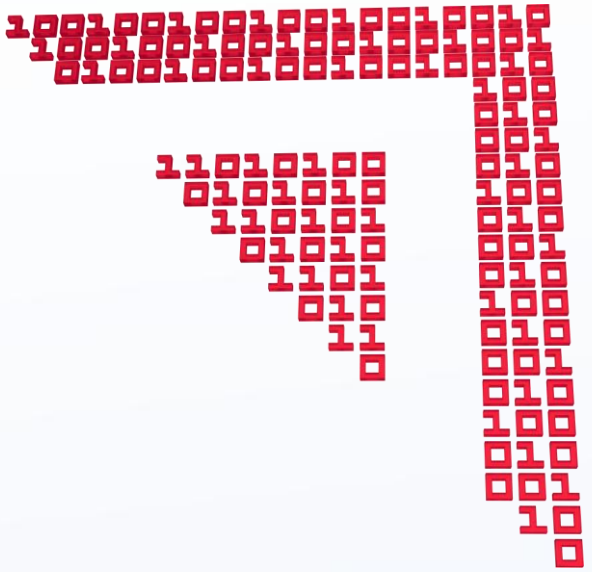
- Внешний аудит;

- Усилить команду подтвержденными экспертами на постоянной основе (или в штат, или на подряде на почасовом контракте);

- Регулярно проводить проверки (это будет дешевле, чем устранять последствия) и исправлять недочеты;

- Проводить регулярное обучение штатной команды и мастер-классы силами профессионалов, чтобы поддержка безопасности ИТ контура стала обычной рутиной.

Аудит



Архитектура информационных систем и ее соответствие задачам бизнеса

- Функциональная карта и зоны ответственности, включая ответственных от бизнеса
- Покрытие функций информационными системами и "белые пятна" Excel и ручного труда
- Адекватность использования конкретных ИТ систем задачам бизнеса
- Интеграции между системами, надежность их работы, сложность поддержки
- Баланс собственной разработки и внешних сервисов, риски

ИТ инфраструктура (сервера, сети) и ее соответствие критериям надежности и безопасности

- Резервное копирование и восстановление, хранение резервных копий
- Катастрофоустойчивость

Информационная безопасность (вырабатываем критерии ИБ и проверяем систему на соответствие критериям)

Компетенции сотрудников ИТ департамента

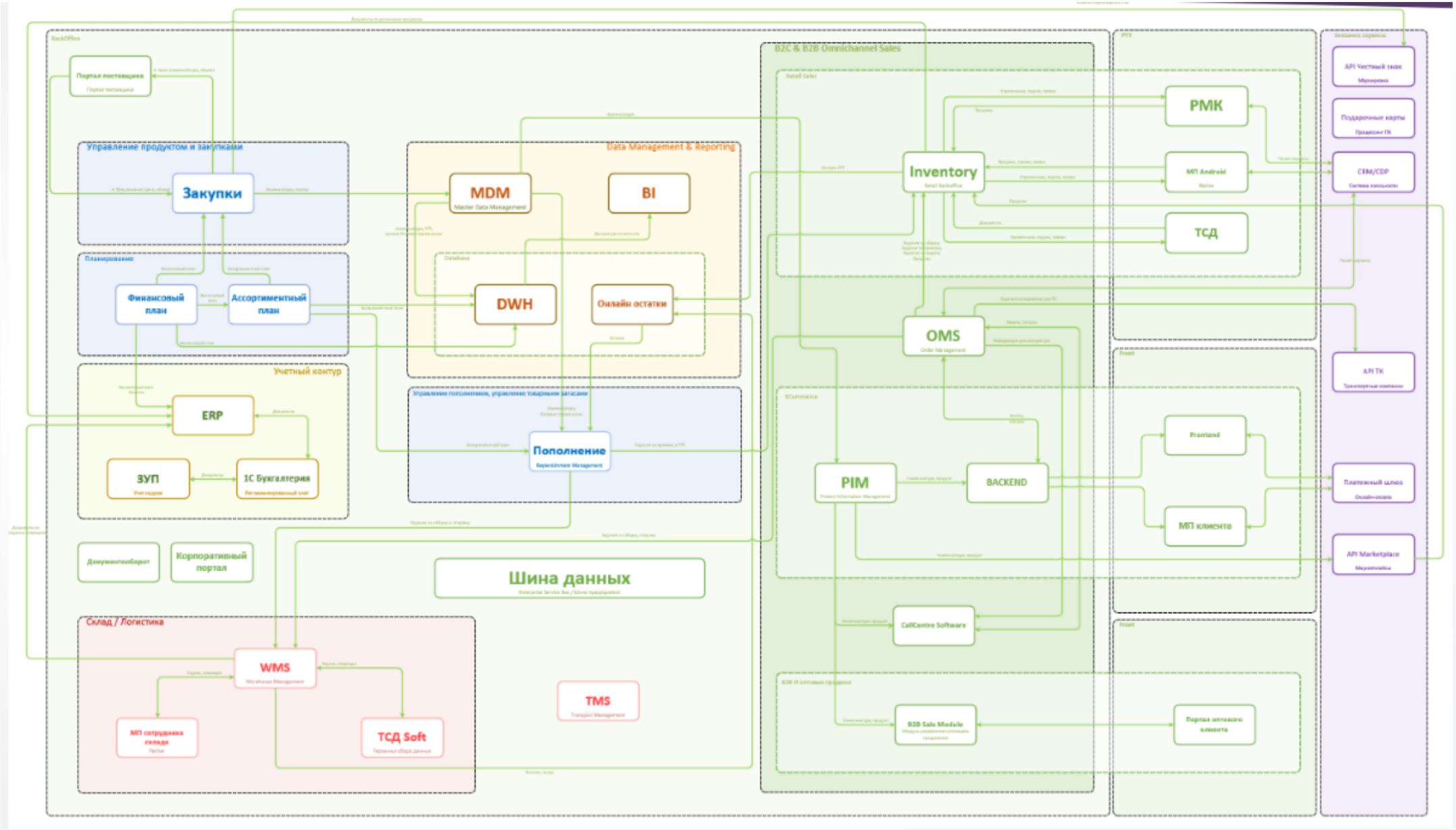
Объем технического долга и возможности по его ликвидации

ИТ процессы операционной функции ИТ (поддержка, обеспечение, закупки, обработка заявок, бесперебойность, SLA и т.п.)

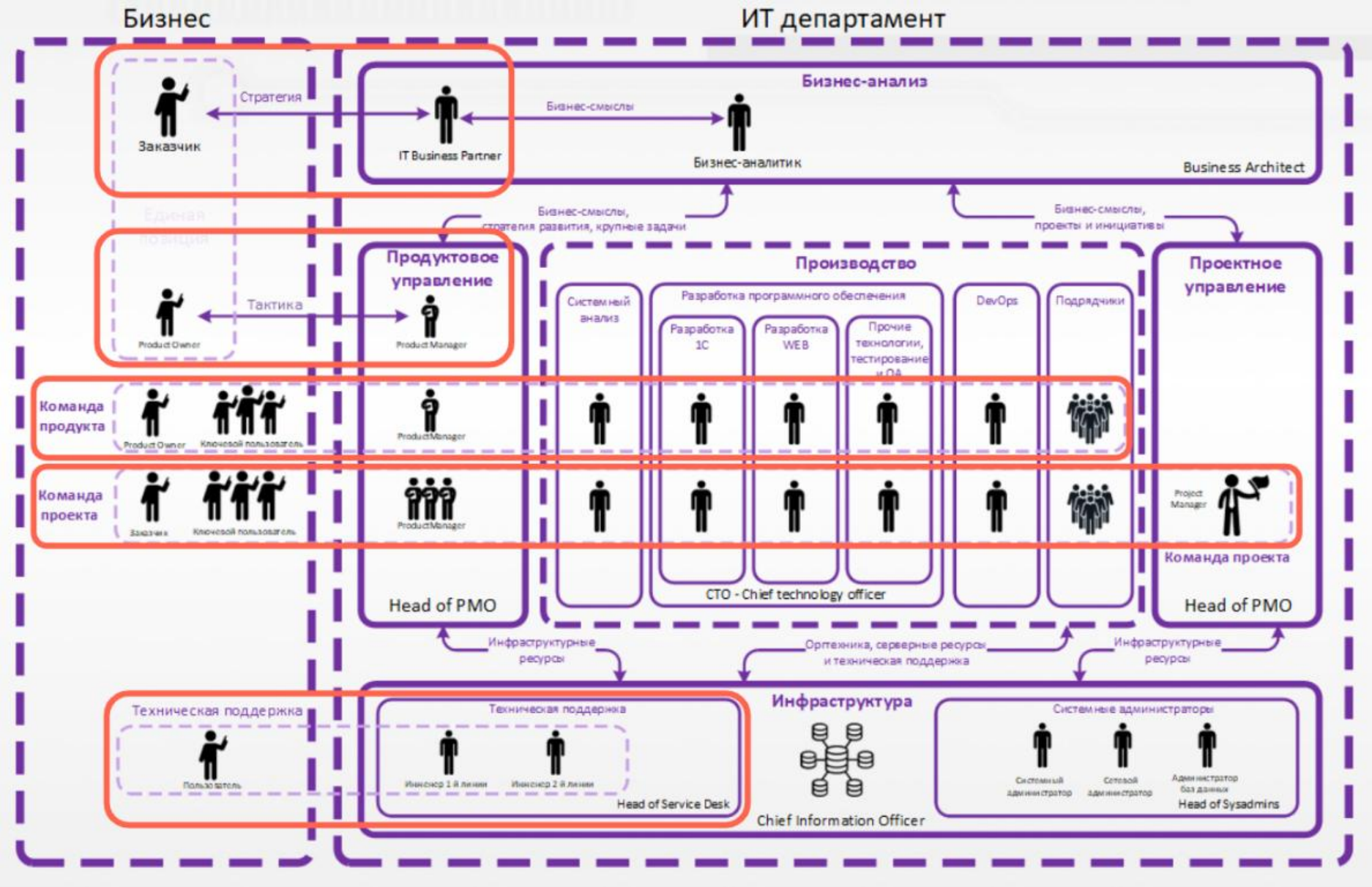
ИТ процессы по изменениям, включая разработку ПО и внедрение новых инструментов и систем

Структура бэклога и процессы работы с задачами (delivery management)

ИТ ландшафт


Управление продуктом и закупками
Закупки
Планирование
Финансовый план
Ассортиментный план
Учетный контур
ERP
ЗУП
1С Бухгалтерия
Документооборот
Корпоративный портал
Склад / Логистика
WMS
МП сотрудника склада
ТСД Soft
Data Management & Reporting
MDM
BI
DWH
Онлайн остатки
Управление поставками, управление товарными запасами
Пополнение
Шина данных
TMS
B2C & B2B Omnichannel Sales
Inventory
OMS
PIM
BACKEND
CallCentre Software
B2B Sale Module
РМК
МП Android
ТСД
Frontend
МП клиента
Портал сетевого клиента
API Честный знак
Подарочные карты
CRM/CDP
API ТК
Платежный шлюз
API Marketplace

Структура коммуникации



Центр мониторинга SOC

Ассоциация ЦРКК

Сергей Грабский

+7 928 207 58 25