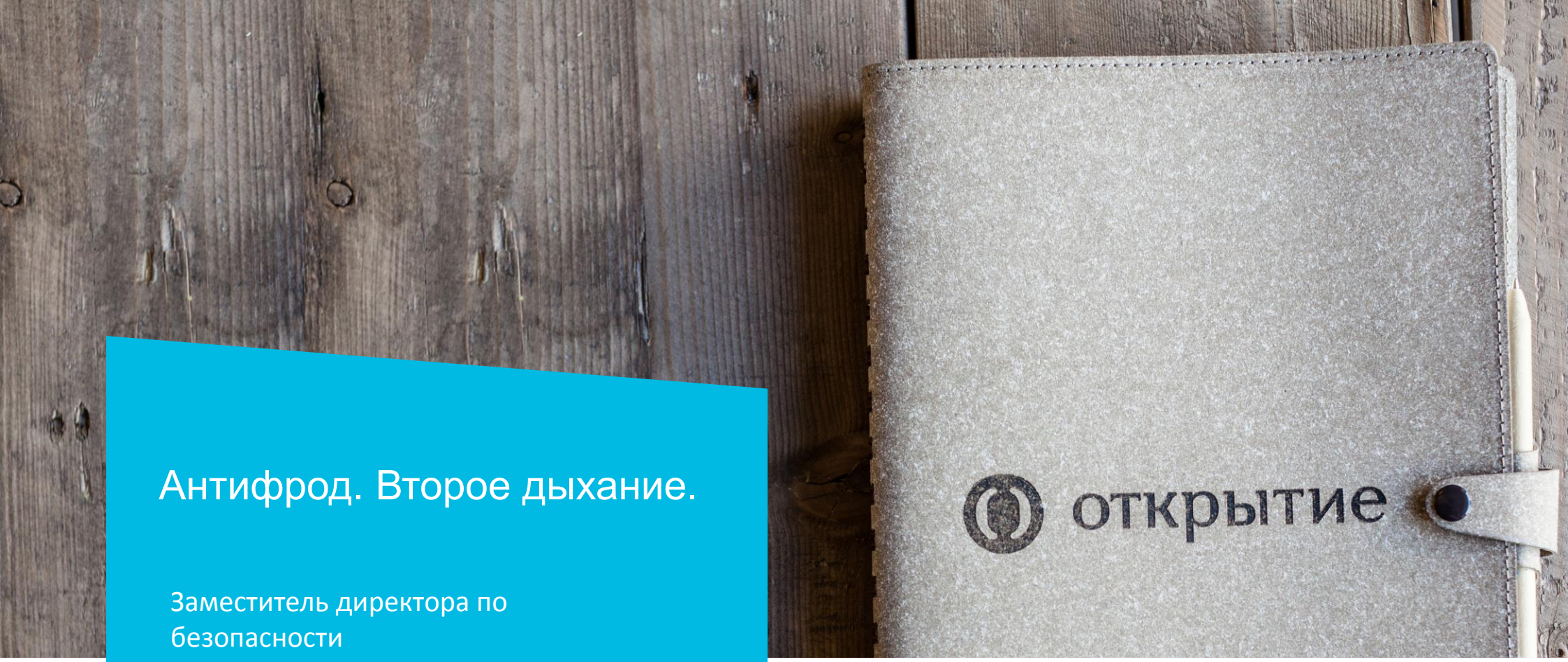


Антифрод. Второе дыхание.

Заместитель директора по
безопасности
Вячеслав Касимов

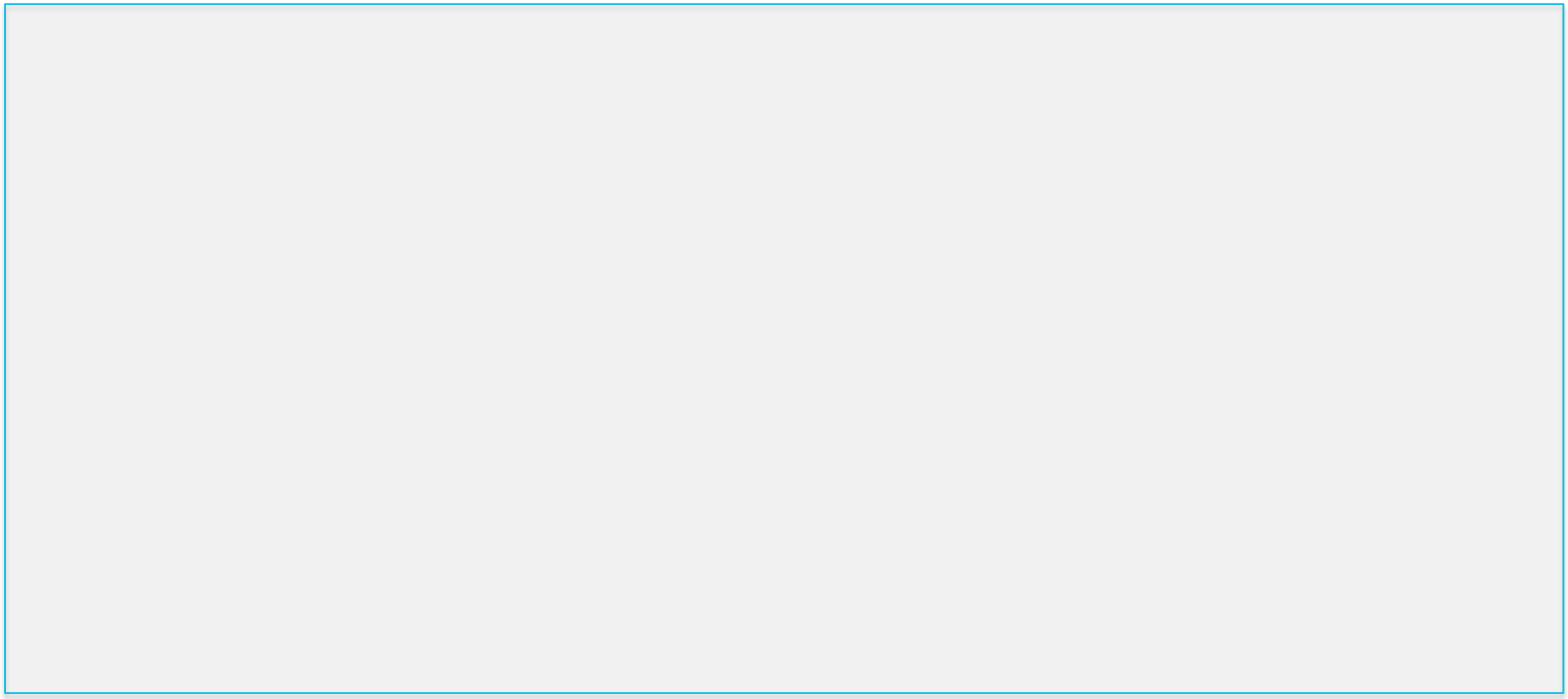
kasimov@open.ru

В жизни всегда
есть место открытию

openbank.ru

открытие | БАНК

ПРИМЕР АБСОЛЮТНО
БЕЗОПАСНОГО ПЛАТЕЖА



Абсолютно безопасных платежей не существует

ПОЧЕМУ ХИЩЕНИЯ ВОЗМОЖНЫ?

- Несовершенства операционных систем, прикладного ПО, инфраструктурных компонентов
- Недостаточность / некорректная настройка дополнительных средств защиты информационных ресурсов
- Доверчивость людей и низкая компьютерная грамотность
- Уязвимости для средств аутентификации

Посещение зараженных сайтов или вредоносы в письмах или проникновение с использованием технических уязвимостей

- Удаленное управление
- Социальная инженерия
- Подмена реквизитов

Хищение средств со счета

КАК «ТАМ» ОРГАНИЗОВАНО

- Мошеннические действия со стороны организованных групп с распределением по регионам и ролям — организация строится по распределённому принципу, в связи с чем практически невозможно вычислить всех участников группы

- Задания передаются через анонимные сетевые сервисы или по СМС, деньги переводятся на карты преступников через цепочку посредников

- Несколько участников группы имеют высшее образование и обладают навыками в области ИТ, психологии, знают приемы НЛП

- Как правило, преступление совершается в несколько этапов, реализация которых может осуществляться участниками группы в различных странах

КАК «ТАМ» ОРГАНИЗОВАНО

- Существует значительное число каналов незаконной торговли похищенной финансовой информацией и обмена сведениями о действиях служб безопасности банков и правоохранительных органов
- Для хищения используются компьютеры, мобильные телефоны, современные средства коммуникации
- Заблаговременно подготовленное обналичивание средств:

Банковские карты

Платежные системы

Электронные кошельки

Мобильные телефоны

МНОГООБРАЗИЕ УГРОЗ
И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

- Подключение / переподключение ДБО вместо клиента
- Несоответствие условий ДБО
- Юридические уязвимости в условиях ДБО
- Отсутствие полного комплекта документов (утрата / кража)

МНОГООБРАЗИЕ УГРОЗ
И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

- Социальная инженерия
- Фишинг
- Удаленное управление устройством пользователя
- Модификация платежного поручения перед его подтверждением на стороне клиента вредоносным ПО
- Кража паролей и ключей (в том числе одновременно с кражей устройства)

МНОГООБРАЗИЕ УГРОЗ
И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

- Уязвимости прикладного уровня
- Внесение нелегитимных изменений в настройки серверной части
- Удаленное управление инфраструктурой банка
- Недостаточная связь подписи с параметрами платежа
- Отсутствие механизмов выявления мошеннических транзакций
- Мошеннические действия персонала

СПОСОБЫ ЗАЩИТЫ

Защита серверной части

- Контроль целостности ДБО
- Регулярный анализ событий ИБ
- Управление уязвимостями
- Анализ исходного кода
- Контроль действий администраторов
- Ограничение доступа к ДБО
- Защита периметра

Организационные меры

- Обеспечение юридической значимости действий клиента в ДБО
- Выстроенные процедуры реагирования на инциденты
- Управление изменениями
- Страхование рисков

Надежная аутентификация

- Обязательный секрет, доступ к которому есть только у клиента
- Двухфакторная аутентификация с привязкой к параметрам транзакции
- Создание схемы, когда только клиент обладает всеми параметрами для подключения к интернет-банку

Повышение осведомленности клиентов

- Доступные и заметные инструкции
- Донесение необходимости принятия мер по защите устройств клиента

Защита от внутреннего злоумышленника

- Контроль действий персонала
- Ролевая модель

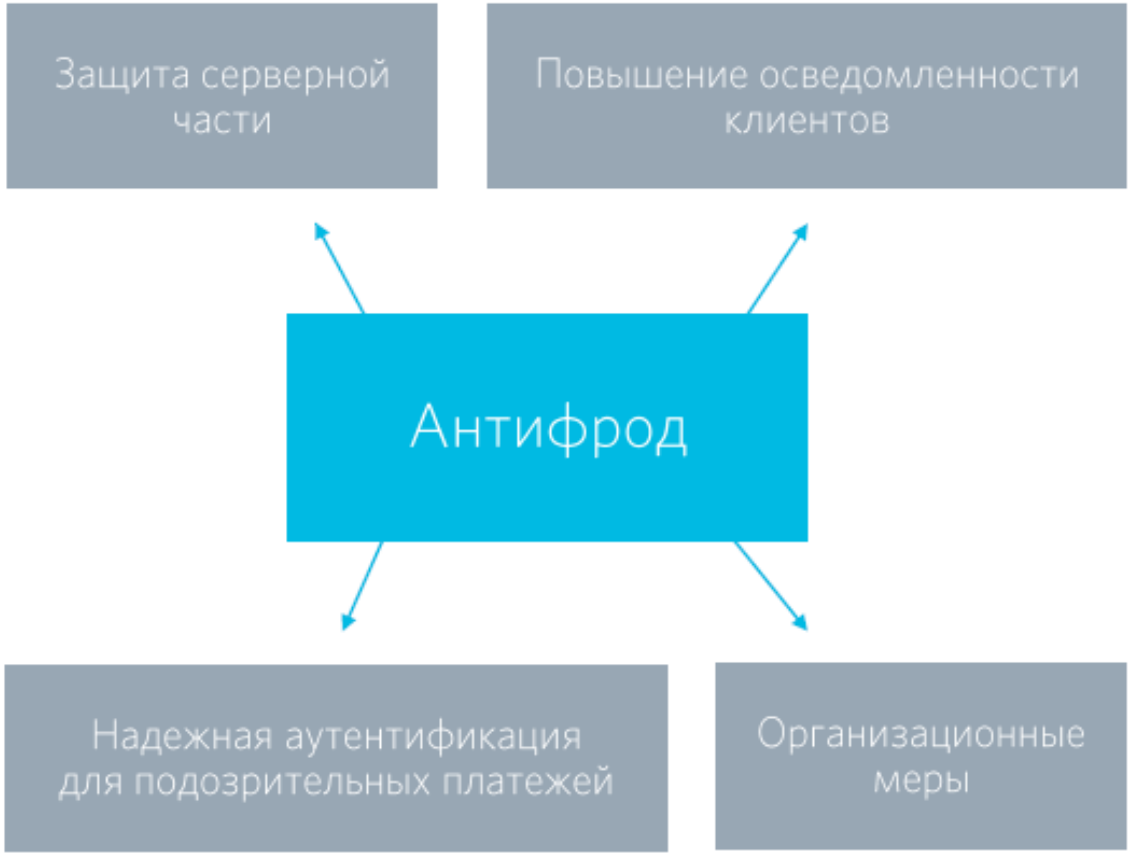
Антифрод

- Интеллектуальная блокировка транзакций без необходимости постоянного отвлечения клиентов

СПОСОБЫ ЗАЩИТЫ

Антифрод

- Интеллектуальная блокировка транзакций без необходимости постоянного отвлечения клиентов



Принципы работы:

- Блокировка платежей на этапах обработки в бэк-офисных системах
- Профили клиентов и их транзакций
- Возможность сравнения любых параметров платежей, клиентов, их входов в СДБО
- Не компонент СДБО
- Фиксация всех взаимодействий с клиентами

Решаемые задачи:

- Интеллектуальная блокировка транзакций без необходимости постоянного отвлечения клиентов
- Противодействие внешним атакам на серверную часть
- Возможность донесения до клиентов как им защититься самостоятельно
- Реагирование на инциденты и дополнительные подтверждения авторства транзакций

ОСОБЕННОСТИ
ЭКСПЛУАТАЦИИ АНТИФРОДА

- Линейная зависимость количества операторов от количества транзакций

- Отсутствие дополнительной информации о транзакциях, субъектах их совершающих

Что делать?

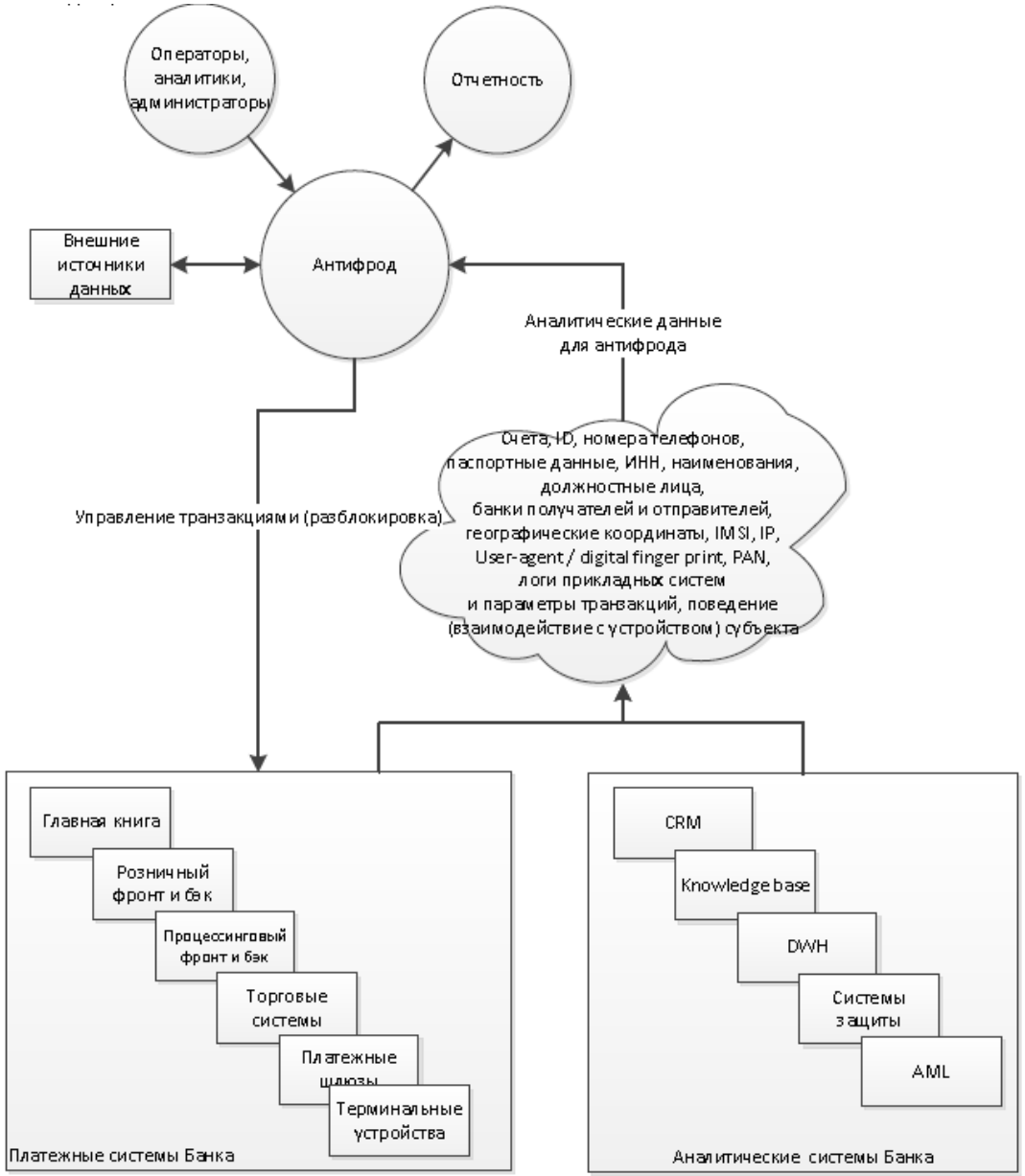
Искать новые источники информации, реализовывать кросс-канальный антифрод

Профилировать клиентов

СУТЬ
КРОСС-КАНАЛЬНОГО АНТИФРОДА

- Получить информацию о получателе денежных средств на основе данных иных учетных систем
- Произвести поведенческий анализ получателя денежных средств
- Выполнить анализ движений денежных средств по реквизитам получателя
- Блокировать отправку денежных средств получателю-злоумышленнику для всех каналов

ПРИМЕРНАЯ АРХИТЕКТУРА
КРОСС-КАНАЛЬНОГО АНТИФРОДА



ИЗ ЧЕГО СДЕЛАТЬ
КРОСС-КАНАЛЬНЫЙ АНТИФРОД

Вариант реализации	Плюсы	Минусы	Подводные камни
Антифрод в СДБО или процессинге	Уже работает для одного из каналов	Нетривиальные доработки с потенциальным изменением ядра решения	Ограничения архитектуры, ограничения производительности
AML + интерфейсы для блокировки транзакций	Правильная логика	Не видны	Далеко не всегда обеспечивает онлайн/псевдоонлайн
Специализированные решения	Целостное и целевое решение	Стоимость	Далеко не маленький проект

Вопросы

Заместитель директора по безопасности

КАСИМОВ
Вячеслав Валерьевич

kasimov@open.ru