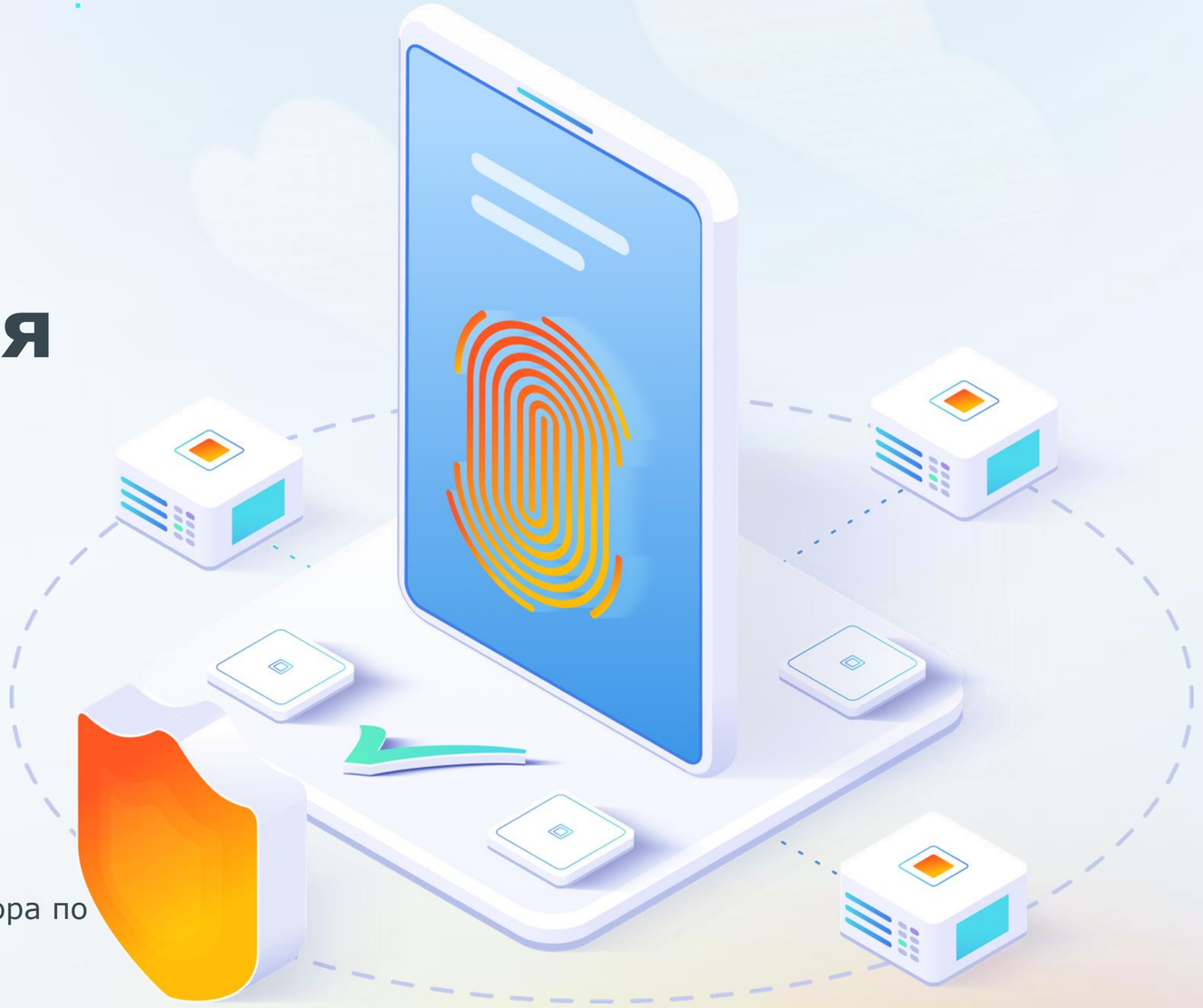
MANGO OFFICE | облачные бизнес-коммуникации

Информационная безопасность

при создании продуктов



Сергей Борисов

Заместитель Генерального директора по информационной безопасности
MANGO OFFICE

О компании

№1
среди провайдеров IP-телефонии*

21
год на рынке облачной телефонии

99,9%
отказоустойчивость

60 000
компаний-клиентов по всей России

100
городов в России

500 000
пользователей

4 млн
звонков в день совершают клиенты

300
разработчиков в команде

24/7
техподдержка и обслуживание клиентов

Mango Office — российский разработчик программного обеспечения и сервисов для коммуникаций. Один из ведущих поставщиков SaaS-решений и лидер отечественного рынка Виртуальных АТС

Компания создает технологичные продукты для отраслей реального сектора экономики. В продуктовой линейке Mango Office более 100 решений класса Unified Communications

* в рейтинге Market.CNews за 2021 год

Система обеспечения ИБ продуктов

1 Защита продуктов при разработке

- Безопасная разработка (SSDLC)

2 Защита продуктов при эксплуатации

- Защита каналов связи
- Защита данных клиентов
- WAF и anti-DDOS
- Сканирование на уязвимости
- Мониторинг и журналирование событий в АС
- Обеспечение непрерывности бизнеса
- Реализация мер для субъектов критической информационной инфраструктуры

3 Реализация бизнес-функций по ИБ в продуктах

- Управление правами доступа (ролевая модель)
- Двухфакторная аутентификация
- Защита сессий и паролей пользователей
- Защита каналов передачи данных
- Журналирование событий в продуктах

Безопасный подход к разработке продуктов

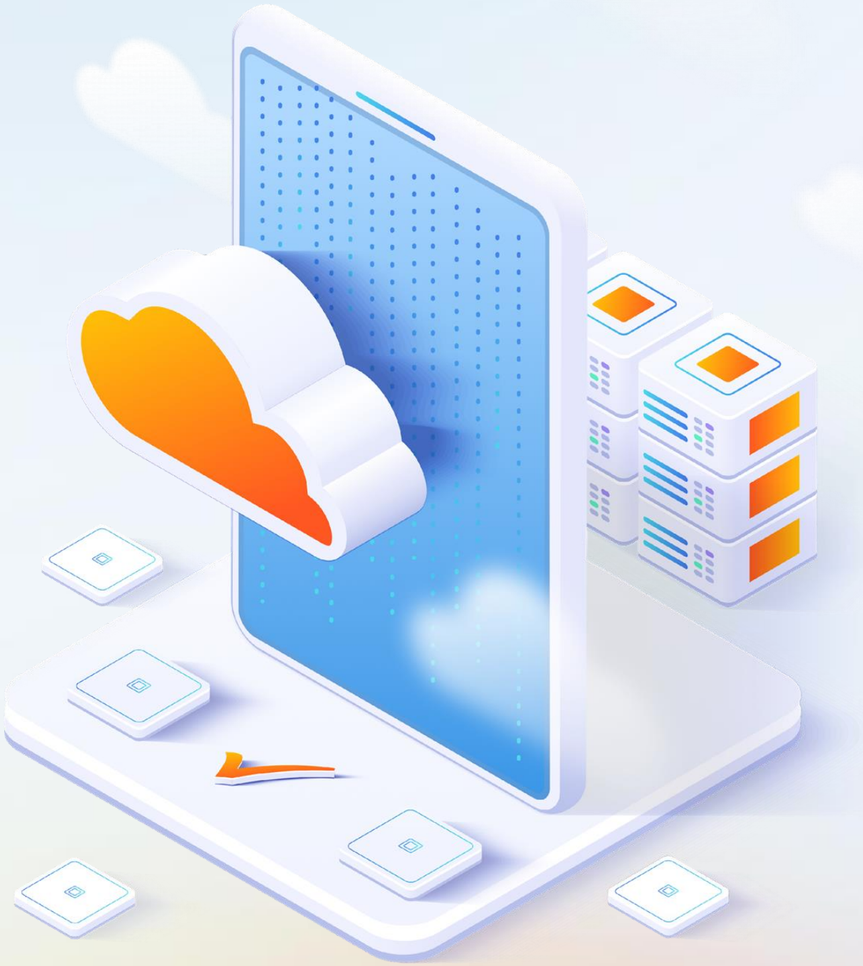
Что такое SSDLC

Данный процесс позволяет обеспечить безопасность разрабатываемых продуктов путем соблюдения требований на всех этапах жизненного цикла.

Что достигается благодаря процессу

Процесс необходим прежде всего для того, чтобы:

- Повысить уровень безопасности приложений еще на стадии разработки
- Уменьшить стоимость уязвимостей за счет исправления на ранних стадиях
- Повысить уровень безопасности CICD процесса и процесса разработки
- Соблюдать требования от крупных клиентов



SSDLC в MANGO OFFICE

В Компании выделено отдельное подразделение, отвечающее
за процесс безопасной разработки.
В этом году мы разработали и внедрили собственный процесс безопасной разработки
с использованием лучших мировых и российских практик.

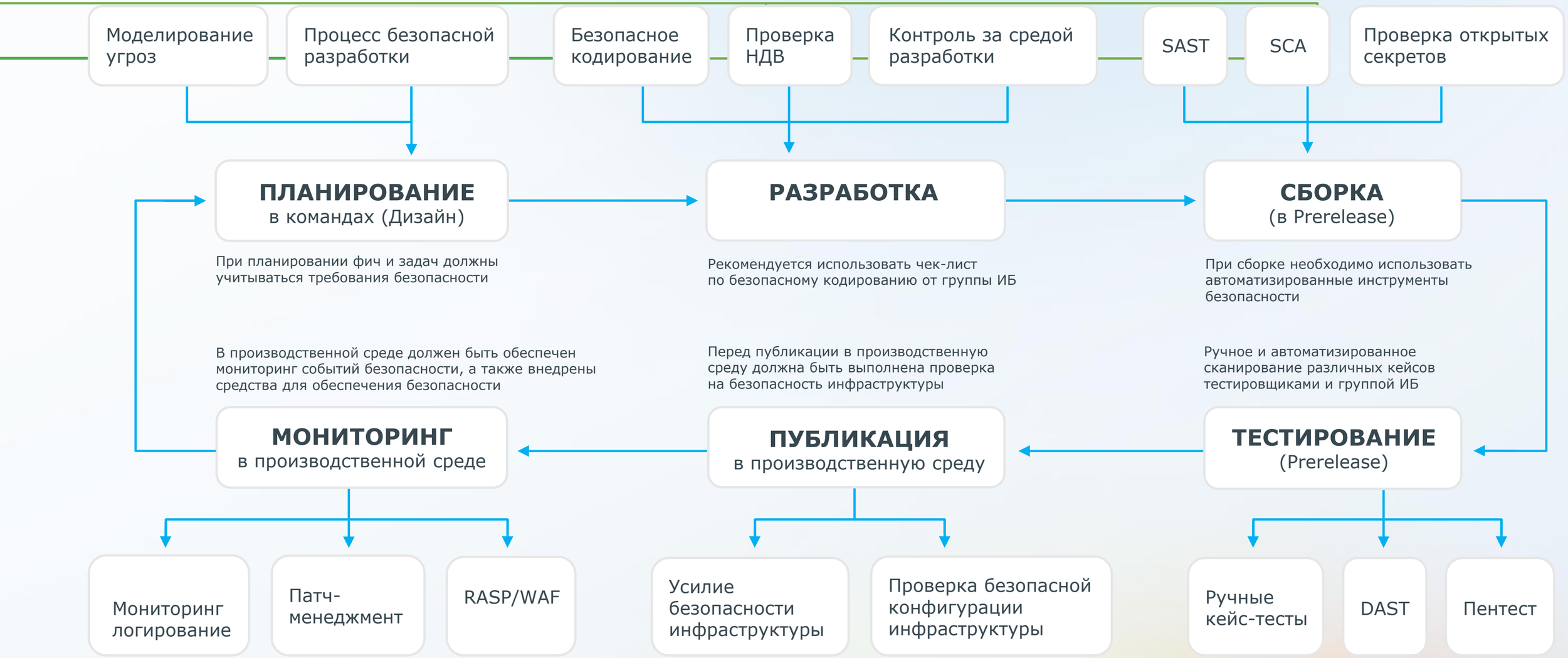
Мы **успешно адаптировали** разработанный процесс в существующий используемый в компании **фреймворк SAFe Agile** и уже применяем его на практике в наших продуктах.

Мы используем статический анализатор кода **(SAST) Solar AppScreener**. Для управления уязвимостями компонентов IT-инфраструктуры продуктов используются автоматизированные решения оценки защищенности, в частности **MPVM, OpenVAS** и средства для динамического анализа кода на базе **Acunetix**.

Мы **проводим ряд мероприятий** с командами, чтобы в долгосрочной перспективе повышать уровень информационной безопасности в процессах разработки:

- Моделирование угроз;
- Обучение команд практикам безопасного кодирования;
- Код-ревью с участием специалистов по ИБ;
- Формирование функционала, связанного с безопасностью в продуктах.

Жизненный цикл безопасной разработки продуктов



Защита продуктов при эксплуатации. Основной минимум

Защита каналов связи (TLS и SRTP)

1. TLS

- Взаимодействие по HTTPS (например, https://lk.mango-office.ru/)
- Передача записей звонков на FTP-сервер (см рис. ниже)
- Передача управляющего трафика в процессе звонков по протоколу SIP

2. SRTP (RTP через IPsec)

Защита данных клиентов

1. Защита осуществляется на уровнях сервисов и базы данных
2. При любом обращении к данным автоматически производится проверка их принадлежности к конкретному продукту и к конкретному владельцу
3. Производится журналирование действий наших сотрудников во внутренней системе
4. Ролевая модель

WAF и anti-DDOS

Используются сервисы от российской компании QRATOR и SolidWall

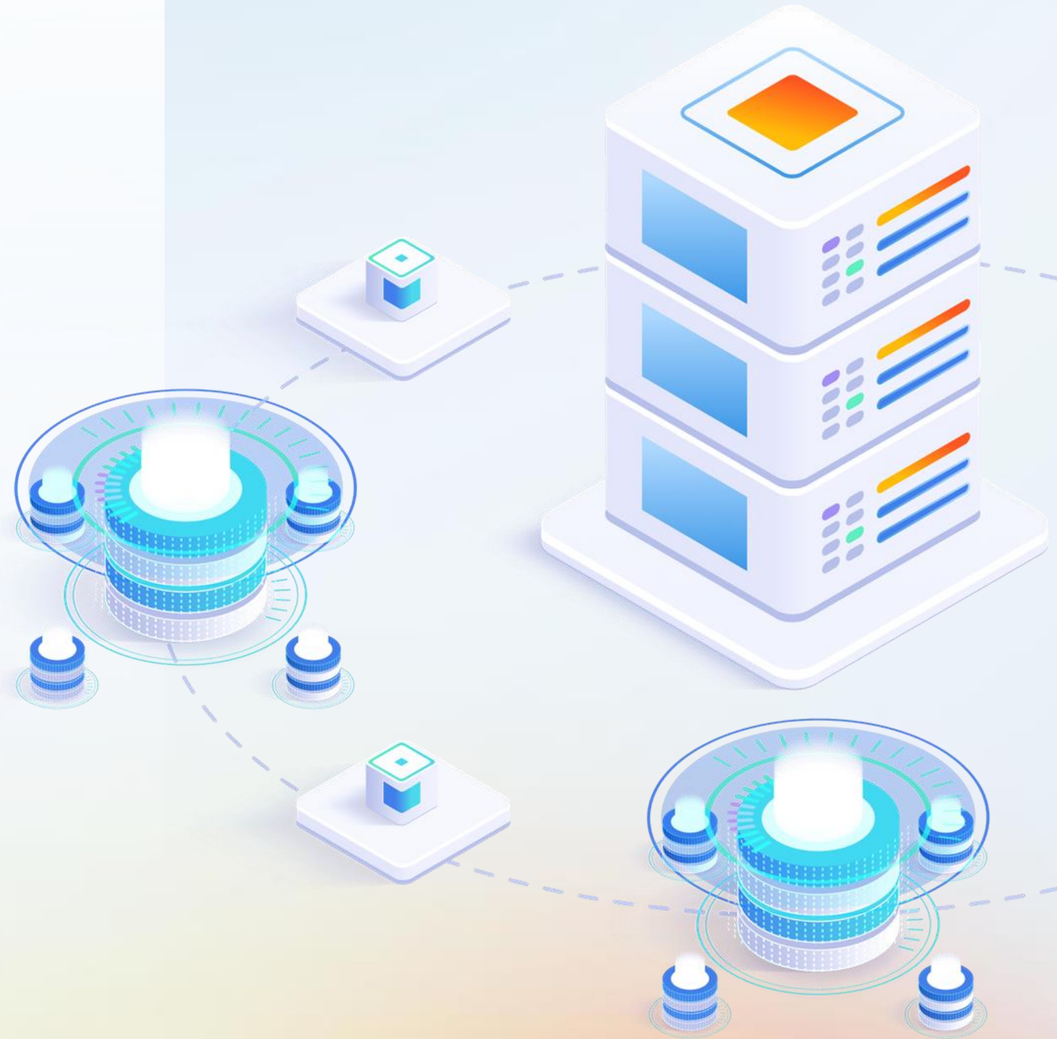
Сканирование на уязвимости

На постоянной основе производится сканирование периметра и узлов АС российским решением MaxPatrol VM

Мониторинг и журналирование событий в АС

Обеспечение непрерывности бизнеса

1. Резервное копирование
2. Резервирование мощностей
3. Тестирование процессов восстановления при авариях
4. 3 распределенных ЦОДа в Москве



MANGO OFFICE

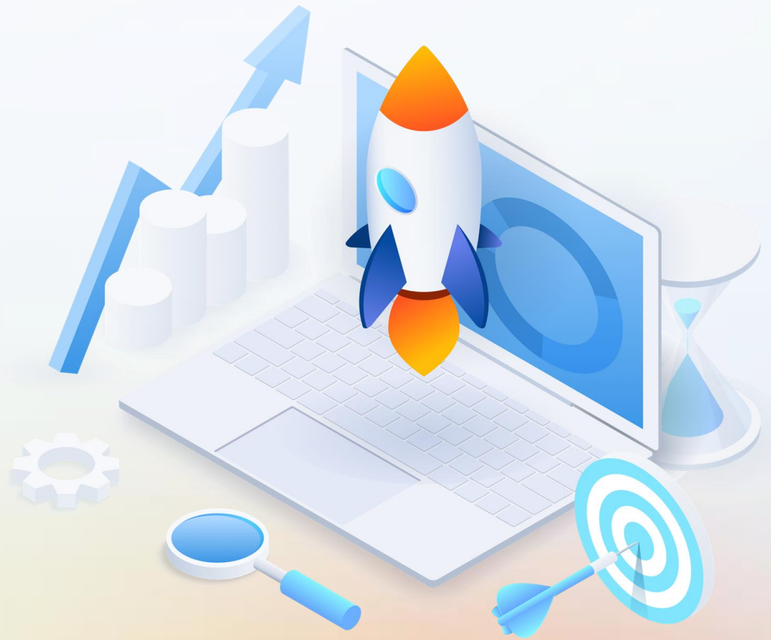
Базовый функционал ИБ для клиентов

Реализовано

- ✓ Защита управляющих данных с помощью протоколов TLS
- ✓ Возможность опционально настроить использование защищенного протокола передачи голосовых сообщений SRTP
- ✓ Контроль сложности паролей при их смене
- ✓ Применение двухфакторной аутентификации для администраторов личного счета с использованием e-mail или SMS
- ✓ Сброс активных пользовательских сессий на всех устройствах при смене пароля пользователя
- ✓ Развитая модель доступа, позволяющая:
  - на уровне ролей определять для пользователей доступ к тем или иным функциям и информационным объектам системы на уровне пользовательских групп
  - гибко настраивать пользователям возможность видимости и прослушивания звонков подконтрольных им сотрудников.

В планах (осень 2022)

- ✓ Двухфакторная авторизация для всех сотрудников
- ✓ Фильтрация входа в систему по чёрным спискам IP адресов
- ✓ Вывод списка ролей с функциями



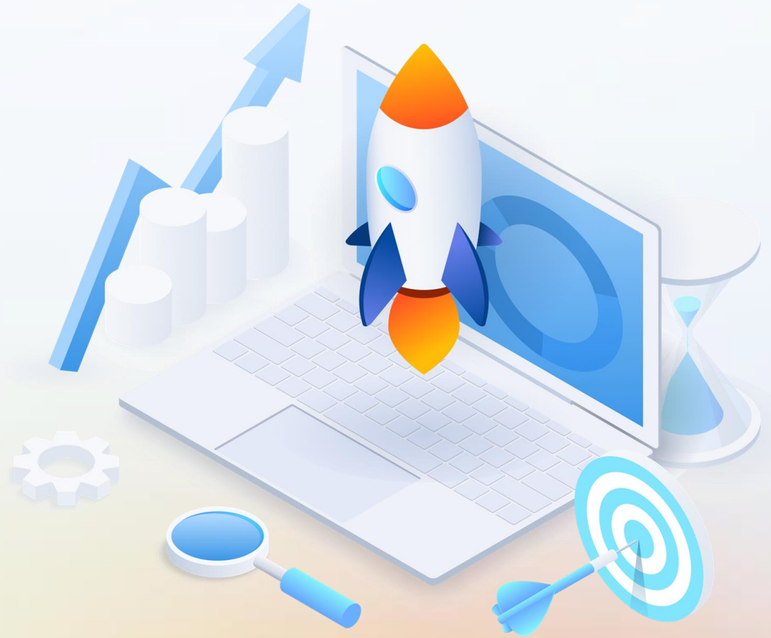
Базовый функционал ИБ для клиентов

Реализовано

- ✓ Настраиваемые предустановленные и пользовательские роли
- ✓ Интеграция с LDAP
- ✓ Данные клиентов разграничиваются на уровнях сервисов и базы данных. При любом обращении к данным автоматически производится проверка их принадлежности к конкретному продукту и к конкретному владельцу
- ✓ Производится журналирование действий наших сотрудников во внутренней системе

В планах (осень 2022)

- ✓ Вывод списка пользователей, которым доступен конкретный объект
- ✓ Присваивание пользователю роли и участие в группах, как у другого пользователя
- ✓ Реализация подачи событий безопасности через SysLog
- ✓ Отслеживание неуспешных попыток входа пользователей



MANGO OFFICE

Базовый функционал ИБ для клиентов

Реализовано

✓ Журналирование событий:

- Создание/редактирование/удаление учетной записи пользователя
- Вход/выход пользователя
- Неуспешная попытка входа пользователя
- Факт запроса паролей от SIP-учёток
- Факт прослушивания и выгрузки записей разговоров
- Изменение списка пользователей, разговоры которых подлежат речевой аналитике

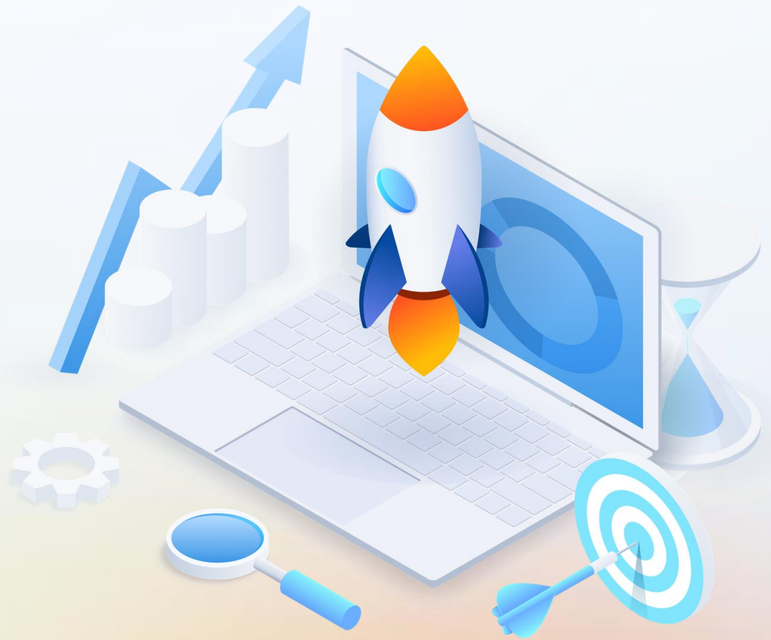
✓ События авторизации в MangoTalker

✓ Возможность определять список стран, куда клиентом разрешены исходящие вызовы

В планах (осень 2022)

✓ Журналирование событий:

- Факт поиска по истории записей разговора
- Факт экспорта истории вызовов



MANGO OFFICE

Функционал ИБ для клиентов зима 2022-2023

Зима 2022-2023

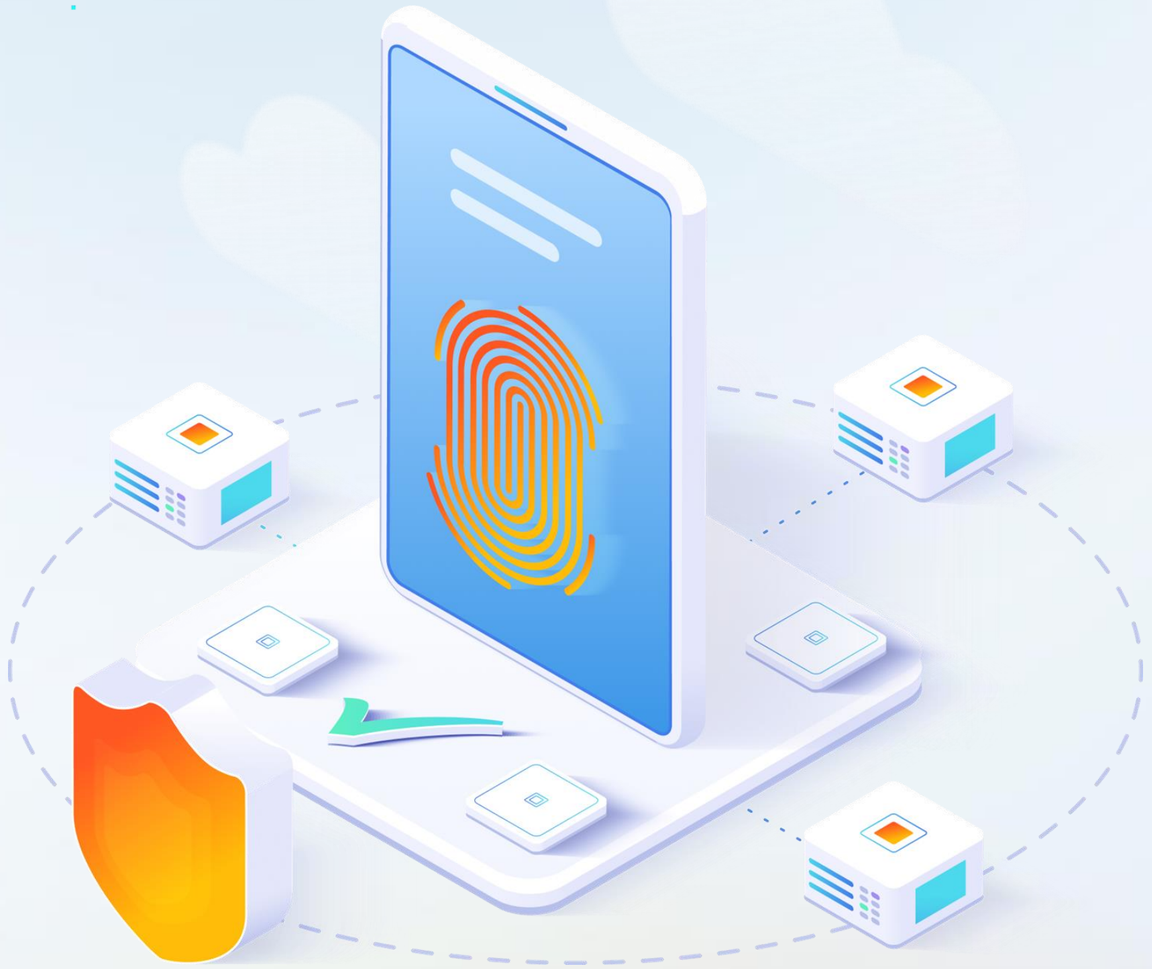
- ✓ Возможность аутентификации и авторизации в продуктах MANGO OFFICE с помощью корпоративных сервисов SSO (WebSSO решения типа SAMLv2)
- ✓ Настройка сложности паролей, устанавливаемых пользователями в аккаунте ЛК
- ✓ Настройка срока жизни паролей для пользователей
- ✓ Настройка длительности сессий для пользователей
- ✓ Настройка срока действия токена API Коннектор
- ✓ Настройка поведения системы при подборе паролей
- ✓ Задание времени жизни учетных записей при их создании (для тестирования или временных работ)
- ✓ Возможность сброса паролей сотрудников ЛС
- ✓ Возможность для клиента выбрать необходимые для логирования события безопасности для отправки в SysLog
- ✓ Выгрузка логов в формате JSON через API
- ✓ Ограничение видимости в журнале событий в зависимости от роли просматривающего пользователя
- ✓ Отправка на e-mail администраторов уведомлений о входе определенных сотрудников в ЛК
- ✓ Оповещение администратора о доступе к данным VIP абонентов
- ✓ Авторизация клиентом действий сотрудников службы поддержки MANGO OFFICE
- ✓ Вывод информации по настроенным дополнительным каналам: интеграциям и оповещениям
- ✓ Подсистема корреляции событий в продуктах MANGO OFFICE для нужд клиентов
- ✓ Постоянный мониторинг событий службой информационной безопасности MANGO OFFICE

MANGO OFFICE | облачные бизнес-коммуникации

Спасибо за внимание!

Сергей Борисов

Заместитель Генерального директора по информационной безопасности
MANGO OFFICE



*8005 mango-office.ru t.me/mango_office