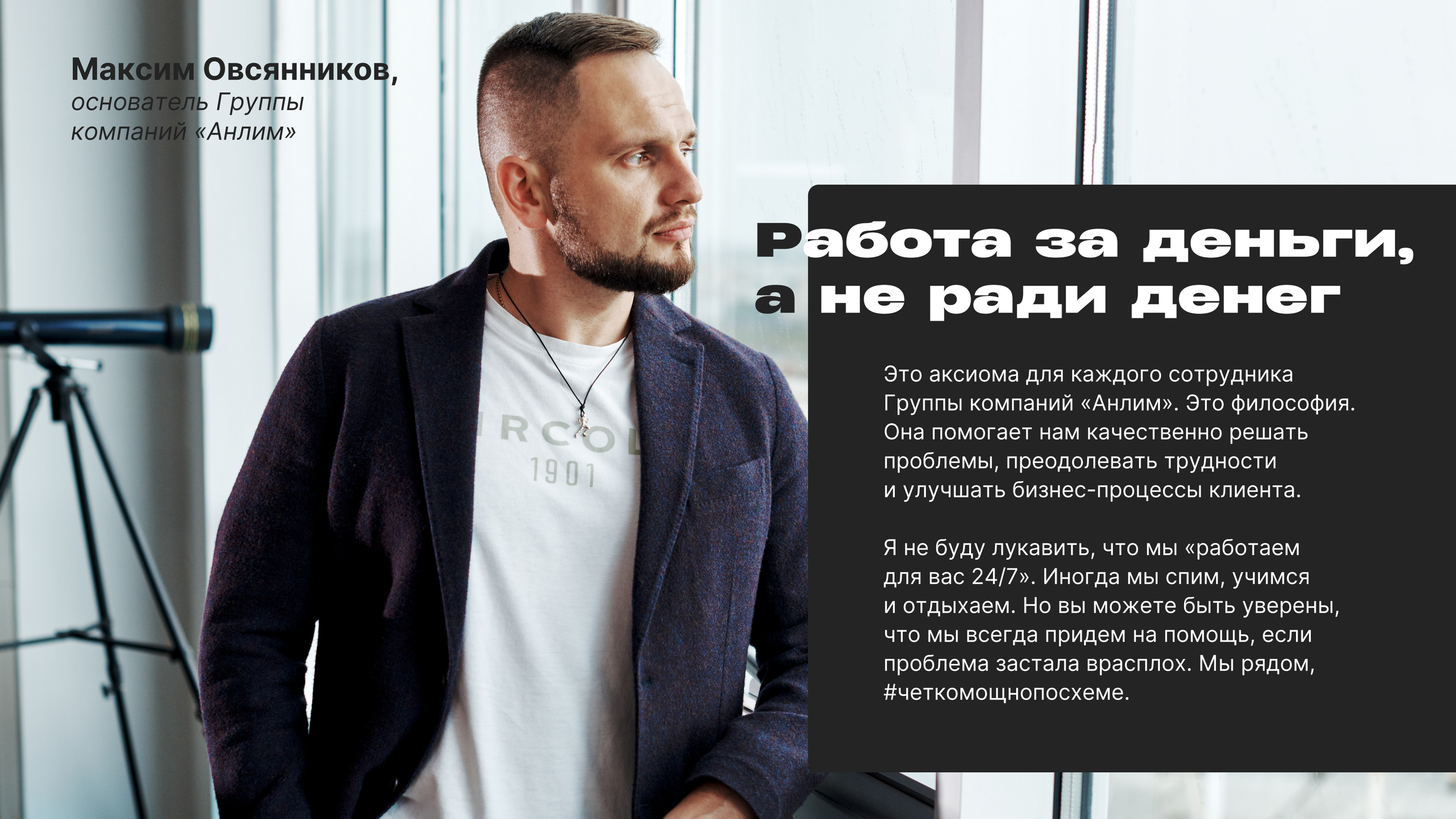
МЫ ТАМ, ГДЕ МЫ НУЖНЫ

СО ЗНАНИЕМ ДЕЛА

УСЛУГИ И ПРОДУКТЫ

Анлим



Максим Овсянников,
основатель Группы компаний «Анлим»

Работа за деньги, а не ради денег

Это аксиома для каждого сотрудника Группы компаний «Анлим». Это философия. Она помогает нам качественно решать проблемы, преодолевать трудности и улучшать бизнес-процессы клиента.

Я не буду лукавить, что мы «работаем для вас 24/7». Иногда мы спим, учимся и отдыхаем. Но вы можете быть уверены, что мы всегда придем на помощь, если проблема застала врасплох. Мы рядом, #четкомощнопосхеме.

СОДЕРЖАНИЕ

4

Внедрение решений по информационной безопасности

Infotecs, Check Point, Positive Technologies, Код безопасности, Конфидент и другие

7

Проектирование и внедрение георасспределенных систем обеспечения информационной безопасности

Проектное управление, комплексная защита ГИС*, создание распределенных систем защиты информации

9

Разведка на основе открытых источников

Разведка на основе открытых источников для оценки уровня защищенности организации и обнаружения слабых мест

11

Тестирование на проникновение

Имитация действий злоумышленника для обнаружения слабых мест в защите

15

Расследование компьютерных преступлений

Определение хронологии и сути инцидента, потенциальных причин возникновения, формирование рекомендаций по устранению

19

Разработка ПО. Анлим-Софт

Разработка и продвижение собственных IT-решений, создание заказного ПО

ВНЕДРЕНИЕ РЕШЕНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для кого?

Для организаций, которые используют средства защиты информации или планируют их использовать

Анлим-ИТ уже 11 лет активно реализует на рынке информационной безопасности проекты в Уральском Федеральном округе и за его пределами.

Это центр компетенций по решениям в сфере информационной безопасности. Особо отметим производителей Infotecs, Лаборатория Касперского, PT, Код безопасности и Конфидент.

Ценность для клиента

Качество выполненных работ, квалифицированная поддержка

Ценность для партнера

Расширение присутствия в системе существующих заказчиков

Партнер	Статус	Сертификаты
Лаборатория Касперского	GOLD	Kaspersky Security Center Scaling, Certified Professional 002.11.6, Kaspersky Endpoint Detection & Response Optimum, Certified Professional 005.11, Certified System Engineer 009.11, P25.37 Certified Professional: KATA Platform & EDR Expert Presales
Infotecs	Платина	Администратор СЗИ VipNet 4
Positive Technologies	Advance партнер: PT Application Inspector, MaxPatrol8, PT Application Firewall, MaxPatrol SIEM, PT Sandbox, PT NAD, MP VM	SC MP 8, CS MP 8, SC PT AF, CS PT AF, CP PT AF, SC MP SIEM, CS MP SIEM, CP MP SIEM, CS PT AI, CS PT NAD, SC PT NAD, CP PT NAD, CS MP VM , SC MP VM, CS PT Sandbox

Партнер	Статус	Сертификаты
АльфаДок КейСистемс-Безопасность	Золотой партнер	–
Конфидент	Platinum	Администрирование СЗИ Dallas Lock
Киберпротект	Авторизованный партнер	–
Astra Linux	Авторизованный партнер	ALSE-1606
Phishman	Авторизованный партнер	–
Код безопасности	Platinum Partner. Специализация: Network, Workstation, Virtualization + Сервисный партнер	Инженер защиты сети «Континент», инженер СЗИ SNS, инженер СЗИ vGate
Check Point	** (из 5-ти звезд) Sandblast Parther Check Point Certified Collaborative Support Provider (CCSP) Harmony Partner	CCSE, Harmony Pre sales, CCTE, CPSC, Quantum Sales, Harmony Sales

Другие партнеры

Аладдин Р.Д., UserGate, Р7-офис, Крипто-Про, GroupIB, SearchInform, Ред Софт, Индид, Мой Офис, Айдеко, Яндекс.Облако, Гарда Технологии

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ ГЕОРАСПРЕДЕЛЕННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для кого?

Для государственного сектора с подразделениями или подведомственными учреждениями в субъектах РФ

При создании новых государственных информационных систем (ГИС) федерального уровня всегда остро встает вопрос обеспечения информационной безопасности.

Оптимальный вариант – параллельное создание информационной системы и системы защиты.

Ценность для клиента

Комплексная «бесшовная» реализация проектов в защищенном исполнении

Ценность для партнера

Комплексная реализация проекта, единое входное окно в виде эксперта по ИБ

Этапы

ТЕСТИРОВАНИЕ 01

ПРОЕКТИРОВАНИЕ 02

НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ 03

РАЗВЕДКА НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ

Для кого?

Для организации, заинтересованной в фактической информационной безопасности

Разведка на основе открытых источников позволяет предварительно оценить уровень защищенности организации и обнаружить самые слабые места во внешнем периметре организации.

КАКУЮ ИНФОРМАЦИЮ СОБИРАЕМ?

Информацию об используемых в организации технологиях

Корпоративные почтовые адреса сотрудников организации

Информацию в соцсетях сотрудников

Список поддоменов и IP-адресов организации, которые могут стать точкой входа для нарушителя

Список паролей в открытом доступе

Любую информацию в сети, которую могут использовать злоумышленники

Ценность для клиента

Получить информацию о своей компании, которая уже может находиться в руках злоумышленников

Ценность для партнера

Повышение доверия клиента, возможность начать взаимодействие по вопросам ИБ

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Для кого?

Для организации, заинтересованной в фактической информационной безопасности

Это наиболее эффективный метод оценки текущего уровня защищенности информационной инфраструктуры.

Это доказательный метод, он даёт объективную оценку информационной безопасности организации.

Ценность для клиента

Защита от реальных атак, объективная оценка защищенности инфраструктуры

Ценность для партнера

Расширение области присутствия, конкурентное преимущество

ЧТО ТЕСТИРУЕМ?

- Прикладное ПО
- Сеть
- Серверную инфраструктуру
- Периметр сети
- Веб-ресурсы
- Автоматизированные рабочие места
- Базы данных

КАК ТЕСТИРУЕМ?

BLACKBOX

Тестирование,
при котором ничего
неизвестно о компании,
только её название

GRAYBOX

Частичная передача
информации
о компании (например,
диапазон IP адресов,
которые можно
просканировать или
список email-адресов)

Проникновение в инфраструктуру и выявление уязвимых мест – не конечная точка. Главная цель – показать проблему, которая может нанести реальный ущерб, рассказать о рисках и путях решения

КЕЙСЫ

2019

Сфера питания

Нашли и проэксплуатировали критические уязвимости в интернет-магазине

Региональный центр обработки данных

Получили пароли администраторов доменов, нашли критические уязвимости, получили доступ к десяткам веб-ресурсов

Кредитная финансовая организация

Получили доступы к автоматизированной банковской системе, сетевому оборудованию, почте, домену, платежным системам

2020

Разработчик программного обеспечения

Проанализировали исходный код и получили доступ к конфиденциальной информации, администрированию приложения, нашли уязвимости, превышение привилегий, обход лицензии

СМИ

Скомпрометировали СЭД, информационную систему по размещению новостей, получили полный доступ к сетевому оборудованию и контроллеру домена

Разработчик программного обеспечения

Получили полный доступ к Wi-Fi и сетевому оборудованию, к файловому хранилищу и исходным кодам приложений, к заказчикам посредством VPN и 1С

2021

МФЦ

Получили доступ к сетевому оборудованию, почте, wi-fi, домену, к локальной сети через web

Медицинская организация

Получили доступ к сетевому и медицинскому оборудованию, к почте и Wi-Fi

Некредитная финансовая организация

Обнаружили уязвимости в веб-ресурсах, получили полный контроль над ним, оформили услугу со скидкой 99%; получили логины, хэши паролей, персональные данные клиентов

2022

Онлайн-сервис для граждан

Получили доступ к десяткам веб-ресурсов и ключевым внутренним ресурсам организации, нашли критические уязвимости.

Международная промышленная компания

Получили доступ к сайту и ключевым внутренним ресурсам организации

Крупный зарубежный банк

Получили доступ к интернет-банкингу и внутренней инфраструктуре

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Для кого?

Для компании, в которой произошел инцидент, связанный с информационной безопасностью; компании, заинтересованной в раннем реагировании на такие случаи

Расследование инцидента информационной безопасности позволяет определить его хронологию и вектор развития, потенциальные причины возникновения, определить рекомендации по их устранению и исключению и (или) снижению вероятности появления подобных инцидентов в будущем

КАК МЫ РАБОТАЕМ?

Ценность для клиента

Выявление причин инцидента, предотвращение повторного происшествия, поиск нарушителей

Ценность для партнера

Расширение области присутствия, конкурентное преимущество

01

Анализируем журналы средств защиты информации

02

Проводим ручной и автоматизированный анализ:

- данных браузера;
- журналов событий;
- лог-файлов серверов;
- файлов реестра;
- лог-файлов ПО;
- сетевого трафика
- дампа оперативной памяти;
- образа накопителя или виртуальной машины;
- адресного пространства неизвлекаемых носителей;
- вредоносного ПО;
- устройства, задействованного в инциденте.

03

Объединяем результаты, строим карту атаки и готовим заключение специалиста/эксперта

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВЫХ СИСТЕМ

Для кого?

Для банков, страховых компаний, ломбардов

Информационная безопасность кредитных организаций всегда была самой развитой и высокотехнологичной в стране, на данный момент ИБ таких компаний жестко регламентируется, поэтому не уделять ей внимание невозможно

ЧТО МЫ ПРЕДЛАГАЕМ?

Ценность для клиента — Исполнение обязательных требований Банка России и реальная защита инфраструктуры

Ценность для партнера — Расширение области присутствия, конкурентное преимущество

	ИБ кредитных организаций	ИБ некредитных организаций
Предварительная оценка соответствия требованиям Банка России*	+	+
Внедрение организационных и технических мер защиты в соответствии требованиями Банка России *	+	+
Оценка по требованиям ГОСТ Р 57580.2 -2018	+	+
Проведение тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры	+	+
Разработка документации в соответствии с СТО БР ИББС	+	–
Оценка по требованиям Положения Банка России от 09.06.2012 № 382-П	+	–
Анализ уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений по требованиям к оценочному уровню доверия (не ниже ОУД 4)	+	+

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

АНЛИМ-СОФТ

Анлим-Софт

Команда высококвалифицированных специалистов по разработке программного обеспечения

РАЗРАБОТКА СОБСТВЕННЫХ IT-РЕШЕНИЙ*

Продвижение через партнерскую сеть по всей стране

*Все программные продукты официально зарегистрированы и внесены в Реестр отечественного ПО

АУРА
система ведения аудиозаписи и анализа звука

Комплексная система записи разговоров с клиентами с микрофона или бейджа. Организует и защищает данные в соответствии с требованиями законодательства.

Заказчики

мои документы государственные и муниципальные услуги

Филиал Томского НИМЦ Тюменский кардиологический научный центр

Служба здоровья Городская поликлиника №5

ОКБ 2

Потенциальный сегмент рынка: МФЦ, медицинские и социальные учреждения, учебные заведения, дилерские центры, банки, ритейл и девелопмент

- Запись «живых» диалогов (микрофон/бейдж)
- Выборочное прослушивание аудиозаписей
- Интеграция со сторонними системами
- Оперативный разбор инцидентов

LOCUS
платформа управления жизненным циклом здания

Единый цифровой контур взаимодействия заказчика, проектировщика, подрядчика и обслуживающей организации. Платформа предназначена для повышения рентабельности за счет сокращения временных затрат, потери ресурсов и оптимизации процесса управления строительными проектами.

Потенциальный сегмент рынка: строительство и обслуживающие организации

- База форм исполнительной документации по видам работ
- Учет и приемка материалов на строительных объектах
- Автоматическое формирование общего и специальных журналов работ, исполнительной документации по проекту
- Согласование исполнительной документации
- Ведение и учет строительного объекта в электронном виде
- Гибкая ролевая модель
- Приглашение участников по реферальной ссылке

АТОМ
система

Обеспечивает централизованный контроль расхода электроэнергии с возможностью сбора статистических сведений и формирования отчетов о расходе в разрезе времени.

Заказчик

НОВОУРЕНГОЙСКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ НУРМК

Потенциальный сегмент рынка: обслуживающие организации, собственники зданий

- Взаимодействие с электрическими счетчиками через протокол Modbus RTU
- Печатные формы актов и отчета снятия показаний приборов учета
- Сбор данных со счетчиков в диапазоне от одного часа и реже
- Централизованное администрирование системы
- Логирование действий пользователей
- Ведение нескольких объектов, принадлежащих разным юридическим лицам

ПУЛЬС
система

Система диспетчерского управления устройствами автоматики и телемеханики движения поездов метрополитена.

Заказчик

Станция метро «Спортивная» города Новосибирск

Потенциальный сегмент рынка: метрополитен

Сбор, передача, контроль, отображение и накопление информации с устройств автоматики и телемеханики движения поездов

Специалист

АРГОС
система

Программа для сбора и обработки информации о событиях с металлодетекторов и ip-камер, с целью обеспечения пропускного режима и безопасности на объектах, требующих пропускного контроля.

Потенциальный сегмент рынка: аэропорты, вокзалы, производство, торговля

- Сбор и обработка информации с возможностью просмотра видеозаписей и фотографий
- Визуальная индикация событий на АРМ диспетчера при наличии металла или радиоактивных элементов
- Система дашбордов для центрального диспетчера
- Возможность записи данных в кэш АРМ диспетчера в случае отсутствия соединения с сервером

КАЙДЗЕН

система автоматизированного управления судебными заседаниями

Позволяет создавать единый цифровой контур по организации процесса подготовки и проведения судебных заседаний.

Заказчик

Арбитражный суд Западно-Сибирского округа

Потенциальный сегмент рынка: арбитражные суды (готовое решение), суды других инстанций (проектное внедрение с доработками

- Интеграция с федеральной картотекой арбитражных дел
- Фиксация явки сторон с момента входа в здание с возможностью отправки push-уведомлений
- Голосовое оповещение сторон
- Контроль действий пользователей в системе
- Управление статусами судебного заседания
- Аудиопротоколирование судебного заседания

ЦИФРОВОЙ АССИСТЕНТ

платформа

Комплексная платформа для оперативного и гибкого формирования задач с помощью telegram-бота.

Потенциальный сегмент рынка: МФЦ, исполнительные органы власти, образовательные учреждения, коммерческие компании (>20 сотрудников), организации, работающие удаленно

БОТ
Виртуальный помощник в Telegram, которого можно добавить в общий чат, чтобы управлять задачами

РАБОЧЕЕ ПРОСТРАНСТВО
Совокупность всех досок с задачами, к которым вам предоставили доступ или которые вы создали сами

КАНБАН-ДОСКА
Цифровое пространство, в котором визуально представлены все задачи

САФР
система

Система анализа эмоционального фона речи. Основана на технологии распознавания эмоций на базе нейронной сети, которая обрабатывает набор признаков, полученных алгоритмами анализа звука.

- Аудиозапись общения сотрудников и клиентов через микрофон или бейдж
- Возможность прослушивать накопленные аудиозаписи
- Автоматическая классификация по наличию или отсутствию признаков инцидента

Создаем **IT-решения**, которые **помогают бизнесу**

ЗАКАЗНАЯ РАЗРАБОТКА

«Анлим-Софт» предлагает разработку уникального продукта под задачи бизнеса. В том числе с полной передачи прав на результат интеллектуальной деятельности

Основные языки программирования:

Backend: Python, C, Kotlin, Java. Фреймворк – web2py, spring
Frontend: JavaScript с использованием фреймворков Vue js и Electron js, React js.

ЦИКЛ ПРОЕКТА

01 CUSTDEV РЫНКА

02 ПОДГОТОВКА ТЕХНИЧЕСКОГО ЗАДАНИЯ, РАЗРАБОТКА МАКЕТОВ ЭКРАННЫХ ФОРМ

03 ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА СИСТЕМЫ ПО МЕТОДОЛОГИИ AGILE

04 КОМПЛЕКСНОЕ ТЕСТИРОВАНИЕ И СОПРОВОЖДЕНИЕ

АНЛИМ
ГРУППА КОМПАНИЙ

Информационная безопасность | Техническое сопровождение | Разработка ПО для бизнеса

Тюмень, БЦ «Нобель Парк»,
ул. Пермякова, 1,
ст. 5, офис 1401

info@unlim.group

+7 (3452) 58-58-37

unlim.group

МЫ НУЖНЫ ТАМ, ГДЕ МЫ