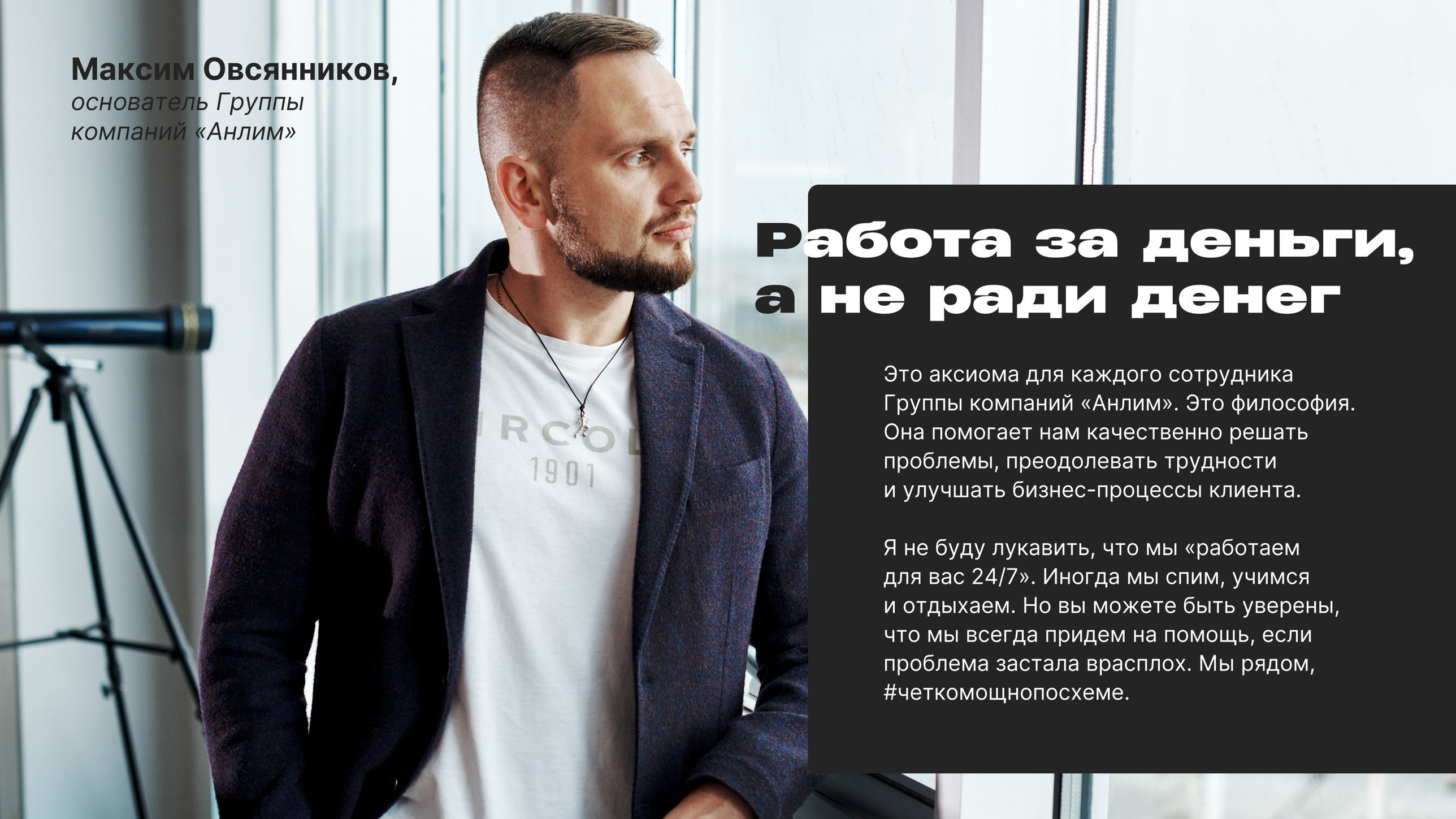
СО ЗНАНИЕМ ДЕЛА

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

ВНЕДРЕНИЕ РЕШЕНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДЛЯ КОГО?

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

Анлим уже 12 лет активно реализует на рынке информационной безопасности проекты в Уральском Федеральном округе и за его пределами.

Группа компаний выступает центром компетенций по решениям в сфере кибербезопасности. Сейчас в число партнеров входит более 50 вендоров, дистрибьюторов и поставщиков. И мы стараемся постоянно увеличивать эту цифру, чтобы иметь возможность подбирать наиболее подходящие решения для наших заказчиков.

50+
ПАРТНЕРОВ

positive technologies
kaspersky
UserGate
КОД безопасности
Security Vision
INFOWATCH
infotecs
CROSSTECH SOLUTIONS GROUP
АЙТИБАСТИОН
CHECK POINT
YOU DESERVE THE BEST SECURITY
КОНФИДЕНТ
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ
AXOFT
rrc Security
альфа
ideco
КИБЕРПРОТЕКТ
phishman
Р7-ОФИС

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ ГЕОРАСПРЕДЕЛЕННЫХ И КОМПЛЕКСНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДЛЯ КОГО?

Для любых компаний, заинтересованных в обеспечении информационной безопасности

01 Определение уязвимых мест в инфраструктуре заказчика

02 Подбор решений по информационной безопасности

03 Демонстрация решений и проведение пилотных проектов

04 Проектирование комплексной системы обеспечения информационной безопасности

05 Внедрение системы обеспечения информационной безопасности

06 Обучение сотрудников заказчика работе с внедренными решениями

07 Техническое обслуживание и сопровождение системы информационной безопасности

КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КЕЙСЫ

КЕЙСЫ

КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КРУПНЫЙ ЗАСТРОЙЩИК

- Тестирование на проникновение
- Проектирование системы защиты
- Внедрение системы защиты
- Консультативная помощь

ФЕДЕРАЛЬНАЯ ВЫСОКОТЕХНОЛОГИЧНАЯ МЕДИЦИНСКАЯ ОРГАНИЗАЦИЯ

- Расследование инцидентов
- Сегментирование сети
- Построение комплексной системы защиты информации

РЕГИОНАЛЬНЫЕ И МУНИЦИПАЛЬНЫЕ ОРГАНЫ ВЛАСТИ

- Формирование концепции информационной безопасности
- Проектирование систем защиты
- Создание условий для построения центров мониторинга уровня региона, муниципалитета

ОРГАНИЗАЦИЯ ТЭК

- Расследование инцидента
- Анализ устойчивости инфраструктуры к атакам
- Подбор решений
- Построение комплексной системы защиты информации

РЕГИОНАЛЬНЫЙ БАНК

- Тестирование на проникновение
- Построение комплексной системы защиты информации

ПОСТРОЕНИЕ РАСПРЕДЕЛЕННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КЕЙСЫ

01 Построение территориально распределенных систем ИБ в рамках одной организации, дочерних обществ или различных организаций, объединяемых для информационного взаимодействия

02 Не привязаны к территории, работаем по всей стране, а при необходимости и за ее приделами

03 Для больших проектов со сжатыми сроками или проектов, область реализации которых выходит за пределы одного субъекта РФ, подключаем широкую сеть доверенных партнеров, в то же время сами готовы осуществлять руководство проектом

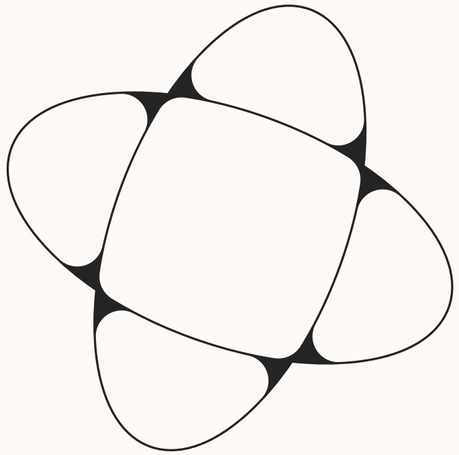
04 Осуществляем проектирование распределенных систем, оптимизируем временные и денежные траты на командировки

КЕЙСЫ

ПОСТРОЕНИЕ РАСПРЕДЕЛЕННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Подключение в единую защищенную сеть более **30** региональных и **30** местных органов власти в двух субъектах РФ

Обеспечение безопасного информационного обмена для **150** медицинских и **200** образовательных организаций в разных субъектах РФ



Построение крупной защищенной сети страховой компании с возможностью безопасного подключения технологических и бизнес-партнеров

ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА

ДЛЯ КОГО?

Для любых компаний, на которые распространяются требования РФ по информационной безопасности

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

- Государственные (муниципальные) информационные системы
- Коммерческая тайна
- Персональные данные
- Критическая информационная инфраструктура РФ
- Регламентация работы систем предотвращения утечек информации, а также других средств защиты информации и мониторинга
- Финансовые системы

ВИДЫ УСЛУГ

- Аудит
- Моделирование угроз
- Проектирование
- Внедрение
- Разработка организационно-распорядительной и эксплуатационной документации
- Оценка соответствия реализованных мер требованиям законодательства
- Сопровождение и консультационная поддержка

СРЕДИ ЗАКАЗЧИКОВ

НИИ, банки, страховые компании, органы государственной и муниципальной власти субъектов РФ, здравоохранение, транспорт, связь, металлургия, ТЭК

РАЗВЕДКА НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ

ДЛЯ КОГО?

Для организации, заинтересованной в фактической информационной безопасности

КАКУЮ ИНФОРМАЦИЮ СОБИРАЕМ?

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

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

ДЛЯ КОГО?

Для организации, заинтересованной в фактической информационной безопасности

Наиболее эффективный метод оценки текущего уровня защищенности информационной инфраструктуры организации за счет имитации действий злоумышленника ИБ-специалистом.

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*

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

2021

МФЦ

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

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

Медицинская организация

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

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

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

Крупный зарубежный банк

Получили доступ к интернет-банкингу и внутренней инфраструктуре

2023

Высшее учебное заведение

Нашли и проэкспуатировали критические уязвимости на периметре, получили полный доступ к сайту, скомпрометировали персональные данные пользователей, удаленно попали в ЛВС и скомпрометировали внутренние ресурсы.

Крупный производитель безалкогольных напитков

Получили полный доступ к сайту, смогли устанавливать свою цену на товары в корзине, скомпрометировали 1С Предприятие и видеонаблюдение.

Федеральный обувной ритейлер

Нашли и проэксплуатировали критические уязвимости на периметре, удаленно попали в ЛВС и скомпрометировали внутренние ресурсы, получили полный доступ к Wi-Fi и сетевому оборудованию, скомпрометировали контроллер домена.

*На слайде представлена только часть кейсов, полная информация может быть предоставлена по запросу

АНЛИМ
ГРУППА КОМПАНИЙ

Информационная безопасность | Техническое сопровождение ИБ-решений

Тюмень, БЦ «Флагман»,
ул. Харьковская, 83А,
корпус 4, 4 этаж

info@unlim.group

+7 (3452) 58-58-37

unlim.group