ВАШ ПРОВОДНИК В СФЕРЕ ИБ

ГАРАНТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТ «МАКСОФТ»

О КОМПАНИИ

16	ЛЕТ ОПЫТА
8	НАПРАВЛЕНИЙ РАБОТЫ
1500+	УСПЕШНЫХ ПРОЕКТОВ
200+	СОТРУДНИКОВ
3	СОБСТВЕННЫХ ПРОДУКТА

КОМАНДА ЭКСПЕРТОВ

Экспертная группа для работы по вашему проекту:

- Руководитель направления информационной безопасности
  Стаж работы 8 лет
- Специалист по организации защиты информации на объектах КИИ
  Стаж работы 8 лет
- Разработчик ПО в сфере кибербезопасности
  Стаж работы 6 лет
- Пентестер
  Стаж работы 7 лет

Курамов Владимир
Заместитель генерального директора по инфраструктуре и информационной безопасности
Стаж работы 24 года

У всех экспертов «Максофт» высшее профильное образование.
Ежегодно команда повышает свою квалификацию по различным направлениям.

Ваш персональный эксперт

Морозов Антон
Директор по развитию направления информационной безопасности
Стаж работы 8 лет

Для представления команды мы выбрали ключевых сотрудников, они первыми приходят на помощь нашим заказчикам.
Если у вас крупный и масштабный проект — мы расширим экспертную группу, чтобы решить вашу задачу оперативно.

ВЫСТРАИВАЕМ СИСТЕМУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Комплексный подход к защите информации

Модернизация или формирование «с нуля» системы ИБ от аудита до техподдержки

Дорожная карта с поэтапным внедрением средств ИБ

План по устранению критичных уязвимостей согласно приоритетам компании и бюджету

Гид по законодательству в сфере ИБ

Защита госкомпаний и объектов КИИ, согласование документации с регулятором

Выбор СЗИ на основе результатов исследований

Возможность бесплатно протестировать решения перед приобретением

Индивидуальный подход

Подбор решений для компаний разного уровня: от небольших офисов до корпораций

Говорим на языке заказчика

Прозрачное и четкое обоснование внедряемый решений для специалистов и руководителей

Помогаем выстроить систему информационной безопасности в комфортном режиме с учетом требований регуляторов и бюджета компании

ОТЗЫВЫ КЛИЕНТОВ

Александр Андросов

Ведущий специалист по ИБ группы выявления
криминальных рисков дирекции корпоративной защиты
ООО «Птицефабрика Акашевская»

Нам важно было оценить реальный уровень защищенности предприятия, поэтому провели комплексный анализ всех систем: внутренний и внешний пентесты, пентест беспроводных сетей, а также проверки с использованием методов социальной инженерии. Дополнительно использовали методы моделирования атак типа «отказ в обслуживании» (DoS, DDoS).
В результате анализа мы получили подробное заключение о состоянии системы и дорожную карту со стратегией модернизации ИБ. Уже достигнуты договоренности по ее реализации.

Алексей Шаманов

Руководитель управления информационных технологий и коммуникаций
ООО «ТНС энерго Пенза»

Аудит информационной безопасности компании включал в себя различные виды пентестов и проверку систем на соответствие требованиям регуляторов и аудит настроек на соответствие бэст-практикам.
Анализ защищенности был комплексным: пентест внутреннего и внешнего периметра, Wi-FI, мобильных и web-приложений на базе iOS и Android. Важной частью работа была разработка организационно-распределительной документации на соответствие системы требованиям ФСТЭК и 152-ФЗ.
Помимо всех проведенных исследований, мы получили необходимый пакет документов и подробные рекомендации по устранению уязвимостей.

Константин Бурмистров

Руководитель службы ИТ
КДЦ «Медиклиник»

Мы несем ответственность перед клиентами за то, чтобы средства защиты работали безупречно, поэтому оценка системы ИБ — это необходимость. Помимо проверки систем на соответствие требованиям регуляторов, эксперты разработали комплект документов согласно закону «О безопасности критической информационной инфраструктуры РФ». «Максофт» взяла на себя процедуру согласования со ФСТЭК до получения положительного заключения.

СЕРВИСЫ ИБ МАКСОФТ

Аудит подсистемы ИБ

ГИС, ИСПДн, КИИ, АСУ ТП,
финансовый сектор,
частные компании

- Аудит организационно-распорядительной документации (ОРД) в части ИБ
- Аудит ИТ-ресурсов и СЗИ (инвентаризация активов)
- Оценка защищенности информационной системы (ИС) и ее соответствия требованиям регуляторов (анализ уязвимостей / пентест)
- Разработка рекомендаций по развитию подсистемы ИБ

Внедрение ИБ-решений

ГИС, ИСПДн, КИИ, АСУ ТП,
финансовый сектор,
частные компании

- Предпроектное обследование
- Техническое проектирование подсистемы ИБ
- Подбор, поставка, установка и настройка СЗИ или приведение подсистемы ИБ в соответствие с требованиями регуляторов
- Импортозамещение продуктов ИБ
- Повторная оценка защищенности (ИС)(анализ уязвимостей / пентест)

СЕРВИСЫ ИБ
МАКСОФТ

Комплаенс по ИБ

(оценка соответствия требованиям регуляторов)

ГИС, ИСПДн, КИИ, АСУ ТП,
финансовый сектор

- Аудит подсистемы информационной безопасности
- Внедрение ИБ-решений
- Экспертный консалтинг по ИБ
- Разработка организационно-распорядительной документации в части ИБ
- Подготовка необходимой отчетной и сопроводительной документации для направления регулятору
- Сопровождение процедуры взаимодействия с регулятором
- Аттестация объекта информатизации в защищенном исполнении

Аутсорс подсистемы ИБ

ГИС, ИСПДн, КИИ, АСУ ТП,
финансовый сектор,
частные компании

- Настройка подсистемы ИБ в соответствии с требованиями заказчика
- Разработка правил взаимодействия заказчика и исполнителя
- Уведомление заказчика о возникновении инцидентов ИБ и выявленных уязвимостях
- Первичный разбор инцидента, анализ контекста, экстренное реагирование на критичные нарушения
- Расследование инцидентов, разработка рекомендаций по профилактике рецидивов
- Предоставление отчетов по графику за выбранный период

ДОРОЖНАЯ КАРТА РАЗВИТИЯ СИСТЕМЫ ИБ

ВИДЫ УСЛУГ

Анализ информационной инфраструктуры организации

Анализ уязвимостей информационной инфраструктуры организации

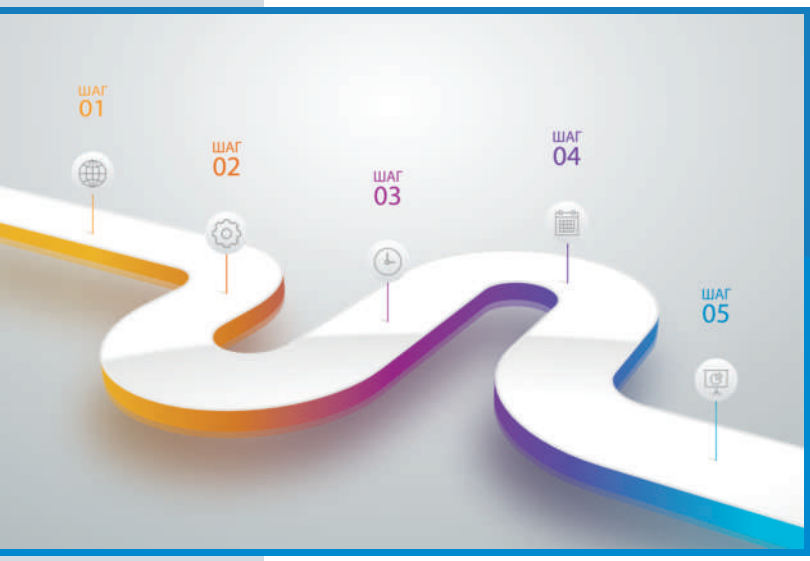
Bug bounty

- Экспресс-аудит инфраструктуры объекта
- Инструментальное сканирование внутреннего периметра сети
- Анализ результатов проверок

ЧТО ПОЛУЧАЕТ ЗАКАЗЧИК

Подготовка отчета по выявленным уязвимостям

- Разработка плана развития системы ИБ с учетом бюджета и сроков реализации
- Реальная картина защищенности с учетом недопустимых для организации событий
- Модернизация системы ИБ



Дорожная карта — это поэтапный стратегический план по обеспечению информационной безопасности в вашей компании. Вы получите четкий план действий со сроками и промежуточными результатами каждого этапа.

PENTEST
И АНАЛИЗ УЯЗВИМОСТЕЙ

ВИДЫ УСЛУГ

- Тестирование на проникновение внешнего периметра
- Тестирование на проникновение внутреннего периметра
- Тестирование беспроводных сетей
- Анализ защищенности web-приложений
- Тестирование с использованием методов социальной инженерии
- Тестирование с использованием методов моделирования атак типа «отказ в обслуживании» (DoS/DDoS)
- Анализ защищенности мобильных приложений

ЧТО ПОЛУЧАЕТ ЗАКАЗЧИК

- Подготовка отчетной документации
- Экспресс-аудит инфраструктуры объекта
- Инструментальное сканирование внутреннего периметра сети
- Анализ результатов проверок

Пентест — это имитация проникновения в систему по всем возможным сценариям, чтобы выявить слабые места инфраструктуры, а потом устранить их.
Протестировать инфраструктуру компании дешевле, чем платить хакерам выкуп.

ЗАЩИТА ОБЪЕКТОВ КИИ (ОКИИ)

ВИДЫ УСЛУГ

Аудит ОКИИ

Категорирование ОКИИ

- Подготовка полного комплект документации по категорированию для дальнейшего направления в ФСТЭК
- Консалтинг на протяжении всего процесса согласования с регулятором результатов категорирования ОКИИ

Подключение ЗОКИИ к ГосСОПКА

Аутсорс ИБ ОКИИ

Приведение подсистемы ИБ значимого ОКИИ (ЗОКИИ) в соответствие с требованиями регулятора

- Предпроектное обследование
- Техническое проектирование подсистемы ИБ ЗОКИИ
- Поставка, установка и настройка СЗИ в подсистеме ИБ ЗОКИИ
- Разработка комплекта документации в соответствии с требованиями регулятора
- Оценка защищенности ИС (анализ уязвимостей / пентест)
- Аттестация объекта информатизации в защищенном исполнении (При необходимости)

ЧТО ПОЛУЧАЕТ ЗАКАЗЧИК

Результат

- Актуальная и достоверная информация о категории ОКИИ
- Результативная и комплексная защита ОКИИ
- Подбор оптимальных решений с учётом бюджета заказчика и сроков реализации проекта
- Соблюдение всех законодательных требований в части ИБ ОКИИ
- Экспертный консалтинг на протяжении всей работы с заказчиком

ЗАЩИТА АСУ ТП

ВИДЫ УСЛУГ

Техническое проектирование подсистемы ИБ АСУ ТП с учетом специфики отрасли объекта

Подключение АСУ ТП к ГосСОПКА

Поставка, установка и настройка СЗИ в подсистеме ИБ АСУ ТП

Аутсорс ИБ АСУ ТП

Аттестация объекта информатизации в защищенном исполнении

ЧТО ПОЛУЧАЕТ ЗАКАЗЧИК

Результат

- Актуальная и достоверная информация о классе защищенности АСУ ТП
- Результативная и комплексная ИБ АСУ ТП
- Подбор оптимальных решений с учётом бюджета заказчика и сроков реализации проекта
- Соблюдение всех законодательных требований в части ИБ АСУ ТП
- Экспертный консалтинг на протяжении всей работы с заказчиком

Грамотно выстроенная защита АСУ ТП не позволит злоумышленнику запустить цепь недопустимых событий и нарушить производственные процессы.

ФИНАНСОВЫЙ СЕКТОР

ВИДЫ УСЛУГ

Аудит (оценка соответствия) требованиям ЦБ РФ

Приведение в соответствие с требованиями ЦБ РФ и повторная оценка

Тест на проникновение (пентест) и анализ уязвимостей

Подготовка документации в соответствии с требованиями регулятора

ЧТО ПОЛУЧАЕТ ЗАКАЗЧИК

Результат

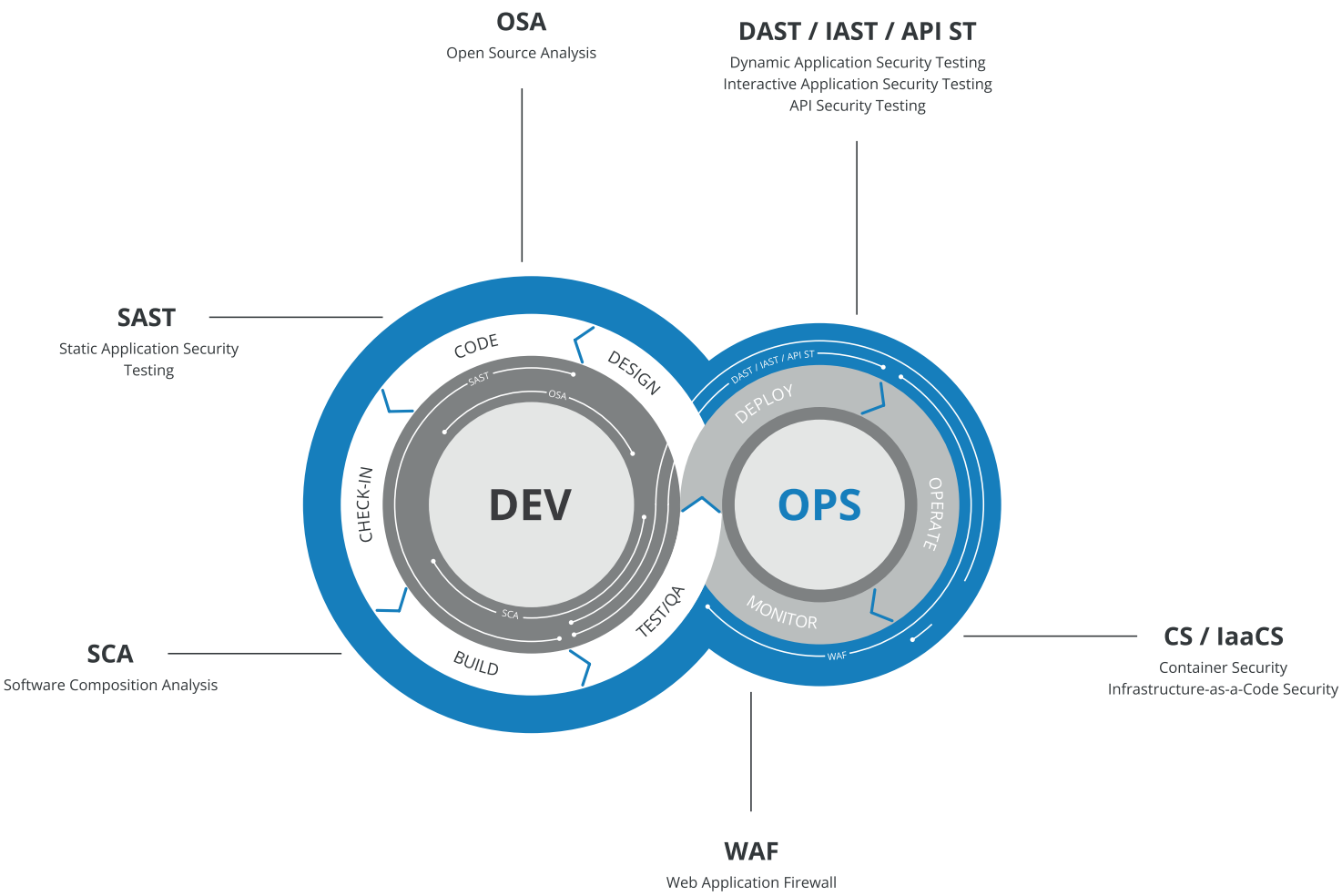
- Актуальная и достоверная информация о защищенности информационной инфраструктуры финансовой организации
- Результативная и комплексная защита ИС финансовой организации
- Подбор оптимальных решений с учётом бюджета заказчика и сроков реализации проекта
- Соблюдение всех законодательных требований ЦБ РФ
- Экспертный консалтинг на протяжении всей работы с заказчиком
- Разработка стратегического плана развития системы ИБ финансовой организации

Обеспечивая защиту вашей IT-инфраструктуры, вы получаете ключевое преимущество для компаний финансового сектора.

БЕЗОПАСНАЯ РАЗРАБОТКА

Безопасная разработка — набор процедур, позволяющий обнаруживать и устранять уязвимости на ранней стадии, до публикации релиза продукта.

- Заказная разработка любой сложности
- DevSecOps и инфраструктура
- Разработка мобильных приложений
- Аутстаф команды разработки



СОБСТВЕННАЯ РАЗРАБОТКА
MaSCA

Многофакторное сканирование и поиск НДВ

Приложение сканирует зависимости, идентифицирует открытый исходный код, находит в нем недекларированные возможности. Удобный инструмент для разработчиков и специалистов ИБ. Построение SBOM модели компонент (спецификация).

Ускоренное обнаружение уязвимостей 1-day

Оперативно исправляет 1-day уязвимости, помогает найти свежие из опубликованных уязвимостей в кодовой базе заказчиков. Предоставляет расширенные данные о CVE с описанием и инструкциями по их устранению.

База знаний

Собственная база знаний содержит информацию об открытых библиотеках из различных источников как отечественных, так и зарубежных (БДУ ФСТЭК, NVD и др.)

Параметры политик и интеграция

Предлагает настраиваемую конфигурацию политик, интегрируется в существующие наборы инструментов SDLC и CI/CD, минимизируя скорость разработки и время на поиск уязвимостей.

Работа со «старым кодом»

MaSCA находит уязвимости в текущем коде, автоматизирует этот процесс и внедряет в процесс безопасной разработки ПО (DevSecOps).

Отчетность

Уровень критичности открытых компонентов выводится на экран в виде сводных таблиц и диаграмм. Отчетность предоставляется в форматах pdf и csv.

MaSCA – импортозамещающее решение для сканирования открытых библиотек на наличие уязвимостей.

MaSCA на страже вашей безопасности
при использовании ресурсов Open Source.

Безопасность новых отечественных разработок ПО под угрозой

30+

ИНОСТРАННЫХ КОМПАНИЙ ПРИОСТАНОВИЛИ РАБОТУ В РОССИИ

на 50%

ВЫРОСЛО КОЛИЧЕСТВО УЯЗВИМОСТЕЙ В ПРОЕКТАХ OPEN SOURCE

85%

ПО В РЕЕСТРЕ МИНЦИФРЫ РФ ИСПОЛЬЗУЕТ ОТКРЫТЫЕ ИСХОДНЫЕ КОДЫ

Как пользоваться решениями OpenSource безопасно?

Анализировать открытые исходные коды с помощью приложений для управления безопасностью.

MaSCA — это комплексное решение для оценки рисков использования библиотек с открытым исходным кодом в приложениях, репозиториях, контейнерах, а также выявления лицензий.

Наше решение предлагает беспрецедентную прозрачность стороннего кода, позволяя контролировать цепочку поставок программного обеспечения из OpenSource на протяжении всего жизненного цикла приложения.

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

БАНК «КУЗНЕЦКИЙ»

Задача: Внедрение SIEM-системы, которая поможет проактивно обнаруживать, анализировать и устранять угрозы.

Решение: Эксперты подобрали пять вариантов SIEM-систем исходя из потребностей заказчика. С помощью демонстрационной серверной инфраструктуры был выбран продукт от Positive Technologies. Проведено успешное базовое внедрение продукта в инфраструктуру, глубоко погружаясь в проект и плотно сотрудничая со специалистами заказчика.

ТФОМС ПЕНЗЕНСКОЙ ОБЛАСТИ

Задача: Усилить информационную безопасность учреждения, в том числе, для предупреждения проникновений в систему и утечки персональных данных.

Решение: Проведен полный комплекс работ: анализ инфраструктуры, разработка проекта по защите ИС, поставка, установка и ввод в эксплуатацию оборудования, а также повторный аудит системы, в т.ч. на соответствие требованиям по ИБ. Выявлены критические уязвимости системы ИБ и проведены мероприятия по их нейтрализации.

ФГБУ ФЦССХ (КАРДИОЦЕНТР)

Задача: Привести информационную систему в соответствие с требованиями регулятора.

Решение: Было проведено категорирование объектов КИИ, внедрены решения по защите от несанкционированного доступа, по централизованному управлению и администрированию средств защиты информации от несанкционированного доступа, по анализу защищенности информационной системы. Проведен пентест в рамках аттестации по требованиям ИБ.

ГБУ «БЕЗОПАСНЫЙ РЕГИОН» (ГОСУСЛУГИ)

Задача: Анализ текущего уровня защищенности регионального сервиса предоставления Госуслуг.

Решение: Было проведено тестирование на проникновение внутреннего и внешнего периметров информационной инфраструктуры, анализ защищенности web-ресурсов. По результатам исследований составлен перечень рекомендаций по дальнейшей модернизации системы защиты информационной инфраструктуры.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Задача: Проектирование системы защиты информации.

Решение: Команда специалистов провела аудит архитектуры локальной сети с целью поиска ошибок ее построения.На основе аудита спроектировали защищенную сеть, провели миграцию наиболее чувствительных сервисов заказчика на отечественное программное обеспечение в рамках мероприятий по импортозамещению.

ОРГАНЫ ВЛАСТИ

Задача: Миграция на отечественные решения по ИБ.

Решение: Был произведен подбор, внедрение и настройка средств защиты информации от отечественных вендоров, входящих в реестр Минпромторга.

МВД РОССИИ

Задача: Содействие в расследовании киберпреступления.

Решение: Помощь специалистам правоохранительных органов: заключение по анализу оперативных данных по инциденту, выявление мошеннической схемы.

«МАКСОФТ» — СИСТЕМНЫЙ ИНТЕГРАТОР

«Максофт» — это не только выявление уязвимостей и предоставление подробных отчетов. После получения результатов оценки ИБ наши клиенты могут продолжить сотрудничество, ведь их задача - не просто найти “дыры” в системе, но и залатать их. Мы занимаемся подбором, поставкой, внедрением оборудования и программного обеспечения.

«Максофт» работает на результат

1. Описание задачи заказчика
2. Оценка системы информационной безопасности
3. Проект по модернизации ИБ компании
4. Составление организационно-распорядительной документации
5. Подбор оборудования и ПО, в т.ч. с применением пилотных проектов
6. Поставка выбранных позиций
7. Внедрение и пусконаладка системы
8. Техническая поддержка

«Максофт» гарантирует поддержку клиентов на всех этапах работы. Вы не остаетесь с задачей один на один: на связи персональный менеджер, который проинструктирует, разъяснит и поможет принять решение.

Информационная безопасность - это одна из сфер деятельности «Максофт». В вашем распоряжении наша экспертиза еще по семи IT-направлениям.

Инженерная инфраструктура

Работа с крупными ресурсоснабжающими предприятиями, поставка и внедрение СКУД, охранных и пожарных систем, промышленного оборудования.

Автоматизация и сервисы

Освобождение ресурсов компании, оптимизация бизнес-процессов, аналитика результативности сервисов, обучение персонала.

IT-инфраструктура

Проектирование и модернизация IT-инфраструктуры, поставка оборудования, внедрение и пусконаладка, техподдержка.

Разработка ПО

Разработка web-сервисов и мобильных приложений с передачей прав заказчику.

Транспорт

Поставка, внедрение и обслуживание элементов интеллектуальных транспортных систем, комплексов фото- видеофиксации, парковок.

Техническая поддержка

Обслуживание IT-инфраструктуры заказчика. Пригласите экспертов «Максофт» в ваш проект и сэкономьте на содержании постоянного штата.

Импортозамещение

Переход на отечественное оборудование и программное обеспечение в удобном для вашей компании темпе. Мы являемся официальными партнерами российских разработчиков, вошедших в Единый реестр российских программ для электронных вычислительных машин и баз данных Минсвязи РФ и Реестр Минпромторга.

Максофт
СИСТЕМНАЯ ИНТЕГРАЦИЯ

+7 (8412) 34-34-34
г. Пенза, ул. Куйбышева, д. 28
/2023

telegram

maksoft.ru