

АЛЬТИРИКС
ГРУПП



цифровая трансформации бизнеса
своевременное внедрение передовых технологий
защита от современных киберугроз

+7-812-716-14-14

+7-800-201-87-02

2023

Info@altirix.ru

www.altirixgroup.com

187-фз.пф

Заголовок	Страница
Деятельность	3
Лицензии	4
Достижения	5
Опыт в АСУ ТП	6
Опыт в разработке	7
Клиенты	8
Партнеры	9
Референсы	10
Рекомендации	11
152-ФЗ и ГИС	12
98-ФЗ	13

Заголовок	Страница
187-ФЗ	14
Защита АСУ ТП	15
Аттестация	16
Проектирование	17
Поставка	18
Анализ защищенности	19
Импортозамещение	20
Блокчейн	21
Машинное обучение	22
DevOps	23
Проектный менеджмент	24

СОКРАЩЕНИЯ

КИИ	Критическая информационная инфраструктура
АСУ ТП	Автоматизированная система управления технологическими процессами
СЗИ	Средства защиты информации

Информационная безопасность

Законодательство и консалтинг

- Защита персональных данных (152-ФЗ)
- Защита коммерческой тайны (98-ФЗ)
- Защита КИИ (187-ФЗ)
- Защита АСУ ТП
- Аттестация информационных систем

Создание систем защиты информации

- Аудит
- Проектирование
- Поставка и внедрение СЗИ
- Оценка эффективности мер защиты
- Сопровождение системы защиты

Анализ защищенности систем

- Тестирование на проникновение
- Инструментальный анализ защищенности
- Red Team
- Нагрузочное тестирование
- Тестирование бизнес-логики приложений

Информационные технологии

Аудит, поставка и внедрение

- Программное обеспечение
- Сетевое оборудование
- Серверы
- Клиентские устройства
- Периферийные устройства и др.

Импортозамещение

- Аудит и стресс-тест
- Стратегия импортозамещения
- Поставка

Разработка информационных систем

- Блокчейн
- Машинное обучение и нейросети
- DevOps-консалтинг
- Безопасная разработка

Наши сервисы



Проектирование



Внедрение



Сопровождение



Тестирование



Обучение



Анализ
защищенности



Поставка



Лицензирование

Достижения

50+

Проектов
ежегодно

100+

Аттестованных
объектов и систем

550+

Категорированных
объектов КИИ

30+

Проектов по защите
АСУ ТП

25+

Квалифицированных
специалистов

13

Лет на рынке

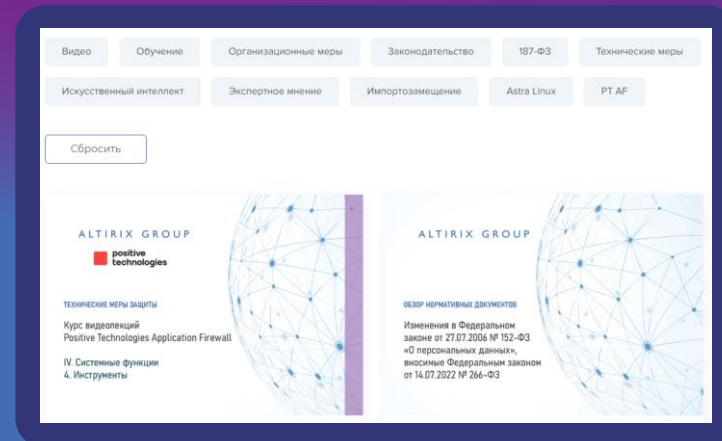
50%

Средний рост за 2020-
2022 гг.

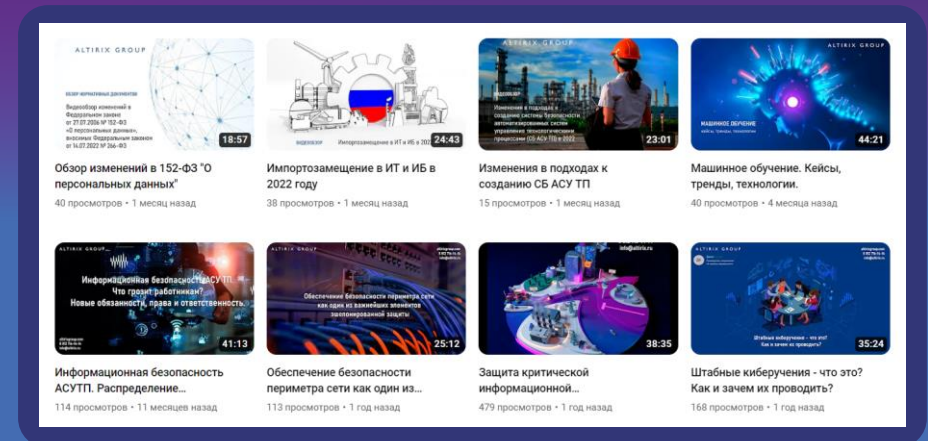
50+

Партнеров и
поставщиков

Блог



Канал YouTube



Опыт в АСУ ТП

Стаж в ИБ
>15 лет

- Профильное высшее образование
- Наличие сертификатов на СЗИ
- Опыт работы с Enterprise заказчиками
- Опыт взаимодействия с регуляторами

Проектов в FY21

52

Рост на 50%

- 50% – по защите КИИ и АСУ ТП
- 12/12 – сферы 187-ФЗ
- География проектов: от Калининграда до Камчатки
- 38 субъектов РФ посетили специалисты

2017



Энергогенерирующая компания

Выполнено обследование **26 филиалов**, выявлено **более 100 объектов защиты**, выполнено технорабочее проектирование СЗ и ее внедрение



Документы прошли согласование с ФСТЭК России

2018



Черная металлургия

Выполнено обследование **более 1000 объектов защиты**, проведено их категорирование, моделирование угроз и разработка ТЗ на СЗ



Документы прошли согласование с ФСТЭК России

2020



Централизованное оперативно-диспетчерское управление

Выполнено обследование **56 филиалов**, технорабочее проектирование СЗ для 3-х распределённых объектов защиты



Документы прошли согласование с ФСТЭК России

2021



Черная металлургия (комплекс проектов)

Выполнено технорабочее проектирование для **6-ти производств** для **20-ти объектов защиты**



Документы прошли согласование с ФСТЭК России

2022



Нефтепереработка (комплекс проектов)

Выполнено обследование **6-ти производств**, выявлено и категорировано **более 70-ти объектов защиты**, идёт стадия ТП...



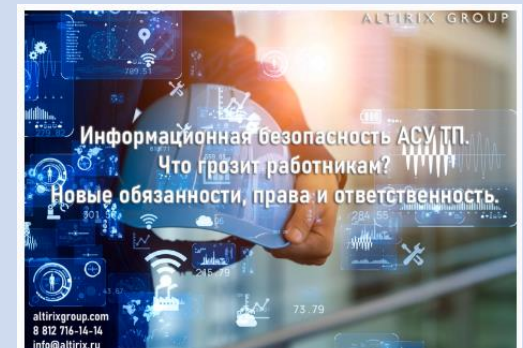
На активной стадии реализации



Вендоров в проектах

>30

Schneider Electric, Siemens, Allen-Bradley, Dräger REGARD, Rotork, Beckhoff, Honeywell, Advantech, Welntek, B&R Industrial Automation's, OBEH, Mitsubishi, Вектор, Автоматика-Север и др.



Опыт в разработке

СОКРАЩЕНИЯ

SCADA

От англ. Supervisory Control And Data Acquisition - диспетчерское управление и сбор данных

7

№	Наименование проекта	Год реализации	Технологии
1	Система лояльности на базе технологии распределенного реестра	2021	Node.JS, MongoDB, React, Nginx, RESTAPI, Hyperledger Fabric
2	Система выявления аномалий в работе АСУ ТП на базе SCADA Rockwell Automation FactoryTalk (анализ скорости потока жидкости, давления и положения вентилей) с применением моделей машинного обучения	2020	Python
3	Система анализа больших данных (лог-файлы систем информационной безопасности) с применением моделей машинного обучения для выявления сетевых аномалий	2020	Elastic Stack, Hadoop, Python
4	Система подтверждения выполнения работы автономных транспортных средств (на базе технологии блокчейн)	2019	C, Rust, RIOT OS, ARM, Java, MongoDB, Hyperledger Fabric, Hyperledger Sawtooth
5	Независимая распределенная система объединения вычислительной мощности blockchain-сети, основанная на принципе делегирования выполнения работы	2018	Node.JS, Go, Rust, C, Solidity, Lua, MongoDB, Redis, Nginx, RESTAPI, JSON-RPC 2.0
6	И другие...		



Altirix Group имеет опыт реализации проектов с применением технологий машинного обучения/искусственного интеллекта

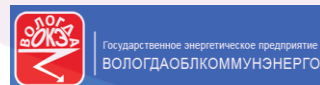
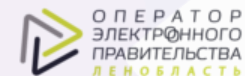
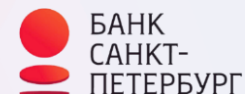


- Предиктивная видеоаналитика
- Обработка естественного языка
- Роботизация производственных процессов
- Виртуальные ассистенты, голосовые роботы и чат-боты
- RPA и автоматизация рутинных операций
- Интеллектуальные системы лояльности
- Анализ социальных сетей
- Прогнозирование отказов и интервалов обслуживания
- Анализ и прогнозирование событий информационной безопасности
- Интеллектуальное финансовое планирование



АЛЬТИРИКС
ГРУПП

Клиенты



Администрация
Санкт-Петербурга



Министерство ИТ и связи
Нижегородской области



И другие...

kaspersky

Dr.WEB

КОД
безопасности

positive
technologies

Аладдин

infotecs®

FORTINET®

КОНФИДЕНТ®
ИНЖЕНЕРНЫЕ СИСТЕМЫ

INFOWATCH

R-Vision

GIS

GROUP-IB

UserGate

НАТЕКС

ELTEX
SOLUTIONS

7elax
Основан в 1988 г.

DEPO
[computers]

RUSIEM

SEARCHINFORM
INFORMATION SECURITY

AQUARIUS

COMMUNICATE SYSTEMS

eset®

Эшелон
комплексная безопасность

s•terra®

ALTEX
S O F T

КРИПТОПРО

ИД

INDEED

ID

ZECURION

АСТРА
группа компаний

НЗС

ideco

NERPA
by OCS Distribution

QNAP®

QTECH
МИР ДОСТУПНЕЕ

ГАРДА
ТЕХНОЛОГИИ

ГРАВИТОН

КИБЕРПРОТЕКТ

МойОфис

Р7-ОФИС

ROSA

КАТЮША

РЕДСОФТ

YADRO

И другие...

Референсы

СОКРАЩЕНИЯ

ЗОКИИ	Значимый объект критической информационной инфраструктуры
НИР	Научно-исследовательские работы
ДЦ	Диспетчерский центр
МЭК	Международная электротехническая комиссия
ИТ	Информационные технологии

10



Системный оператор единой энергетической системы

1. Альтирикс групп выполнила проектирование системы безопасности значимых объектов критической информационной инфраструктуры (ЗОКИИ). Выполнено обследование инфраструктуры в масштабе 56 филиалов, моделирование и анализ угроз по расширенной модели Kill Chain, разработка технического задания и типовых технических требований для различных категорий ЗОКИИ, технорабочее проектирование. Документы согласованы с ФСТЭК России и ФСБ России.

2. Альтирикс групп выполнила НИР на тему «Анализ угроз информационной безопасности при информационном обмене между объектами электроэнергетики и ДЦ по протоколу МЭК 60870-5-104».

Московский физико-технический институт

Альтирикс групп оказала услуги по обследованию ИТ-инфраструктуры, оценке зрелости процессов управления ИТ, аудиту процессов обработки и защиты персональных данных (ПДн), анализу защищенности портала mipt.ru (pentest) для Московского физико-технического института.



АО «Тандер»

Альтирикс групп предоставила услуги по проведению нагрузочного тестирования (имитации DDoS-атак) на исчерпание ширины канала связи и на исчерпание ресурсов сетевого оборудования различными методами: UDP-flood, TCP-flood, SYN/ACK/PUSH ACK-flood, ACK/PUSH ACK-flood fragmentation, Multiple ACK Fake Session Attack, Fake Session Attack, Multiple TCP-flood, Session Attack, HTTP/HTTPS-flood, сформирован перечень рекомендаций по повышению устойчивости функционирования информационной инфраструктуры от атак типа DDoS.




Конституционный суд Российской Федерации

Альтирикс групп выполнила поставку и внедрение средств защиты информации, оценку актуальных угроз безопасности, разработку организационно-распорядительных документов и аттестацию автоматизированной системы в защищенном исполнении.



Рекомендации

 РУСАТОМ СЕРВИС
РУСАТОМ

Акционерное общество
«Русатом Сервис»
(АО «Русатом Сервис»)
Павловский проспект, д. 58
Москва, 117335
Телефон (495) 995-76-80
E-mail: info@rusatom-service.ru
ОКСКО 37158687, ОГРН 1117746845523
ИНН 7705966318, КПП 772801001

Генеральному директору
ООО «Альтирикс Системс»
Кузьмину А.Р.

№ 04.2522 от 28.04.2015

О направлении
благодарственного письма

Уважаемый Александр Ростиславович!

АО «Русатом Сервис» выражает искреннюю благодарность специалистам ООО «Альтирикс Системс» за профессиональное и качественное оказание услуг по проектированию системы защиты объектов критической информационной инфраструктуры (КИИ).


В ходе проекта специалистами ООО «Альтирикс Системс» были выполнены следующие работы:

- проведена оценка результатов категорирования объектов КИИ;
- разработана модель угроз безопасности информации;
- сформированы требования к системе защиты информации с учетом законодательства Российской Федерации в области безопасности КИИ и отраслевых требований Госкорпорации «Росатом»;
- предложена архитектура системы защиты объектов КИИ и решения по информационной безопасности, учитывающие лучшие практики и требования по импортозамещению;
- разработана проектная документация на систему защиты объектов КИИ и проведено макетирование ее подсистем;
- разработана организационно-распорядительная документация по информационной безопасности единая для всех объектов КИИ, обрабатывающих различные виды информации (персональные данные, коммерческую тайну, служебную тайну и общедоступную информацию);
- оказана всесторонняя методическая помощь по вопросам исполнения законодательства Российской Федерации в области безопасности КИИ.

При реализации проекта со стороны ООО «Альтирикс Системс» была собрана команда специалистов, которая смогла в короткий срок найти решение всех сложных организационных и технических задач, стоящих перед АО «Русатом Сервис» в области защиты объектов КИИ.

Проведенные работы позволили вышестоять требованиям Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и перейти к модернизации системы защиты информации АО «Русатом Сервис».

Надеемся на дальнейшее плодотворное сотрудничество между нашими организациями при реализации проектов в области информационной безопасности.

Заместитель генерального
директора по безопасности  С.П. Решетников

 ПОЛИМЕТАЛЛ

Общество с ограниченной ответственностью
«СВЕТЛОЕ»
ООО «СВЕТЛОЕ»
ИПН 2731071992
КПП 44750001
ОГРН 1032700297200

Иск. СВ/28-1300
От 25.07.22

Генеральному директору
ООО «Альтирикс Системс»
А.Р. Кузьмину
197022, г. Санкт-Петербург,
пр. Медиков, д.3 А.

Рекомендательное письмо


ООО «Светлое» выражает благодарность ООО «Альтирикс Системс» за профессиональное и качественное оказание услуг по категорированию объектов критической информационной инфраструктуры (КИИ) в сфере горнодобывающей промышленности.

В ходе проекта специалистами ООО «Альтирикс Системс» были проанализированы критические процессы предприятия, опасные производственные объекты и используемые предприятием информационные системы и автоматизированные системы управления. Исполнителем подготовлены все необходимые материалы для работы комиссии по категорированию и обосновано отсутствие необходимости присвоения категории значимости объектам КИИ.


В результате проведенных работ предприятием выполнены требования Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и получено подтверждение ФСТЭК России о правильности результатов категорирования объектов КИИ.

Надеемся на дальнейшее сотрудничество и готовы рекомендовать ООО «Альтирикс Системс» как надежного партнера для реализации проектов в области информационной безопасности.

С уважением,
И. о. управляющего директора  А.Н. Бляников



Исп. Несминов П.А.
Тел. 48-183

 Акционерное общество
«ТАНДЕР»
350002 г. Краснодар, ул. Леваневского, 185
Р/с 40702810930010120159; К/с 30101810100000000602
КРАСНОДАРСКОЕ ОТДЕЛЕНИЕ №8619 ПАО СБЕРБАНК, БИК 040349602;
ИНН 2310031475; КПП 997350001; ОКПО 41351125;
тел. 210-98-10, 255-19-18, 275-09-15


Генеральному директору
ООО «Альтирикс Системс»
А.Р.Кузьмину


Рекомендательное письмо

АО «Тандер» выражает благодарность ООО «Альтирикс Системс» за выполнение проекта по проведению анализа защищенности (тестирование на проникновение) веб-приложений и мобильных приложений.

Реализация проекта с использованием международных стандартов, методологий и лучших практик (OWASP Top 10, OWASP web application penetration checklist, OWASP Mobile Security Testing Guide и другие) позволила повысить устойчивость тестируемых сервисов к кибератакам за счет устранения выявленных уязвимостей.

Готовы рекомендовать ООО «Альтирикс Системс» как компетентного подрядчика и надежного партнера для реализации проектов по информационной безопасности.

С уважением, Директор департамента
информационной безопасности Василенко А.С. 



152-ФЗ и ГИС

СОКРАЩЕНИЯ

ПДн	Персональные данные
ИСПДн	Информационная система персональных данных
ГИС	Государственная информационная система
СЗПДн	Система защиты персональных данных
ОРД	Организационно-распорядительные документы

Реализация требований 152-ФЗ

Обеспечение соответствия требованиям законодательства в области обеспечения безопасности персональных данных

Минимизация рисков ИБ

Минимизация последствий (ущерба) в случае утечки персональных данных и других угроз информационной безопасности

Непрерывность деятельности

Предотвращение нарушений в функционировании процессов обработки ПДн из-за угроз информационной безопасности

Практическая безопасность

Повышение степени защищенности смежных информационных систем и процессов обработки информации

Обследование

- Аудит процессов обработки ПДн
- Аудит ИТ-инфраструктуры и ИСПДн
- Оценка степени реализации требований 152-ФЗ

Формирование требований

- Акты классификации ИСПДн
- Модель угроз ИСПДн
- Техническое задание на создание СЗПДн

Технорабочее проектирование

- Технорабочий проект СЗПДн
- Поставка средств защиты информации
- План пусконаладочных работ СЗПДн
- Разработка ОРД

Внедрение и сопровождение

- Пусконаладочные работы средств защиты информации
- Внедрение ОРД
- Анализ защищенности
- Приемочные испытания
- Сопровождение СЗПДн

Аттестация

- Аттестационные испытания
- Выдача аттестата соответствия

Обязательна для ГИС, в остальных случаях – по решению оператора



Один из ключевых документов – Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»



Для государственных информационных систем (ГИС) - Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Обеспечение юридической значимости

Введение режима защиты коммерческой тайны, который обеспечивает правовую основу для защиты конфиденциальных сведений организации

Непрерывность деятельности

Предотвращение нарушений в функционировании процессов обработки конфиденциальных сведений из-за угроз информационной безопасности

Минимизация рисков ИБ

Минимизация последствий (ущерба) в случае реализации угроз информационной безопасности

Практическая безопасность

Повышение степени защищенности смежных информационных систем и процессов обработки информации

98-ФЗ

СОКРАЩЕНИЯ

ИС	Информационная система
СОИБ	Система обеспечения информационной безопасности
NIST	Национальный институт стандартов и технологий США

Обследование

- Аудит процессов обработки конфиденциальных сведений
- Аудит ИТ-инфраструктуры и ИС, обрабатывающих конфиденциальные сведения
- Выявление активов и их владельцев

Формирование требований

- Качественная и количественная оценка рисков
- Ранжирование рисков и активов
- Разработка Перечня сведений конфиденциального характера
- Моделирование угроз
- Техническое задание на создание СОИБ

Технорабочее проектирование

- Технорабочий проект СОИБ
- Поставка средств защиты информации
- План пусконаладочных работ СОИБ
- Разработка ОРД

Внедрение и сопровождение

- Пусконаладочные работы средств защиты информации
- Внедрение ОРД
- Анализ защищенности
- Приемочные испытания
- Сопровождение СОИБ

13



В процессе выбора технических и организационных мер защиты информации применяются лучшие международные практики (NIST, ISO и др.), а также нормативно-правовая база Российской Федерации (Приказы ФСТЭК и ФСБ России) и государственные стандарты (ГОСТ)

Реализация требований 187-ФЗ

Обеспечение соответствия требованиям законодательства в области безопасности критической информационной инфраструктуры

Минимизация рисков ИБ

Минимизация последствий (ущерба) в случае реализации угроз информационной безопасности

Непрерывность деятельности

Предотвращение нарушений в функционировании объектов критической информационной инфраструктуры из-за угроз информационной безопасности

Практическая безопасность

Повышение степени защищенности смежных информационных систем и процессов обработки информации

187-ФЗ

СОКРАЩЕНИЯ

СБ ЗОКИИ

Система безопасности значимых объектов критической информационной инфраструктуры

Обследование

- Аудит процессов и видов деятельности
- Аудит ИТ-инфраструктуры и объектов КИИ
- Выявление критических процессов
- Организация деятельности комиссии по категорированию

Формирование требований

- Категорирование объектов КИИ
- Оформление итогов заседания комиссии по категорированию
- Подготовка документов для ФСТЭК России
- Моделирование угроз
- Техническое задание на создание СБ ЗОКИИ

Технорабочее проектирование

- Технорабочий проект СБ ЗОКИИ
- Поставка средств защиты информации
- План пусконаладочных работ СБ ЗОКИИ
- Разработка ОРД

Внедрение и сопровождение

- Пусконаладочные работы средств защиты информации
- Внедрение ОРД
- Анализ защищенности
- Приемочные испытания
- Сопровождение СБ ЗОКИИ

Аттестация

- Аттестационные испытания
- Выдача аттестата соответствия

Обязательна для ГИС, в остальных случаях – по решению оператора



Ключевые документы: Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» и Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

Защита АСУ ТП

СОКРАЩЕНИЯ

- COB** Система обнаружения вторжений
- DMZ** От англ. Demilitarized Zone - демилитаризованная зона
- NGFW** От англ. Next-Generation Firewall – межсетевой экран следующего поколения

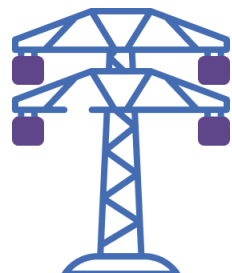
15



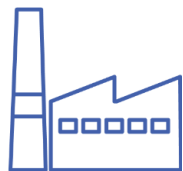
Атомная станция



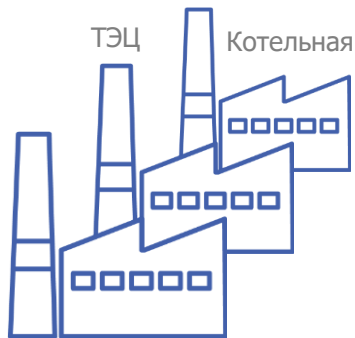
Металлургия



Подстанция



Легкая
промышленность



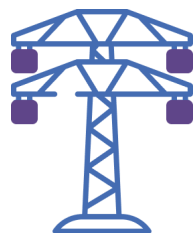
ТЭЦ Котельная
Тяжелая
промышленность



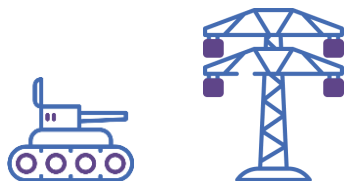
Медицина



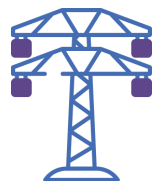
Добыча



РЭС



ОПК



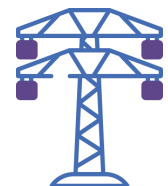
Энергетика



Космическая
промышленность



РДУ



ОДУ



Транспорт



Химическая
промышленность

Услуги по направлению

Консалтинг

- Соответствие 187-ФЗ
- Соответствие Приказу ФСТЭК России № 31
- Соответствие лучшим международным практикам

Практическая безопасность

- Внедрение промышленной COB
- Организация DMZ АСУ ТП с использованием NGFW
- Внедрение системы мониторинга событий безопасности
- Внедрение системы антивирусной защиты
- Оценка эффективности системы защиты
- Взаимодействие с разработчиками (поставщиками) АСУ ТП по вопросам реализации встроенных мер защиты информации и безопасной разработки

Ключевые партнеры



VIPNet SIES



Аттестация

16

Аттестации подлежат объекты информатизации (ОИ)

Обязательно

- Государственные и муниципальные информационные системы, в том числе государственные, муниципальные информационные системы персональных данных
- Информационные системы управления производством, используемые организациями оборонно-промышленного комплекса, в том числе автоматизированные системы станков с числовым программным управлением
- Помещения, предназначенные для ведения конфиденциальных переговоров (защищаемые помещения)

Добровольно

- Значимые объекты критической информационной инфраструктуры Российской Федерации
- Информационные системы персональных данных
- Автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды
- Любые другие автоматизированные системы



Объект информатизации (ОИ) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров

Обследование

- Уточнение границ систем
- Инвентаризация технических средств
- Оценка реализованных мер защиты информации



Формирование требований

- Классификация систем
- Моделирование угроз
- Формирование требований по защите (ТЗ)



Проектирование

- Разработка проектной документации
- Разработка организационно-распорядительных документов (ОРД)



Внедрение и аттестация

- Пусконаладка средств защиты информации
- Ввод в действие ОРД
- Анализ защищенности
- Аттестационные испытания
- Выдача аттестата соответствия



Согласование с ФСТЭК России

- В течение 5 рабочих дней после подписания аттестата соответствия предоставление во ФСТЭК России (территориальный орган ФСТЭК России по месту расположения объекта информатизации) в электронном виде копий необходимых документов



Осуществление периодического контроля не реже 1 раза в 2 года

Наши преимущества



Быстро: наши бизнес-процессы позволяют выполнять задачи клиентов в сжатые сроки



Выгодно: покупая у нас продукты (решения) Вы получаете существенные скидки на весь портфель наших услуг



Надежно: сопровождаем наших клиентов с момента подбора решений и до вывода их из эксплуатации (модернизации)



Профессионально: Обучаем клиентов эффективному применению выбранных решений



Альтирикс Групп осуществляет комплексные поставки программного и аппаратного обеспечения, а также помогает своим клиентам интегрировать выбранные решения в существующую инфраструктуру. Мы выстраиваем долгосрочные отношения, являемся интегратором полного цикла.

Поставляемые решения

- Серверное и инфраструктурное оборудование
- Сетевое оборудование
- Антивирусные решения для рабочих станций и серверов
- Межсетевые экраны (NGFW, UTM, WAF)
- Средства обнаружения вторжений (IPS/IDS)
- Средства защиты информации от несанкционированного доступа (СЗИ от НСД)
- Защита электронной почты
- Резервное копирование данных
- Сканеры уязвимостей (АНЗ)
- Средства удаленного доступа
- Управление привилегированным доступом (PAM)
- Системы предотвращения утечек данных (DLP)
- Управление событиями и информацией о безопасности (SIEM)
- Средства криптографической защиты информации (СКЗИ)
- Песочницы
- Средства автоматизированного проектирования (САПР)
- И другое...

КАТАЛОГ РЕШЕНИЙ

Это актуально



Для субъектов КИИ,
выполняющих требования
ФСТЭК России



Для финансовых и кредитных
организаций, выполняющих
требования ЦБ РФ



Для владельцев ГИС,
выполняющих требования
ФСТЭК России



Для любой организации,
желающей обезопасить себя от
киберрисков

Виды услуг



Пентест (тестирование на проникновение)

Осуществляем поиск уязвимостей в корпоративных сетях и системах путем моделирования действий злоумышленника



Штабные киберучения

Разрабатываем сценарий многоуровневой кибератаки и проводим оценку действий персонала по обнаружению атаки и противодействию на основе действующих в организации регламентов



Red Team

Делаем попытки получить доступ к инфраструктуре любыми согласованными способами на протяжении длительного времени, информируем Blue Team о найденных уязвимостях



Оценка эффективности мер защиты

Анализируем действия персонала при проведении пентеста и даем рекомендации по улучшению процессов и механизмов противодействия кибератакам

Комплексные пакеты услуг

направлены на выявление самых актуальных проблем и выполнение нормативных требований

<p>All-In-One 490 000 Р</p> <p>Включено:</p> <ul style="list-style-type: none"> • анализ тестирование на более 30 устройств/адресов • функциональный тестирование на более 30 устройств/адресов (включая веб-приложения) • тесты социальнo-инженерных уязвимостей, фишинг, spear-phishing и т.д. (в зависимости от пакета) • подробный отчет о тестировании • рекомендации для устранения уязвимостей • материалы для обучения сотрудников <p>Длительность проекта: 45 рабочих дней</p> <p>Заказать →</p>	<p>All-In-One web 490 000 Р</p> <p>Включено:</p> <ul style="list-style-type: none"> • детальное тестирование 1 уровня веб-приложения • тестирование веб-приложений • тесты социальнo-инженерных уязвимостей, spear-phishing и т.д. (в зависимости от пакета) • рекомендации для устранения уязвимостей • материалы для обучения сотрудников • материалы для разработки ИСМ безопасности <p>Длительность проекта: 22 рабочих дня</p> <p>Заказать →</p>	<p>Социальная инженерия 490 000 Р</p> <p>Включено:</p> <ul style="list-style-type: none"> • создание реалистичных фишинговых писем и корпоративных адресов • тестирование email-адресов (включая веб-приложения) на более 30 устройств/адресов • тестирование email-адресов (включая веб-приложения) на более 30 устройств/адресов • тестирование email-адресов (включая веб-приложения) на более 30 устройств/адресов • тестирование email-адресов (включая веб-приложения) на более 30 устройств/адресов • тестирование email-адресов (включая веб-приложения) на более 30 устройств/адресов • тестирование email-адресов (включая веб-приложения) на более 30 устройств/адресов <p>Длительность проекта: 45 рабочих дней</p> <p>Заказать →</p>
---	---	--

Стартовые пакеты услуг

направлены на выполнение узких задач и получение быстрых результатов и подорог для небольших компаний

<p>Оценка защищенности веб-приложения 99 000 Р</p> <p>Включено:</p> <ul style="list-style-type: none"> • не более 10 адресов веб-приложения • анализ тестирование • рекомендации для устранения уязвимостей <p>Длительность проекта: 10 рабочих дней</p> <p>Заказать →</p>	<p>Сканирование внешнего периметра 99 000 Р</p> <p>Включено:</p> <ul style="list-style-type: none"> • не более 3 адресов • отчет о тестировании • рекомендации для устранения уязвимостей <p>Длительность проекта: 22 рабочих дня</p> <p>Заказать →</p>	<p>Контроль осведомленности персонала 99 000 Р</p> <p>Включено:</p> <ul style="list-style-type: none"> • тестовые рассылки на более 300 человек • отчет о тестировании • материалы для обучения сотрудников <p>Длительность проекта: 22 рабочих дня</p> <p>Заказать →</p>
---	--	--

Анализ защищенности

Подсистема каталогов
инфраструктуры

✗ Microsoft Windows,
SQL Server

✓ Astra Linux Special
Edition, PostgreSQL
Pro



Подсистема серверной
инфраструктуры и
хранения данных

✗ Hewlett Packard
Enterprise, Lenovo,
Eaton, Schneider Electric

✓ DEPO, QTECH,
БАСТИОН, ГРАВИТОН



Подсистема сбора и
анализа событий ИБ

✗ HP ArcSight

✓ MaxPatrol SIEM



Подсистема межсетевого
экранирования и
обнаружения вторжений

✗ Cisco Systems

✓ UserGate



Подсистема
виртуализированной
инфраструктуры

✗ VMware vSphere

✓ Средства
виртуализации
«Брест»



Подсистема сетевой
инфраструктуры

✗ Cisco Systems

✓ QTECH, HATEКС



Подсистема резервного
копирования

✗ Veeam Backup

✓ Кибер Бэкап



Система
защиты

Подсистема
криптографической
защиты каналов связи

✓ Код безопасности

Подсистема контроля
технических
уязвимостей

✓ MaxPatrol 8 (VM)

Подсистема
антивирусной защиты

✓ Kaspersky Endpoint
Security

Подсистема контроля
действий
привилегированных
пользователей

✓ СКДПУ ИТ, Indeed
PAM

Подсистема
управления
информационной
безопасностью

✓ R-Vision

Пример замены импортных решений на отечественные аналоги

Импортозамещение в ИТ

Каталог отечественных ИТ-решений для бизнеса

Подробнее ▶

Импортозамещение в ИБ

Каталог отечественных ИТ-решений по информационной безопасности

Подробнее ▶

Требования

- Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
- Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Преимущества Смарт-контрактов



Автоматизация

Смарт-контракты запускаются автоматически при наступлении указанного события



Автономность

После развертывания смарт-контракты становятся автономными и цензуростойкими



Доверие

Полная прозрачность для всех сторон контракта



Целостность

Более одной копии данных хранятся в распределенном реестре



Экономия

Отсутствие третьих сторон обеспечивает экономию средств



Точность формулировок

Смарт-контракты не только быстрее и дешевле, но и снижают вероятность разночтения формулировок и количество ошибок, совершенных вручную

Наш подход к разработке смарт-контрактов



Выработка архитектуры

Поскольку цифровой протокол требует рабочего процесса без ошибок, мы внедряем лучшие практики для создания архитектуры смарт-контрактов



Проектирование и разработка

Разработчики смарт-контрактов создают их с настраиваемыми функциями, адаптируемыми к любой отрасли



Аудит логики и безопасности

Мы предлагаем услуги аудита смарт-контрактов, чтобы обеспечить безопасность и работу без ошибок



Оптимизация и управление версиями

Мы оптимизируем смарт-контракты перед развертыванием, чтобы помочь клиентам сэкономить

Блокчейн

21

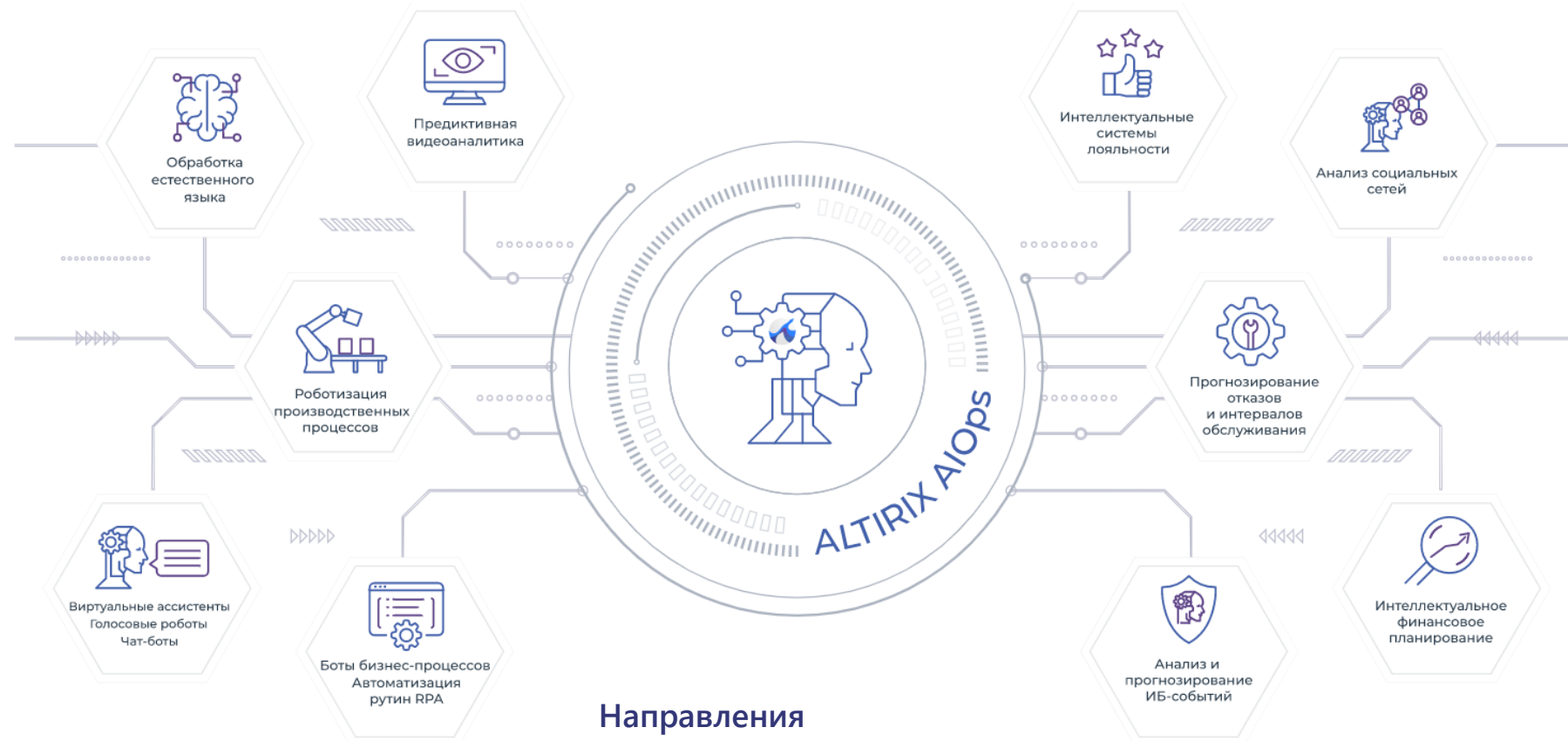
Смарт-контракты — это цифровые протоколы, созданные для проверки условий юридического контракта между двумя или более сторонами

ПОДРОБНЕЕ

Виды услуг

- Разработка распределенных приложений на языке Solidity для EVM-based блокчейнов
- Разработка чейнкод на языках Go/JS для распределенных реестров на базе Hyperledger Fabric
- Внедрение и кастомизация собственных off-chain решений

Мы обеспечиваем трансформацию бизнеса и технологий на протяжении всего жизненного цикла, используя гибкие методологии, проверенные схемы сотрудничества с клиентами и партнерами, передовые инструменты разработки и тестирования, гибридные команды и нашу методологию быстрой доставки и разворачивания программных решений



Машинное обучение

22

Виды услуг

- Разработка систем обработки естественного языка и изображений/образов
- Разработка систем анализа больших данных и статистической информации

Направления

- Предиктивная видеоаналитика
- Обработка естественного языка
- Роботизация производственных процессов
- Виртуальные ассистенты, голосовые роботы и чат-боты
- RPA и автоматизация рутинных операций
- Интеллектуальные системы лояльности
- Анализ социальных сетей
- Прогнозирование отказов и интервалов обслуживания
- Анализ и прогнозирование событий информационной безопасности
- Интеллектуальное финансовое планирование

DevOps – это новый способ организации работы, который повышает ценность продукта для пользователя. DevOps дает преимущества как для масштабирования, так и для оперативного устранения ошибок и улучшения эксплуатации вашего продукта.

Определение

DevOps – это новый подход к оптимизации и управлению комплексным предоставлением услуг и операциями, который основан на принципах преобразования всего жизненного цикла поставки программного обеспечения с целью быстрого внедрения новых практик.

Принципы

- Культура совместной ответственности и сотрудничества
- Сквозное управление услугами
- Многопрофильные команды
- Создание дополнительной ценности
- Автоматизация (почти;) всего
- Измерение (почти;) всего
- Непрерывное совершенствование

Жизненный цикл программного обеспечения



Новые практики:

- Непрерывная интеграция
- Непрерывное тестирование
- Непрерывная доставка
- Непрерывная эксплуатация

Применение принципов DevOps к SDLC приводит к новым методам работы, которые приносят пользу как разработке, так и эксплуатации.

Альтирикс Групп оказывает полный спектр DevOps-услуг с использованием следующих инструментов: Ansible, Docker, ELK Stack, Git (GitLab, GitHub, Bitbucket), Kubernetes, Prometheus, Jenkins, Rancher, Zabbix

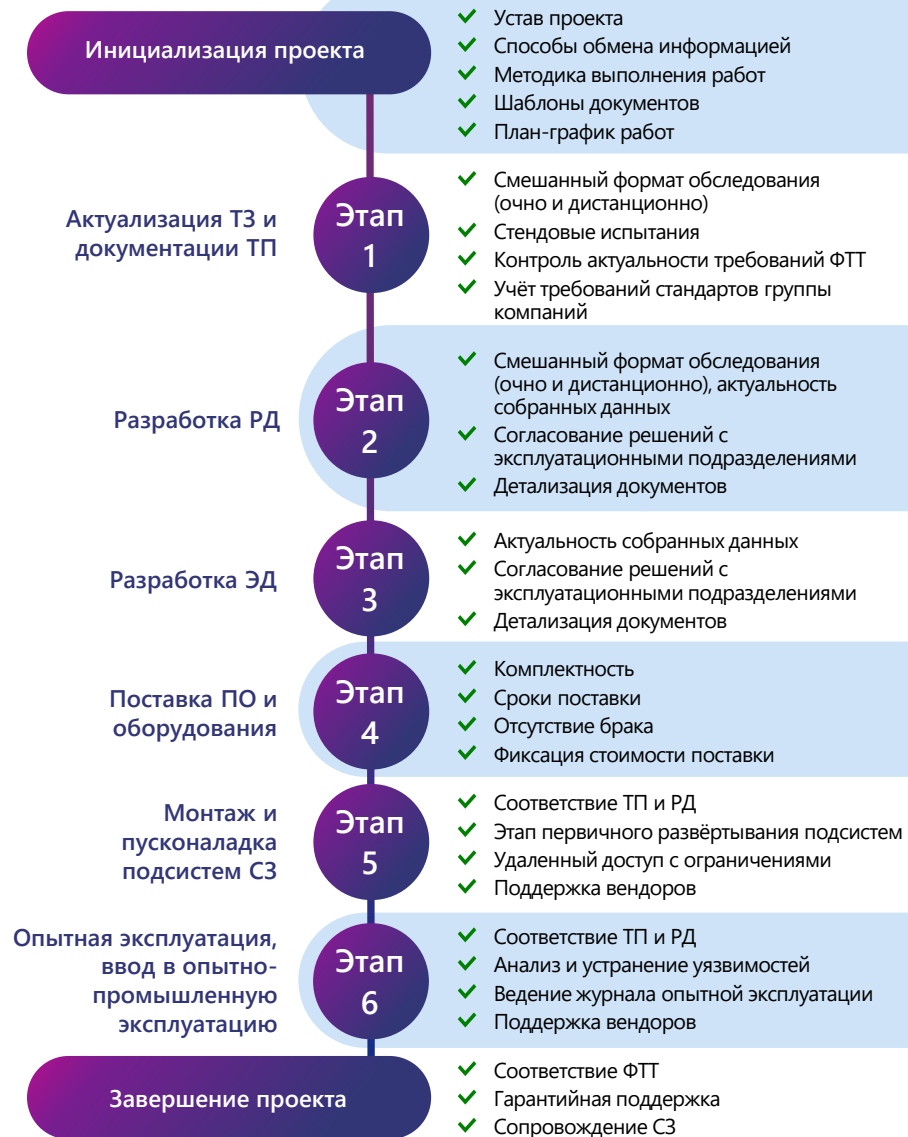
Цель

Основная цель DevOps – улучшить переход от идеи к созданию ценности для клиента, благодаря применению среды, в которой многопрофильные команды работают совместно, чтобы постоянно и в более быстром темпе предоставлять высококачественные решения, которые подходят для успешного выполнения работы.

Выгода

- Повышает частоту и качество развертываний и выпусков
- Повышает эффективность инноваций и принятия рисков
- Ускоряет вывод на рынок
- Создание дополнительной ценности
- Повышает качество решения и эксплуатационную надежность
- Улучшает среднее время восстановления (MTTR)

Пример организации работ по защите АСУ ТП



✓ Важно

СОКРАЩЕНИЯ

ТЗ	Техническое задание
ТП	Технический проект
РД	Рабочая документация
ФТТ	Функциональные технические требования
СЗ	Система защиты
ЭБ	Электробезопасность
ОТ	Охрана труда

Проектный менеджмент

24

Состав проектной команды:

- 1 руководитель проекта
- 1 администратор проекта
- 1 главный инженер проекта (ГИП)
- 3 ведущих инженера ИБ
- 4 инженера ИБ
- 1 ведущий аналитик ИБ
- 2 аналитика ИБ
- 2 конструктора-проектировщика
- 4 инженера
- 2 технических писателя

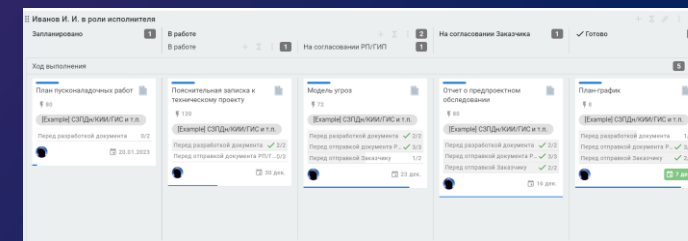
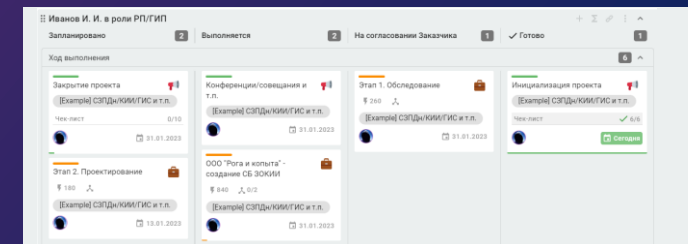
Характеристика команды:

- Гражданство РФ
- Сертифицированная спец. одежда
- Инструменты
- Удостоверения по ЭБ, ОТ, промышленной безопасности
- Готовность к командировкам
- Опыт работы в промышленности и труднодоступных местах

Состав команды может быть расширен на любом этапе проекта с учётом организационных возможностей Заказчика (длительность согласований, единовременное сопровождение нескольких бригад и т.п.)

Ведение проекта

- Еженедельные совещания
- Протоколирование встреч
- Защита этапов работ
- Автоматизированная система учёта (Kanban / Agile)
- Контроль соблюдения сроков проекта
- Очное и дистанционное обследование
- Параллельная работа над задачами



Архитектор

Исполнитель