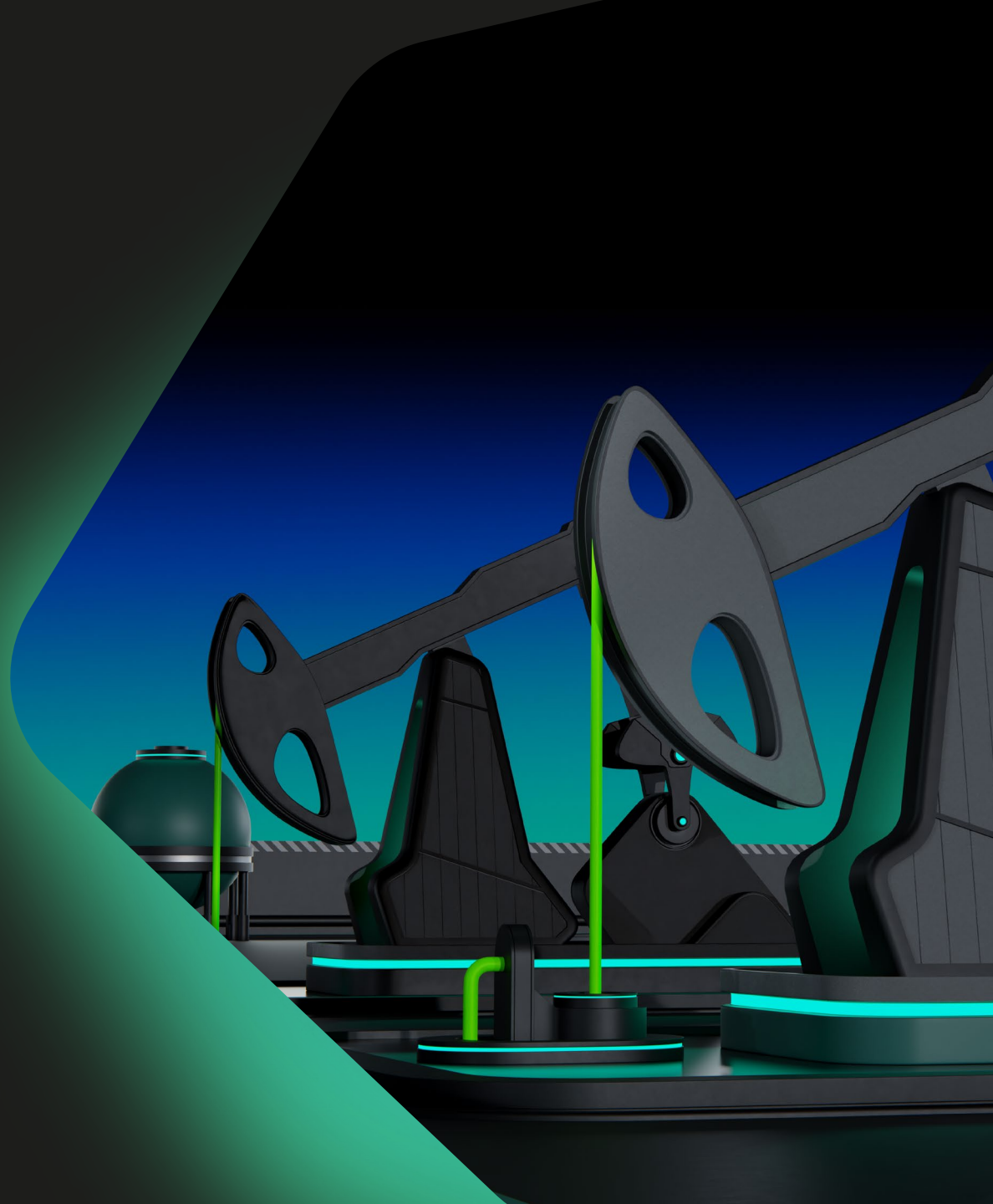
# Kaspersky OT Cybersecurity

## Отраслевые решения для нефтегазовых компаний



kaspersky

# Нефтегазовая отрасль России

Нефтегазовая промышленность играет ключевую роль в экономике Российской Федерации, обеспечивая 30% поступлений в федеральный бюджет. Кроме этого, Россия – один из крупнейших экспортеров нефти и газа в мире. Помимо этого, нефть, газ и сжиженный природный газ (СПГ) играют важнейшую роль в таких отраслях, как:

- Производство высокотехнологичных и строительных материалов
- Производство химикатов и удобрений
- Фармацевтическое и медицинское производство
- Многие другие жизненно важные сферы

Российские нефтегазовые компании привлекают свои ресурсы, опыт и инфраструктуру для достижения целей устойчивого развития, реализации национальных проектов и приоритетов Российской Федерации. Их стратегические усилия сосредоточены на следующих аспектах:

- Устойчивое развитие и ESG-трансформация[1]
- Повышение операционной эффективности

## Технологии для достижения целей устойчивого развития и повышения операционной эффективности

### Цифровые технологии и инструменты

- Решения в области машинного обучения и искусственного интеллекта для профилактического обслуживания и повышения надежности
- Конвергенция сред IT и OT
- IIoT и датчики для мониторинга
- Цифровые двойники для моделирования и оптимизации процессов
- Технологии дополненной и виртуальной реальности (AR, VR) для обучения сотрудников
- Роботизация и автоматизация для выполнения опасных задач

### Другие действия

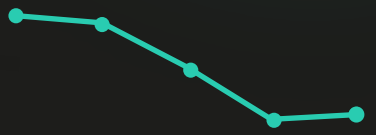
- Соблюдение нормативных требований
- Повышение уровня безопасности и устойчивости информационных систем
- Ответственное потребление и энергоэффективность
- Модернизация оборудования

## Инициативы нефтегазовых компаний в области устойчивого развития и повышения операционной эффективности

- Декарбонизация и углеродная нейтральность
- Сокращение выбросов парниковых газов
- Снижение негативного воздействия на окружающую среду
- Внедрение принципов циркулярной экономики
- Снижение уровня аварийности и производственного травматизма
- Реализация национальных проектов и приоритетов Российской Федерации

Достижение целей устойчивого развития и повышения операционной эффективности за счет внедрения инструментов цифровизации невозможно без обеспечения должного уровня информационной безопасности, позволяющего минимизировать риски, связанные с простоем производства.

Рост инвестиций в кибербезопасность привел к снижению числа атак.



**–9 п. п.**

Сокращение числа атак на компьютеры с АСУ ТП в нефтегазовой промышленности во втором полугодии 2023 года (по сравнению со вторым полугодием 2021 года)[2]

(1) 17 целей устойчивого развития были сформулированы Организацией Объединенных Наций как призыв к действиям, направленным на обеспечение мира и процветания на планете к 2030 году.
(2) Согласно статистике «Лаборатории Касперского» по ландшафту угроз для систем промышленной автоматизации за второе полугодие 2023 года.

# Цифровизация в нефтегазовой отрасли

## Применение цифровых технологий

### IIoT и облака

1. Сбор и обработка сейсмических данных
2. Оптимизация бурения
3. Обнаружение утечек из трубопроводов
4. Мониторинг нефтеперерабатывающих заводов
5. Оптимизация маршрутов и мониторинг складов

### Промышленная метавселенная: AR, VR

1. Обучение персонала, совместная работа и обслуживание в виртуальных средах

### Роботизация и частные сети LTE / 5G

1. Беспилотные воздушные и подводные роботы и аппараты для инспектирования и проведения бурильных работ
2. Мониторинг и сбор данных о состоянии трубопроводов в труднодоступных местах
3. Инспектирование заводов и возможность быстрого останова в случае неполадок

### Цифровые двойники

1. Моделирование сценариев бурения
2. Мониторинг систем трубопроводов с помощью цифровых виртуальных копий
3. Моделирование процессов на НПЗ для выявления узких мест

### Гиперавтоматизация, ИИ, ML, RPA

1. Поиск и определение точек бурения
2. Прогнозирование отказа насосов
3. Анализ данных о трубопроводах и транспорте
4. Прогнозирование отказов на НПЗ
5. Прогнозирование спроса

### Конвергенция IT и OT

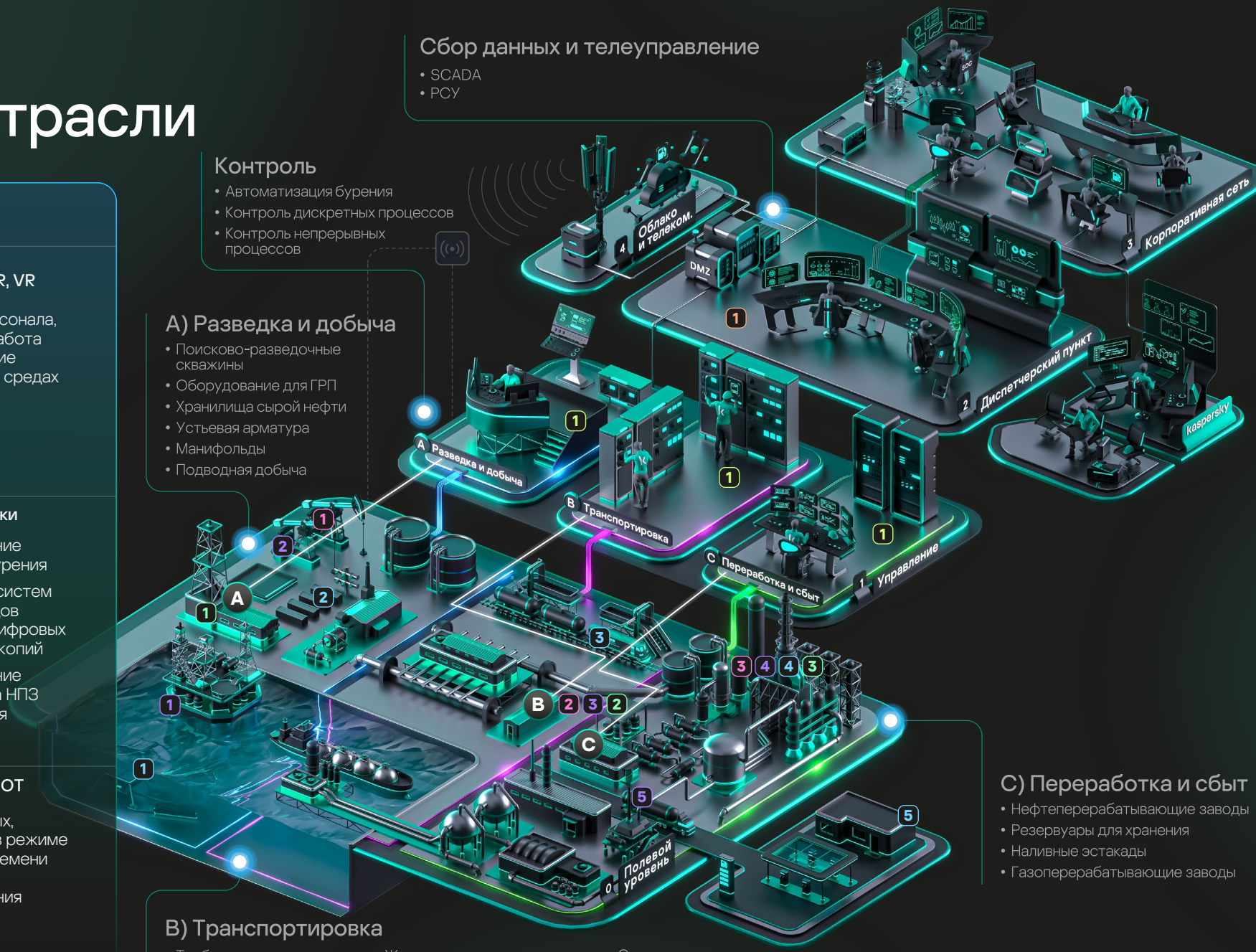
1. Анализ данных, получаемых в режиме реального времени от датчиков и оборудования

## Сбор данных и телеуправление

- SCADA
- PCY

## Контроль

- Автоматизация бурения
- Контроль дискретных процессов
- Контроль непрерывных процессов




## A) Разведка и добыча

- Поисково-разведочные скважины
- Оборудование для ГРП
- Хранилища сырой нефти
- Устьевая арматура
- Манифольды
- Подводная добыча

## B) Транспортировка

- Трубопроводы
- СПГ- и нефтяные танкеры
- Железнодорожные цистерны
- Газовые компрессоры
- Складские помещения

## C) Переработка и сбыт

- Нефтеперерабатывающие заводы
- Резервуары для хранения
- Наливные эстакады
- Газоперерабатывающие заводы

# Кибербезопасность как ключ к технологическому развитию

## Цветовая легенда цифровых технологий

- IIoT и облака
- Цифровые двойники
- Роботизация и частные сети LTE/5G
- Промышленная метавселенная: AR, VR
- Гиперавтоматизация, ИИ, ML, RPA
- Конвергенция IT и OT


## В то же время цифровая трансформация в нефтегазовой отрасли неразрывно связана с вопросами и задачами безопасности...

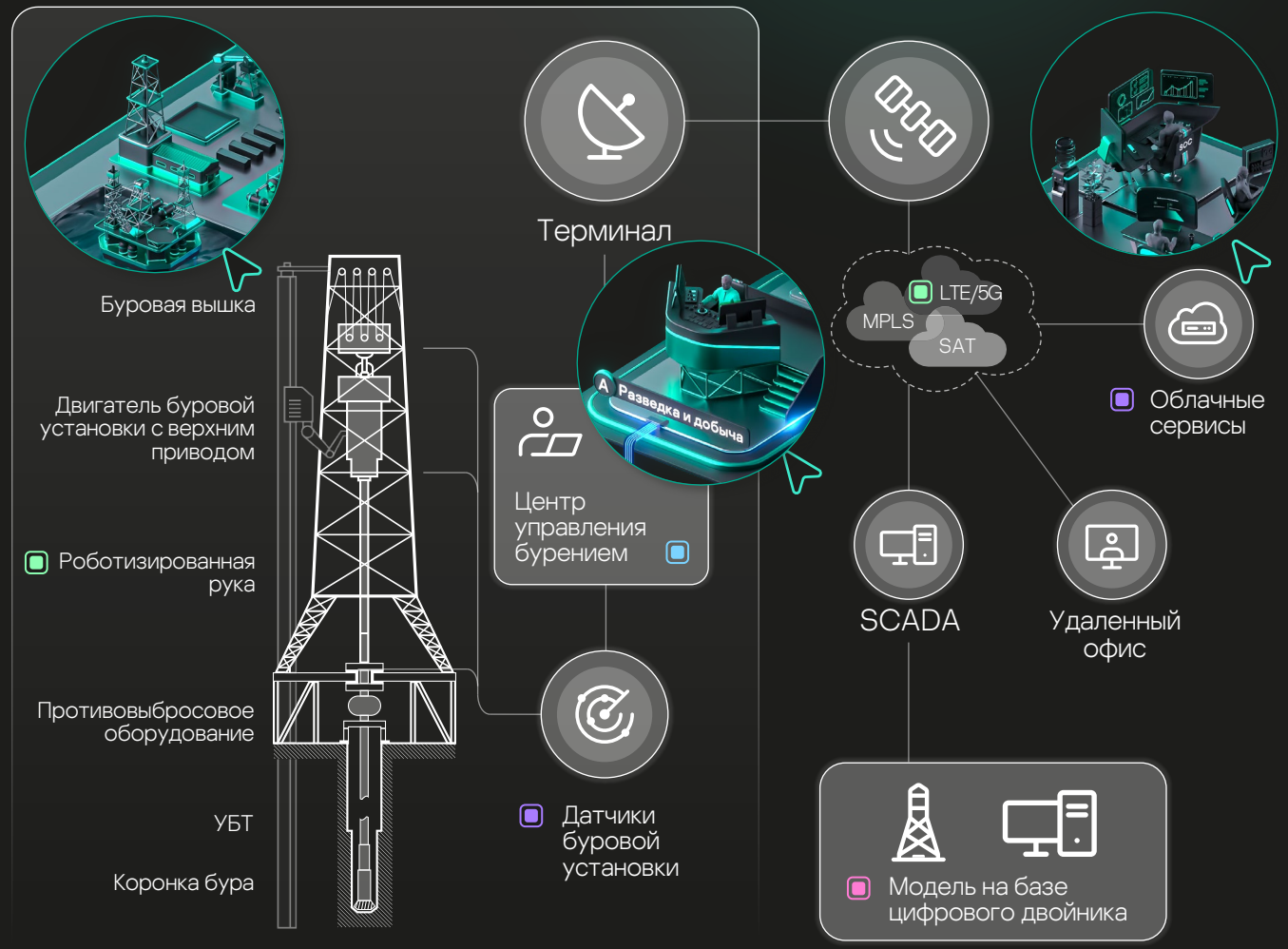
1. Увеличение поверхности атаки
2. Устаревшая инфраструктура и неконтролируемая конвергенция IT и OT
3. Внешний доступ к OT-инфраструктуре
4. Дефицит персонала
5. Нормативные требования по защите объектов критической инфраструктуры

Нажмите на элемент, чтобы продолжить

# 1. Увеличение поверхности атаки

IIoT и облака | Цифровые двойники | Гиперавтоматизация | Роботизация и LTE/5G

## Пример процесса добычи




АСУ ТП предназначены для управления сложными технологическими средами, куда входят буровые площадки, трубопроводы и НПЗ. Подобные взаимосвязанные системы уязвимы для кибератак, поскольку подключение к одному компьютеру или терминалу открывает доступ к более широкому сегменту инфраструктуры.

## Характеристики решения


## Как может помочь «Лаборатория Касперского»

**Kaspersky Industrial CyberSecurity**

- Полное покрытие OT/ IIoT-инфраструктуры
- Мониторинг систем и сетей
- Регулярные глубокие аудиты безопасности

## Вспомогательные сервисы

**Kaspersky ICS Security Assessment**

- Выявление уязвимостей и недостатков систем безопасности в инфраструктурах АСУ ТП
- Проверка критических компонентов

**Kaspersky Managed Detection and Response**

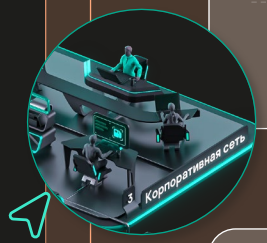
- Проактивный поиск угроз
- Автоматизированное и управляемое реагирование
- Глубокие знания в области кибербезопасности АСУ ТП

Нажмите на значок продукта, чтобы узнать больше

# 2. Устаревшая инфраструктура и неконтролируемая конвергенция IT и OT

Конвергенция IT и OT

Пример архитектуры системы переработки нефтепродуктов




IT

**Телекоммуникации** MPLS 5G/LTE SAT

**Корпоративная сеть**

Промышленная ДМЗ

**Управление переработкой** Единая операторная; Серверы архивных данных

**Контроль** Рабочие станции постов мониторинга и диагностики

**Контроллеры** ПЛК и автоматика

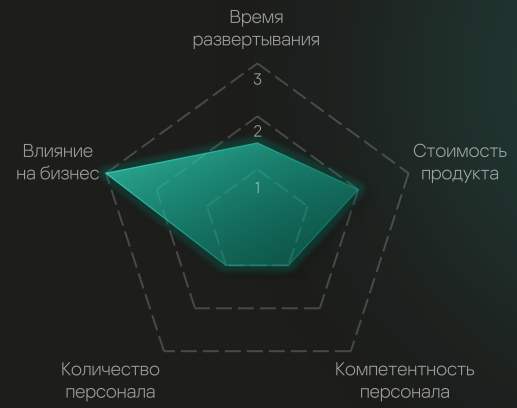
**Устройства** Контрольно-измерительные и исполнительные устройства, IoT

OT

Интеграция IT- и OT-сред уже стала важнейшим элементом архитектуры процессов в нефтегазовой отрасли, однако ее реализация может быть сопряжена с рисками безопасности

- Незащищенная ранее развернутая инфраструктура с устаревшими технологиями
- Несоответствие приоритетов в области кибербезопасности в разных системах, что может привести к противоречиям в механизмах защиты
  - IT-инфраструктура: фокус на конфиденциальности и целостности данных
  - OT-инфраструктура: фокус на обеспечении функционирования и доступности в режиме реального времени

## Характеристики решения




## Как может помочь «Лаборатория Касперского»

**Kaspersky Industrial CyberSecurity**

- Обнаружение угроз и аномалий, меры безопасного реагирования на хостах и в сетях
- Централизованное управление рисками, политикой безопасности и активами на всех уровнях промышленной системы автоматизации и контроля

**Kaspersky Machine Learning for Anomaly Detection**

- Прогноз отказа установки, нарушений процессов и качества методами машинного обучения, обслуживание по состоянию
- Обнаружение киберугроз, нацеленных на системы и процессы

## Вспомогательные сервисы

**Kaspersky Threat Intelligence**

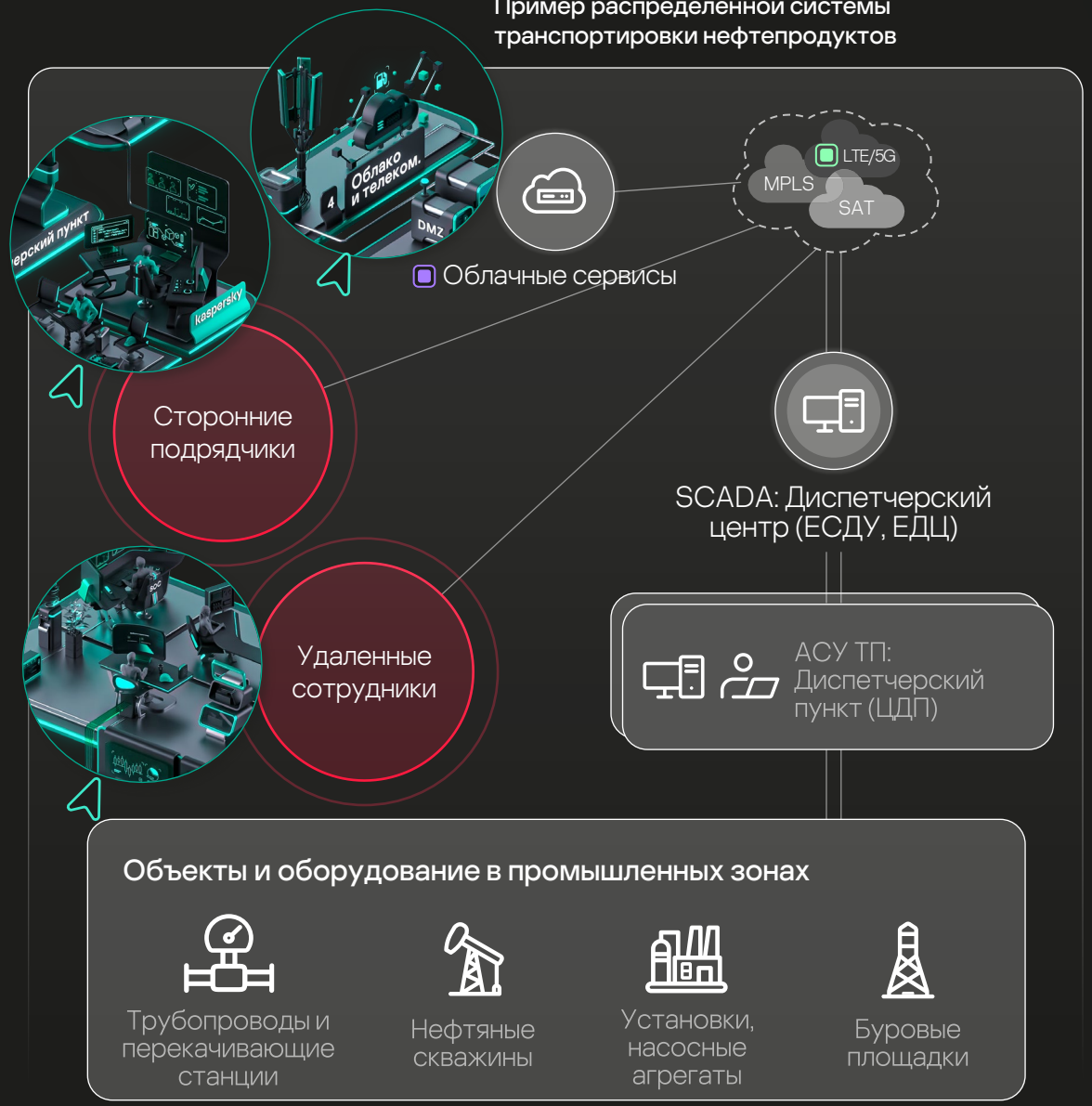
- Обнаружение угроз
- Расследования и поиск активных угроз
- Исчерпывающая информация об угрозах и уязвимостях

Нажмите на значок продукта, чтобы узнать больше

# 3. Внешний доступ к OT-инфраструктуре

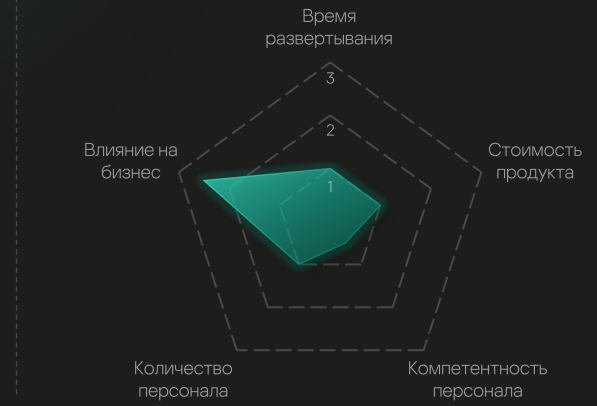
IIoT и облака | Роботизация и LTE/5G

Пример распределенной системы транспортировки нефтепродуктов




Благодаря конвергенции IT- и OT-сред сотрудники, работающие удаленно, и сторонние подрядчики могут получать доступ к технологическим установкам, трубопроводам и другим системам предприятий нефтегазовой отрасли с целью отслеживания производственных процессов, управления ими и анализа данных. Подобная оптимизация подразумевает защиту внешних подключений, поскольку пользователи с удаленным доступом к OT-инфраструктуре могут подвергнуть ее серьезному риску.

## Характеристики решения




## Как может помочь «Лаборатория Касперского»

**Kaspersky SD-WAN**

### Быстрое развертывание распределенной сети

- Простое масштабирование
- Простое администрирование
- Централизованное управление безопасностью

**Kaspersky Thin Client**

- Кибериммунные тонкие клиенты для безопасного удаленного доступа
- Центральный модуль управления для упрощения администрирования инфраструктуры тонких клиентов

Нажмите на значок продукта, чтобы узнать больше

# 4. Дефицит персонала

Промышленная метавселенная | Конвергенция IT и OT


Уже более десяти лет нефтегазовая отрасль сталкивается с трудностями в привлечении и удержании квалифицированных специалистов. Эта проблема обостряется в связи с цифровой трансформацией и высоким спросом на работников, обладающих как техническими навыками, так и знаниями в области цифровых технологий.

**41%**

Компаний в разных странах сталкиваются с нехваткой квалифицированных кадров в сфере ИБ

По данным глобального исследования «Лаборатории Касперского»

## Характеристики решения


## Как может помочь «Лаборатория Касперского»

### Kaspersky Industrial CyberSecurity

- Снижение нагрузки на персонал, отвечающий за кибербезопасность
- Быстрое реагирование на угрозы

### Kaspersky Unified Monitoring and Analysis Platform

- Централизованный сбор, анализ и корреляция ИБ-событий из различных источников данных
- Единый подход к кибербезопасности в промышленном и корпоративном сегментах

## Вспомогательные сервисы

### Kaspersky Security Awareness

- Материалы для тренингов
- Обучение в игровой форме с помощью моделирования бизнес-процессов
- Интерактивные учебные модули и имитация фишинговых атак

### Kaspersky ICS CERT

Практические знания от экспертов

- Цифровая криминалистика и реагирование на инциденты
- Исследование уязвимостей
- Межфункциональные программы подготовки

Нажмите на значок продукта, чтобы узнать больше

# 5. Нормативные требования по защите объектов критической инфраструктуры

Нефтегазовые компании в России относятся к объектам критической информационной инфраструктуры (КИИ), поскольку их деятельность имеет стратегическое значение для экономики страны.

Соответственно, они подчиняются требованиям, установленным для КИИ, а также дополнительным отраслевым стандартам и рекомендациям.

### Федеральные законы

- № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ)»
- № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»
- № 116-ФЗ «О промышленной безопасности опасных производственных объектов»
- № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- № 152-ФЗ «О персональных данных»

### Международные стандарты

- ISO 27001 международный стандарт, определяющий требования к Системе Управления Информационной Безопасностью (СУИБ)
- IEC 62443 всемирно признанный стандарт промышленной кибербезопасности, который обеспечивает комплексную структуру для защиты промышленных систем автоматизации и управления (IACS)
- NIST SP 800-82 стандарт информационной безопасности (ИБ) промышленных систем управления

### Основные НПА

- Постановление Правительства РФ № 127 определяет порядок категорирования объектов критической информационной инфраструктуры (КИИ) России
- Приказ ФСТЭК России № 31 устанавливает требования к обеспечению защиты информации в АСУ ТП на критически важных, потенциально опасных и иных объектах
- Приказ ФСТЭК России № 235 устанавливает требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования
- Приказ ФСТЭК России № 239 об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ

### Стандарты технической организации и внутренние политики нефтегазовых компаний

- СТО Газпром 4.2-2-002-2009: Система обеспечения информационной безопасности ОАО Газпром. Требования к автоматизированным системам управления технологическими процессами
- Политика ПАО «НК «Роснефть» в области информационной безопасности № П3-11.01 П-01
- Политика ПАО «Татнефть» им. В.Д. Шашина в области информационной безопасности

Узнайте все требования регуляторов к вашему бизнесу и получите рекомендации по их выполнению.

## Как может помочь «Лаборатория Касперского»

Мы сотрудничаем с государственными регуляторами и поставщиками средств промышленной автоматизации в целях сертификации своих решений.

Мы проводим сертификацию решений и тесты на совместимость, готовим эталонные модели и интегрируем наши многочисленные продукты и решения.

Полный список сертификатов

## Государственные сертификаты

### KICS for Networks

- Сертификат ФСТЭК России на соответствие профилю СОВ С4
- Сертификат ФСБ России на соответствие требованиям СОА класса В

### KICS for Nodes

- Сертификат ФСТЭК России на соответствие профилю САВЗ В2, СКН П2
- Сертификат ФСБ России на соответствие требованиям АВЗ класса В2

## Протестировано на совместимость

Прософт-системы · TraceMode · РегЛаб · НПФ «КРУГ» · Schneider Electric · Атомик Софт · SIEMENS · YOKOGAWA · EMERSON · Honeywell

>130 систем от 50+ вендоров

## Kaspersky Security Awareness и экспертные тренинги

позволяют развить у сотрудников навыки кибербезопасности и повысить устойчивость бизнеса к инцидентам, связанным с человеческим фактором.

Узнайте подробнее о продуктах Kaspersky Security Awareness

# Устойчивость к киберугрозам с решениями «Лаборатории Касперского»

| 1 Инвентаризация активов и оценка рисков | 2 Базовая защита | 3 Обнаружение продвинутых угроз и защита от них | 4 Аудит безопасности и оценка соответствия нормативным требованиям | 5 Отлаженные процессы обеспечения безопасности | 6 Готовность персонала и отказоустойчивость |
|---|---|---|---|---|---|
| Уровень знаний | Опыт + технологии | Знания + технологии + опыт | Знания + технологии + опыт | Знания + технологии + опыт | Знания + опыт |

**Обнаружение активов**

- Идентификация всех активов IT-, OT- и IIoT-инфраструктуры
- Каталогизация аппаратных и программных компонентов рабочих мест
- Определение критических активов и уязвимостей для разработки стратегии кибербезопасности

**Оценка рисков и разработка политик**

- Оценка текущего уровня риска кибербезопасности
- Разработка комплексных политик, процедур и показателей устойчивости к киберугрозам
- Использование анализа опасностей и последствий для установления уровней кибербезопасности и определения необходимых средств контроля

**Укрепление**

- Безопасная настройка систем и регулярная установка исправлений и обновлений
- Использование SD-WAN и VLAN для сегментации сети и безопасного удаленного доступа
- Контроль безопасности даже на удаленных и небольших объектах

**Контроль программ**

- Поддержание целостности системы благодаря ограничению использования неразрешенных приложений

**Защита рабочих мест**

- Внедрение решений для борьбы с вредоносным ПО для защиты устройств в конвергентных IT/OT-средах
- Защита от эксплойтов и проверка съемных устройств

**Контроль на уровне сети**

- Мониторинг сетевого трафика для выявления аномалий и понимания моделей атак

**Обнаружение вторжений и аномалий**

- Использование машинного обучения и глубокого анализа трафика (DPI) для выявления сетевых вторжений
- Использование технологии EDR для мониторинга телеметрии OT-хостов

**Предотвращение вторжений**

- Расширение возможностей обнаружения и предотвращения атак за счет интеграции с имеющимся сетевым оборудованием

**Аудит безопасности**

- Регулярное сканирование на предмет уязвимостей и аудит на соответствие нормативным требованиям

**Контроль конфигураций**

- Проведение подробных системных аудитов и контроль конфигураций

**Обеспечение соответствия внешним требованиям**

- Помощь в соблюдении нормативов и отраслевых стандартов защиты критической инфраструктуры

**Аналитические данные об угрозах для промышленных SOC**

- Использование получаемых в режиме реального времени данных об угрозах для защиты от вредоносных программ, фишинга и эксплойтов

**Консультирование по вопросам SOC**

- Привлечение экспертов для расширения возможностей SOC по борьбе с комплексными угрозами

**Обнаружение угроз и реагирование на них в конвергентных IT/OT-средах**

- Интеграция систем безопасности IT- и OT-сред с целью унификации механизмов обнаружения угроз и реагирования на них

**Защита силами экспертов**

- Использование управляемых служб обнаружения и реагирования для непрерывного мониторинга и квалифицированной обработки инцидентов

**Обучение специалистов**

- Проведение специализированных тренингов по кибербезопасности для сотрудников, чтобы те могли эффективно справляться с проблемами и устранять их

**Тренинги для повышения осведомленности о киберугрозах**

- Регулярные тренинги для повышения общей отказоустойчивости систем и готовности к кибератакам среди всех сотрудников

**Анализ производительности активов**

- Использование инструментов и методологий для анализа производительности активов, обеспечения надежности и выявления потенциальных отказов

**Культура устойчивости к киберугрозам**

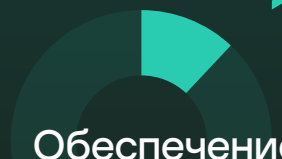
- Создание комплексной модели управления кибербезопасностью
- Продвижение концепции изначальной устойчивости к киберугрозам

Узнайте больше о комплексном подходе «Лаборатории Касперского» к обеспечению кибербезопасности на всех уровнях

# Опыт «Лаборатории Касперского» в нефтегазовой отрасли

**Более 10 лет**
опыта работы
в нефтегазовом секторе

**138 проектов**
завершено



**12%**

**Обеспечение защиты для нефтегазовых компаний, на долю которых приходится 12% от общего объема мировой добычи нефти**

**60 компаний**
уже под защитой

Решения Kaspersky OT Cybersecurity обеспечивают комплексную защиту промышленной инфраструктуры нефтегазовых предприятий. Платформа способна централизованно обнаруживать сложные атаки и реагировать на них в масштабах всей промышленной сети.

## Типичные примеры клиентских задач

- Помощь в объединении корпоративного и промышленного секторов в единую защищенную инфраструктуру с обеспечением безопасности на всех уровнях
- Централизация всех функций информационной безопасности в географически распределенных сетях для большей прозрачности действий в рамках инфраструктуры и более эффективного использования человеческих ресурсов
- Помощь в защите чувствительного к сканированию оборудования, работающего с устаревшими и неподдерживаемыми операционными системами и системами безопасности
- Обеспечение стабильной работы системы информационной безопасности с учетом требований высокой доступности и ограничений по потреблению ресурсов

## Почему нефтегазовые компании выбирают «Лабораторию Касперского»

- Богатый опыт противодействия киберугрозам и постоянного мониторинга ландшафта угроз
- Системы информационной безопасности, созданные с учетом последних тенденций в индустрии
- Содействие в выполнении требований регулирующих органов
- Отсутствие влияния на производственные процессы и работу устройств
- Продукты, регулярно признаваемые лучшими в тестах международных исследовательских институтов
- Продукты «Лаборатории Касперского» проверены на совместимость с решениями ведущих производителей систем промышленной автоматизации

**>80%**
мер приказа ФСТЭК РФ № 239 покрываются решениями «Лаборатории Касперского»

**242**
системы от 57 поставщиков АСУ ТП прошли сертификацию

# Примеры успешного сотрудничества с компаниями нефтегазовой отрасли

## За последние 10 лет «Лаборатория Касперского»:

Защитила от киберугроз крупнейший холдинг с 80 месторождениями, расположенными в тысячах километров друг от друга

Обеспечила безопасность уникального для региона терминала нефтехимической продукции с пропускной способностью 205 000 тонн, внедрив решения для контроля перевалки нефтехимических продуктов с железной дороги на морской транспорт

Внедрила систему кибербезопасности на крупном газотранспортном предприятии, входящем в перечень объектов критической инфраструктуры и обеспечивающем газом более 20 миллионов человек

## Ведущая морская нефтегазовая компания в Каспийском регионе

Для сотрудников «КазМунайТениз» проведен тренинг из портфолио Kaspersky Industrial CyberSecurity, с учетом специфики нефтяной отрасли

Подробнее

## Один из крупнейших НПЗ в мире

Результат выбора XDR-платформы Kaspersky Industrial CyberSecurity (KICS):

- Повышение уровня информационной безопасности на НПЗ
- Быстрое обнаружение потенциальных угроз и реагирование на них
- Улучшенные защита от киберугроз, мониторинг и аналитика производственных процессов

Подробнее

www.kaspersky.ru



## Управляйте своей безопасностью вместе с решениями «Лаборатории Касперского» и станьте ее партнером

Свяжитесь с нами и примите участие в нашей международной конференции для клиентов

Подробнее

#kaspersky
#активируйбудущее