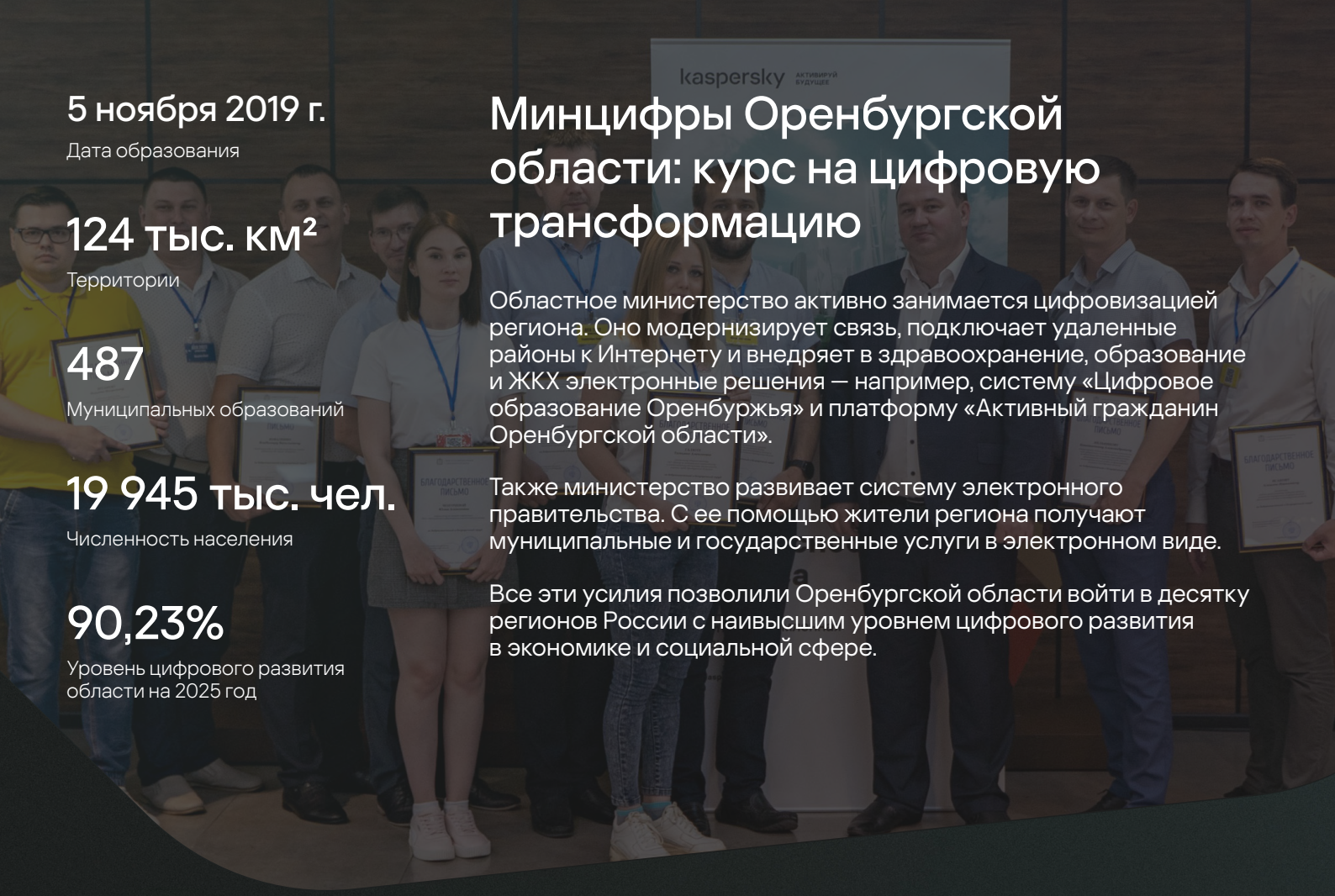
# Рабочие устройства под контролем с KEDR Expert

## Министерство цифрового развития и связи Оренбургской области

kaspersky активируй будущее

Минцифра Оренбургской области
digital.orb.ru




**5 ноября 2019 г.**
Дата образования

**124 тыс. км²**
Территории

**487**
Муниципальных образований

**19 945 тыс. чел.**
Численность населения

**90,23%**
Уровень цифрового развития области на 2025 год

# Минцифры Оренбургской области: курс на цифровую трансформацию

Областное министерство активно занимается цифровизацией региона. Оно модернизирует связь, подключает удаленные районы к Интернету и внедряет в здравоохранение, образование и ЖКХ электронные решения — например, систему «Цифровое образование Оренбуржья» и платформу «Активный гражданин Оренбургской области».

Также министерство развивает систему электронного правительства. С ее помощью жители региона получают муниципальные и государственные услуги в электронном виде.

Все эти усилия позволили Оренбургской области войти в десятку регионов России с наивысшим уровнем цифрового развития в экономике и социальной сфере.

### Успешное применение

Министерство цифрового развития и связи Оренбургской области пользуется решениями Kaspersky с 2020 года.

# Как рост цифровизации меняет требования к киберзащите

Рабочие места сотрудников (конечные устройства) — один из самых уязвимых элементов любой ИТ-инфраструктуры. Злоумышленники часто используют их, чтобы проникнуть в систему. Поэтому контроль за рабочими местами должен быть постоянным: только так ИБ-отдел успеет вовремя заметить и отразить атаку.

Скорость реагирования особенно важна для государственных органов, которые работают с конфиденциальной информацией. Атаки на конечные устройства могут привести к утечке ценных данных и поставить под угрозу безопасность жителей региона, нанести удар по репутации ведомства.

С ростом числа онлайн-сервисов в Оренбуржье министерству цифрового развития потребовалась более масштабная ИТ-инфраструктура. В связи с этим расширилась поверхность атаки и появилась необходимость снять часть нагрузки с ИБ-отдела, не прекращая непрерывно следить за безопасностью рабочих устройств. Для решения этих задач министерство внедрило Kaspersky EDR Expert. Решение предоставляет необходимые инструменты для мониторинга угроз, анализа инцидентов и автоматического реагирования.

## Возможности Kaspersky Endpoint Detection and Response Expert

- Непрерывный мониторинг событий безопасности
- Централизованное реагирование
- Проактивный поиск угроз
- Распознавание угроз по индикаторам IoC и IoA и правилам YARA
- Визуализация каждой стадии расследования
- Ретроспективный анализ
- Сбор данных компьютерной криминалистики для расследования инцидента
- Доступ к порталу Kaspersky Threat Intelligence

# Решение

Kaspersky EDR Expert — решение класса Endpoint Detection and Response. Оно позволяет ИБ-специалистам следить за потенциально опасной активностью на рабочих устройствах, детально анализировать обнаруженные угрозы и оперативно наних реагировать.

KEDR Expert регистрирует события безопасности на конечных точках, что позволяет ИБ-специалистам анализировать потенциальные угрозы. Эти сведения доступны через единую веб-консоль управления.

Министерство цифрового развития и связи Оренбургской области использует решения «Лаборатории Касперского» уже пять лет — так, рабочие устройства ведомства защищает Kaspersky Security для бизнеса. Это решение работает на той же агентской базе, что и KEDR Expert, что позволило быстро интегрировать последний в действующую ИБ-инфраструктуру.

# Преимущества Kaspersky EDR Expert

### Интеграция с существующей инфраструктурой

Для комплексной защиты рабочих мест. KEDR Expert интегрирован с Kaspersky Security для бизнеса и дополняет защиту рабочих мест продвинутыми функциями обнаружения, расследования и реагирования. Решения работают на базе единого агента и обмениваются информацией, повышая защищенность инфраструктуры.

### Оперативное реагирование на киберинциденты

Единая консоль KEDR Expert помогает быстро реагировать на инциденты независимо от масштаба инфраструктуры — ИБ-специалисты видят полную картину происходящего и могут оперативно локализовать угрозы и устранять последствия атак.

### Интеграция с Kaspersky Security Network (KSN)

KEDR Expert проверяет репутацию файлов и URL-адресов в реальном времени — через подключение к приватной копии KSN или к ее публичной, глобальной версии. Это позволяет сравнивать обнаруженные индикаторы с актуальной базой данных угроз от производителя решения.

### Выявление и анализ угроз

KEDR Expert использует индикаторы атаки (IoA), индикаторы компрометации (IoC) и правила YARA для анализа подозрительной активности.

### Доступ к аналитике угроз

KEDR Expert интегрирован с Kaspersky Threat Lookup, чтобы ИБ-аналитики могли обращаться к онлайн-базе аналитических данных об угрозах и получать расширенный контекст для обнаруженных индикаторов компрометации (IoC).

### Встроенная «песочница»

В составе решения KEDR Expert доступен компонент Sandbox, который позволяет запускать подозрительные файлы в изолированной среде, чтобы проанализировать их поведение и заблокировать вредоносную активность даже в случае ранее неизвестных киберугроз.

# Результаты и отзывы

С внедрением Kaspersky Endpoint Protection and Response Expert Министерство цифрового развития и связи Оренбургской области усилило защиту конечных точек и укрепило ИТ-инфраструктуру. Внедрение KEDR Expert стало частью стратегии министерства по повышению кибербезопасности. Решение дополнило существующую инфраструктуру, предоставив инструменты для мониторинга и реагирования на угрозы.

**Дмитрий Сергеевич Вечеренко**

Министр цифрового развития и связи Оренбургской области

«

Применение EDR-решения способствовало более оперативному выявлению угроз и минимизации рисков инцидентов в инфраструктуре государственных информационных систем Оренбургской области.

**Ксения Александровна Горшкова**

Исполняющая обязанности заместителя министра — начальника управления информационной безопасности министерства цифрового развития и связи Оренбургской области

«

Решение позволило сократить время анализа инцидентов и улучшить контроль за угрозами.

Такой комплексный подход помогает постоянно укреплять безопасность конечных точек — а это важно в условиях постоянно меняющегося ландшафта киберугроз.

**Анна Кулашова**

Вице-президент «Лаборатории Касперского» по развитию бизнеса в России и странах СНГ

«

Наша система класса EDR для борьбы со сложными киберугрозами и целевыми атаками дополняет платформу защиты рабочих мест Kaspersky Security для бизнеса, которая много лет успешно используется в Министерстве цифрового развития и связи Оренбургской области. В совокупности эти решения позволяют своевременно выявлять риски инцидентов внутри инфраструктуры и реагировать на них, способствуя построению эшелонированной защиты в организации.

# Kaspersky Endpoint Detection and Response

## Expert

Подробнее

www.kaspersky.ru



#kaspersky
#активируйбудущее