


# Комплексная киберзащита для непрерывного вещания

«Газпром-Медиа Холдинг»

**kaspersky** активируй  
будущее

 **ГАЗПРОМ МЕДИА**

# 1998

год основания

# 140 млн

общая аудитория холдинга

# 85 млн

пользователей в месяц охватывает RUTUBE

# 10 из 10

самых рейтинговых комедийных сериалов вышли на TNT

# 10 лет

подряд радиостанция холдинга «ГПМ Радио» занимает первое место в Москве по охвату аудитории

## «Газпром-Медиа Холдинг»

«Газпром-Медиа Холдинг» — крупнейший медиахолдинг России и Восточной Европы. Он был основан в 1998 году как дочернее предприятие ПАО «Газпром» для управления медиаактивами. Холдинг объединяет телеканалы, радио, интернет-платформы, издательства, кинопроизводство, рекламные и цифровые сервисы.

В состав холдинга входят каналы НТВ, TNT, TNT4, ТВ-3, «Пятница!», «Матч ТВ», RUTUBE, радиостанции, издательский дом «Семь дней», киностудия, рекламные агентства и технологическая компания «ГПМ Цифровые технологии».

Медиахолдинг генерирует тысячи часов оригинального контента в год, а платформы PREMIER и YAPPY охватывают десятки миллионов пользователей.

# к

### Масштаб ресурсов, нуждающихся в защите



10 млн. одновременных подключений во время премьер



500+ терабайт эксклюзивного контента



1500+ рабочих станций в креативных командах



24/7 вещание на многомиллионную аудиторию

## Инновационный подход и киберзащита

«Газпром-Медиа Холдинг» прочно удерживает лидирующие позиции в отрасли, в том числе благодаря активному внедрению новейших технологий во все области деятельности. Холдинг применяет **инновационные решения как в цифровых сервисах, так и в технической поддержке, обеспечивая клиентам быстрый и удобный доступ к услугам.** Автоматизация процессов администрирования и оптимизация коммуникации с пользователями позволяют компании сохранять высокий уровень сервиса.

В ответ на усложнение ландшафта угроз холдинг решил усилить меры кибербезопасности, а именно — внедрить **передовые системы защиты от сложных инцидентов и современных видов атак.** При выборе новых инструментов киберзащиты было решено опираться на подтвержденную экспертизу поставщика и проверенную эффективность решения. Немаловажную роль сыграл опыт вендора в реализации аналогичных проектов и глубокое понимание специфики бизнеса. Дополнительным фактором стала надежная служба технической поддержки, оперативно реагирующая на любые вопросы и инциденты.

## Преимущества решений «Лаборатории Касперского»

- Многолетний международный опыт и глубокая экспертиза специалистов
- Защитные решения на основе передовых технологий и собственных запатентованных разработок
- Поддержка экспертов на любом этапе внедрения и использования наших решений
- Соответствие требованиям государственных регуляторов

## Решение

Для обеспечения нужного уровня киберзащиты в инфраструктуру «Газпром-Медиа Холдинга» было внедрено сразу несколько решений:



### Kaspersky Anti Targeted Attack

**КАТА — мощный инструмент, обеспечивающий надежную защиту от сложных и неизвестных ранее угроз.**

Благодаря передовым алгоритмам платформа позволяет специалистам отслеживать потенциальные точки атаки — сетевые подключения, веб-трафик, электронную почту — и минимизировать риски. Решение в режиме реального времени анализирует сетевой трафик, проактивно выявляя угрозы и ускоряя реагирование на них.



### Kaspersky Endpoint Detection and Response Expert

**Для защиты рабочих мест было выбрано решение Kaspersky EDR Expert.** Оно предназначено для расширенного обнаружения, эффективного расследования, проактивного поиска угроз и устранения комплексных атак, направленных на инфраструктуру конечных устройств. Kaspersky EDR Expert позволяет выполнять глубокий анализ инцидентов, а также сопоставлять данные с актуальными репутационными базами «Лаборатории Касперского».



### Kaspersky Unified Monitoring and Analysis Platform

**Платформа KUMA была выбрана в качестве комплексного решения по централизованному мониторингу угроз** для распределенной ИТ-инфраструктуры холдинга. Платформа автоматизирует процессы обнаружения атак и при этом соответствует отраслевым стандартам безопасности, что особенно важно для медиакомпании такого масштаба.

# Ключевые возможности решений «Лаборатории Касперского»



## Централизованное управление

KATA позволяет управлять всеми инсталляциями решения из единой консоли и использовать для них единую базу правил и отчетов.



## Комплексная защита

С помощью Kaspersky EDR Expert специалисты по безопасности получают передовой контроль конечных точек и полную картину событий в инфраструктуре.



## Широкие возможности

KUMA легко встраивается в инфраструктуру и объединяет в цельную систему как решения от «Лаборатории Касперского», так и другие продукты.



## Глубокая интеграция

Благодаря интеграции с другими защитными решениями KATA позволяет формировать комплексные инциденты, включающие сетевые и узловые предупреждения системы безопасности.



## Расследование и анализ

Kaspersky EDR Expert позволяет детально воссоздавать последовательность действий злоумышленников без лишней нагрузки на службу ИБ.



## Высокая надежность

Благодаря микросервисной архитектуре KUMA обладает высокой отказоустойчивостью и низкими системными требованиями.

## Результаты и отзывы

Внедрение комплекса решений позволило холдингу значительно **повысить уровень кибербезопасности**, сократив время реагирования на инциденты. Теперь пользовательские данные защищены еще надежнее, а цифровые платформы работают стабильно даже в периоды пиковых нагрузок.



### Алексей Жуков

Руководитель отдела информационной безопасности «Газпром-Медиа Холдинг»

Для медиаиндустрии безопасность — это не просто техническая необходимость, а основа доверия нашей аудитории. Внедренные решения «Лаборатории Касперского» позволяют нам эффективно защищать как инфраструктуру, так и интеллектуальную собственность.



### Марина Усова

Директор по корпоративным продажам «Лаборатории Касперского» в России

Защита инфраструктуры подобных масштабов — серьезный вызов. Необходимо следить за сотнями узлов, выявлять даже самые изощренные атаки и, конечно, не допускать перебоев в работе. В наши решения заложена возможность справляться с большой нагрузкой, и они значительно облегчают работу сотрудников ИБ-отделов. Единая комплексная система позволяет видеть события с любых источников в инфраструктуре и реагировать максимально быстро.



## Kaspersky Unified Monitoring and Analysis Platform

[Подробнее](#)



## Kaspersky Endpoint Detection and Response Expert

[Подробнее](#)



## Kaspersky Anti Targeted Attack

[Подробнее](#)