



# Осуществление импорто- независимости

в крупнейшем  
российском провайдере

# 1993 год

Дата основания

# 40%

Доля рынка

# 250

Сотрудников  
в ИБ-департаменте



Признанный технологический лидер в инновационных решениях в области электронного правительства, дата-центров и облачных вычислений, биометрии, здравоохранения, образования, жилищно-коммунальных услуг и кибербезопасности

## Компания «Ростелеком»

Крупнейший в России интегрированный провайдер цифровых услуг и решений, который присутствует во всех сегментах рынка и охватывает миллионы домохозяйств, государственных и частных организаций. Число сотрудников составляет более 100 тысяч человек. Компания занимает лидирующие позиции на рынке услуг высокоскоростного доступа в интернет и платного телевидения.

### Количество клиентов компании:

1

Услуги доступа в интернет с использованием оптических технологий — около 11 млн

2

Платное ТВ «Ростелекома» — 11 млн

3

IPTV — 6,4 млн

### Многолетнее партнерство

Многолетнее сотрудничество между «Ростелекомом» и «Лабораторией Касперского», продолжающееся более 10 лет, обусловило выбор SIEM-системы «Лаборатории Касперского».

## Надежный выбор на будущее

В процессе реализации задачи по осуществлению импортонезависимости «Ростелеком» искал отечественное решение для замены существующей зарубежной SIEM-системы. Крупнейшему в России провайдеру было необходимо найти достойную альтернативу, которая могла бы обеспечить гибкость и масштабируемость для управления растущим потоком событий и обеспечивать высокую производительность без негативного влияния на безопасность и надежность.

Для решения этих задач провайдер обратился к услугам интегратора «КОМПЛАИНС СОФТ». Партнер начал процесс поиска с проработки и оценки доступных российских решений, удовлетворяющих конкретные потребности «Ростелекома». После тщательного изучения ряда SIEM-систем компания сделала осознанный выбор в сторону Kaspersky Unified Monitoring and Analysis Platform (KUMA) от «Лаборатории Касперского».



«Ростелеком» успешно внедрил решение без потери качества мониторинга и значительного увеличения покрытия инфраструктуры. Архитектура решения обеспечивает высокую доступность и масштабируемость, а также легко интегрируется с внешними системами тикетинга и отчетности. KUMA зарекомендовала себя как эффективный и действенный инструмент безопасности, отвечающий потребностям заказчика в условиях современного ландшафта угроз.

## Эффективное замещение инструментов защиты

Сейчас компания «Ростелеком» активно использует практически весь спектр продуктов и услуг «Лаборатории Касперского», включая передовые технологии обнаружения целевых атак. Решение **Kaspersky Unified Monitoring and Analysis Platform** было выбрано вследствие проверенного качества отечественного вендора, отличной производительности по сравнению с аналогами, а также гибкости вендора при адаптации планов развития продукта.

Благодаря успешному внедрению SIEM-системы, «Ростелеком» эффективно отслеживает и анализирует события ИБ в режиме реального времени, что облегчает выявление и реагирование на потенциальные угрозы. Усовершенствованный, с учетом специфики требований «Ростелекома», механизм генерации оповещений повышает способность KUMA точно обнаруживать и приоритизировать угрозы в зависимости от их потенциального воздействия, что позволяет сотрудникам департамента ИБ провайдера в первую очередь сосредоточиться на наиболее важных проблемах.



**Виктор Веренцов**

Руководитель  
Корпоративного центра ГосСОПКА,  
ПАО «Ростелеком»



Наш центр мониторинга прошел долгий путь по выбору подходящего SIEM-решения, не уступающего зарубежным лидерам рынка. Огромное количество различных автоматизаций и интеграций с внешними системами, разнородность источников событий и сложность ранее реализованного контента мониторинга, в совокупности с большим потоком событий и ограниченностью вычислительных мощностей, оказали ключевое влияние на выбор подходящего отечественного вендора.



**Андрей Самоляк**

Начальник отдела внедрения  
средств защиты информации,  
ООО «КОМПЛАЙНС СОФТ»



История успеха данного проекта началась со сравнения отечественных решений SIEM в части производительности и гибкости при переходе с зарубежных платформ, по результатам которого было принято решение о тестировании в инфраструктуре «Ростелекома» и проверке функциональности KUMA.

В рамках пилотного проекта удалось протестировать заявленную производительность и перенести корреляционную логику из имеющейся системы — решение от «Лаборатории Касперского» показало достаточный уровень зрелости для столь крупной инфраструктуры.

# Используемое решение

**Kaspersky Unified Monitoring and Analysis Platform** – высокопроизводительное решение класса SIEM, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации.



**Анна Кулашова**

Управляющий директор  
в России и странах СНГ,  
АО «Лаборатория Касперского»



Мы очень рады сотрудничеству с крупнейшим российским провайдером цифровых услуг и решений «Ростелеком» и гордимся тем, что они выбрали KUMA для обеспечения своей безопасности.

Наша команда всегда внимательно относится к задачам заказчиков. В ближайшем релизе, в соответствии с потребностями «Ростелекома», мы улучшили механизм агрегации оповещений. Приятно видеть, что наш продукт эффективно работает в критически важной среде безопасности.



## Kaspersky Unified Monitoring and Analysis Platform

[Подробнее](#)