AIRNITE

ZERO DAY

ВЫПУСК 08/2026 · ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Недели без конвейеров: во что обошлась кибератака на Jaguar Land Rover

В конце августа 2025 года Jaguar Land Rover после кибератаки был вынужден отключить свои IT-системы, производство стояло неделями. Британские эксперты оценивают ущерб для экономики страны в 1,9 миллиарда фунтов. Какие выводы сделать производителям.

Опубликовано: 21 ноября 2026 г. Время чтения: 6 мин Автор: Редакция Airnite

SOFTWARE. SECURITY. CODE.

// СИТУАЦИЯ В ЦИФРАХ

£1,9 млрд
оценка ущерба для Великобритании
диапазон £1,6–2,1 млрд, модель Cyber Monitoring Centre

Категория 3
«системное событие»
по пятиуровневой шкале CMC

2700+
организаций с существенными последствиями
по данным CMC; в другом месте центр называет более 5000 затронутых

08.10.2025
объявлен ограниченный перезапуск
по данным CMC

В конце августа 2025 года Jaguar Land Rover (JLR), крупнейший автопроизводитель Великобритании, после кибератаки отключил свои IT-системы. Последствия вышли далеко за пределы компании: производство стояло неделями, поставщики оказались под давлением, а британское правительство поддержало JLR кредитной гарантией.

// Что произошло?

Согласно оценке независимого британского **Cyber Monitoring Centre (CMC)** от 22 октября 2025 года, инцидент в конце августа привёл к отключению IT и длительной остановке производства. **8 октября 2025 года**, по данным CMC, было объявлено о возвращении к ограниченному производству. По данным CMC, правительство предоставило **кредитную гарантию на 1,5 миллиарда фунтов**, чтобы обеспечить JLR ликвидностью.

CMC относит инцидент к **системным событиям категории 3** по своей пятиуровневой шкале и оценивает ущерб для британской экономики примерно в **1,9 миллиарда фунтов** — в диапазоне от 1,6 до 2,1 миллиарда. CMC допускает, что это самое дорогостоящее для экономики киберсобытие в истории Великобритании. Что касается самой компании, BleepingComputer со ссылкой на данные JLR сообщил о расходах около 196 миллионов фунтов только за квартал с июля по сентябрь — без учёта упущенной выручки.

// Как устроена атака?

Как именно злоумышленники проникли в системы, JLR, насколько нам известно, подробно не раскрывал. CMC говорит об утечке данных, по всей видимости связанной с инцидентом, не приводя подробностей. Достоверно известна цепочка последствий: производитель отключает IT, чтобы остановить распространение атаки, а поскольку современное производство без IT не работает — заказ комплектующих, планирование, управление, логистика, — останавливаются и конвейеры.

Модель CMC прямо учитывает простои у JLR, поставщиков и других компаний в цепочке. Расходы, связанные с утечкой данных или возможным выкупом, в неё не включены. Модель исходит из поэтапного восстановления с 8 октября до начала января 2026 года.

// Кого это касается?

Пострадал не только JLR. По данным CMC, существенные финансовые последствия понесли **более 2700 британских организаций**; в другом месте оценки речь идёт о более чем 5000 затронутых организаций. Поставщики, которые больше не могли отгружать детали, логистические компании и

дилеры ощутили простой напрямую.

Это делает случай актуальным для любого производственного предприятия: чем теснее связаны производство, цепочка поставок и IT, тем масштабнее последствия кибератаки. И даже тот, кто сам хорошо защищён, может неделями остаться без заказов, если атакуют его клиента.

// Что делать сейчас?

Главный вопрос: как долго вы можете производить без IT и как быстро вернётесь к работе? Сюда относятся чёткое разделение офисной и производственной IT, резервные копии, которые переживут атаку, отработанные планы восстановления и коммуникация на случай ЧП с поставщиками и клиентами. Чек-лист ниже сводит все шаги воедино.

// Чем поможет Airnite?

В рамках **консалтинга** Airnite вместе с вами оценивает зависимости между IT и производством и составляет план восстановления. С помощью **тестирования на проникновение** мы проверяем, сможет ли злоумышленник попасть из офисной сети в производство. На **обучении** и учениях ваши команды отрабатывают чрезвычайную ситуацию.

> Примечание: цифры ущерба CMC — модельные расчёты. Данные JLR о собственных расходах взяты из публикаций в прессе; оригинальные сообщения JLR и британского правительства мы напрямую не изучали. Данные актуальны на 21 ноября 2026 г.

Чек-лист: что сделать прямо сейчас

[+] Разделить на сетевом уровне офисную IT и производственные системы (OT) и строго контролировать точки перехода.

[+] Разработать планы восстановления производства и регулярно отрабатывать их — включая порядок, в котором возвращаются системы.

[+] Организовать резервное копирование так, чтобы злоумышленники не смогли зашифровать копии вместе с остальным (офлайн или неизменяемые копии), и проверять восстановление.

[+] Включить поставщиков и заказчиков в планирование на случай ЧП: кого и когда информировать, что происходит с текущими заказами?

[+] Просчитать финансовые последствия многонедельного простоя и проверить страховое покрытие.

[+] Защитить доступы многофакторной аутентификацией, особенно удалённый доступ, процессы службы поддержки и учётные записи администраторов.

Чем поможет Airnite

- Консалтинг – Взгляд со стороны на ваши планы и проекты.
- Пентест и безопасность – Контролируемые атаки с понятным отчётом и планом мер.
- Обучение – Ваша команда осваивает наши инструменты и процессы.

Как долго простаивало бы ваше производство?

Airnite вместе с вами проверяет, насколько тесно связаны офисная IT-инфраструктура и производство, где злоумышленник мог бы перейти из одной зоны в другую и как быстро вы восстановите работу после инцидента. Вы получаете конкретные меры по сегментации, резервному копированию и восстановлению.

Запросить первичную консультацию · Написать на эл. почту · Через WhatsApp

Контакты

Есть вопросы по статье? Напишите нам в WhatsApp: +49 174 6834842

Читать онлайн: https://airnite.de/ru/zhurnal/kiberataka-jaguar-land-rover-ostanovka-proizvodstva/

Источники

Каждый факт в этой статье подтверждён следующими источниками. Первоисточники отмечены.

1. **Cyber Monitoring Centre · Statement on the Jaguar Land Rover Cyber Incident – October 2025** · 22 октября 2025 г. · ПЕРВОИСТОЧНИК
   Независимая оценка: категория 3, ущерб £1,9 млрд (модель), затронутые организации, перезапуск, кредитная гарантия
   https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/

2. **BleepingComputer · Jaguar Land Rover cyberattack cost the company over $220 million** · 2025 г.
   Отраслевая пресса: расходы в квартале июль–сентябрь по данным JLR
   https://www.bleepingcomputer.com/news/security/jaguar-land-rover-cyberattack-cost-the-company-over-220-million/

3. **Insurance Journal · Jaguar Land Rover Bailout Shows Rising Cost of Cybercrime** · 7 октября 2025 г.
   Деловая пресса: государственная поддержка, контекст
   https://www.insurancejournal.com/news/international/2025/10/07/842850.htm

Общая редакционная информация, а не юридическая консультация и не индивидуальная проверка ваших систем. Актуально на дату публикации.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de