Оглавление Обзор зарубежных изданий (сентябрь 2026 г.)

1. 88% американских компаний испытывают трудности в управлении геополитическими рисками 2

2. Восстановление доверия клиентов после кризиса, связанного с безопасностью пищевых продуктов 2

3. Как война в Иране влияет на выполнение обязательств по коммерческим контрактам 4

4. Как организациям справляться с растущими расходами по искам из профессиональной ответственности 6

5. Что специалистам по управлению рисками необходимо знать об Законе ЕС об искусственном интеллекте и развивающемся регулировании ИИ 7

6. Ключевые риски в программах руководства ИИ: на что обратить внимание 9

7. Дипфейки и дезинформация усложняют управление рисками безопасности для компаний 11

8. Компании недооценивают риск кибератак через цепочки поставок... 13

9. Кэптивы могут закрыть пробелы в покрытии, возникающие из-за исключений по рискам ИИ 144

10. **S&P: риски центров обработки данных растут и недооцениваются**

1. 88% американских компаний испытывают трудности в управлении геополитическими рисками

В статье от 17 сентября 2026 года Морган О'Рук анализирует опрос страховой компании Sentry Insurance, показавший, что пессимизм среди руководителей американских компаний растет. Согласно данным, приведенным в статье, 82% опрошенных обеспокоены будущим своего бизнеса сильнее, чем в начале 2026 года.

Основная причина – геополитические риски. 61% лидеров сообщили, что из-за международных конфликтов их компании столкнулись с негативными последствиями: от задержек поставок до роста цен на бензин. Ключевая проблема, по данным опроса, заключается в том, что 88% руководителей испытывают сложности с управлением рисками из-за большого количества событий и быстрой смены геополитической обстановки.

Это вынуждает компании менять подход к работе. 98% руководителей пересматривают долгосрочное планирование и управление рисками: 70% сокращают интервалы планирования, а 61% внедряют больше сценариев на случай непредвиденных обстоятельств.

В заключительной части статьи О'Рук цитирует Джеффа Коула (Jeff Cole), младшего вице-президента Sentry по работе с национальными клиентами, который отмечает, что дело не просто в количестве рисков, а в скорости их трансформации и взаимного влияния. Организации, регулярно занимающиеся оценкой рисков, увеличивают гибкость своих решений, это позволяет им быть более подготовленными к возможным изменениям.

Источник:

https://www.rmmagazine.com/articles/article//2026/09/17/88--of-u.s.-businesses-are-struggling-to-manage-geopolitical-risk

2. Восстановление доверия клиентов после кризиса, связанного с безопасностью пищевых продуктов

Статья Дженнифер Пост, опубликованная в журнале Risk Management Magazine 11 сентября 2026 года, посвящена восстановлению доверия потребителей после кризиса, связанного с безопасностью пищевой продукции. Автор показывает, что последствия подобных инцидентов не ограничиваются отзывом небезопасных товаров: они также наносят ущерб деловой репутации компаний, снижают продажи и могут приводить к значительным финансовым потерям.

В статье отмечается, что опасения по поводу пищевых отравлений и отзывов продукции влияют на поведение покупателей. После подобных случаев потребители могут отказаться не только от конкретного бренда, но и от целой категории товаров. По данным опроса GS1, так поступали 67% взрослых американцев. Автор разбирает вспышку циклоспороза летом 2026 года: заболели более 11 тыс. человек в 20 штатах, источником FDA назвало салат айсберг Taylor Farms de Mexico. В качестве примеров автор приводит ситуации с Taco Bell, Chipotle и McDonald’s. Эти случаи показывают, что даже если компания не несёт прямой ответственности за загрязнение продукции, упоминание её имени в связи с инцидентом способно отрицательно сказаться на посещаемости, стоимости акций и отношении клиентов. Отдельно рассматривается пример Sweetgreen, использовавшей социальные сети и информацию о прослеживаемости цепочки поставок, чтобы разъяснить свою позицию.

Автор выделяет три основных направления антикризисных действий. Во-первых, компании могут предлагать покупателям скидки и другие меры стимулирования, помогающие вернуть их расположение. Во-вторых, необходимо обеспечивать последовательную и своевременную коммуникацию: предоставлять точную информацию и регулярно сообщать об изменениях, не дожидаясь, пока будут установлены все обстоятельства происшествия. В-третьих, компаниям следует сотрудничать с компетентными органами и принимать необходимые меры в отношении небезопасных товаров.

Значительное внимание в статье уделяется страхованию расходов по отзыву продукции. В зависимости от условий полиса оно может покрывать расходы на отзыв, перерывы в деятельности, упущенную прибыль, консультационные услуги и восстановление бренда. При этом автор подчёркивает необходимость заранее изучать страховое покрытие: страхование ответственности за качество продукции как правило, не компенсирует собственные расходы компании на отзыв и восстановление репутации. Кроме того, нужно проверить, покрывает ли полис добровольный отзыв, а не только отзыв по требованию регулятора.

Таким образом, статья рассматривает кризис в сфере пищевой безопасности как одновременно операционный, репутационный и финансовый риск. По мнению автора, восстановление доверия требует согласованных действий: прозрачного информирования потребителей, сотрудничества с регулирующими органами, продуманной работы с клиентами и соответствующей страховой защиты.

Источник:
https://www.rmmagazine.com/articles/article//2026/09/11/ensuring-recovery-from-a-food-safety-crisis

3. Как война в Иране влияет на выполнение обязательств по коммерческим контрактам

В своей статье Саймон Хемс рассматривает влияние конфликта в Иране на международную торговлю и исполнение договорных обязательств. Военные действия и ситуация вокруг Ормузского пролива привели к перебоям в поставках нефти, газа и продовольствия, а также к росту цен. Многие компании стремятся расторгнуть договоры, поскольку не могут выполнять свои обязательства или хотят воспользоваться более выгодными рыночными условиями. Однако автор подчёркивает, что сама по себе война не освобождает стороны от исполнения договоров.

Почему закрытие Ормузского пролива так важно?

Ормузский пролив играет ключевую роль в мировой торговле. Его минирование, санкционные ограничения и рост стоимости страхования судов затрудняют перевозки. Дополнительные проблемы возникают из-за повреждения нефтеперерабатывающих заводов и газовых терминалов.

Некоторые поставщики перенаправляют продукцию новым покупателям, поскольку спотовые цены оказываются выгоднее. В таких случаях продавец может нарушить действующий договор, выплатить компенсацию, но всё равно получить прибыль благодаря более высоким ценам.

Почему военные конфликты не прекращают действие договоров?

В английском праве действует доктрина frustration (прекращение договора вследствие невозможности исполнения). Она применяется, только если исполнение становится буквально невозможным: простого увеличения расходов или усложнения поставок недостаточно. По мнению Хемса, пока рано делать окончательные выводы о применении этого правила к ситуации вокруг Ормузского пролива. Ошибочная ссылка на него может привести к существенному нарушению договора (repudiatory breach) и обязанности возместить убытки. Поэтому в первую очередь необходимо изучить условия соглашения.

Причины и способы правовой защиты

1. Санкции. Санкционные ограничения могут затрагивать участников сделки, платёжную инфраструктуру, товары и их конечное использование. Если сделка нарушает санкции, от её исполнения необходимо отказаться. При

сомнениях следует обратиться за юридической консультацией. При этом рассчитывать на то, что нарушение останется незамеченным, не стоит: суда, грузы и участники сделок контролируются различными организациями, включая страховые компании.

2. Военные риски и безопасность. В договорах фрахтования могут предусматриваться специальные условия, позволяющие отказаться от захода судна в опасную зону, выбрать альтернативный порт или выполнять требования государственных органов. Кроме того, капитан судна, как правило, вправе отказаться от распоряжений, создающих угрозу для судна или экипажа.

3. Форс-мажор и расторжение договора. Условия о форс-мажоре позволяют временно приостановить исполнение обязательств, если возникают обстоятельства, предусмотренные договором, например война, блокада или эмбарго. В английском праве нет общей доктрины форс-мажора, поэтому применение таких условий зависит от формулировок самого договора. Важно учитывать, должно ли событие полностью препятствовать исполнению обязательств и было ли оно непредвиденным.

Расторжение договора является более радикальным решением. Оно может происходить по усмотрению стороны или при наступлении определённых обстоятельств, например, нарушения обязательств или неплатёжеспособности контрагента. Война редко прямо названа в договорах основанием для расторжения, поэтому на практике чаще остаётся расторжение по усмотрению стороны, а оно, как правило, требует выплаты компенсации.

4**. Дополнительные расходы и пересмотр условий**. Договоры могут заранее определять, кто оплачивает пошлины, налоги, портовые сборы, страхование и расходы на безопасность. Сам факт войны обычно не освобождает стороны от платежей. В некоторых случаях сторона, чьи распоряжения привели к возникновению дополнительных рисков, может быть обязана компенсировать соответствующие расходы. В долгосрочных договорах также могут предусматриваться пересмотр цен и повторные переговоры.

В заключение Хемс отмечает, что международная торговля уже выработала механизмы защиты от чрезвычайных обстоятельств. Поэтому компаниям следует прежде всего изучать условия договоров и предусмотренные способы правовой защиты. Работа в регионах военных конфликтов может приносить дополнительную прибыль, но одновременно повышает риск утраты имущества и нарушения санкционных ограничений.

Источник:

https://www.rmmagazine.com/articles/article//2026/07/22/how-the-war-in-iran-impacts-legal-contracts

4. Как организациям справляться с растущими расходами по искам из профессиональной ответственности

В статье Нельсона Кефоувера (Nelson Kefauver), руководителя направления финансовых и профессиональных рисков Северной Америки в Intact Insurance Specialty Solutions, опубликованной в Risk Management Magazine 26 августа 2026 года, рассматривается рост стоимости убытков в сфере управленческой и профессиональной ответственности.

Автор утверждает, что эти риски больше не укладываются в рамки одного департамента или типа инцидента: требования, связанные с кадровыми решениями, действиями руководства и практиками работы с данными, всё чаще пересекаются, быстрее эскалируются, стоят дороже и привлекают общественное внимание на ранних этапах. Автор считает, что при публичном освещении последствия выходят за пределы юридических и HR-подразделений, нарушая операционную деятельность и создавая финансовое давление, однако ранние и дисциплинированные действия позволяют сдержать это влияние.

Автор уточняет, что исторически компании оценивали риски EPL (страхование ответственности за нарушение трудовых прав) и D&O (страхование ответственности директоров и руководителей) по отдельности, но сегодня такое разделение не отражает взаимосвязанный характер среды страховых требований. По его мнению, растёт активность вокруг дискриминации по инвалидности, сокращений персонала и споров о фаворитизме; управленческие решения подвергаются усиленной проверке; риски, связанные с неприкосновенностью частной жизни, выходят за рамки киберинцидентов, а юрисдикция момент предъявления требований усиливают риск: Калифорния и Орегон считаются более благоприятными для истцов, а в периоды слияний, реструктуризаций и смены руководства иски становятся сложнее и дороже. В качестве примеров автор приводит смену руководства в OpenAI, иски акционеров вокруг продажи Activision Blizzard и спор о компенсации Илона Маска в Tesla, показывая, как корпоративные споры создают репутационные риски и осложняют стратегические инициативы.

Автор считает, что страхование остаётся важным инструментом передачи риска, но покрытие само по себе не снижает подверженность ответственности. Он рекомендует пересматривать покрытие с учётом

меняющихся рисков, укреплять документирование и процессы принятия решений, координировать функции риск-менеджмента, юридического отдела и HR, а также признавать финансовое влияние промедления, рассматривая ранние действия как проактивное управление рисками.

В заключение автор утверждает, что роль покупателя страхования расширяется, и риск-менеджеры все чаще прогнозируют, как повседневные решения трансформируются в ответственность. Автор заключает, что устойчивость начинается с признания того, что профессиональная ответственность не статична: лидеры формируют её ежедневно через решения, документацию и надзор.

Источник:

https://www.rmmagazine.com/articles/article/2026/08/26/how-organizations-can-manage-the-rising-cost-of-professional-liability-claims

5. Что специалистам по управлению рисками необходимо знать об Законе ЕС об искусственном интеллекте и развивающемся регулировании ИИ

В статье Лили Ли (Lily Li), основателя Metaverse Law, опубликованной в Risk Management Magazine 19 августа 2026 года, рассматривается, что риск-менеджерам нужно знать о EU AI Act и регулировании ИИ в США. Закон ЕС об искусственном интеллекте (EU AI Act) распространяется не только на европейские компании: под его действие могут подпадать и американские организации, которые разрабатывают, внедряют или продают системы ИИ. Закон вводит модель управления ИИ, основанную на оценке рисков, документировании предполагаемого применения, контроле со стороны человека и мониторинге систем после их выхода на рынок. Для компаний это означает переход от формального соблюдения нормативных требований к управлению рисками на протяжении всего жизненного цикла продукта. Одновременно в США формируется неоднородная система регулирования, состоящая из законов штатов, отраслевых требований и судебных разбирательств.

Некоторые положения EU AI Act уже действуют, включая запреты на отдельные виды применения ИИ и новые требования к прозрачности. Вступление в силу ряда обязательств для систем высокого риска, первоначально запланированное на август 2026 года, перенесено на декабрь 2027 года. Однако компаниям не следует откладывать подготовку: создание полноценных механизмов управления ИИ может занять 12-24 месяца, поскольку требует оценки рисков, согласования документации, обновления

договоров и взаимодействия юридических, технических, продуктовых и других подразделений.

Ключевое значение имеет классификация системы как высокорисковой. К этой категории относятся ИИ-системы, связанные с безопасностью продукции и критической инфраструктуры, а также решения в таких областях, как трудоустройство, образование, здравоохранение, финансовые услуги, биометрическая обработка и некоторые виды анализа поведения и эмоций. Классификация зависит не только от технических характеристик системы, но и от предполагаемого применения. Например, инструмент, изначально разработанный для автоматизации внутренних процессов, может попасть в категорию высокого риска, если маркетинговые материалы, договоры или действия отдела продаж предполагают его использование при отборе сотрудников, оказании медицинских услуг или принятии финансовых решений. Поэтому решения о позиционировании и продаже продукта непосредственно влияют на регуляторные риски.

Управление ИИ при этом всё больше напоминает управление безопасностью продукции. Для высокорисковых систем могут потребоваться процедуры оценки соответствия, внутренние или независимые проверки, системы управления рисками, качественные обучающие и тестовые данные, техническая документация, регистрация действий системы, механизмы прозрачности и человеческого контроля, а также гарантии точности, устойчивости и кибербезопасности. Эти задачи не могут оставаться исключительно в ведении юридических подразделений: ответственность за их выполнение должна распределяться между продуктовыми командами, специалистами по данным и кибербезопасности, закупками и руководством.

В США единого комплексного федерального закона об ИИ пока нет, поэтому компаниям приходится учитывать разрозненные требования. Калифорния приближается к европейской модели: с 1 января 2027 года для определённых случаев использования автоматизированных технологий при принятии значимых решений в отношении потребителей штата должны начать действовать требования по оценке рисков, а в 2028 году - требования к сертификации и непосредственной отчётности перед соответствующим регулятором. Они охватывают, среди прочего, трудоустройство, жильё, здравоохранение, финансовые услуги и образование. Другие штаты сосредоточены на отдельных сферах, включая медицинский ИИ, страхование, чат-ботов-компаньонов и защиту детей. В результате международным компаниям приходится одновременно готовиться к

широким европейским требованиям и учитывать более узкие, но детализированные американские нормы.

Особенно заметно сближение подходов ЕС и США в вопросах прозрачности. EU AI Act требует в определённых случаях информировать пользователей о взаимодействии с ИИ и раскрывать информацию об искусственно созданных текстах, изображениях, аудио и видеоматериалах. Аналогичные требования развиваются в американских юрисдикциях, включая регулирование чат-ботов и биометрических данных. При этом судебные и регуляторные риски в США могут возникнуть ещё до появления специального комплексного законодательства. Компании, использующие чат-боты, медицинские ИИ-системы и автоматизированные службы поддержки, уже сталкиваются с исками, связанными с предполагаемой записью или перехватом разговоров без надлежащего согласия, а также с расследованиями по поводу вводящей в заблуждение рекламы и недобросовестных торговых практик.

Поэтому отсутствие окончательной регуляторной определённости не оправдывает бездействие. Компаниям следует уже сейчас создавать межфункциональные группы по управлению ИИ, внедрять оценку рисков, проверки конфиденциальности и безопасности, стандарты документации, ограничения на использование продуктов, процедуры раскрытия информации, контроль поставщиков, оценку судебных рисков и мониторинг систем после внедрения. Организации, которые начнут эту работу заранее, смогут легче адаптироваться к изменению законодательства. Главный вывод автора состоит в том, что управление рисками ИИ становится текущей операционной необходимостью, а не задачей на будущее: компаниям важно обеспечить соответствие механизмов контроля темпам внедрения ИИ и масштабу его применения.

Источник:

https://www.rmmagazine.com/articles/article//2026/08/19/what-risk-managers-need-to-know-about-the-eu-ai-act-and-evolving-ai-regulation

6. Ключевые риски в программах руководства ИИ: на что обратить внимание

Авторы статьи, юристы по трудовому праву фирмы Reed Smith, рассматривают правовые риски и риски для конфиденциальности, которые возникают при использовании генеративного ИИ в бизнесе. Они отмечают, что многие руководители и сотрудники по-прежнему слабо понимают эти

риски, и предлагают краткую схему их выявления, чтобы предотвращать нарушения заранее.

Авторы формулируют три принципа программ комплаенса в сфере ИИ. По их мнению, человеческая проверка необходима на каждом этапе работы с ИИ. Они утверждают, что предотвращение нарушений требует активных действий работодателя, а не пассивной надежды. Кроме того, как подчёркивают авторы, риски растут, когда создатели получают или стремятся получить прибыль от спорных результатов. Компании, не выстроившие такие программы, рискуют получить санкции регуляторов, судебные иски, репутационный ущерб и потерю интеллектуальной собственности.

В статье рассматриваются четыре группы рисков. Первая касается конфиденциальности и защиты данных. Авторы приводят случаи, когда сотрудники загружали персональные данные в публичные ИИ-платформы или включали в презентации материалы конкурентов, не подозревая, что ИИ мог использовать защищённые источники. Они рекомендуют определить допустимое использование ИИ, закрепить обработку конфиденциальной информации за внутренними системами и заранее проверять безопасность инструментов, сроки хранения данных и соответствие нормам о приватности. Вторая группа связана со смешением личных и корпоративных данных на одной платформе. Здесь авторы предлагают систему распределения задач между внутренними и сторонними сервисами. Они также призывают чётко разграничивать личное и корпоративное использование ИИ и поддерживать диалог юридических, бизнес- и операционных подразделений, чтобы сформировать культуру соблюдения правил, а не формальное следование им. Третья группа охватывает внутреннее правоприменение и ответственность. Авторы считают, что в политике должны быть прописаны последствия нарушений и распределение ответственности при небрежности сотрудников. Пример юристов, подавших в суд, выдуманные ИИ ссылки на несуществующие дела, по их мнению, показывает, что одного уровня проверки недостаточно. Четвёртая группа касается интеллектуальной собственности. Поскольку ИИ не всегда называет источники и может создавать вымышленную информацию, компания рискует потерять права на продукт или столкнуться с претензиями владельца чужого контента. Авторы указывают, что внутреннее и учебное использование менее рискованно, чем коммерческое, и советуют определять меры защиты до включения контента в ценные активы.

Отдельно авторы рассматривают трудовые отношения, где ИИ применяют для подбора и отбора кандидатов, проверки биографии, интервью, оценки работы и даже выбора работников для увольнения. Они отмечают, что законы штатов всё чаще нацелены на отдельные сферы, включая здравоохранение, страхование и трудовые отношения. Как пример рекомендуемой практики приводится рассматриваемый в Коннектикуте законопроект. Он требует заранее уведомлять работников об автоматизации и давать письменное уведомление о принципах работы системы, порядке обжалования и последнем аудите на предвзятость. Окончательное решение должен принимать человек, который реально может его изменить, а простое одобрение рекомендации ИИ недостаточно. Независимые аудиторы обязаны оценивать дискриминационное воздействие до внедрения и ежегодно, а результаты нужно передавать регуляторам и публиковать. Если выявлено дискриминационное воздействие, систему нельзя применять, пока работодатель не докажет законные деловые основания и не примет корректирующие меры.

В заключение авторы указывают, что ждать полной ясности в регулировании нельзя, поскольку ограничения уже действуют. Единой регуляторной структуры нет, федеральный надзор остаётся неопределённым, а сфера регулируется набором норм отдельных штатов и отраслей. Колорадо и Калифорния уже приняли законы об ответственности в сфере ИИ. Практический вывод авторов состоит в том, что компаниям следует соблюдать законы своей юрисдикции, создавать гибкие программы и считать человеческий контроль основой управления ИИ.

Источник:

https://www.rmmagazine.com/articles/article/2026/08/06/key-risks-to-address-in-ai-governance-programs

7. Дипфейки и дезинформация усложняют управление рисками безопасности для компаний

В статье Сары Джолли (Sarah Jolly), опубликованной на портале Commercial Risk 8 июля 2026 года, разбираются результаты промежуточного исследования International SOS «Risk Outlook 2026 Pulse Check». В опросе участвовали 257 организаций более чем из 50 стран. Основная тема – недостоверная информация о рисках безопасности, которая влияет на здоровье и благополучие сотрудников за рубежом. Большая часть такой информации создаётся с помощью ИИ и распространяется массово.

С вводящими в заблуждение или непроверенными сведениями о рисках безопасности столкнулись 42% организаций. 21% опрошенных специалистов по рискам, безопасности и здравоохранению за последний год лично имели дело с инцидентом, связанным с ложной информацией. Респонденты приводят примеры дипфейк-видео с горящими известными зданиями и сообщений о ранении политиков: такие ролики набирали десятки миллионов просмотров, и компаниям приходилось тратить время и ресурсы, чтобы убедить сотрудников в их подложности. Ирен Лай (Irene Lai), глобальный медицинский директор International SOS, называет дипфейки реальных медиков, дающих ложные рекомендации по сдерживанию вспышки заболевания, «новым рубежом биологической войны», для которой биологический агент уже не нужен.

Компании всё чаще проверяют информацию о рисках с помощью ИИ, и почти 60% участников опроса считают его полезным инструментом. Цвете Конеска (Cvete Koneska), глобальный директор по безопасности International SOS, предупреждает об опасности переоценить зрелость нынешних инструментов. Преждевременная опора на ИИ, по её словам, может усилить риск дезинформации и затянуть принятие решений. Она предлагает модель, в которой ИИ встраивается в риск-менеджмент, но ведущая роль остаётся за человеком.

Вторая часть исследования посвящена скорости реагирования. Только 10% организаций заявили, что способны очень быстро реагировать на новые риски, 68% – что реагируют довольно быстро, а 20% признали, что быстро не реагируют вовсе. Шесть из десяти респондентов считают, что глобальные риски возникают быстрее, чем компании успевают с ними справляться. Джеймс Вуд (James Wood), директор по безопасности International SOS в Северной Европе, видит главное препятствие не в недостаточной осведомлённости, а в самом моменте принятия решения: организации выстроены под стабильность, а не под волатильность. К источникам нестабильности отчёт относит экстремальные погодные явления, новые конфликты и развитие существующих, социальные беспорядки и киберугрозы.

Отчёт приходит к выводу, что лучшие позиции в сложной среде рисков у организаций, которые умеют быстро выявлять новые риски и реагировать на них. С этим согласны и сами участники опроса: 80% считают, что более быстрое обнаружение рисков дало бы им конкурентное преимущество.

Источник:

https://www.commercialriskonline.com/deepfakes-and-misinformation-complicate-security-risks-for-corporates/

8. Компании недооценивают риск кибератак через цепочки поставок

В статье Николаса Пратта (Nicholas Pratt), опубликованной на портале Commercial Risk 22 июля 2026 года, рассматривается исследование «2026 Data Health Check» компании Databarracks, поставщика решений в сфере ИТ-безопасности. Опрос охватил 500 руководителей, принимающих решения в области ИТ.

Каждая четвёртая компания (26%) пострадала от кибератаки, которая началась в её цепочке поставок. Почти половина из них (48%) продолжила работать с этими поставщиками, хотя знала о проблемах с их устойчивостью или безопасностью. Отчасти это объясняется отсутствием альтернатив: 26% респондентов называют зависимость от поставщиков препятствием для повышения устойчивости. Организации, которые сознательно сотрудничают с рискованными поставщиками, сталкиваются с кибератаками в четыре раза чаще. Уязвимость цепочки поставок вошла в тройку главных вызовов для компаний на ближайшие три года.

Оценка поставщиков сосредоточена в основном на начальном этапе: 89% компаний проверяют устойчивость контрагента при начале сотрудничества, и лишь 61% делают это регулярно – ежегодно, ежеквартально или непрерывно.

Крис Батлер (Chris Butler), директор по устойчивости Databarracks, критикует формальный подход к проверке. Анкеты на соответствие требованиям с каждым годом становятся длиннее, но, по его словам, создают ложное ощущение защищённости вместо реальной устойчивости. Батлер предлагает рассматривать устойчивость поставщика как часть собственной. Если замены поставщику нет, а у него самого нет компетенций по обеспечению непрерывности бизнеса, компании стоит предложить ему помощь: включать поставщиков в учения по непрерывности бизнеса и отрабатывать реакцию на сбои совместно, а не по отдельности.

Источник:

https://www.commercialriskonline.com/firms-neglect-risk-of-supply-chain-cyberattacks/

9. Кэптивы могут закрыть пробелы в покрытии, возникающие из-за исключений по рискам ИИ

В статье Гэвина Саутера (Gavin Souter), опубликованной на портале Commercial Risk 20 августа 2026 года, излагаются выступления на ежегодной конференции Ассоциации кэптивного страхования штата Вермонт (Vermont Captive Insurance Association). ИИ рассматривается с двух сторон: как инструмент андеррайтинга и внутреннего контроля и как источник рисков, которые коммерческие страховщики всё чаще исключают из покрытия.

Сара Хопкинс (Sarah Hopkins), старший юрист фирмы Fenwick & West, указывает, что ИИ уже используется во многих компаниях даже без официального внедрения – через сотрудников и внешних подрядчиков. Поэтому правила использования ИИ и проверку того, как подрядчики обращаются с данными компании, не стоит откладывать до появления регулирования. Принятую политику, по её словам, всегда можно изменить.

Эми Антчак (Amy Antczak), операционный директор GreenieRE – ассоциативного кэптива из Вермонта, специализирующегося на чистой энергетике, – рассказывает, что ИИ позволяет работать небольшой командой. Андеррайтеры используют его для анализа погодных данных: из-за изменения климата исторические данные об убытках по части рисков теряют ценность, а ИИ помогает учитывать актуальную и прогнозную информацию. Кэптив также тестирует «аудит-бота» для проверки андеррайтинговых материалов, которые предоставляют фронтирующие страховщики и управляющие генеральные агенты (MGA).

По словам Хопкинс, риски ИИ всё чаще исключаются из покрытия, в том числе в киберстраховании. Джеймс Венсил (James Wencil), актуарий-консультант Pinnacle Actuarial Resources, объясняет причину: при тарификации полисов общей гражданской ответственности, киберстрахования, E&O, D&O и EPL такие риски не учитывались, и их покрытие оказалось бы недооценённым. В отличие от истории с «молчаливым» киберриском (silent cyber), страховщики реагируют на риски ИИ быстро. Среди возможных претензий Венсил называет утечку конфиденциальных данных через публичные ИИ-сервисы, нарушение прав интеллектуальной собственности при создании контента и обучении моделей, а также убытки из-за ошибочных результатов работы ИИ. Хопкинс отдельно предупреждает о типовых договорах с подрядчиками, которые всё чаще дают им широкие права на данные клиента, вплоть до обучения собственных моделей.

Кэптивы, по мнению Венсила, подходят для закрытия таких пробелов, поскольку дают контроль и гибкость, пока коммерческий рынок только формируется. Главное препятствие – тарификация: у актуариев пока мало статистики убытков, связанных с ИИ. На первом этапе кэптивам понадобятся консервативные допущения и жёсткие лимиты – на случай и агрегатные. Со временем кэптив может стать испытательной площадкой: удерживать часть риска ИИ и накапливать собственную статистику убытков.

Источник:

https://www.commercialriskonline.com/captives-can-help-fill-coverage-gaps-from-ai-exclusions/

10. S&P: риски центров обработки данных растут и недооцениваются

В статье Николаса Пратта (Nicholas Pratt), опубликованной на портале Commercial Risk 25 сентября 2026 года, излагается отчёт S&P Global Ratings о рисках центров обработки данных (ЦОД). Агентство приходит к выводу, что эти риски растут и при этом недооцениваются – как по набору уязвимостей, так и по кругу затронутых сторон.

Цифровизация, спрос на облачные сервисы и ИИ создали беспрецедентную зависимость от ЦОДов во многих отраслях. Рынок контролирует небольшое число крупных технологических компаний, что усиливает риск концентрации и создаёт единую точку отказа. Интеграция операционных технологий ЦОДов с сетевыми ИТ-системами открыла новые уязвимости. Кибератака на оператора ЦОДа затронет одновременно многих арендаторов в сложной цепочке поставок и вызовет масштабные финансовые и операционные последствия. Защита от таких рисков при этом часто выходит за пределы того, чем занимаются службы кибербезопасности самих арендаторов.

S&P рекомендует многоуровневую защиту как у арендаторов, так и у операторов ЦОДов. Среди технических мер названы сегментация сетей, установка обновлений программного обеспечения сторонних поставщиков услуг, архитектура нулевого доверия (zero trust) и более широкое применение ИИ и машинного обучения.

Отдельный раздел отчёта посвящён страховщикам. Взаимосвязь цифровой и физической инфраструктуры размывает границы между типами страховых событий и создаёт пробелы в покрытии. Агентство призывает

страховщиков к осторожности в андеррайтинге. Страховщики могут ограничивать покрытие триггером физического ущерба, сублимитами, оговорками о поименованных поставщиках или кибериключениями, а киберполисы – исключать убытки, связанные с критической инфраструктурой или системными событиями. Это снижает экспозицию страховщика, но может перекладывать убытки между полисами или оставлять их без покрытия. S&P ожидает, что по мере роста вовлечённости страховщиков в риски ЦОДов они будут больше внимания уделять сценарному анализу и управлению экспозицией. Понимание зависимостей между страхователями, поставщиками инфраструктуры и видами страхования позволит выявлять ситуации, когда одно кибер- или физическое событие приводит к значительной аккумуляции застрахованных убытков.

Источник:

https://www.commercialriskonline.com/data-centre-risk-growing-and-underestimated-sp/