ALLIANZ РИСК БАРОМЕТР

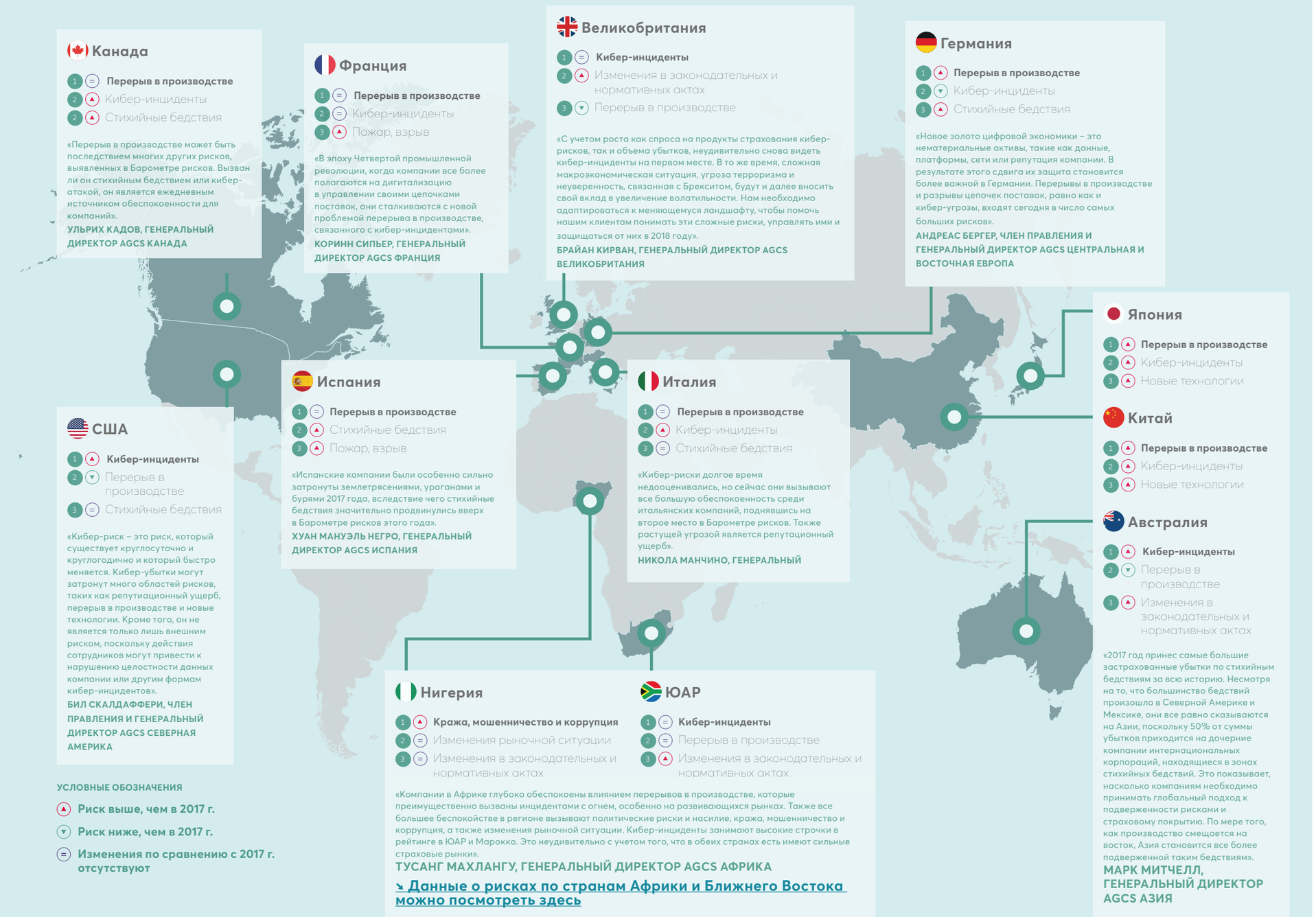
ГЛАВНЫЕ РИСКИ ДЛЯ БИЗНЕСА НА 2018 Г.

Самые важные опасности для корпораций на предстоящий год и далее, какими их видят более 1,9 тыс. экспертов по риск-менеджменту из 80 стран

Allianz

ОДНИМ КАДРОМ: КЛЮЧЕВЫЕ РИСКИ ДЛЯ БИЗНЕСА ПО ВСЕМУ МИРУ НА 2018 Г.

↘ Все данные о рисках по странам, регионам и отраслям можно посмотреть здесь



Канада

1 (=) **Перерыв в производстве**
2 (▲) Кибер-инциденты
2 (▲) Стихийные бедствия

«Перерыв в производстве может быть последствием многих других рисков, выявленных в Барометре рисков. Вызван ли он стихийным бедствием или кибер-атакой, он является ежедневным источником обеспокоенности для компаний».
УЛЬРИХ КАДОВ, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS КАНАДА

США

1 (▲) **Кибер-инциденты**
2 (▼) Перерыв в производстве
3 (=) Стихийные бедствия

«Кибер-риск – это риск, который существует круглосуточно и круглогодично и который быстро меняется. Кибер-убытки могут затронут много областей рисков, таких как репутационный ущерб, перерыв в производстве и новые технологии. Кроме того, он не является только лишь внешним риском, поскольку действия сотрудников могут привести к нарушению целостности данных компании или другим формам кибер-инцидентов».
БИЛ СКАЛДАФФЕРИ, ЧЛЕН ПРАВЛЕНИЯ И ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS СЕВЕРНАЯ АМЕРИКА

Франция

1 (=) **Перерыв в производстве**
2 (=) Кибер-инциденты
3 (▲) Пожар, взрыв

«В эпоху Четвертой промышленной революции, когда компании все более полагаются на дигитализацию в управлении своими цепочками поставок, они сталкиваются с новой проблемой перерыва в производстве, связанного с кибер-инцидентами».
КОРИНН СИПЬЕР, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS ФРАНЦИЯ

Испания

1 (=) **Перерыв в производстве**
2 (▲) Стихийные бедствия
3 (▲) Пожар, взрыв

«Испанские компании были особенно сильно затронуты землетрясениями, ураганами и бурями 2017 года, вследствие чего стихийные бедствия значительно продвинулись вверх в Барометре рисков этого года».
ХУАН МАНУЭЛЬ НЕГРО, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS ИСПАНИЯ

Великобритания

1 (=) **Кибер-инциденты**
2 (▲) Изменения в законодательных и нормативных актах
3 (▼) Перерыв в производстве

«С учетом роста как спроса на продукты страхования кибер-рисков, так и объема убытков, неудивительно снова видеть кибер-инциденты на первом месте. В то же время, сложная макроэкономическая ситуация, угроза терроризма и неуверенность, связанная с Брекситом, будут и далее вносить свой вклад в увеличение волатильности. Нам необходимо адаптироваться к меняющемуся ландшафту, чтобы помочь нашим клиентам понимать эти сложные риски, управлять ими и защищаться от них в 2018 году».
БРАЙАН КИРВАН, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS ВЕЛИКОБРИТАНИЯ

Италия

1 (=) **Перерыв в производстве**
2 (▲) Кибер-инциденты
3 (=) Стихийные бедствия

«Кибер-риски долгое время недооценивались, но сейчас они вызывают все большую обеспокоенность среди итальянских компаний, поднявшись на второе место в Барометре рисков. Также растущей угрозой является репутационный ущерб».
НИКОЛА МАНЧИНО, ГЕНЕРАЛЬНЫЙ

Германия

1 (▲) **Перерыв в производстве**
2 (▼) Кибер-инциденты
3 (▲) Стихийные бедствия

«Новое золото цифровой экономики – это нематериальные активы, такие как данные, платформы, сети или репутация компании. В результате этого сдвига их защита становится более важной в Германии. Перерывы в производстве и разрывы цепочек поставок, равно как и кибер-угрозы, входят сегодня в число самых больших рисков».
АНДРЕАС БЕРГЕР, ЧЛЕН ПРАВЛЕНИЯ И ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS ЦЕНТРАЛЬНАЯ И ВОСТОЧНАЯ ЕВРОПА

Япония

1 (▲) **Перерыв в производстве**
2 (▲) Кибер-инциденты
3 (▲) Новые технологии

Китай

1 (▲) **Перерыв в производстве**
2 (▲) Кибер-инциденты
3 (▲) Новые технологии

Австралия

1 (▲) **Кибер-инциденты**
2 (▼) Перерыв в производстве
3 (▲) Изменения в законодательных и нормативных актах

«2017 год принес самые большие застрахованные убытки по стихийным бедствиям за всю историю. Несмотря на то, что большинство бедствий произошло в Северной Америке и Мексике, они все равно сказываются на Азии, поскольку 50% от суммы убытков приходится на дочерние компании интернациональных корпораций, находящиеся в зонах стихийных бедствий. Это показывает, насколько компаниям необходимо принимать глобальный подход к подверженности рисками и страховому покрытию. По мере того, как производство смещается на восток, Азия становится все более подверженной таким бедствиям».
МАРК МИТЧЕЛЛ, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS АЗИЯ

Нигерия

1 (▲) **Кража, мошенничество и коррупция**
2 (=) Изменения рыночной ситуации
3 (=) Изменения в законодательных и нормативных актах

ЮАР

1 (=) **Кибер-инциденты**
2 (=) Перерыв в производстве
3 (▲) Изменения в законодательных и нормативных актах

«Компании в Африке глубоко обеспокоены влиянием перерывов в производстве, которые преимущественно вызваны инцидентами с огнем, особенно на развивающихся рынках. Также все большее беспокойстве в регионе вызывают политические риски и насилие, кража, мошенничество и коррупция, а также изменения рыночной ситуации. Кибер-инциденты занимают высокие строчки в рейтинге в ЮАР и Марокко. Это неудивительно с учетом того, что в обеих странах есть имеют сильные страховые рынки».
ТУСАНГ МАХЛАНГУ, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР AGCS АФРИКА

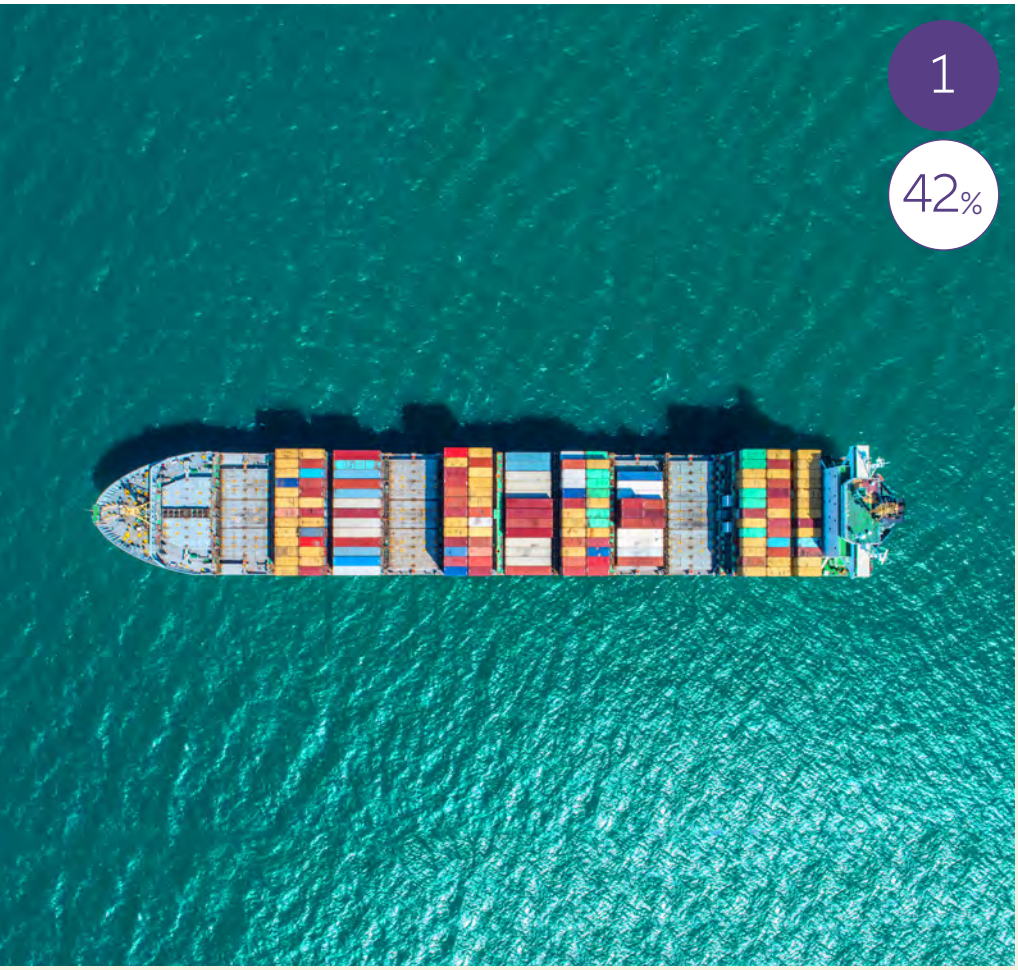
↘ Данные о рисках по странам Африки и Ближнего Востока можно посмотреть здесь

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

- ▲ **Риск выше, чем в 2017 г.**
- ▼ **Риск ниже, чем в 2017 г.**
- = **Изменения по сравнению с 2017 г. отсутствуют**

На данной карте показаны три главных риска для компаний в избранных странах.
Источник: Allianz Global Corporate & Specialty

СОДЕРЖАНИЕ



Источник: Allianz Global Corporate & Specialty. Цифры показывают отношение упоминаний данного риска к общему числу ответов на опрос (2376).
У респондентов, общее число которых составило 1911, была возможность дать ответы не более чем по двум отраслям и назвать для каждой до трех рисков.

↘ **Посмотреть весь рейтинг рисков согласно Барометру рисков на 2018 год можно здесь**

(=) 2017: 37% (1)

Перерыв в производстве
(включая разрыв цепочек поставок)

(▲) 2017: 30% (3)

2. Кибер-инциденты
(например, кибер-преступления, отказы IT, нарушение целостности данных) - 40%

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

- (▲) **Риск выше, чем в 2017 г.**
- (▼) **Риск ниже, чем в 2017 г.**
- (=) **Изменения по сравнению с 2017 г. отсутствуют**
- **(1) Место в рейтинге 2017 г.**

(▲) 2017: 16% (7)

Пожар, взрыв - 20%

(▲) 2017: 12% (10)

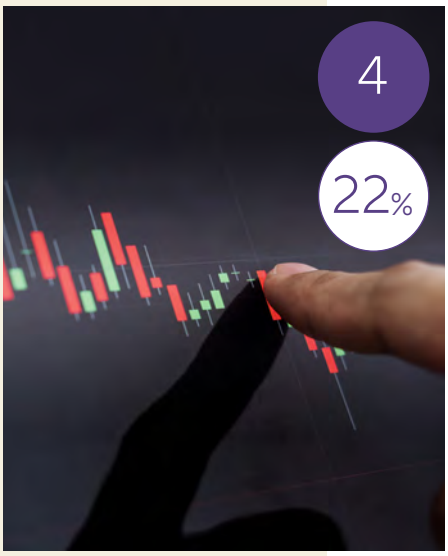
Новые технологии
(например, влияние повышения взаимосвязанности, 3D-печать, беспилотники) - 15%

БАРОМЕТР РИСКОВ ALLIANZ

ДЕСЯТЬ САМЫХ СЕРЬЕЗНЫХ РИСКОВ ДЛЯ КОМПАНИЙ В МИРЕ НА 2018 ГОД

▲ 2017: 24% (4)

Стихийные бедствия
(например, буря, наводнение, землетрясение) - 30%



▼ 2017: 31% (2)

Изменения рыночной ситуации
(например, волатильность, ужесточение конкуренции / новые игроки, слияния и поглощения, стагнация рынка, конъюнктурные колебания) - 22 %

= 2017: 24% (5)

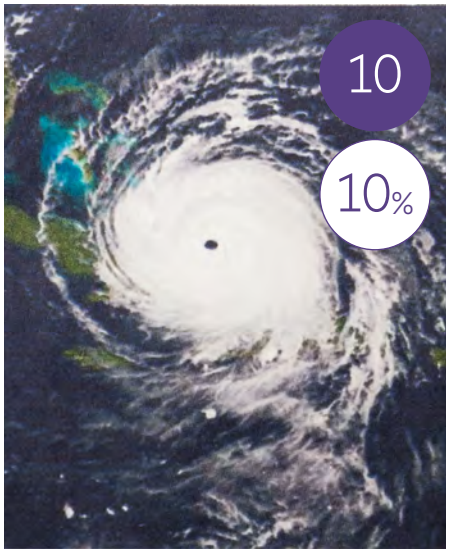
Изменения в законодательных и нормативных актах
(например, смена правительства, экономические санкции, протекционизм, Брексит, распад евро-зоны) - 21 %

▲ 2017: 13% (9)

Репутационный ущерб или снижение ценности бренда - 13%

▼ 2017: 14% (8)

Политические риски и насилие - 11%



▲ **НОВИНКА**

Изменения климата/ повышение изменчивости погоды - 10% (новый)

КРАТКОЕ ИЗЛОЖЕНИЕ

Перерывы в производстве и кибер-инциденты, тесно взаимосвязанные друг с другом, занимают верхние строчки рейтинга самых крупных угроз для компаний на 2018 год и далее. Такая картина складывается на основе опроса 1911 экспертов по рискам из 80 стран, проведенного для Барометра рисков Allianz на 2018 год.

Перерыв в производстве занимает верхнюю строчку среди важнейших рисков в мире вот уже шестой год подряд (42% ответов) в связи с его колоссальным влиянием на поступления. Компании сталкиваются с растущим числом сценариев – от традиционных воздействий, таких как влияние физического ущерба, причиненного объектам и цепочкам поставок стихийными бедствиями и пожарами, до новых порождающих факторов, проистекающих их дигитализации и взаимосвязанности, которые обычно влекут собой не физический ущерб, а большой финансовый убыток. Кибер-инциденты впервые стали самым пугающим порождающим фактором перерывов в производстве. Перерывы в производстве также впервые признаны основной причиной экономического ущерба для компаний после кибер-инцидента. Количество кибер-инцидентов, вызывающих перерыв в производстве, растет. Их причиной могут являться хакерские атаки, такие как инциденты с программами-вымогателями, но чаще они связаны с отказами техники и ошибками персонала. ↘ Стр. 11

Кибер-инциденты продолжают движение вверх в рейтинге и сейчас являются вторым по важности риском для компаний (40%). Пять лет назад они находились на 15-й строчке. Подобно стихийному бедствию, кибер-атака может оказать негативное влияние на сотни компаний, и число таких инцидентов растет. Так называемые «кибер-ураганы», когда хакеры вмешиваются в деятельность большого количества компаний, используя зависимости их общей интернет-инфраструктуры, происходят все чаще. В то же время, в связи с предстоящим вступлением в силу Общего регламента по защите данных (GDPR), который начнет действовать по всей Европе в мае 2018 года, становятся реальными перспективы наложения большего количества и более крупных штрафов на компании, которые его не выполняют. Действия, предпринимаемые компанией в свете нарушения целостности данных, непосредственно влияют на окончательную стоимость такого нарушения. Это станет еще более справедливым после вступления в силу GDPR. Репутационный ущерб неизбежен, если реакция на кибер-инцидент неадекватна. ↘ Стр. 15

Осведомленность о кибер-угрозе среди среднего и малого бизнеса стремительно растет. ↘ Стр. 27

Рекордный размер застрахованных убытков от **стихийных бедствий**, составивший $135 млрд. в 2017 году[1] , обеспечил возврат этого риска в тройку крупнейших на 2018 год (3-е место, 30% ответов). Компании обеспокоены тем, что ситуация прошлого года может предвещать еще больший рост интенсивности и частоты данных убытков, вследствие чего в верхнюю десятку рейтинга впервые попали **климатические изменения** (10-е место, 10% ответов). Потенциальная возможность убытков еще более увеличивается ввиду быстрой урбанизации прибрежных областей. ↘ Стр. 19

Компании стали меньше, чем 12 месяцев назад, беспокоиться по поводу **изменений рыночной ситуации** (4-е место, 22% ответов). Восприятие **изменений в законодательных и нормативных актах** (5-е место, 21% ответов) как потенциального риска остается прежним, несмотря на сокращение числа протекционистских мер. Обеспокоенность по поводу **пожара и взрыва** (6-е место, 20% ответов) растет – анализ убытков показывает, что средняя сумма убытка от перерыва в производстве, вызванного крупным

1 Служба стихийных бедствий Munich Re

пожаром, составляет $2 млн. (€1,7 млн.), в то время как **репутационный ущерб и утрата ценности бренда** (8-е место, 13% ответов) также вызывает все большее беспокойство с учетом того, что в наши дни информация о кризисе может разлететься по всему миру за считанные минуты.

Политические риски и насилие (9-е место, 11% ответов) опустились в рейтинге по сравнению с предыдущим годом, однако компании все более обеспокоены негативным воздействием терроризма. В 2018 году ожидается общая тенденция к росту политической активности населения. ↘ Стр. 24

Новые технологи в качестве фактора риска (7-е место, 15% ответов) сделали один из самых мощных скачков вверх по сравнению с прошлогодним рейтингом. Он также является вторым крупнейшим долгосрочным риском, уступая лишь кибер-инцидентам, с которыми он тесно взаимосвязан. Уязвимость машин к отказу или к действиям кибер-злоумышленников будет в будущем расти, что потенциально может привести к значимым нарушениям критической инфраструктуры. Компаниям также следует готовиться к новым сценариям несения ответственности, поскольку компетентность переходит от человека к машине. ↘ Стр. 30

Новые риски требуют новых инструментов, помогающих отреагировать на их потенциальное воздействие и смягчить его. Роль страхования меняется, и эти изменения заключаются как в предложении новых покрытий, такие как защита от перерывов в производстве, вызванных кибер-инцидентами, и от перерывов в производстве, не связанных с ущербом, которая может компенсировать поступления, утраченные из-за прерывания какого-либо события, так и во все большей степени в возможности доступа к услугам, которые могут помочь смягчить негативные последствия инцидента по мере его развития, таким как привлечение специалистов по кризисному управлению после нарушения целостности данных или другого события, несущего репутационный ущерб. Это отражает тот факт, что сегодняшний мир риск-менеджмента более изменчив, чем когда-либо, и воздействие многих опасностей, занимающих верхние строчки **Барометра рисков Allianz, взаимосвязано**.

МЕТОДОЛОГИЯ СОСТАВЛЕНИЯ БАРОМЕТРА РИСКОВ ALLIANZ

Седьмой **Барометр рисков Allianz** является самым масштабным на сегодняшний день. Он составлен на основе мнений рекордного количества респондентов – 1911 человек из 80 стран. Ежегодный опрос по корпоративным рискам был проведен среди клиентов (глобальных корпораций) Allianz и брокеров. Также были опрошены консультанты по рискам, андеррайтеры, старшие руководители и эксперты по урегулированию убытков в корпоративном сегменте бизнеса как Allianz Global Corporate & Specialty, так и других организационных единиц Allianz.
Респонденты опрашивались в октябре-ноябре 2017 года. Особое внимание уделялось крупным, средним и малым предприятиям.
Респондентов просили выбрать отрасли, в которых они разбираются лучше всего, и назвать не более трех рисков, которые, по их мнению, являются самыми важными. Поскольку можно было отвечать как по одной, так и по двум отраслям, и для каждой называть несколько рисков, было получено 2376 ответов, в которых упоминались 6472 риска.
Большинство ответов (1257, т.е. 53% от общего числа) пришлось на крупные предприятия (с годовыми поступлениями свыше €500 млн). Средние предприятия (с годовыми поступлениями от €250 млн. до €500 млн.) подали 516 ответов (22%), а малые - (с годовыми поступлениями менее €250 млн.) – 603 ответа (25%).
В опросе участвовали эксперты по рискам из 22 отраслей экономики.
Изменения в рейтинге Барометра рисков Allianz определяются тем, какое место занимает тот или иной риск по сравнению с предыдущим годом, а не тем, как изменился процент упомянувших его респондентов.
Все денежные суммы даны в долларах США ($), если не указано иное.

↘ Полные данные по регионам, странам и отраслям можно посмотреть здесь

1,911 респондентов

80 стран

2,376 ответов

22 отрасли

(=) 2018: 42%/2017: 37% (1)

1 ПОДРОБНЕЕ О ВАЖНЕЙШИХ РИСКАХ ПЕРЕРЫВ В ПРОИЗВОДСТВЕ

В связи с возникновением все большего количества порождающих убытки факторов и роста количества кибер-инцидентов, вызывающих перерывы в производстве, перерыв в производстве является самым серьезным риском в «подключенном к сети» обществе.

Динамика рейтинга за последние 5 лет (% ответов и место):
2017: 37% (1)
2016: 38% (1)
2015: 46% (1)
2014: 43% (1)

Главный риск в следующих странах:
Канада
Китай
Франция
Германия
Гонконг
Индонезия
Италия
Япония
Марокко
Новая Зеландия
Южная Корея
Испания
Швейцария

Главный риск в следующих отраслях:
Авиация
Пищевая промышленность
Производство (включая автомобиле-строение)
Электроэнерге-тика и коммуна-льное хозяйство
Розничная и оптовая торговля
Перевозки

Угрозы могут меняться, но результат остается прежним. Перерыв в производстве (включая разрыв цепочки поставок) является самым значимым риском для компаний уже 6 год подряд, согласно данным Барометра рисков Allianz. Этот риск указан в числе трех самых важных рисков, стоящих перед компаниями в 2018 году, в 42% ответов, что больше, чем год назад. Независимо от того, является ли он результатом пожара на фабрике, уничтоженных грузовых контейнеров или, что случается все чаще, кибер-инцидентов, перерыв в производстве может оказать колоссальный эффект на поступления компании. В то же время, данный эффект - один из самых сложных для измерения. Грубое вмешательство в функционирование компании может иметь для нее летальные последствия, особенно если речь идет о небольшой компании. Более того, рост взаимосвязанности влечет за собой увеличение вероятности более крупных убытков. Перерыв в производстве может быть последствием многих других рисков, упомянутых в верхних строчках Барометра рисков Allianz этого года.

РОСТ КОЛИЧЕСТВА СЦЕНАРИЕВ ВМЕШАТЕЛЬСТВА

Перерыв в производстве может быть вызван традиционным имущественным ущербом, который стал результатом стихийного бедствия, или разрывом цепочки поставок в связи с имущественным ущербом на территории поставщика или клиента (так называемый условный перерыв в производстве (CBI)).

Убытки, понесенные компанией от перерыва в производстве, часто оказываются значительно больше, чем стоимость физического ущерба. Средний размер крупного убытка по имущественному страхованию, связанного с перерывом в производстве, сейчас превышает $2 млн [1]. Это больше чем на треть выше, превышает средний прямой имущественный ущерб ($2,4 млн. и $1,75 млн. соответственно).

Однако по мере того, как многие компании переходят от обладания дорогими физическими активами к получению большей ценности из нематериальных активов и услуг, перерыв в производстве все чаще оказывается вызван нетрадиционными опасными воздействиями, которые не причиняют физического ущерба, однако приводят к потере дохода. Это так называемый перерыв в производстве, не связанный с ущербом (NDBI).

«Компании сталкиваются со все большим количеством сценариев вмешательства, что связано с тем, что в нашем «подключенном к сети обществе» природа риска перерыва в производстве меняется, - объясняет **Фолкер Мюнч, руководитель направления глобальной практики имущественного страхования AGCS**. – *Им по-прежнему приходится иметь дело с традиционными опасными воздействиями, такими как влияние стихийных бедствий, резкий рост которых мы увидели в 2017 году. Но им также бросает вызов множество новых порождающих факторов, вытекающих из дигитализации (данные становятся критическим активом), взаимозависимостей поставщиков и инцидентов с качеством продукции, а также косвенного воздействия терроризма и политических событий либо забастовок, что может вызвать утрату дохода от людей, которые избегают подвергшихся воздействию таких событий районов».*

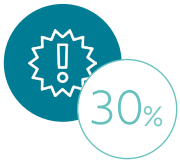
На этом угрозы не заканчиваются. В современном нестабильном политическом и деловом климате, где перспектива резких изменений правил, ставящих под удар бизнес-модели, вызывает все большую обеспокоенность, отзыв разрешения регулятора или лицензии на выпуск продукции является еще одним потенциальным источником риска перерыва в производстве.

ВЛИЯНИЯ КАКИХ ПРИЧИН ПЕРЕРЫВА В ПРОИЗВОДСТВЕ КОМПАНИИ БОЯТСЯ БОЛЬШЕ ВСЕГО?

1. Кибер-инциденты

2. Пожар, взрыв

3. Стихийные бедствия



4. Отказ поставщика, непластичные процессы

5. Поломка машин

Источник: Allianz Global Corporate & Specialty. Цифры показывают процент ответов, в которых назван данный риск, от общего числа ответов опрошенных (845). Цифры не дают в сумме 100%, поскольку возможно было выбрать до трех рисков.

ВО СКОЛЬКО МОЖЕТ ОБОЙТИСЬ ПЕРЕРЫВ В ПРОИЗВОДСТВЕ?

Средняя цена убытка от перерыва в производстве в разбивке по причинам ущерба (избранное). Инциденты на энергодобывающих платформах и забастовки / бунты / акты вандализма являются событиями с низкой частотой и высокой тяжестью ущерба.
Источник: Allianz Global Corporate & Specialty

ВСПЛЕСК ПЕРЕРЫВОВ В ПРОИЗВОДСТВЕ, ВЫЗВАННЫХ КИБЕР-ИНЦИДЕНТАМИ, И РИСКОВ ДЛЯ ЦЕПОЧЕК ПОСТАВОК, ИДУЩИХ ЧЕРЕЗ ИНТЕРНЕТ

Впервые по итогам опросов компаний для Барометра рисков Allianz воздействие кибер-инцидентов признано самым пугающим порождающим фактором перерыва в производстве (42% ответов). Перерыв в производстве также назван главной причиной экономического ущерба (см. стр. 11) после кибер-инцидента (67% ответов). Эти результаты демонстрируют значимый сдвиг в восприятии риска перерыва в производстве респондентами за последние 12 месяцев, что отражает значимый рост масштабов кибер-инцидентов. События 2017 года, такие как атаки программ-вымогателей WannaCry и Petya (см. стр. 10), вызвали нарушение работы значительного числа сервисов и нанесли финансовый ущерб большому числу компаний. Другие события, такие как масштабная атака типа «отказ в обслуживании» на интернет-провайдера Dyn в октябре 2016 года (см. стр. 10), также демонстрируют взаимосвязанность рисков и общую зависимость от совместной интернет-инфраструктуры, поставщиков услуг и технологий. К такому выводу пришли эксперты Cyence Risk Analytics, компании в составе Guidewire, которая является партнером AGCS в оценке кибер-риска.

Хотя перерыв в производстве, связанный с кибер-инцидентами, может быть вызван такими событиями, как атака программ-вымогателей, частота которых за последний год удвоилась, и в ходе которых хакеры шифруют файлы и требуют компенсацию за их разблокирование, еще более частой причиной перерыва в производстве, связанного с кибер-инцидентами, может быть обычный отказ оборудования или ошибка персонала. Например, в феврале 2017 года сервис облачного хранения компании Amazon был недоступен в течение четырех часов, что оказало негативное влияние на ряд интернет-сервисов, сайтов и других компаний. Поступила информация о том, что данное отключение было вызвано человеческой ошибкой[2] . По оценке Cyence Risk Analytics, в результате компании из списка S&P 500, зависимые от сервисов Amazon, потеряли примерно $150 млн[3].

Cyence Risk Analytics отмечает, что перерыв в производстве является одним из сильнейших факторов, причиняющих убытки компаниям после кибер-инцидента. Например, согласно сделанным оценкам, в случае недоступности облачного сервиса у поставщика облачных услуг, длящегося более 12 часов, убытки могут составить $850 млн. в Северной Америке или $700 в Европе, исходя из того, что от недоступности пострадает 50 тыс. компаний трех разных отраслей (финансы, здравоохранение и розничная торговля) в каждом регионе.

СНИЖЕНИЕ РИСКОВ, СЕМАНТИЧЕСКИЙ АНАЛИЗ И ЭВОЛЮЦИЯ СТРАХОВАНИЯ

В Барометре рисков этого года перерыв в производстве также стал вторым в списке самых недооцененных рисков (см. стр. 11).

«Влияние перерыва в производстве легко недооценить, - говорит Томас Варни, региональный менеджер по Северной и Южной Америке компании Allianz Risk Consulting в составе AGCS. – Риски могут быть чрезвычайно сложными. Во многих случаях трудно понять, какова фактическая сумма под риском, как рассчитывать ущерб или даже когда на самом деле произошел обрыв цепочки поставок».

«Компании часто недооценивают сложность «возвращения к нормальному режиму работы», и в их планах реагирования на чрезвычайные ситуации имеются «узкие места», в частности, касающиеся наличия альтернативных поставщиков, - говорит Мюнч. – Еще один пример – кибер-риски. У них может быть план обеспечения непрерывности работы при кибер-атаке, но является ли оценка угрозы перерыва в производстве адекватной? А как насчет влияния кибер-инцидента у одного из их поставщиков, из-за которого они окажутся неспособны поставлять продукцию или оказывать услуги»?

Тем не менее, риски возможно снизить. «Компаниям следует постоянно корректировать свои планы реагирования на чрезвычайные ситуации, чтобы они отражали новую реальность перерывов в производстве, предусматривать широкий круг сценариев и добиваться согласованности между всеми подразделениями, занимающимися прогнозным выявлением рисков», - говорит Мюнч.

Страховщики, такие как AGCS, могут поддержать компании еще больше, предложив им новые страховые решения, в частности, покрытие рисков перерыва в производстве, связанного с кибер-инцидентами, и покрытие NDBI, по которому компания получает возмещение за поступления, утраченные из-за перебоя, вызванного каким-либо событием. AGCS также применяет инструменты семантического анализа, чтобы лучше понимать риск цепочки поставок компании. Это позволяет составить карту отношений с поставщиками до четвертого слоя, что помогает выявить подверженность рискам и их аккумуляцию.

«Важно, чтобы компании понимали, что новые факторы, вызывающие NDBI, меняются, - отмечает Варни. – Сегодняшние угрозы можно понять, но как насчет завтрашних? Необходимо постоянно стремиться к тому, чтобы держать руку на пульсе тех воздействий, которые изменятся по ходу развития самой компании. Компаниям нужно понимать те новые объекты, которые у них есть, те слияния и поглощения, в которых они участвуют, тех поставщиков, которых они используют – все они постоянно меняются по мере того, как компания растет».

1 Allianz Global Corporate & Specialty, Global Claims Review: Business Interruption in Focus
2 The Guardian, Typo blamed for Amazon's internet-crippling outage, March 3, 2017
3 Evolution of Cyber Risks: Quantifying Systemic Exposures, George Ng and Philip Rosace, Cyence Risk Analytics, Guidewire, MMC Cyber Handbook 2018

▲ 2018: 40%/2017: 30% (3)

2 ПОДРОБНЕЕ О ВАЖНЕЙШИХ РИСКАХ
КИБЕР-ИНЦИДЕНТЫ

Динамика рейтинга за последние 5 лет (% ответов и место):
2017 30% (3)
2016 28% (3)
2015 17% (5)
2014 12% (8)

Главный риск в следующих странах:
- Австралия
- Австрия
- Бельгия
- Бразилия
- Индия
- Индонезия
- Голандия
- Сингапур
- ЮАР
- Великобритания
- США

Главный риск в следующих отраслях:
- Развлечения и средства массовой информации
- финансовые услуги
- профессиональные услуги
- технологии
- телекоммуникации

Новые угрозы, такие как «кибер-ураганы», нарастающие репутационные риски и более жесткие правила обращения с данными означают, что компании и эксперты по риск-менеджменту обеспокоены сильнее, чем когда-либо.

Производство жизненно важной вакцины прервано, что вызвало опасения в нехватке лекарств. Один из самых оживленных в мире «умных» портов парализован, и контейнеры брошены на произвол судьбы. Эти и другие события июня 2017 года, вызванные атакой вируса-вымогателя **Petya**, показывают, насколько уязвимы компании перед постоянно эволюционирующей кибер-угрозой и ее влиянием на баланс – согласно оценкам, застрахованные убытки только от инцидента с вакциной составили $275 млн[1] , а компания-перевозчик «налетела» на $300 млн[2]. из-за инцидента с терминалом. Экономический ущерб от атаки вируса **WannaCry** месяцем ранее может, по мнению Cyence Risk Analytics, в конечном итоге достичь $8 млрд. Подобно стихийному бедствию, кибер-атака может потенциально затронуть сотни компаний, приведя к длительному перерыву в производстве, потере клиентов и репутационному ущербу. Неудивительно, что в **Барометре рисков Allianz** кибер-инциденты уже 6 год подряд поднимаются вверх в рейтинге, и в 2018 году они названы главным риском в 11 странах.

НЕДООЦЕНКА РАЗНООБРАЗИЯ УГРОЗ

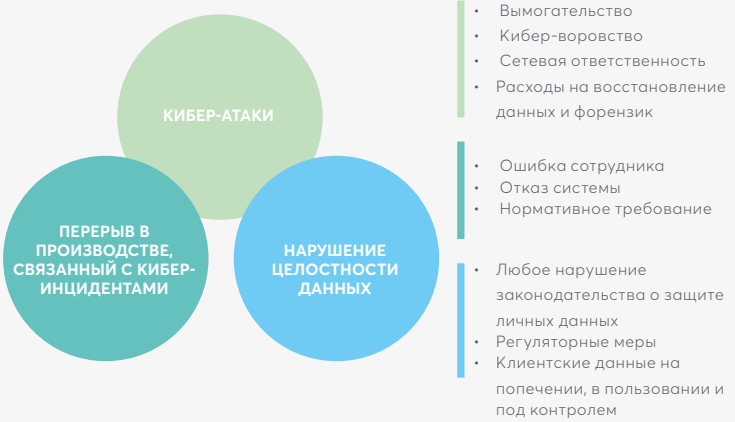
«Кибер-риски затронули или затронут каждую компанию. Их роль отнюдь не преувеличена. Скорее наоборот, она недооценена, потому что угрозы не во всех случаях понимаются правильно», - говорит **Эми Донаван, глава Глобального департамента страхования кибер-рисков AGCS**, отмечая также, что 50% респондентов Барометра рисков называют кибер-риски самыми недооцененными среди компаний. *«Сейчас у цифрового присутствия компании множество угроз».* Под удар могут попасть личные данные или интеллектуальная собственность. Компания может понести сетевую ответственность, если поврежденный файл передан в другую компанию. Респонденты все более обеспокоены новыми опасностями, такими как кибер-вымогательство и особенно перерыв в производстве (см. стр. 9). Тем временем, выявление двух серьезных брешей в защите компьютерных чипов – Meltdown и Spectre – вызвало в январе 2018 года повышенные опасения того, что хакеры могут украсть данные с компьютеров и устройств по всему миру, и в очередной раз показало, как кибер-взаимосвязанность продолжает преподносить неожиданные угрозы.

ОЖИДАЕМЫЙ РОСТ МАСШТАБА ИНФРАСТРУКТУРНЫХ АТАК

Компании обеспокоены тем, что кибер-атаки становятся все более изощренными. В декабре 2017 года появилось первое сообщение об успешном взломе хакерами системы безопасности промышленного предприятия. Ранее аналогичные инциденты происходили на других видах критической инфраструктуры[3] . Тем временем, появление программ-вымогателей WannaCry, Petya и **Mirai** и масштабная распределенная атака типа «отказ в обслуживании» (DDoS) на интернет-провайдера Dyn, которая в октябре 2016 года привела к сбою в работе Twitter, CNN и Netflix в октябре 2016 года, вписываются в набирающую силу тенденцию к расширению аккумуляции инцидентов в области безопасности – появления «кибер-ураганов». Хакеры могут повлиять на функционирование большого количества компаний, выбрав в качестве цели, например, общие элементы интернет-инфраструктуры, от которых они зависят. Эта тенденция, скорее всего, продолжится в 2018 году. *«Компаниям разных размеров, относящихся к разным отраслям, необходимо уделять внимание разным угрозам, чтобы предотвратить реализацию основных кибер-рисков, таких как перерыв в производстве,* - говорит Донаван. – *Атака*

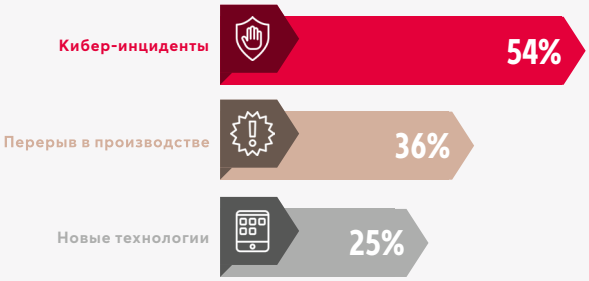
ЦИФРОВАЯ ОПАСНОСТЬ: НЕ ТОЛЬКО КИБЕР-АТАКИ

Существует множество угроз цифровому присутствию компании



Источник: Allianz Global Corporate & Specialty

КАКИЕ РИСКИ ДЛЯ БИЗНЕСА СЕЙЧАС НАИБОЛЕЕ НЕДООЦЕНЕНЫ?



Источник: Allianz Global Corporate & Specialty.
Цифры показывают процент ответов, в которых назван данный риск, от общего числа ответов опрошенных (902). Цифры не дают в сумме 100%, поскольку возможно было выбрать до трех рисков.

КАКОВЫ ОСНОВНЫЕ ПРИЧИНЫ ЭКОНОМИЧЕСКОГО УЩЕРБА ПОСЛЕ КИБЕР-ИНЦИДЕНТА?

Источник: Allianz Global Corporate & Specialty.
Цифры показывают процент ответов, в которых назван данный риск, от общего числа ответов опрошенных (857). Цифры не дают в сумме 100%, поскольку возможно было выбрать до трех рисков.

программы-вымогателя может полностью вывести из строя мелкую компанию, в то время как более крупные компании являются мишенью для более широкого спектра угроз, таких как DDoS-атаки, способные одерживать верх над системами. Полностью предотвратить кибер-инциденты почти невозможно, но существует много подходов, позволяющих сделать те, которые все-таки произойдут, менее вредоносными».

По словам Донаван, одна из наиболее эффективных техник предотвращения – это создание защищенных изолированных резервных копий, которое должно производиться регулярно. Присвоение каждому пользователю индивидуальных прав доступа также может быть эффективным. Если обеспокоенность вызывает возможность DDoS-атаки, жизненно важную роль играют избыточность систем и резервные серверы.

РЕПУТАЦИЯ НА КАРТЕ

Кибер-инциденты вызывают не только хакеры. Часто их виной является отказ оборудования или преднамеренные или случайные действия сотрудников. Какой бы ни была причина, с ней неразрывно связан репутационный ущерб. По данным института репутационного анализа и исследований MediaTenor, 75% компаний, пострадавших от кибер-атаки, также несут репутационный ущерб[4]. Компании, работающие в индустрии развлечений, банковском секторе или розничной торговле, являются особенно уязвимыми из-за того, что они имеют дело с конфиденциальными данными. Более того, компании могут понести репутационный ущерб даже без негативных публикаций в СМИ. Если произошла утечка конфиденциальных данных, доверие заинтересованных сторон может быть подорвано и без участия СМИ.

СТРАХОВАНИЕ КИБЕР-РИСКОВ КАК УСЛУГА

Возросший уровень взаимосвязанности ведет к тому, что сейчас компаниям более, чем когда-либо, важно проводить аудит кибер-безопасности и устойчивости и рассматривать страхование кибер-рисков как элемент риск-менеджмента.

По мере эволюции кибер-угроз меняется и предложение в области страхования кибер-рисков, которое уже не ограничивается лишь покрытием финансового ущерба, например, от перерыва в производстве, и расходов на восстановление производственной деятельности. Например, если организация пострадала от нарушения целостности данных, ей потребуется оперативный доступ к специализированным юристам, специалистам IT-форензик и консультантам по кризисному управлению, чтобы справиться с воздействием инцидента по ходу его развития. Страхование все это обеспечивает.

«Компании не могут прятать голову в песок. Чем скорее они отреагируют, тем лучше будет конечный итог. Компании, которые реагируют на кибер-инцидент плохо, столкнутся с более долгосрочными последствиями для цены своих акций, чем те, которые реагируют правильно», - говорит Донаван.

1 Reuters, Merck cyber-attack may cost insurers $275 million: Verisk's PCS, October 19, 2017
2 Financial Times, Moller-Maersk puts cost of cyber-attack at up to $300m, August 16, 2017
3 Reuters, Hackers halt plant operations in watershed cyber-attack, December 14, 2017
4 MediaTenor, Enhancing risk management by helping companies shield and build their reputations

GDPR – самое значимое событие в области кибер-рисков в 2018 году

Меры по защите данных снова вернулись в центр внимания после масштабнейших нарушений у Equifax и Uber, которые в конце 2017 года потенциально поставили под угрозу личные данные 200 млн. человек. Вступление в силу **Общего регламента по защите данных (GDPR)** по всей Европе в мае 2018 года сделает проверки еще более тщательными. GDPR предусматривает ужесточение процедур, в частности, требование уведомлять регулятора и владельцев данных о нарушении целостности данных, а также значительное увеличение штрафов для компаний, занимающихся бизнесом в ЕС, которые не следуют данным процедурам. Компании могут быть оштрафованы на сумму до 4% от годовых поступлений, так что можно ожидать более частого наложения штрафов и увеличения их сумм. Ожидается, что спрос на страхование кибер-рисков также вырастет, поскольку в ответ компании усиливают защиту.

«Действующие в США законы уже достаточно жесткие, и регулирование в области личных данных постоянно эволюционирует, но теперь и в Европе фирмам приходится готовиться к более жестким требованиям по ответственности и уведомлению, - говорит **Эми Донаван, глава Глобального департамента страхования кибер-рисков AGCS**.
– У многих компаний открываются глаза на наличие у них потенциальных уязвимостей, и осознание того, что проблемы с личными данными вызывают серьезные расходы, придет достаточно быстро после вступления GDPR в силу. Хорошая подготовленность к тому, что может произойти нарушение целостности данных, поможет снизить репутационный ущерб, равно как и сократить перерыв в производстве. Опыт показывает, что реакция компании на нарушение непосредственно влияет на вызванные им расходы. Это станет еще более справедливым, когда начнет действовать GDPR».

▲ 2018: 30%/2017: 24% (4)

3 ПОДРОБНЕЕ О ВАЖНЕЙШИХ РИСКАХ СТИХИЙНЫЕ БЕДСТВИЯ

Глядя на все более часто происходящие события, возникает вопрос: является ли эта экстремальная погода теперь нормой? Респонденты Барометра рисков Allianz обеспокоены тем, что это действительно так, а также вероятностью еще более крупных убытков.

Динамика рейтинга за последние 5 лет (% ответов и место):
2017 24% (4)
2016 24% (4)
2015 30% (2)
2014 33% (2)

Главный риск в следующих отраслях:
- Строительство
- Развлечения и средства массовой информации
- Морские перевозки
- Нефтегазовый комплекс
- Возобновляемые источники энергии

Примерно $330 млрд. общих убытков от стихийных бедствий. Около $135 млрд. застрахованных убытков[1] . Как минимум $90 млрд. из них вызваны тремя ураганами категории 4 и выше – **«Харви», «Ирма» и «Мария» (вместе их называют ХИМ)**, которые бушевали в сентябре, и благодаря которым он стал месяцем наивысшей активности ураганов за всю историю наблюдений[2] , а 2017 год в целом – одним из самых затратных за всю историю наблюдений. Более $2 млрд. застрахованных убытков от землетрясения в Мексике – также в сентябре. Страховые требования на сумму почти $10 млн. по возмещению убытков от лесных пожаров в Калифорнии только за один октябрь[3] . Куда ни посмотри, нетрудно увидеть шокирующую статистику по стихийным бедствиям 2017 года. И эти цифры могут стать еще более страшными. С учетом широты охвата ХИМ – от ущерба от наводнения, которое «Харви» устроил в Хьюстоне, до перерыва в производстве, вызванного рекордными перебоями в электроснабжении в Пуэрто-Рико, где свирепствовала «Мария» - потребуется еще некоторое время для того, чтобы установить окончательную сумму общего ущерба. Стихийные бедствия не ограничивались Северной и Южной Америкой. Сильные наводнения потрясли Бангладеш, Зимбабве, Китай, Перу и Шри-Ланку. Селевые потоки с человеческими жертвами опустошили Колумбию и Сьерра-Леоне. Масштабные лесные пожары бушевали на Иберийском полуострове, и засуха продолжалась на протяжении многих месяцев в Средиземноморском регионе и отдельных частях Африки и Австралии. На последнюю также обрушился циклон «Дебби» в марте. На Филиппинах тропический циклон «Тембин» вызвал наводнения и оползни в день католического Рождества. Если компании расслабились за несколько последних лет, относительно спокойных в плане катастроф (по крайней мере, по стандартам страхования), то 2017 год стал сигналом к пробуждению, подняв риск стихийных бедствий на третью строчку Барометра рисков на 2018 год.

«Недавние события напомнили о том, насколько значительным может быть влияние стихийных бедствий как в социальном, так и в экономическом плане, - говорит **Али Шахкарами, директор Департамента исследований катастрофических рисков AGCS**.

– По мере того, как отрасли становятся более компактными и теснее взаимосвязанными глобально, все больше людей понимает, что стихийные бедствия могут вызвать или усугубить многие другие риски, такие как, например, перерыв в производстве или потеря доли рынка. Это определенно повлияло на то внимание, которое стабильно уделяется стихийным бедствиям в Барометре рисков».

«Влияние стихийных бедствий не ограничивается физическим ущербом сооружениям в тех районах, где они происходят. Они вмешиваются в обычную динамику функционирования общества и промышленности как в непосредственно пострадавших регионах, так и за их пределами, оказывая негативное влияние на широкий круг отраслей, которые могут на первый взгляд показаться незатронутыми».

МЕНЯЮЩИЙСЯ КЛИМАТ И БЫСТРАЯ УРБАНИЗАЦИЯ

Респонденты опасаются, что 2017 год может быть предвестником того, что ждет нас в будущем, и многие считают, что интенсивность стихийных бедствий будет расти под влиянием изменений климата. Исследование показывает, что с 2000 года количество стихийных бедствий погодного характера выросло на 46%, и только в 2016 году было зафиксировано 797 катастрофических событий, принесших $129 млрд. убытков[4]. В верхней десятке 2018 года появился новый риск – «Изменения климата / Повышение изменчивости погоды» (10-е место) (см. стр. 15), и многие ученые согласны с тем, что изменения климата и погодных моделей потенциально могут вызвать экстремальные природные явления по всему миру. Основных направлений такого влияния три – повышение силы ураганных ветров, учащение ливней, вызывающих наводнения, и возникновение большего количества засух. Перестраховочная компания Munich Re считает, что, хотя статистика не предлагает значимых свидетельств этого, изменения климата уже сыграли свою роль в сезоне ураганов 2017 года[5]. Она также предупреждает, что сезон 2017 года может «дать представление о том, что нас ждет в будущем», и что ожидания в отношении увеличения количества экстремально сильных бурь могут реализоваться в виде более частого возникновения исключительных сезонов, таких как сезоны 2004 года, 2005 года и прошлого года.

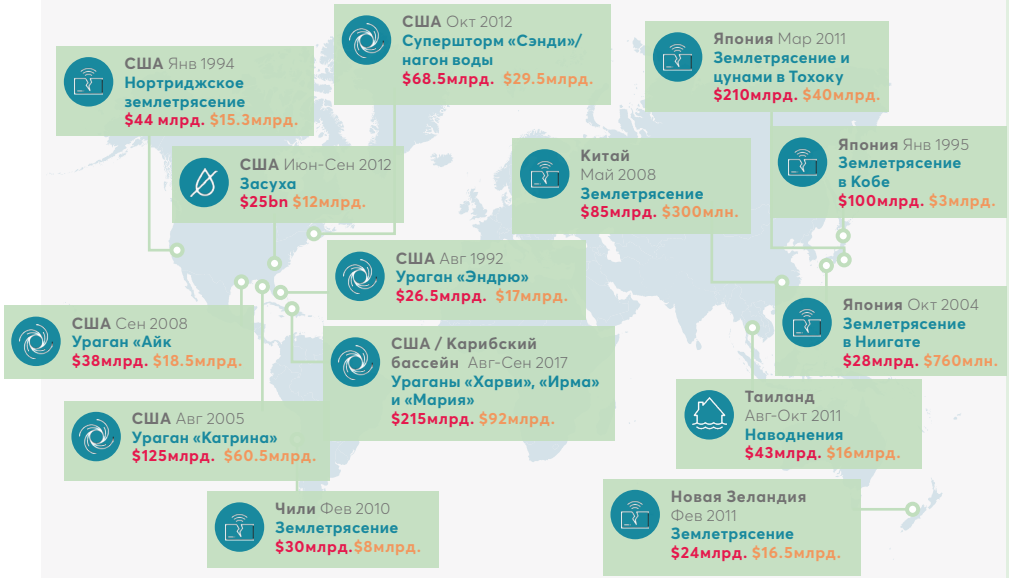
Потенциал будущих убытков, которые компании могут

1 Munich Re NatCatService, Natural Catastrophe Review 2017
2 The Weather Channel, 2017 Atlantic hurricane season recap: 17 moments we'll never forget, November 28, 2017
3 California Department of Insurance, October wildfire claims top $9.4 billion statewide
4 The Lancet Countdown on health and climate change
5 Munich Re, The hurricane season 2017: a cluster of extreme storms

САМЫЕ ДОРОГОСТОЯЩИЕ СТИХИЙНЫЕ БЕДСТВИЯ

1992-2017 (общие убытки и застрахованные убытки)

Общий убыток (в долл. США)
Застрахованный убыток (в долл. США)



Источники: Служба стихийных бедствий Munich Re. Графика: Allianz Global Corporate & Specialty
Данные по состоянию на март 2016 г., за исключением данных об ураганах «Харви», «Ирма» и Мария» - по состоянию на 4 января 2018 г. Места понесения ущерба указаны исключительно в ознакомительных целях.

5 шагов по повышению готовности к стихийным бедствиям

Если процедуры управления риском стихийных бедствий не внедрены или не пересматривались, то размеры таких убытков могут значительно возрасти:

1. Протестируйте и скорректируйте планы подготовки к чрезвычайным ситуациям.
2. Определите к каким событиям готовиться, например, к наводнению, сильному ветру, нагону воды, и суммы под риском.
3. Пересмотрите и обновите планы обеспечения непрерывности бизнес-процессов.
4. Проанализируйте ваш страховой полис – найдите пробелы в покрытии и закройте их.
5. Усовершенствуйте свой объект заранее, чтобы минимизировать удар.

↘ Список контрольных вопросов по ураганному ветру

↘ Список контрольных вопросов по наводнениям

↘ Список контрольных вопросов по землетрясениям

понести от стихийных бедствий, усугубляется дополнительными факторами риска, такие как быстрая урбанизация и недостаточные темпы развития соответствующей инфраструктуры, растущая взаимосвязанность, выливающаяся в увеличение числа условных перерывов в производстве (CBI), и опасности, связанные с цепочками поставок. Например, в последние 10 лет в США фиксируется значительный рост населения и развитие объектов недвижимости коммерческого назначения. По оценке компании AIR Worldwide, занимающейся моделированием, страховая сумма жилых и коммерческих объектов недвижимости в прибрежных округах США в настоящее время превышает $13 трлн[6]. Эта сумма выросла на 13% за три года.

«Все больше людей и все больше объектов девелопмента в опасности, особенно на побережьях США, - говорит **Эндрю Хиггинс, технический менеджер по Северной и Южной Америке компании Allianz Risk Consulting в составе AGCS**. *– Для защиты береговых населенных пунктов необходимы законы о зонировании, достаточные для того, чтобы предотвратить чрезмерное хозяйственное освоение. Кроме того, должно быть меньше бетона и больше зеленых пространств, чтобы тропические дожди в достаточной степени уходили в почву. Например, в некоторых районах Хьюстона количество осадков, принесенных ураганом «Харви», составило лишь около половины от рекорда, который был зафиксирован в городе Недерленд, штат Техас (154 см / 60,6 дюймов[7]), но наводнение в них было значительно хуже. Разница обусловлена чрезмерным хозяйственным освоением».*

НОВЫЕ ИНСТРУМЕНТЫ ДЛЯ БЫСТРО МЕНЯЮЩЕЙСЯ КОНЦЕНТРАЦИИ РИСКОВ

Чтобы не отставать от быстро меняющейся концентрации рисков, такие страховщики, как AGCS, используют широкий спектр новых инструментов управления катастрофическими рисками и страховых решений, чтобы осуществлять мониторинг ураганов и делать оценку ущерба от стихийных бедствий, таких как произошедшие в 2017 году. К этим инструментам относятся беспилотники, которые используются на открытом воздухе, чтобы оценить повреждения крыш, причиненные ветром, и другие недоступные объекты, а также в помещениях, чтобы оценить ущерб от залива на крупных объектах, а также спутниковые технологии и 3D-изображения, чтобы устанавливать местонахождение рисков более оперативно и более точно.

«В настоящее время мы реализуем несколько инициатив, в которых передовые инструменты анализа данных и географические информационные системы (GIS) сочетаются с новейшими технологиями в области спутниковых изображений, больших массивов данных и машинного обучения с целью значительно облегчить принятие критических решений, - объясняет Шахкарами. *– Например, это позволит нам получать аэроснимки пострадавших регионов и потенциально оценивать уровень причиненного объектами ущерба сразу после лесного пожара или оценить размеры наводнения или ущерба крышам зданий после ураганного ветра. С точки зрения технологий, мы живем в интересное время, и мы хотим использовать все доступные инструменты для того, чтобы лучше обслуживать наших клиентов».*

1100+

количество страховых требований, которые были связаны с четырьмя событиями (тремя ураганами и одним лесным пожаром), и которые AGCS обработал за 60 дней

6 AIR Worldwide, The Coastline at Risk: 2016 Update to the Estimated Insured Value of U.S. Coastal Properties
7 Washington Post, 60 inches of rain fell from Hurricane Harvey in Texas, shattering U.S. storm record, September 29, 2017

ВАЖНЕЙШИЕ РИСКИ ДЛЯ КОМПАНИЙ: МЕСТА 4-10

4 ИЗМЕНЕНИЯ РЫНОЧНОЙ СИТУАЦИИ

22% ▼ 2017: 31% (2)

Компании менее обеспокоены этим риском сейчас, чем 12 месяцев назад, потому что 2017 год был «особенным» для транснациональных корпораций, считает Людовик Субран, директор Глобального департамента макроэкономических исследований Allianz. Три экономических супердержавы (США, Европа и Китай) настроились на одну волну, объемы мировой торговли снова стала расти, и рынки предлагали отличные финансовые условия и рекордно низкую волатильность, даже несмотря на нарастание политической и концептуальной неопределенности. Ожидается, что такое согласие продолжится, но с оговорками. С учетом наличия рекордных сумм наличности на балансе, в 2018 году ожидается новая волна слияний и поглощений в свете того, что рост объема выкупа акций ставит под сомнение способность к органическому росту перед лицом цифровой революции. Кроме того, если взаимосвязь между рынками и политикой восстановится, волатильность потенциально может дорасти до уровня середины 90-х. Хотя ситуация с банкротствами в мире в целом стабильна, их число растет в розничной торговле, сфере оказания услуг и строительстве. Те отрасли, которые находятся ближе всего к конечному потребителю, первыми рухнут и уже испытывают на себе ценовой прессинг.

5 ИЗМЕНЕНИЯ В ЗАКОНОДАТЕЛЬНЫХ И НОРМАТИВНЫХ АКТАХ

21% = 2017: 24% (5)

В 2017 году по всему миру было принято лишь 404 новых протекционистских меры, что вдвое меньше, чем в предыдущие годы, говорит **Людовик Субран, директор Глобального департамента макроэкономических исследований Allianz**. В то же время, компании не перестают думать о протекционизме, поскольку новые барьеры на пути торговли пришли преимущественно из США и сказались на Китае, показав, что концентрация таких помех для торговли имеет политический характер. В 2018 году мир останется чрезвычайно фрагментированным. Соглашения о мировой торговле и многосторонние платформы отодвинуты на второй план, в то время как экономическая и финансовая балканизация становится нормой: запущенная США налоговая война, неравные финансовые и нормативные условия в регионах и политизация валют угрожают потокам капитала. Главные политические риски по-прежнему связаны с определяющими факторами развития экономики, а именно, раздробленность региона Персидского залива сохраняется на фоне низких цен на нефть, а риски выхода из состава ЕС подстегиваются экономическими диспропорциями.

7 НОВЫЕ ТЕХНОЛОГИИ

15% ▲ 2017: 12% (10)

Технологический прогресс последнего десятилетия является основным фактором, увеличивающим подверженность компаний кибер-рискам. Ни одна из отраслей не осталась незатронутой проникновением дигитализации и обмена большими объемами информации на всех этапах цепочки создания ценности. Эта взаимосвязанность дает возможность роста, оптимизации затрат и использования более гибких бизнес-моделей, находящихся ближе к конечному потребителю. Частота мелких убытков может быть снижена путем распространения прогнозного технического обслуживания, которое осуществляется по результатам мониторинга в реальном времени и аналитики данных. В то же время, взаимосвязанность часто является источником существенных рисков, связанных с невозможностью поставки продукции или оказания услуг, и может быть чревата крупными убытками от кибер-атак и отказов инфраструктуры. Взаимосвязанные отрасли будут все больше сталкиваться с новыми сценариями ответственности, что обусловливает попадание этого риска на второе место в списке самых серьезных опасностей для компаний на следующие 10 лет (см. стр. 18) по мнению респондентов.

8 РЕПУТАЦИОННЫЙ УЩЕРБ ИЛИ СНИЖЕНИЕ ЦЕННОСТИ БРЕНДА

13% ▲ 2017: 13% (9)

Инциденты, имеющие последствия для здоровья и безопасности, отзывы продукции и нарушения безопасности данных – в эпоху, когда информация о кризисе может распространиться по всему миру за считанные минуты благодаря социальным сетям и взаимосвязанным цепочкам поставок, риск репутационного ущерба, который может быть вызван множеством причин, вырос в геометрической прогрессии. Согласно различным оценкам, почти четверть ценности компании (24%) заключена в его бренде[1]. Исследования также показывают, что за временной промежуток в пять лет публичная компания с вероятностью 80% теряет 20% стоимости акционерного капитала из-за удара по репутации[2] . Пострадать может даже самый малый бизнес. Защита репутации часто бывает недостаточной, но страховка может оказать ощутимую поддержку в противостоянии неощутимому риску, в частности, обеспечить средства на привлечение экспертов по кризисному управлению и контакты с ними. Профессиональная реакция на кризис может существенно помочь делу. Исследования показывают, что цена акций компаний, которые эффективно преодолели кризис, росла более чем на 10% за следующий год. А те, кто не смогли, потеряли в цене от 15% и более[3].

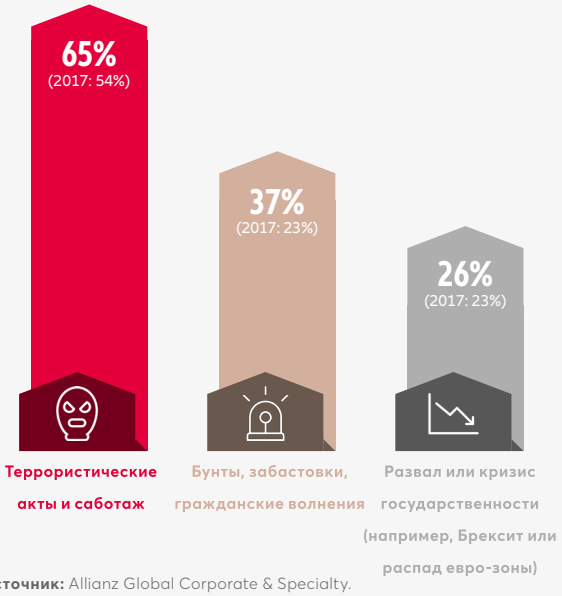
1 Brand Finance Global 500 Report 2012 **2 and 3** Oxford Metrica/Aon Reputation Review 2012

6 ПОЖАР, ВЗРЫВ

20% ▲ 2017: 16% (7)

Анализ более 11 тыс. крупных убытков в области промышленного страхования, проведенный AGCS, показывает, что пожары и взрывы являются второй крупнейшей причиной убытков для компаний в целом. И влияние последующего перерыва в операционной деятельности часто перевешивает влияние причиненного физического ущерба. Пожары и взрывы являются главной причиной страховых требований по перерыву в производстве за пятилетний период, и средние убытки в результате крупного инцидента составляют €1,7 млн. ($2 млн.). Неудивительно, что этот риск год за годом остается близок респондентом – он также является второй из причин перерыва в производстве, которых компании боятся больше всего, уступив лишь кибер-риску. Кроме того, пожар и взрыв остаются главной угрозой для компаний в двух странах – Буркина-Фасо и Того, которые представлены в Барометре рисков впервые.

КАКИЕ ПОЛИТИЧЕСКИЕ РИСКИ И ПРОЯВЛЕНИЯ НАСИЛИЯ ВЫЗЫВАЮТ НАИБОЛЬШЕЕ БЕСПОКОЙСТВО У КОМПАНИЙ?



Источник: Allianz Global Corporate & Specialty.
Цифры показывают процент ответов, в которых назван данный риск, от общего числа ответов опрошенных (246). Цифры не дают в сумме 100%, поскольку возможно было выбрать до трех рисков.

9 ПОЛИТИЧЕСКИЕ РИСКИ И НАСИЛИЕ

11% ▼ 2017: 14% (8)

Восприятие компаниями угрозы, которую несут с собой политические риски и насилие, по сравнению с предыдущими годами меняется несущественно. В то же время, респонденты стали больше обеспокоены терроризмом. Компаниям не требуется побывать в роли непосредственных жертв, чтобы ощутить на себе его влияние. Если террористический акт происходит неподалеку, окрестности могут быть перекрыты, что скажется на деятельности компаний. По мнению Кристофа Бентеле, директора Глобального департамента кризисного управления AGCS, в 2018 году ожидается рост числа террористических актов в Западной Европе и Северной Америке. Преобладать и дальше будут террористические акты с использованием кинетического оружия и акты малой интенсивности, однако могут произойти и новые взрывы бомб, подобно тем, что недавно случились в Манчестере (Великобритания) и Брюсселе (Бельгия), что связано с возвращением бойцов Исламского государства (организация запрещена на территории РФ) с Ближнего Востока. Главными целями с наибольшей вероятностью могут стать транспортная инфраструктура и места скопления людей, включая розничные магазины. Во всем мире ожидается тенденция к повышению политической активности, которая также чревата нарушениями функционирования компаний.

10 ИЗМЕНЕНИЯ КЛИМАТА / ПОВЫШЕНИЕ ИЗМЕНЧИВОСТИ ПОГОДЫ

10% ▲ 2017: 6% (14)

2017 год стал самым разорительным за всю историю наблюдения за стихийными бедствиями, так как одни только застрахованные убытки составили $135 млрд[4]. Он положил конец череде относительно мягких лет убыточности – по страховым стандартам. В целом, многие утверждают, что частота и тяжесть погодных катаклизмов увеличиваются. Согласно данным исследования[5], С 2000 по 2016 годы количество стихийных бедствий погодного характера выросло на 46%, и в 2016 году количество погодных метеорологических явлений, расцениваемых как «экстремальные», составило 797. Найти прямую связь между изменениями климата и увеличением числа погодных катаклизмов не так просто. За рекордными убытками стоят и другие факторы, такие как быстрая урбанизация, однако очевидно, что негативное влияние климатических изменений вызывает все большую обеспокоенность у респондентов Барометра рисков. Оно впервые вошло в десятку самых серьезных рисков в 11 странах. Полностью ликвидировать такой риск невозможно, благодаря хорошей подготовленности и мерам по снижению последствий рисков компания может избежать катастрофического ущерба от погодного катаклизма, ограничившись серьезным ущербом.

4 Munich Re NatCatService, Natural Catastrophe Review 2017
5 The Lancet Countdown on health and climate change

РИСКИ ДЛЯ СРЕДНЕГО И МАЛОГО БИЗНЕСА

Осведомленность о кибер-угрозе среди среднего и малого бизнеса стремительно растет, поскольку возможные последствия нарушений целостности данных и фишинговых атак производят серьезное впечатление. Сопротивление им влечет за собой вызовы совсем другого характера, чем для более крупных компаний.

В общей сложности, бизнес-эксперты малых и средних предприятий составляют почти половину респондентов Барометра рисков (47%). Для компаний среднего размера (*годовые поступления от €250 млн. до €500 млн.*) кибер-инциденты впервые стали риском номер один (*39% ответов*), а для мелких компаний (*годовые поступления менее €250 млн.*) они являются вторым крупнейшим риском (*30% ответов*).

«Скачок, который кибер-инциденты сделали в последний год – с третьего на первое место в рейтинге рисков для среднего бизнеса и с 6-го на 2-е в рейтинге рисков для малого бизнеса – значителен и отражает всплеск внимания к нарушениям целостности данных со стороны как компаний среднего и малого бизнеса, так и их страховых брокеров, - говорит **Винко Марковина, директор Глобального департамента MidCorp AGCS.** – *Осведомленность растет, как показывают результаты Барометра рисков, однако многие средние и малые компании по-прежнему недооценивать свою подверженность рискам и не готовы или не способны отреагировать на инцидент. Эта ошибка может стать фатальной».*

По мере того, как происходит и попадает в печать все большее количество кибер-инцидентов, свидетельства их финансовых последствий становятся все очевиднее для средних и малых предприятий. Эти последствия могут быть катастрофическими. Исследования показывают, что в 2017 году средние затраты средних и малых предприятий Северной Америки, связанные с нарушением целостности данных, составляли $117 тыс.[1] , в то время как другие исследования позволяют сделать вывод о том, что хакеры взломали более 50% мелких компаний, и это число год от года растет[2].

↘ Полный рейтинг рисков в разбивке по крупным, средним и мелким компаниям можно посмотреть здесь

↘ Полный рейтинг рисков в разбивке по 16 отраслям можно посмотреть здесь

Топ-5 рисков для мелких компаний (годовые поступления менее €250 млн.)

Место		%	Место в 2017 году	Тренд
1	**Перерыв в производстве (включая разрыв цепочек поставок)**	**33%**	2 (27%)	▲
2	Кибер-инциденты (например, кибер-преступления, отказы IT, нарушение целостности данных)	**30%**	6 (22%)	▲
3	Стихийные бедствия (например, буря, наводнение, землетрясение)	**28%**	4 (25%)	▲
4	Изменения рыночной ситуации (например, волатильность, ужесточение конкуренции / новые игроки, слияния и поглощения, стагнация рынка, конъюнктурные колебания)	**27%**	1 (32%)	▼
5	Изменения в законодательных и нормативных актах (например, смена правительства, экономические санкции, протекционизм, Брексит, распад евро-зоны)	**22%**	3 (26%)	▼

Источник: Allianz Global Corporate & Specialty. Цифры показывают отношение упоминаний данного риска к общему числу ответов на опрос от компаний данного размера. Кол-во ответов: 603. Цифры не дают в сумме 100%, поскольку возможно было выбрать до трех рисков.

Перерыв в производстве занял первую строчку в рейтинге самых важных рисков для мелких компаний (33% ответов), поднявшись на одну строчку вверх с прошлогоднего второго места (27%), и стал второй самой важной опасностью на 2018 год для компаний среднего размера, пропустив вперед лишь риск кибер-инцидентов.

«Неудивительно, что перерыв в производстве занимает верхние строчки в рейтингах рисков для компаний среднего и малого бизнеса, поскольку угрозы множатся, и их последствия невозможно недооценить, - говорит **Винко Марковина, директор Глобального департамента MidCorp AGCS.** – *Разрыв цепочки поставок – это лишь один из элементов риска перерыва в производстве, которые могут сказаться на средних и малых предприятиях. В качестве ключевых стратегий смягчения последствий перерыва могут выступать поддержание достаточного уровня товарных запасов в наличии, избегание географической концентрации поставщиков, мониторинг слияний и поглощений среди поставщиков и избегание продуктовой специализации, которая приводит к аутсорсингу. Если на перерыв в производстве не отреагировать эффективно, то нежелательные побочные последствия могут быстро нарастать».*

1 Лаборатория Касперского
2 Ponemon Institute, 2017 State of SMB Cybersecurity Report

Средние и мелкие компании могут быть уязвимыми, поскольку у многих их них не хватает средств на то, чтобы содержать собственный IT-департамент или получить доступ к знаниям и ресурсам, необходимым для защиты от постоянно меняющихся угроз. Они могут быть особенно чувствительными к фишинговым атакам по электронной почте или мошенническим действиям, происходящим в их электронных магазинах.

Считается, что для борьбы с кибер-угрозой абсолютно необходимо иметь директора по IT-безопасности (CISO), который сможет внедрить всеобъемлющую систему информационной безопасности, однако это может потребовать значительных финансовых и временных ресурсов, которые могут себе позволить далеко не все средние и малые предприятия. Тем не менее, AGCS заключили соглашение о партнерстве с компанией-разработчиком Zeguro, базирующейся в Силиконовой долине, по которому в рамках страхового покрытия устанавливается платформа "Виртуальный CISO", позволяющая средним и малым предприятиям получить доступ к адаптированным рекомендациям по безопасности и обучающим программам для сотрудников, помогающим снизить риск финансового ущерба после инцидента.

«Раньше страхование кибер-рисков было для средних и малых предприятий непонятным и относительно дорогим покрытием. Однако сейчас, когда покрытие стало более доступным, приемлемым по цене и простым для понимания, мы наблюдаем рост спроса, - говорит Марковина. *– В 2018 году в среде среднего и малого бизнеса активность, связанная с кибер-рисками, будет только нарастать».*

Топ-5 рисков для средних компаний (годовые поступления от €250 млн. до €500 млн.)

Место		%	Место в 2017 году	Тренд
1	**Кибер-инциденты (например, кибер-преступления, отказы IT, нарушение целостности данных)**	**39%**	3 (29%)	▲
2	Перерыв в производстве (включая разрыв цепочек поставок)	**37%**	1 (35%)	▼
3	Стихийные бедствия (например, буря, наводнение, землетрясение)	**32%**	5 (23%)	▲
4	Пожар, взрыв	**23%**	7 (17%)	▲
5	Изменения рыночной ситуации (например, волатильность, ужесточение конкуренции / новые игроки, слияния и поглощения, стагнация рынка, конъюнктурные колебания)	**21%**	2 (33%)	▼

Источник: Allianz Global Corporate & Specialty. Цифры показывают отношение упоминаний данного риска к общему числу ответов на опрос от компаний данного размера. Кол-во ответов: 516. Цифры не дают в сумме 100%, поскольку возможно было выбрать до трех рисков.

Четыре риска, поднимающиеся в рейтингах рисков для среднего и малого бизнеса

Стихийные бедствия
Рекордный в плане убыточности 2017 год стал сигналом к пробуждению для мелких и средних компаний после нескольких относительно спокойных лет

Климатические изменения
Мелкие (7-я строчка) и средние (8-я строчка) компании выражают большую обеспокоенность их влиянием, чем крупные компании (годовые поступления более €500 млн.) для которых они не входят в верхнюю десятку рисков

Политические риски и насилие
Компании среднего размера (10-я строчка) все более обеспокоены косвенным влиянием террористических актов и гражданских волнений, из-за которых клиенты могут лишиться доступа к ним

Пожар, взрыв
Их влияние значительно больше беспокоит средние компании, для которых это риск номер 4. Для них нежелательные побочные последствия могут быть фатальными и привести к уничтожению товарных запасов, перерыву в производстве и приостановке денежных потоков

БУДУЩИЕ РИСКИ

Технологический прогресс безвозвратно меняет ландшафт рисков, являясь как благом, так и вызовом для компаний. С одной стороны, технологические инновации предлагают новые способы снижения рисков. С другой стороны, они создают новые опасности, из-за чего респонденты Барометра рисков Allianz выражают по их поводу все большую обеспокоенность

АВТОНОМНЫЕ МАШИНЫ. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ (AI). УМНЫЕ ФАБРИКИ И ДИГИТАЛИЗОВАННЫЕ ЦЕПОЧКИ ПОСТАВОК.

7

место риска новых технологий в Барометре рисков Allianz; подъем на три позиции по сравнению с рейтингом 2017 года

↘ Просмотр позиции на автономных машинах

Возможности, которые компании получают благодаря внедрению новых технологий, колоссальны и охватывают широкий диапазон. Ожидается, что более тесная взаимосвязь зданий, заводов и устройств и улучшенное применение данных и аналитики обеспечат более высокую производительность и более индивидуализированные клиентские предложения. Безопасность повысится за счет минимизации человеческих ошибок – которые сейчас выступают ведущей причиной убытков во многих отраслях – путем автоматизации задач. Автономные машины могут выполнять задачи во вредной рабочей среде, например, в шахтах, снижая риск травматизма на рабочем месте, или в опасных или недоступных местах, обеспечивая лучшее реагирование и помощь при стихийных бедствиях. При этом постоянный мониторинг состояния и использование аналитики больших массивов данных могут значительно улучшить качество риск-менеджмента, обеспечивая более эффективное уменьшение и предотвращение рисков, более продуманное планирование мер на случай бедствия и даже способность извлекать уроки из ситуаций, едва не приведших к бедствию.

НОВЫЕ УЯЗВИМОСТИ

В то же время, даже если не брать в расчет ряд таких спорных с этической и общественной точек зрения моментов, сопутствующих росту нашей зависимости от новых технологий, как потенциальное исчезновение рабочих мест и их использование в войнах и во влиянии на взгляды общества посредством «фейк-ньюз», компаниям приходится сталкиваться со все большим количеством новых рисков.

В сегодняшнем мире взаимосвязанных отраслей, где работают умные фабрики, и дигитализованы цепочки поставок, где нематериальные активы, такие как данные, сети, отношения с клиентами и интеллектуальная собственность, порой являются главным фактором определения стоимости компании, потери могут быть гораздо выше, если что-то пойдет не так. Непреднамеренные ошибки или неожиданные последствия применения новых технологий могут быстро разрушить доверие потребителей и причинить репутационный ущерб, поскольку риски, связанные с личными данными, становятся все серьезнее, а подверженность риску перерыва в производстве усугубляется.

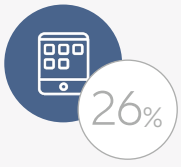
Уязвимость связанных систем к системному сбою или хакерской атаке и другим злонамеренным кибер-инцидентам, таким как вымогательство или шпионаж, в дальнейшем будет еще большей. Согласно недавнему отчету Lloyd's и Cyence Risk Analytics[1], злонамеренный взлом, который парализует работу облачного сервиса, может принести ущерб в размере свыше $50 млрд.

Частота убытков может быть снижена за счет того, что автоматизация минимизирует фактор

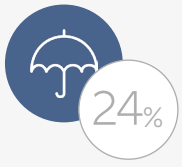
1 Lloyd's and Cyence Risk Analytics, Counting the cost: Cyber exposure decoded

КАКОВЫ ТРИ ГЛАВНЫХ РИСКА ДЛЯ КОМПАНИЙ В ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВЕ? (10 И БОЛЕЕ ЛЕТ)

1. Кибер-инциденты



2. Новые технологии



3. Изменения климата / повышение изменчивости погоды

Источник: Allianz Global Corporate & Specialty. Цифры показывают отношение упоминаний данного риска к общему числу ответов на опрос (1911). Цифры не дают в сумме 100%, поскольку возможно было выбрать до трех рисков.

человеческой ошибки. Однако на ее место может образоваться потенциал для убытков еще большего масштаба. Та же ошибка программирования или хакерская атака могут быть воспроизведены на множестве машин. Или одна машина может повторить ту же ошибочную операцию несколько раз, вызвав непредвиденную аккумуляцию убытков и сложности в точном выявлении того, что именно пошло не так.

«Системный сбой автономных машин, контролирующих критическую инфраструктуру (IT-сети, энергоснабжение) может оказать значительное негативное влияние на нашу взаимосвязанную глобальную экономику и общество, - говорит Михаэль Брух, Глава Управления возникающих тенденций AGCS. – И действительно ли человеческих ошибок станет меньше, или изменится лишь тип человеческих ошибок – быть может, вместо оператора / машиниста их будет совершать программист, составляющий алгоритмы, или аналитик данных, то есть сам производитель»?

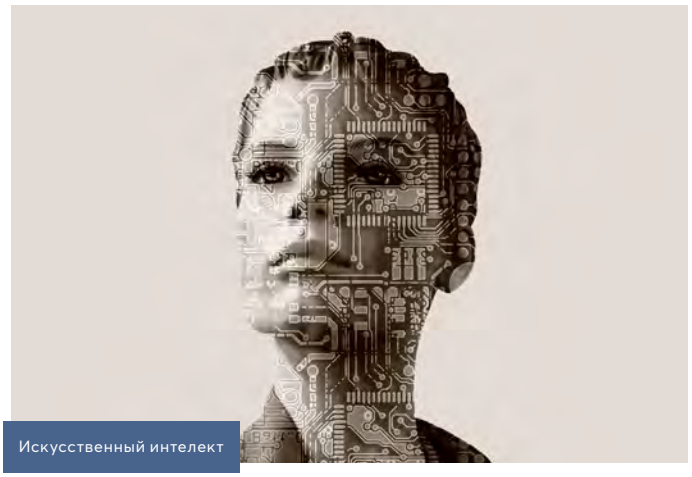
НОВЫЕ СЦЕНАРИИ НЕСЕНИЯ ОТВЕТСТВЕННОСТИ И РОСТ РИСКА, СВЯЗАННОГО С ПРОДУКТОМ

Компаниям предстоит столкнуться с новыми сценариями несения ответственности, появление которых вызвано описанным выше переходом ответственности от человека к машине и, как следствие этого, к производителю или его поставщикам, и это сделает возложение ответственности и предоставление страхового покрытия для такой ответственности более сложным делом. Цифровая продукция имеет повышенную сложность. Поэтому ответственность может быть вызвана дефектом продукции, например, 3D-печати, или быть отслежена до ошибки пользователя. Она даже может стать результатом ошибок коммуникации между двумя машинами, машинами и датчиками или машинами и инфраструктурой.

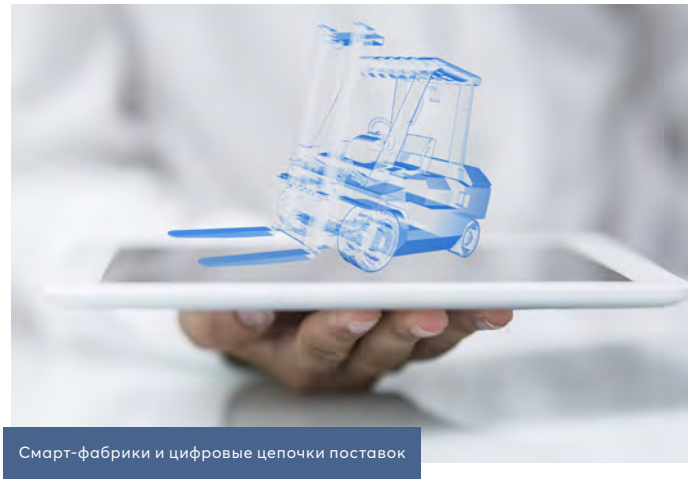
Кроме того, в будущем технологии скорее всего станут более частой причиной отзывов продукции, как в связи с уязвимостями кибер-безопасности, так и в связи с непротестированными перспективными разработками в области AI, нанотехнологий или биотехнологий.

«Сейчас кибер-риск как причина отзыва продукции недооценен, несмотря на то, что уже имели место отзывы автомобилей и фотоаппаратов в связи с уязвимостями кибер-безопасности, - говорит Брух. – В будущем отзывы по причинам, связанным с новыми технологиями, могут обрести еще больший объем и более сложный характер, чем сегодня. Если серия несчастных случаев вызывает обеспокоенность в вопросах безопасности технологии AI, использующейся в беспилотных автомобилях, это может вызвать масштабный отзыв, который затронет разных производителей и разные страны».

В будущем переходные периоды, когда люди и автономные машины будут взаимодействовать и сосуществовать, также могут привести к периоду нарастания риска. Например, когда на дорогах будут и автономные (полностью или частично) транспортные средства с выходом в интернет, и обычные автомобили, ожидается увеличение числа аварий, пока не будет достигнут прорыв в обеспечении безопасности на дорогах.



Искусственный интелект



Смарт-фабрики и цифровые цепочки поставок

Интернет-технологии

Автоматические машины

Photo: Grendelkhan/Wikimedia Commons

Сфера деятельности Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) – это специализированная компания Группы Allianz, занимающаяся страхованием корпоративных и особых рисков. AGCS предлагает услуги страхования и риск-консалтинга по всему спектру особых рисков, альтернативного перевода рисков и корпоративного бизнеса. В частности, линейка его продуктов охватывает следующие виды страхования:

- Альтернативный перевод рисков
- Авиационное страхование (вкл. космическое страхование)
- Страхование энергетических рисков
- Страхование технических рисков
- Страхование развлекательных мероприятий
- Страхование финансовых рисков (вкл. страхование ответственности директоров и высшего руководства (D&O))
- Страхование ответственности
- Морское страхование
- Mid-Corporate
- Страхование имущества

Выходные данные

Над данным документом работали:
Кристина Хубманн, Хайди Полке-Маркманн, Патрик Ванхейден

Специалист по контенту и публикациям:
Джоэл Уайтхед (joel.whitehead@agcs.allianz.com)

Дизайн:
Kapusniak Design

Иллюстрации:
Adobe Stock

Редактор:
Greg Dobie (greg.dobie@allianz.com)

НАШИ КОНТАКТНЫЕ ДАННЫЕ

Чтобы получить более подробную информацию, обращайтесь в службу коммуникаций Allianz Global Corporate & Specialty по месту вашего нахождения.

Лондон
Майкл Бернс
michael.burns@allianz.com
+44 203 451 3549

Нью-Йорк
Сабрина Главан
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

Сингапур
Венди Кох
wendy.koh@allianz.com
+65 6395 3796

Мюнхен
Даниель Ашофф
daniel.aschoff@allianz.com
+49 89 3800 18900

Париж
Флоренс Кларе
florence.claret@allianz.com
+33 158 858863

ЮАР
Лесиба Сетога
lesiba.sethoga@allianz.com
+27 11 214 7948

Весь мир
Хьюго Кидстон
hugo.kidston@allianz.com
+44 203 451 3891

Хайди Полке-Маркманн
heidi.polke@allianz.com
+49 89 3800 14303

Москва
Екатерина Сафронова
Ekaterina.Safronova@allianz.ru
+7 (495) 232-33-33 (доб. 4864)

Чтобы получить более подробную информацию, пишите на **agcs.communication@allianz.com**

Подписывайтесь на Allianz Global Corporate & Specialty в

Facebook Twitter **@AGCS_Insurance #ARB2018** и LinkedIn

www.agcs.allianz.com

Allianz Global Corporate & Specialty SE

Fritz-Schaeffer-Strasse 9, 81737 Munich, Germany

Запись в реестре коммерческих предприятий Мюнхена за номером HRB 208312

Январь 2018 г.