Результаты глобального исследования PwC по кибербезопасности 2022 Global Digital Trust Insights

PwC
ProfIT security day

Докладчик

Олег Прокудин

Менеджер отдела анализа и контроля рисков

Oleg.prokudin@pwc.com

Более чем 10 лет опыта работы по анализу бизнес-процессов, систем и контролей, включая проведение ИТ и ИБ аудитов и разработки ИТ и ИБ стратегий, а также проектов, связанных с обеспечением соответствия требованиям регуляторов.

Области наибольших компетенций:

Приведение процессов и систем компаний в соответствие ИТ и ИБ требованиям
Построения систем управления информационной безопасности на базе семейства стандартов ISO:27000
Разработка ИБ стратегий

Образование и профессиональные квалификации:

BSc in IT, KIMEP university.
Сертифицированный Профессионал в области Информационной Безопасности (CISSP)
Ведущий аудитор и специалист по внедрению (Lead Implementer/Lead auditor) стандарта ISO27001.
Сертифицированный аудитор информационных систем (CISA)

Digital Trust Insights

1. Кратко об исследовании и его методологии

Краткий обзор методологии

3,602 Руководители бизнеса и ИТ-руководители (клиенты и не клиенты)

Онлайн-панельные интервью на местном языке. Клиенты также подписались на участие через сайт онлайн-регистрации.

66 стран мира среди **7** регионов:

- Африке
- Тихоокеанский регион
- Восточная Европа
- Латинская Америка
- Средний Восток
- Северная Америка
- Западная Европа

Опрос проводился с Июля по середину Августа 2021 г.

Фокус исследования

Получение мнения руководителей высшего звена о проблемах и возможностях улучшения кибербезопасности в их организации в ближайшие 12 месяцев.

Ключевые вопросы:

- ✓ Может ли руководство повлиять на кибербезопасность вашей организации?
- ✓ Ваша организация слишком сложна для защиты?
- ✓ Защищаетесь ли вы от наиболее серьезных рисков сегодня и завтра?
- ✓ Насколько хорошо вы знаете риски, связанные с вашими третьими сторонами и цепочкой поставок?

Исследование

Обзор всех ответов по миру

Западная Европа

1203 ответа
33% от всех ответов

Северная Америка

936 ответа
26% от всех ответов

Латинская Америка

378 ответов
10% от всех ответов

Ближний Восток

144 ответа
4% от всех ответов

Восточная Европа

162 ответа
5% от всех ответов

Тихоокеанский регион

633 ответа
18% от всех ответов

Африка

146 ответов
4% от всех ответов

Источник: Опрос PwC Global Digital Trust Insights 2021, сентябрь 2021 г.. Глобальная база: 3602

Исследование

Обзор по направлениям деятельности

Технологии, СМИ и телекоммуникации
24%

Промышленное производство
22%

Финансовые услуги
20%

Потребительские рынки
16%

Энергетика, ком.услуги и ресурсы
8%

Здравоохранение
7%

Правительство / гос. службы
3%

Демография

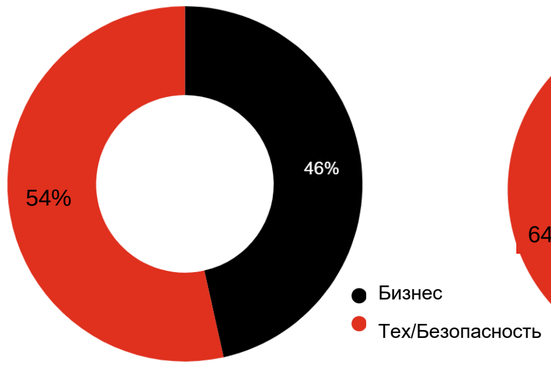
Отчет о глобальном опросе для стран Центральной и Восточной Европы включает ответы руководителей из Польши, Чехии, Венгрии, Румынии, Казахстана, Украины, Хорватии, Болгарии и Латвии.

Среди респондентов из ЦВЕ **62%** из частных организаций, **31%** из публичных списков, а остальные из государственного сектора.

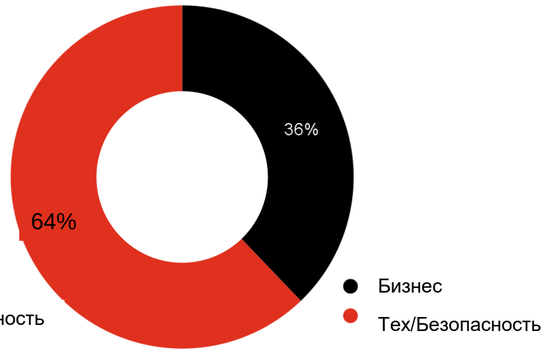
36% респондентов из ЦВЕ являются руководителями крупных компаний (доход от 1 миллиарда долларов и более)

21% женщин-руководителей

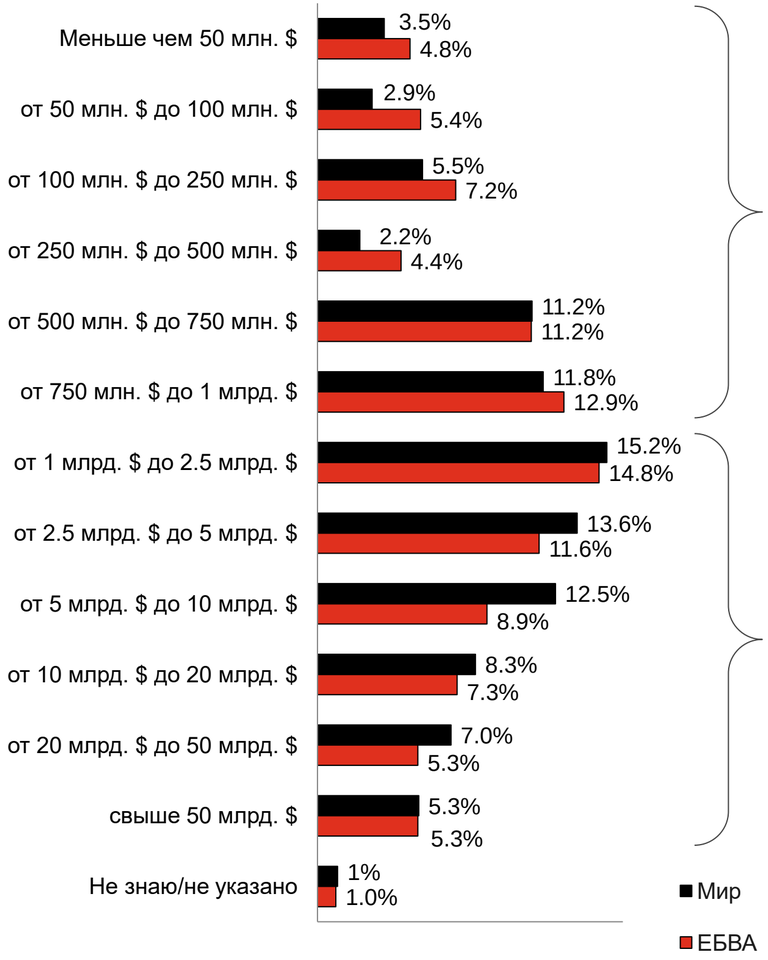
Мир



ЦВЕ



Выручка компаний-участников опроса



Меньше 1 миллиарда $

Мир: 37.1%

ЦВЕ: 45.9%

Больше 1 миллиарда $

Мир: 61.9%

ЦВЕ: 53.1%

Источник: Опрос PwC Global Digital Trust Insights 2021, сентябрь 2021 г.. Глобальная база: 3602

Digital Trust Insights

3. Ключевые результаты

Осведомленность о киберрисках растет

Организации знают, что рисков становится больше.

Более **50%** руководителей ожидают, что в следующем году количество инцидентов, о которых будет сообщено широкой общественности, превысит уровень 2021 года.

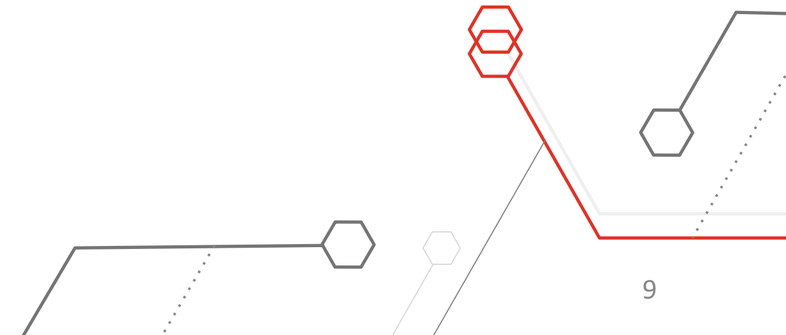
В частности, **72%** респондентов из Центральной и Восточной Европы ожидают увеличения угроз со стороны киберпреступников в 2022 году по сравнению с **60%** респондентов из стран мира и Европы, Ближнего Востока и Африки.

72%

лидеров ЦВЕ ожидают роста киберпреступности в 2022 году

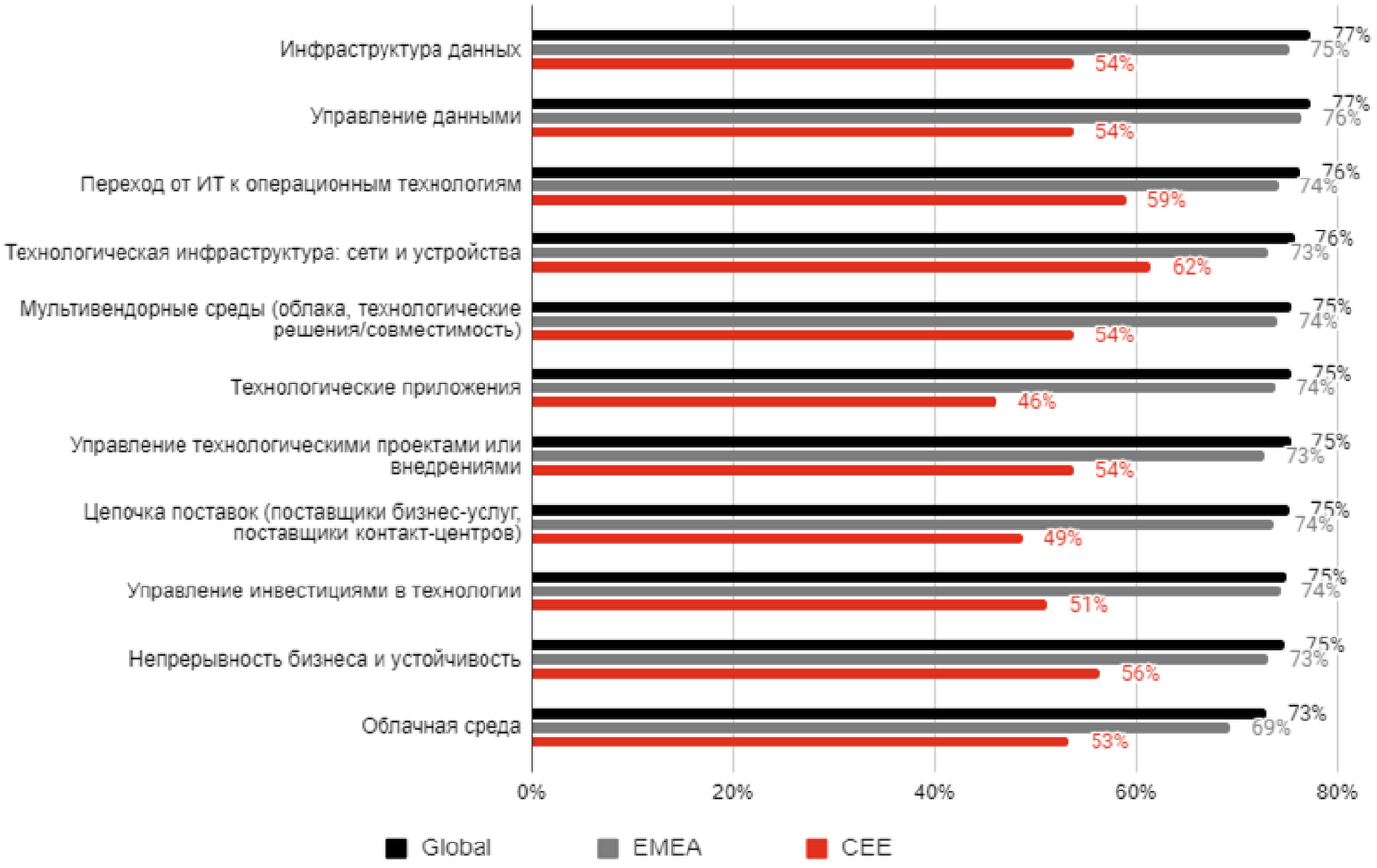
Топ 5 инцидентов, по ожиданиям руководителей ЦВЕ, о которых будет заявлено общественности:

1. Атака на облачные сервисы
2. Компрометация корпоративной почты
3. Атака на цепочку поставок ПО
4. Дезинформация
5. Атаки через обновление ПО



Руководители обеспокоены организационной сложностью в их организациях.

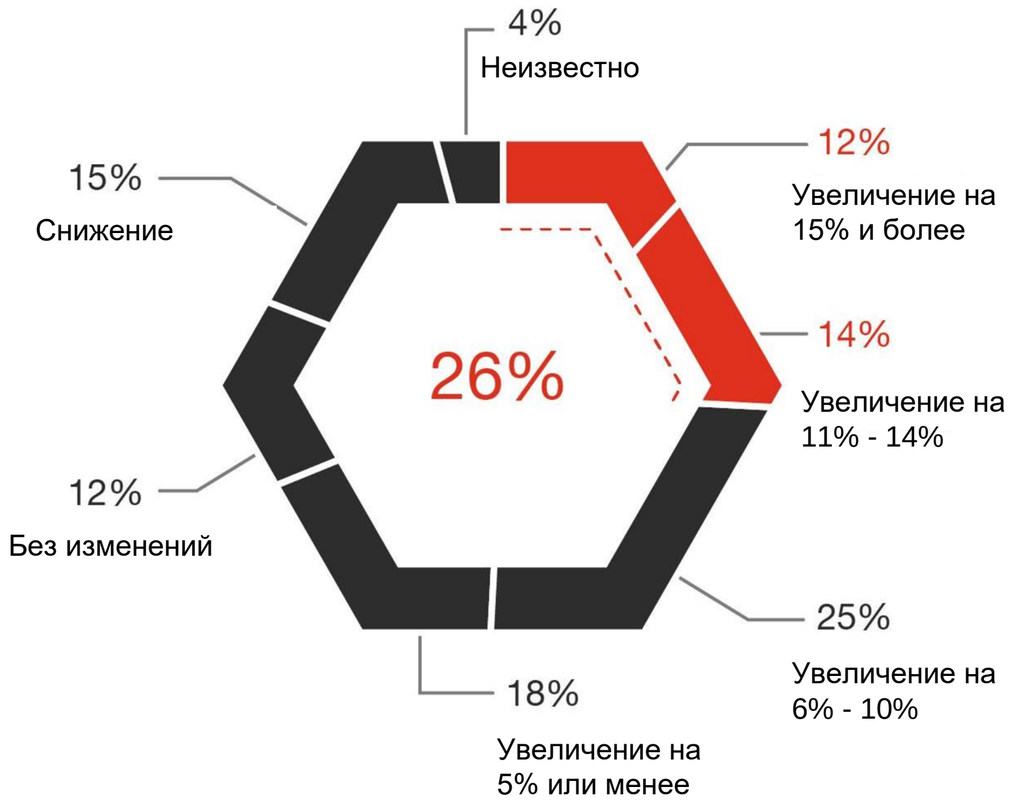
Руководители обеспокоены операционной сложностью в их организациях *



* Глобальная база: 3602 ответа, не все респонденты ответили на данный вопрос

75 % руководителей компаний сообщили, что их организации слишком сложные, что приводит к возникновению «вызывающих беспокойство» рисков, связанных с кибербезопасностью и конфиденциальностью данных. Управление данными и инфраструктура данных поставлены на первое место в перечне областей с «излишним уровнем сложности, которого можно было бы избежать». **Однако показатели ЦВЕ показывают в целом более низкий, но все же значительный уровень беспокойства по поводу риска операционной сложности.**

По мере роста осведомленности о киберрисках инвестиции продолжают расти



Во всем мире 69% организаций прогнозируют рост кибер-расходов в 2022 году по сравнению с 55% в прошлом году.

Более четверти (26%) прогнозируют рост кибер-расходов на 10% и более.

Интересно, что когда руководителей спросили, на чем они сосредоточат свои расходы для упрощения управления кибербезопасностью, цифры в странах Центральной и Восточной Европы, Европы, Ближнего Востока и Африки и по всему миру не показали реального предпочтения, предполагая, что целенаправленная стратегия по упрощению управления кибербезопасностью может отсутствовать.

Несмотря на рост инвестиций, мало кто признал выгоды на сегодня*

* Глобальная база: 3602 ответа, не все респонденты ответили на данный вопрос

Несмотря на рост кибер-инвестиций, лишь немногие получили выгоды от внедрения на сегодняшний день, что ставит вопрос о том, что можно было бы сделать лучше для будущих кибер-инвестиций.

На вопрос о таких инициативах, как облачная безопасность, обучение осведомленности о безопасности, безопасность конечных точек, управляемые службы безопасности, возможности анализа угроз, идентификация предприятия и потребителя и управление доступом, планирование аварийного восстановления и стороннее управление рисками, менее 20% отметили, что получили выгоды от инвестиций.

- Получили выгоды от внедрения
- Внедрено на должном уровне
- Начато внедрение / Планируется сделать в будущем

Последствия киберсложности

Главным последствием сложности в странах Европы, Ближнего Востока, Африки и Центральной и Восточной Европы является **«Отсутствие операционной устойчивости или неспособность восстановиться после кибератаки или технологического сбоя».**

В ЦВЕ за этим следуют Неспособность удержать высшие кадры (7-е место в ЕБВА) и Финансовые потери из-за утечек данных или кибератак (3-е место в ЕБВА и 1-е место в мире).

Во всех отраслях основными последствиями сложности являются: финансовые потери из-за взломов или атак, неспособность внедрять инновации и отсутствие устойчивости.

Вопрос: Каковы наиболее важные последствия сложности для вашего бизнеса?

Оцените от одного до трех, где 1 - самое важное последствие.

	Мир	ЕБВА	ЦВЕ
Финансовые потери из-за успешных утечек данных или кибератак	1	3	3
Неспособность внедрять инновации так быстро, как предлагают рыночные возможности	2	2	4
Отсутствие операционной устойчивости или неспособность оправиться от кибератаки или технологического сбоя.	3	1	1
Неспособность достичь краткосрочных целей роста	4	4	7
Неспособность поддерживать рост в долгосрочной перспективе	5	5	5
Неспособность сохранить специалистов	6	7	2
Неспособность достичь целей лояльности клиентов	7	6	8
Низкие рейтинги ESG по безопасности и конфиденциальности данных	8	8	6

Наиболее совершенные организации с большей вероятностью будут поступать правильно

10% лучших сообщают о значительном прогрессе в достижении важных кибер-целей, таких как: привитие культуры кибербезопасности, управление киберрисками, улучшение взаимодействия между советами директоров и руководством и координация кибер-стратегии со стратегией бизнеса. Более совершенные организации будут поступать правильно с большей вероятностью.

В 5 раз
с большей вероятностью смогут оптимизировать операции в масштабах всего предприятия

В 10 раз
с большей вероятностью будет полностью реализован формальный процесс для практики доверия к данным

В 12 раз
с большей вероятностью скажут, что их руководители оказывают им необходимую поддержку

В 11 раз
с большей вероятностью скажут, что они хорошо понимают кибер-риски и риски для конфиденциальности со стороны третьих лиц

В 18 раз
с большей вероятностью заявят, что все инструменты и подходы являются неотъемлемой частью их операционной модели.

В 34 раза
с большей вероятностью заявят, что они достигли всех целей сотрудничества «очень эффективно».

Ключевые шаги к кибер-упрощению

Ниже описаны четыре шага к реализации кибер потенциала в полном объеме на примере наиболее продвинутых и совершенных организаций. Передовые практики данных организаций с большой вероятностью дали им в два раза больше шансов добиться значительного прогресса в области кибербезопасности за последние два года. Вот эти практики:

1. **Принципы**. Генеральный директор должен сформулировать четкие, недвусмысленные основополагающие принципы, согласно которому безопасность и конфиденциальность являются императивом бизнеса.
2. **Люди.** Нужно нанять правильного лидера, и позволить CISO и команде ИБ наладить связь с бизнес-командами. Ваши люди могут быть авангардом упрощения, даже если вы создаете «хорошую сложность» в своей организации.
3. **Приоритезация**. Риски постоянно меняются по мере роста ваших цифровых амбиций. Нужно собирать информацию и обрабатывать ее для проведения анализа рисков.
4. **Осведомленность.** Невозможно защитить то, что не видно. Нужно выявлять «слепые пятна» в взаимосвязях и цепочках поставок.

Спасибо за внимание!

Хотите получить полные результаты исследования и/или принять в нем участие?

Пожалуйста пройдите опрос по этой ссылке или QR:
https://forms.gle/3UUQ7QtHbccZnoNC8

pwc.com