

Беларусь в международном исследовании EY по информационной безопасности



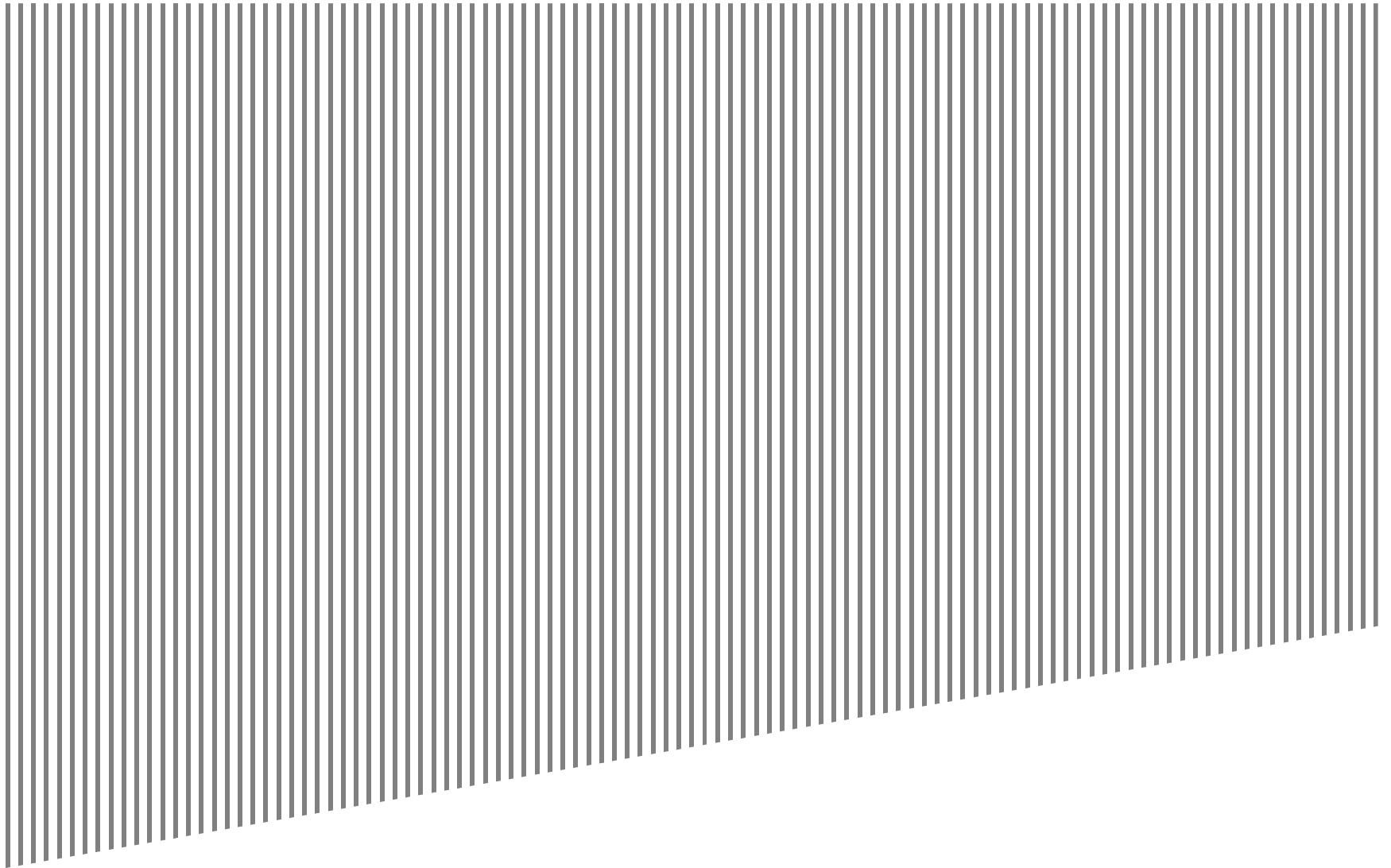
Building a better
working world

Кирилл Домнич, CISA, CISM

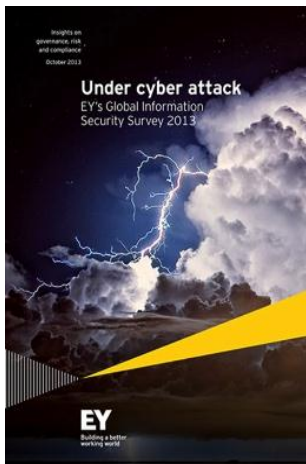
старший консультант, отдел услуг в области
управления информационными технологиями
и ИТ-рисками

Минск, 2 декабря 2013

Международное исследование EY по информационной безопасности за 2013 год

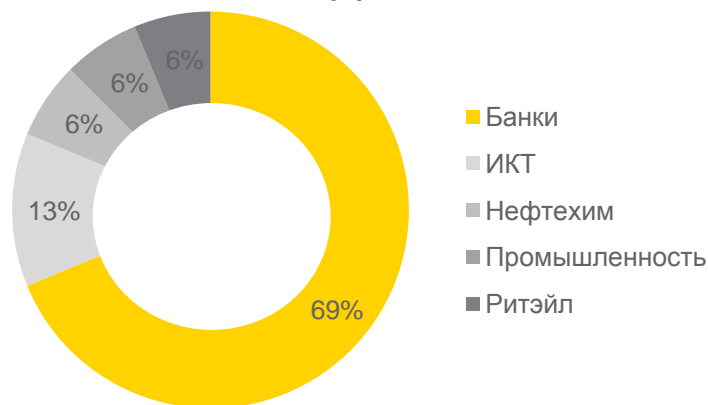


Об исследовании



- ▶ Международное исследование компании EY по информационной безопасности существует 16 лет
- ▶ 4 года проводится в Беларуси
- ▶ В 2013 году в исследовании приняли участие:
 - ▶ 1909 респондентов
 - ▶ из 64 стран
 - ▶ из 25 секторов экономики

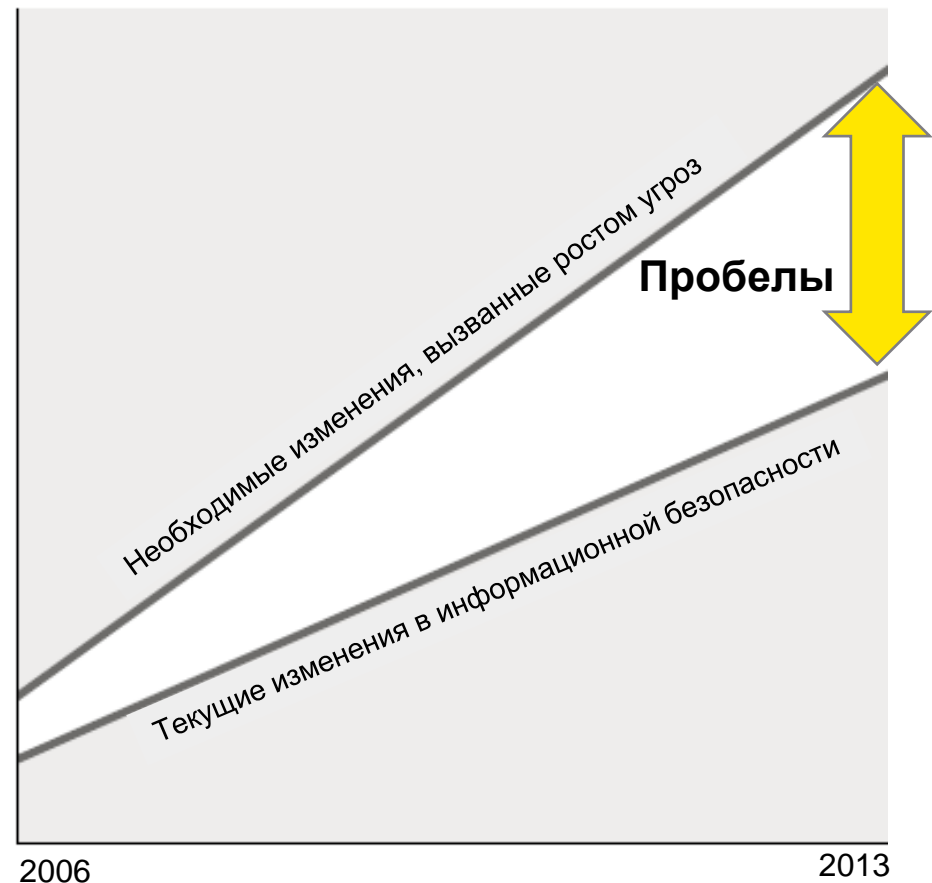
▶ Структура участников исследования в Беларуси



- ▶ Полные результаты исследования и аналитика на www.ey.com/giss

Ликвидация пробелов – обзор исследования

- ▶ Компании приняли значительные меры для устранения угроз в области информационной безопасности, такие как выделение дополнительных ресурсов, обучение и совершенствование управления
- ▶ Вместе с этим, количество и сложность угроз возросла, что ставит перед сотрудниками, ответственными за информационную безопасность, задачу не отставать от времени
- ▶ В результате, разрыв между тем, что делают системы информационной безопасности, и тем, что они должны делать, увеличивается



Угрозы становятся всё более сложными и многочисленными



59%

респондентов отмечают увеличение внешних угроз



31%

респондентов отмечают рост количества инцидентов безопасности



70%

респондентов отмечают, что функция информационной безопасности лишь частично удовлетворяет потребностям организации и улучшения все еще на подходе



45%

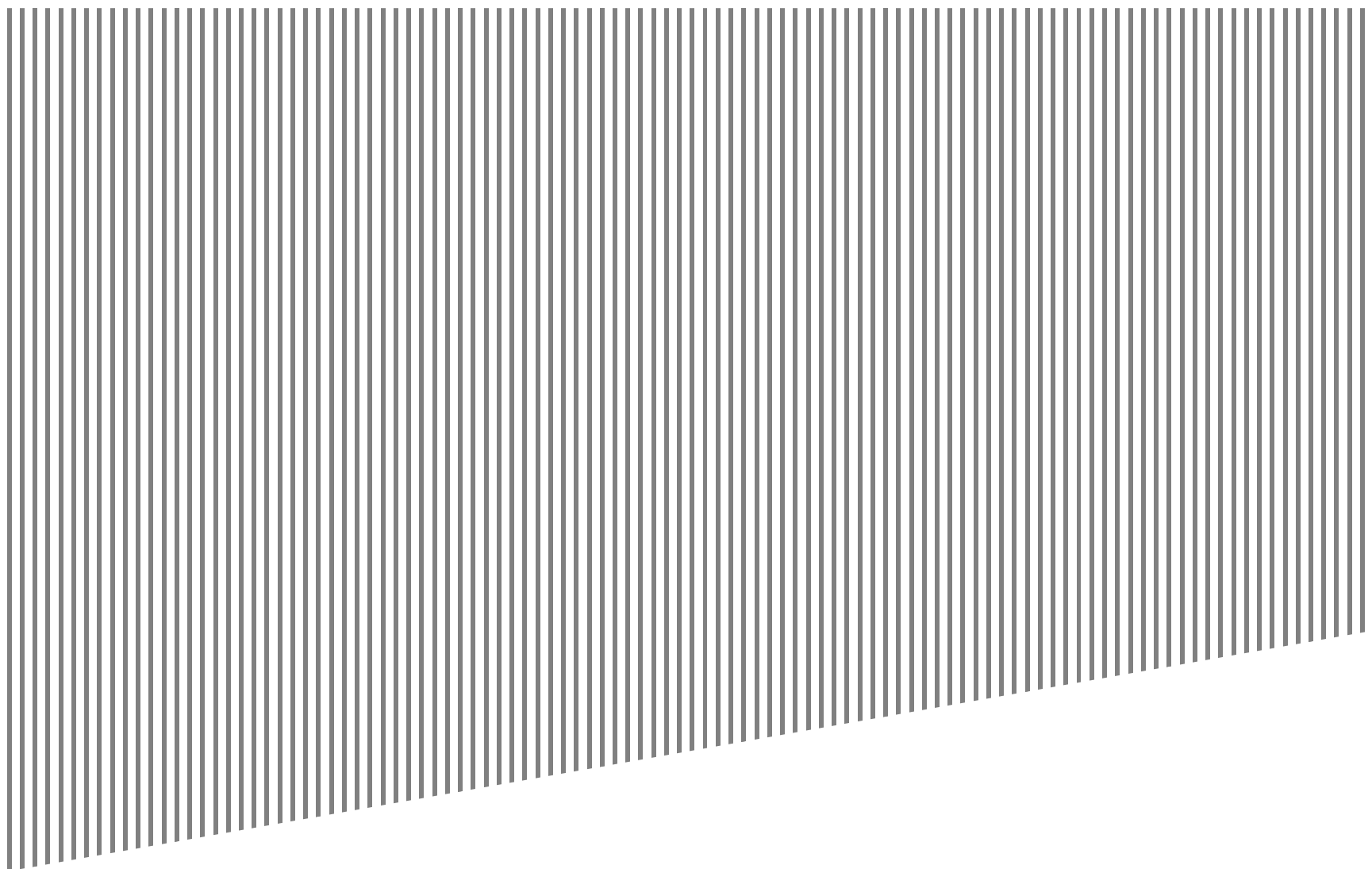
респондентов считают, что мобильные вычисления наиболее значительно изменили их профиль рисков



65%

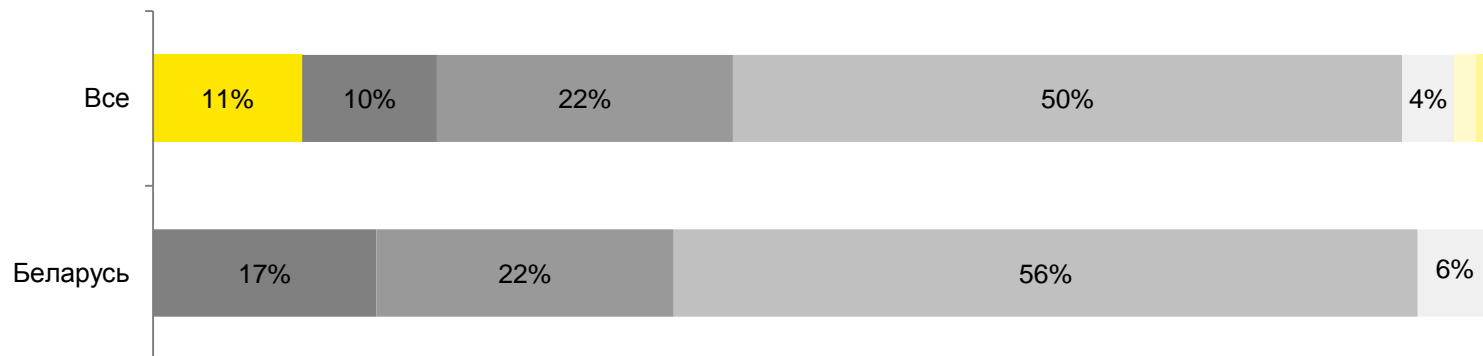
респондентов называют бюджетные ограничения своим главным препятствием созданию ценностей для бизнеса

Беларусь в международном исследовании EY по информационной безопасности 2013

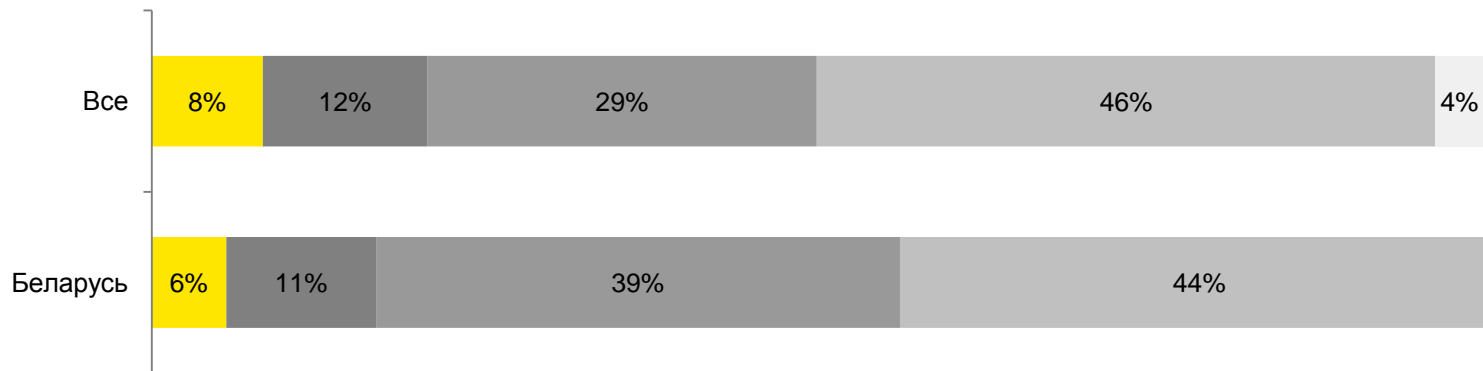


Динамика бюджета на информационную безопасность

2013 факт



2014 план



- Увеличение более чем на 25%
- Увеличение на 15%-25%
- Увеличение на 5%-15%
- Тот же уровень (между +5% и -5%)
- Уменьшение на 5%-15%
- Уменьшение на 15%-25%
- Уменьшение более чем на 25%

- ▶ У 39% организаций в Беларуси увеличились затраты на ИБ в текущем году, и более 56% организаций планируют увеличить затраты на ИБ в 2014 году

Структура затрат на информационную безопасность

2013 факт
2014 план



- ▶ В то время, как во всем мире большая часть затрат на ИБ связана с поддержкой существующих процессов, организации в Беларуси находятся на этапе внедрения и совершенствования этих процессов, поэтому вынуждены инвестировать большую часть бюджета именно на это

Основной приоритет направлений деятельности в области ИБ*



* на графике представлен неполный перечень направлений (12 из 21)

- ▶ Основные приоритеты в РБ — это обеспечение непрерывности деятельности, обнаружение утечек, управление доступом и реагирование на инциденты. Заметны явные проблемы с наймом персонала ИБ. При этом организации не осознают необходимость в глубокой реструктуризации функции ИБ.

Подчинение подразделений, ответственных за ИБ



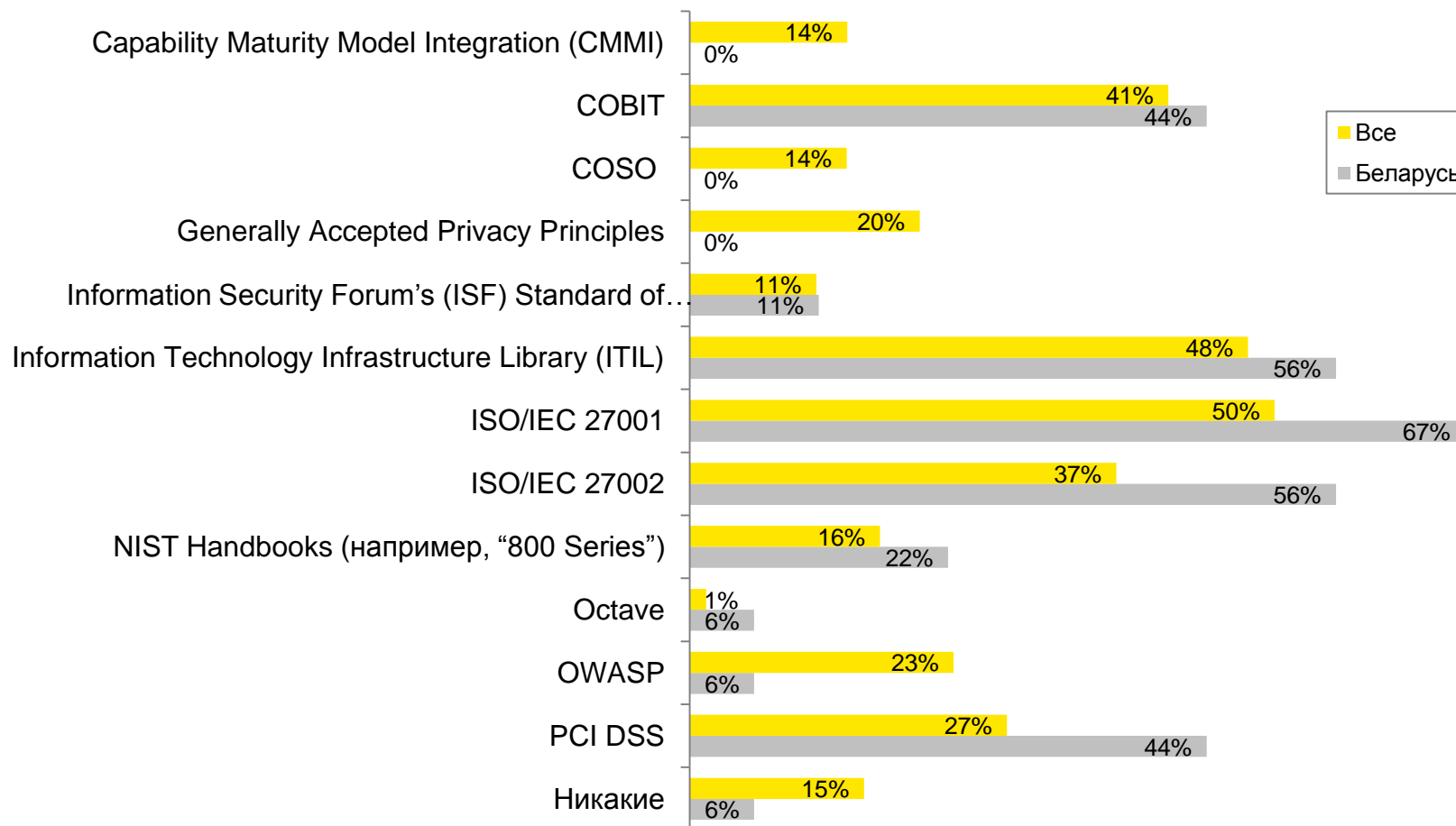
- ▶ В РБ подразделения ИБ подчиняются почти в половине случаев напрямую первому лицу организации. При этом, в каждой пятой организации служба ИБ подчинена операционному или финансовому директору.

Характеристики стратегии ИБ



- ▶ Две из трех организаций в Беларуси считают, что их стратегия ИБ не отражает актуальные риски, при этом очень редко стратегия ИБ учитывает риск-аппетит и допустимые уровни риска для организации

Использование ведущих практик



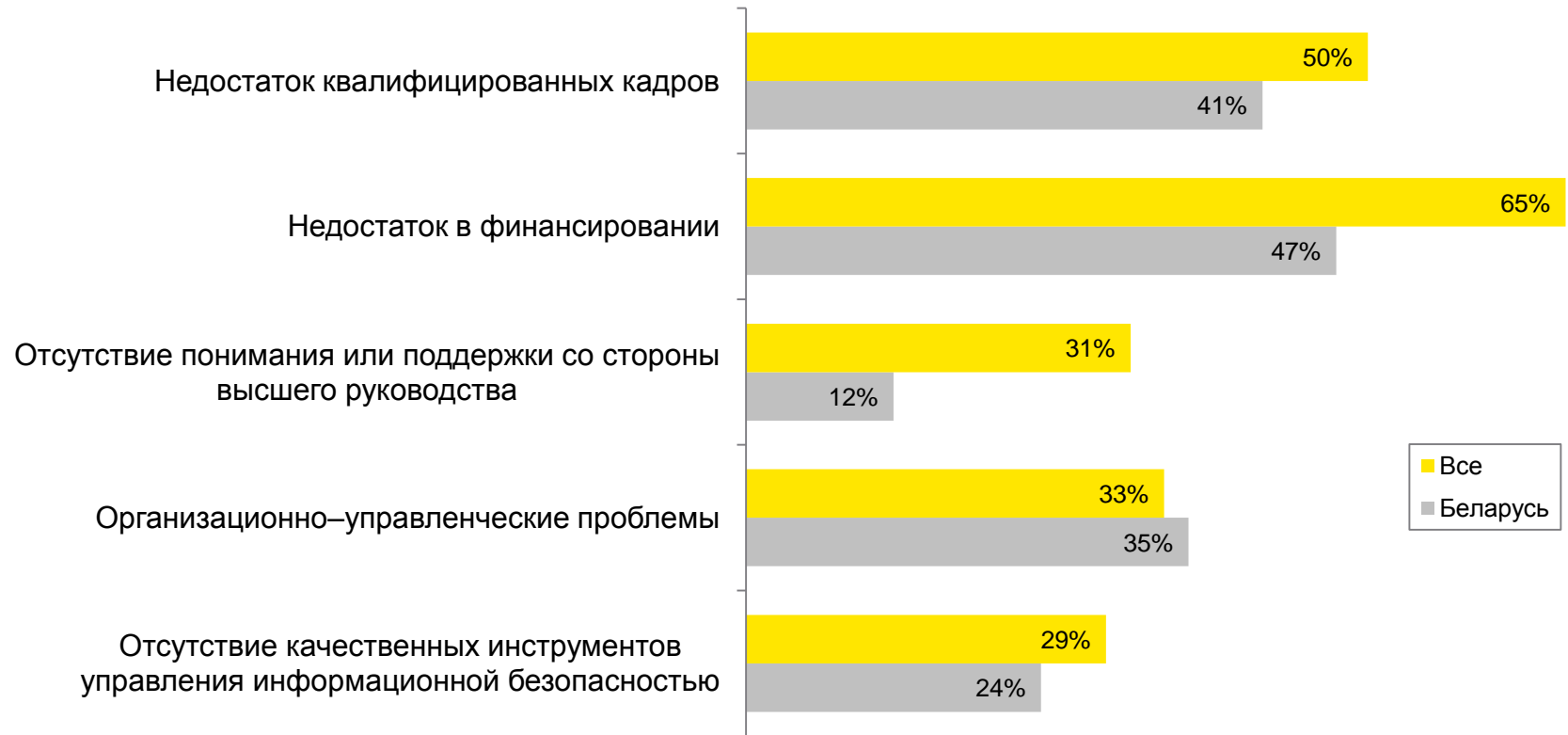
- ▶ Самыми популярными в Беларуси являются такие ведущие практики, как ISO 27001/2, ITIL и COBIT

Соответствие службы ИБ потребностям организаций



- ▶ Только 6% респондентов в Беларуси считают, что службы ИБ полностью удовлетворяют потребностям организации

Основные препятствия эффективной работе службы ИБ



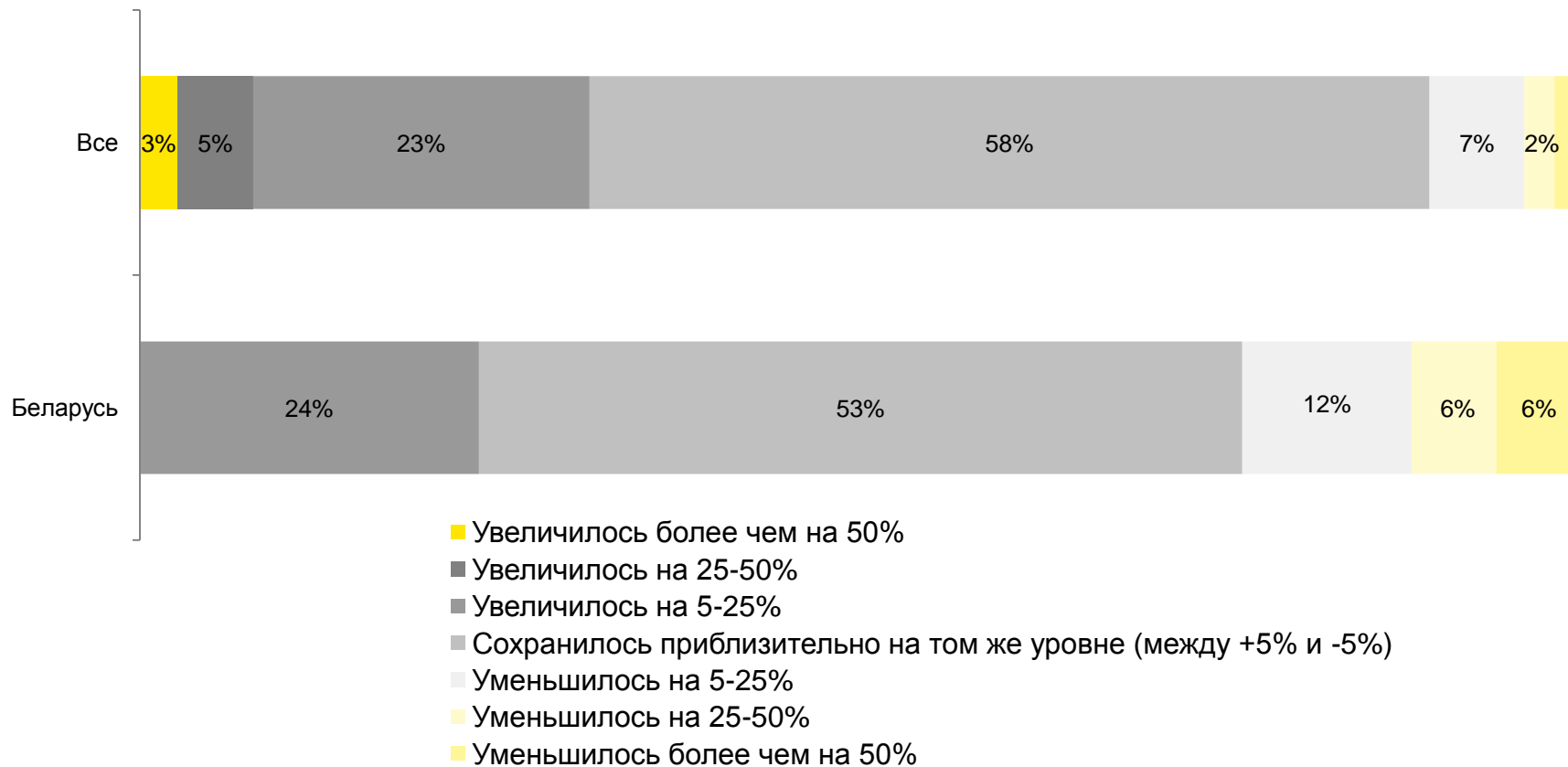
- ▶ Основными препятствиями в Беларуси считают недостаточное финансирование ИБ и нехватку квалифицированных кадров. При этом отсутствие поддержки со стороны высшего руководства не является столь значимым фактором, в отличие от участников исследования со всего мира

Характеристики программы выявления уязвимостей



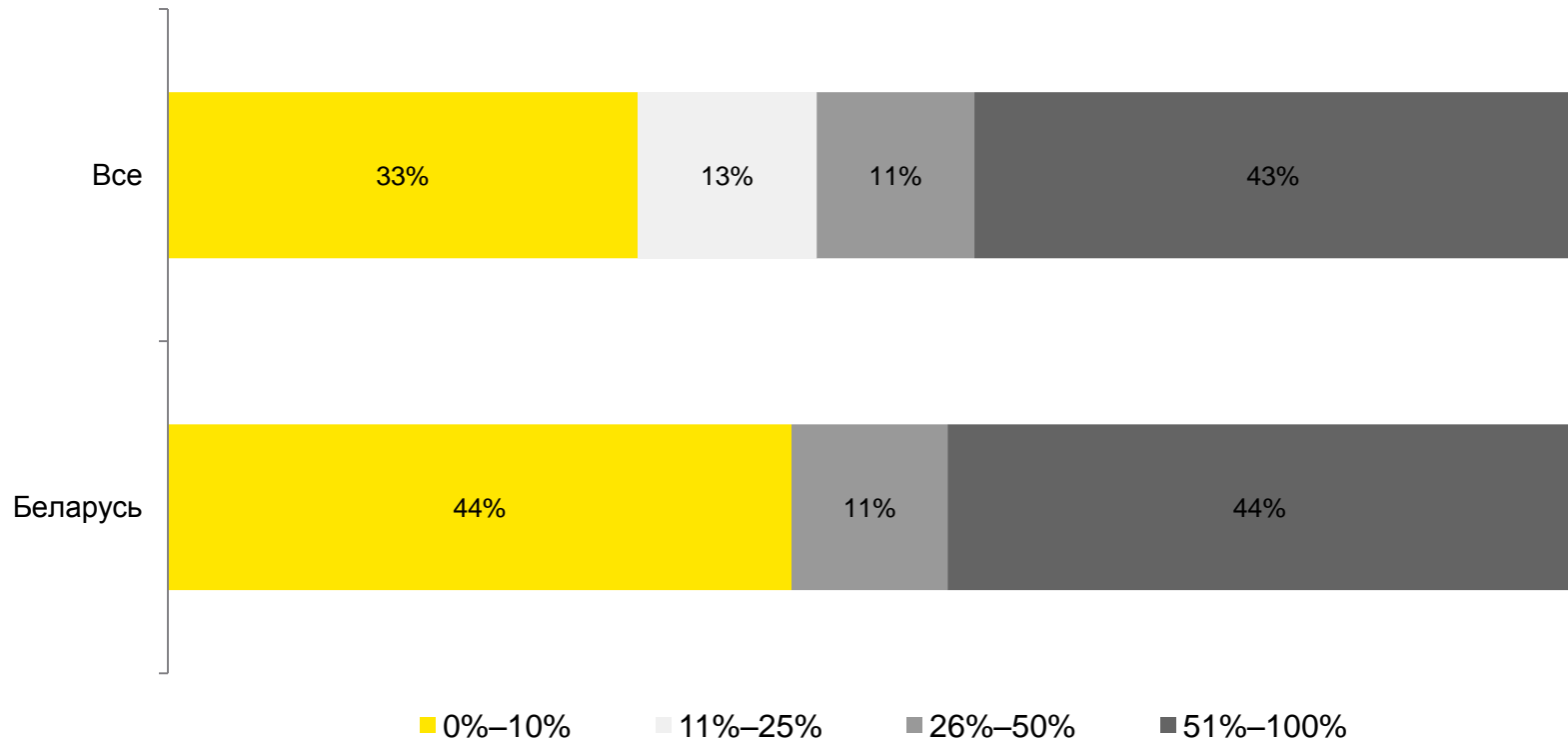
- ▶ Только у 22% процентов организаций в Беларуси есть формализованная программа выявления уязвимостей, которая включает в себя моделирование сложных атак и системную работу над корректирующими мероприятиями

Количество инцидентов безопасности за 2013 год



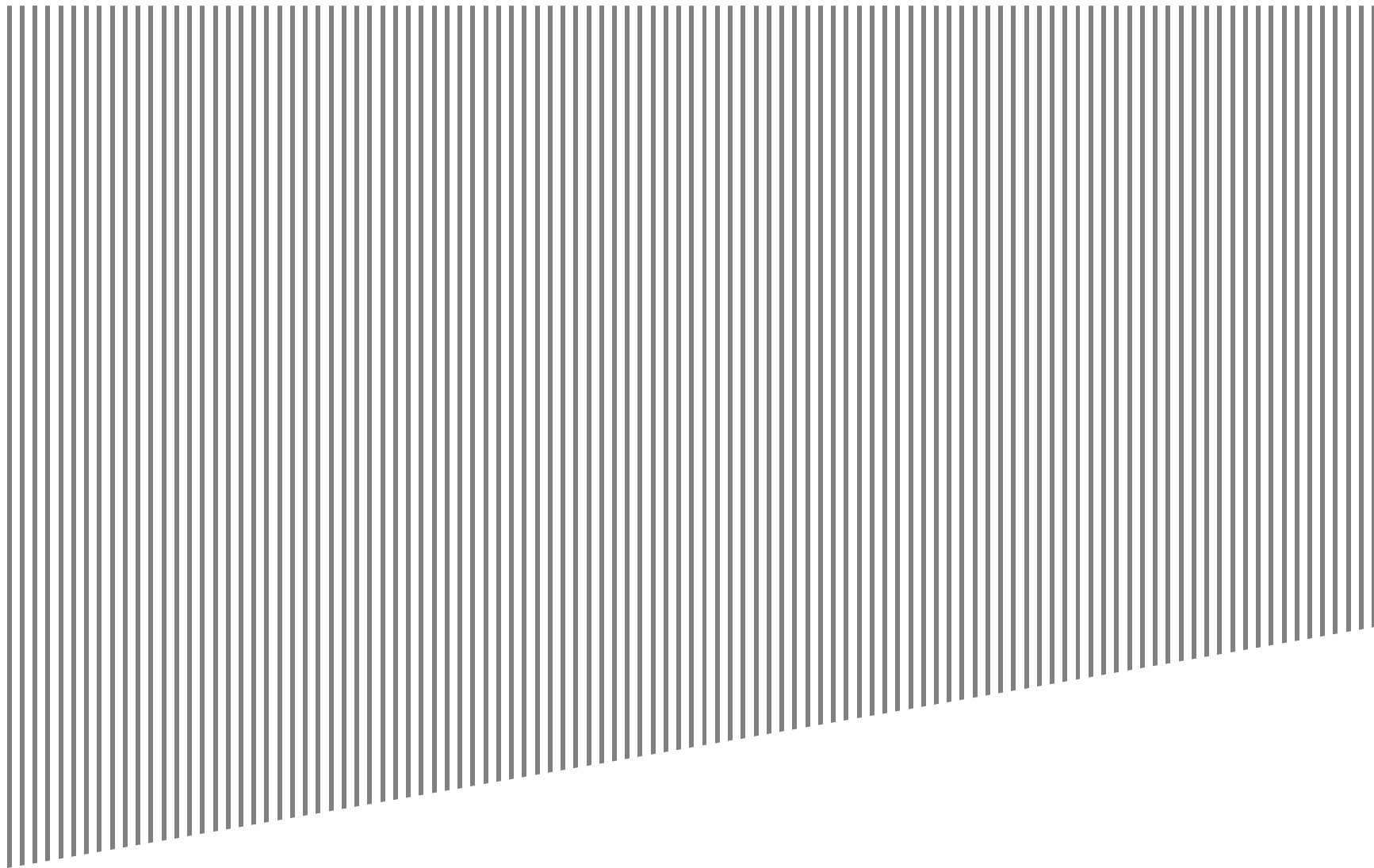
- ▶ Четверть респондентов в Беларуси отметили увеличение инцидентов безопасности в 2013 году, при этом оценка роста инцидентов более консервативная, по сравнению с мировыми показателями

Сколько систем, взаимодействующих с Интернетом, тестируется ежегодно



- ▶ 44% организаций в Беларуси либо не тестируют безопасность собственных информационных систем вообще, либо тестируют очень небольшой процент таких систем, даже несмотря на то, что эти системы взаимодействуют с сетью Интернет

Построение эффективной программы информационной безопасности



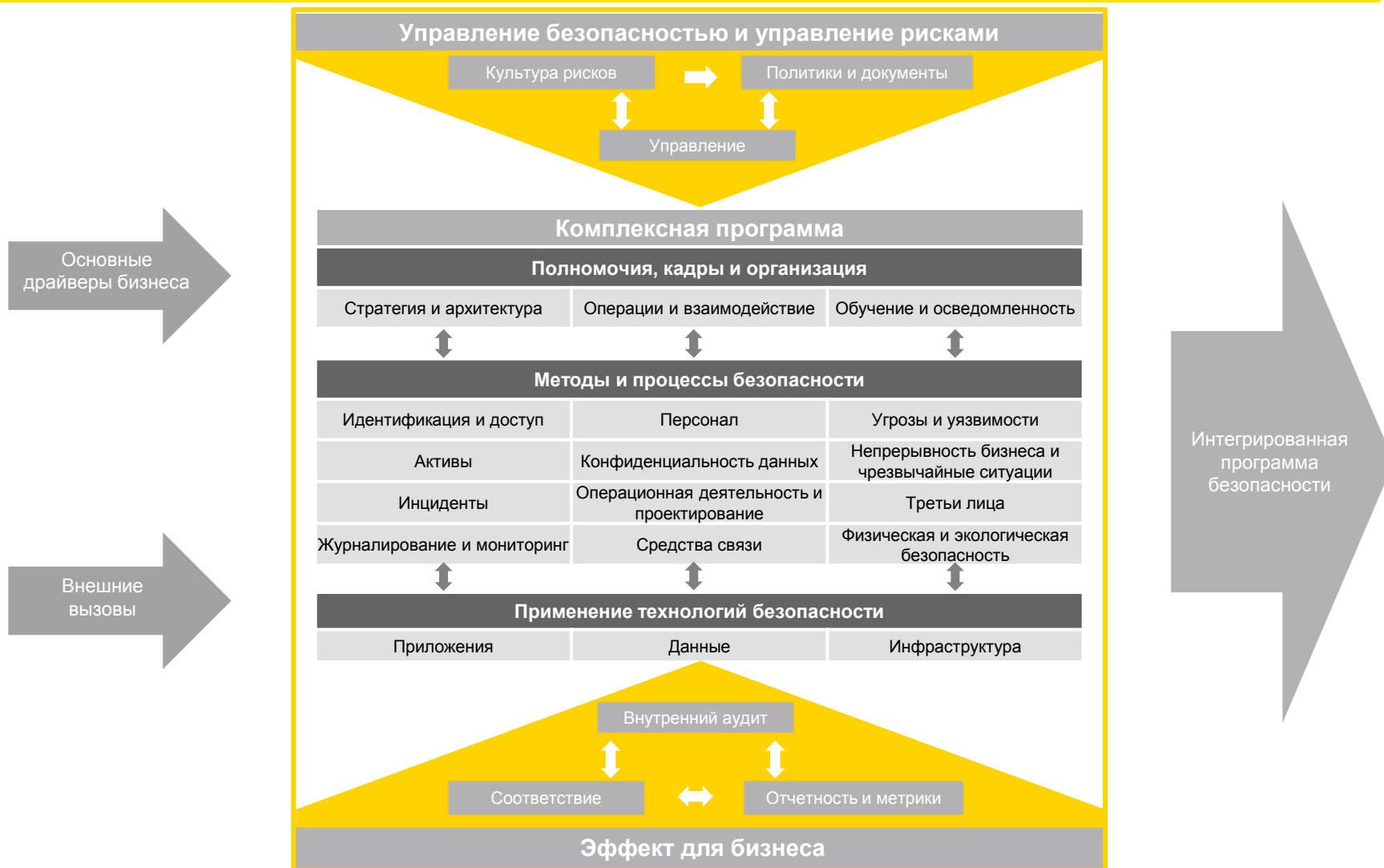
Трансформируйте вашу программу информационной безопасности



Пять вопросов высшему руководству

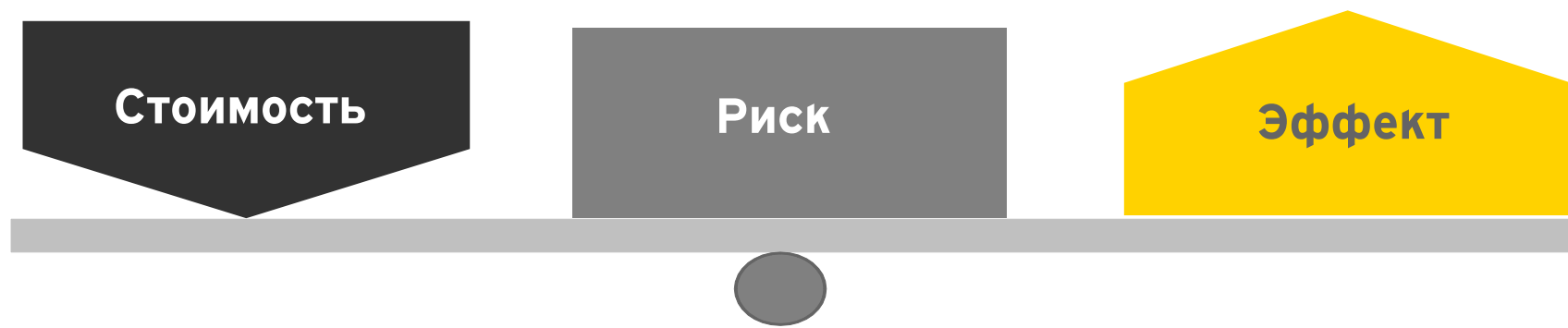
- ▶ Представляете ли вы возможный ущерб, который может нанести инцидент безопасности вашей репутации или бренду?
- ▶ Учитываются ли внутренние и внешние угрозы при интеграции стратегии безопасности в управление рисками организации?
- ▶ Как вы соотносите ключевые риски с приоритетами финансирования?
- ▶ Имеете ли вы представление о вашем риск-аппетите и как он позволяет вам принимать контролируемые риски?
- ▶ Как стратегия управления рисками связана с вашей общей бизнес стратегией?

Основные принципы построения программы безопасности



Найдите баланс между усилиями на обеспечение ИБ и их эффектом

- ▶ Только сбалансированный подход по приоритезации инвестиций в безопасность, основанный на понимании целей и задач бизнеса, будет способствовать успеху организации и в тоже время обеспечит необходимые действия по защите организации



Являются ли наши усилия по обеспечению ИБ результативными и эффективными?

Есть ли у нас:

- ▶ Правильные ресурсы?
- ▶ Правильные инициативы, процессы и технологии?
- ▶ Правильные инвестиции?

Позволяет ли наша программа безопасности:

- ▶ Управлять рисками безопасности в рамках общекорпоративного риск-менеджмента?
- ▶ Адекватно защищать нас от новейших угроз?
- ▶ Выявлять пробелы и устранять коренные причины проблем в безопасности?
- ▶ Проактивно реагировать на изменения в законодательной и деловой среде?

Позволит ли наша программа ИБ:

- ▶ Оставаться конкурентоспособными?
- ▶ Поддерживать новые бизнес-инициативы?
- ▶ Защищать репутацию и бренд?
- ▶ Защищать наиболее ценные активы?

Наши рекомендации

- ▶ Поднимите вопросы информационной безопасности на уровень высшего руководства, сделав их более заметными в компании с помощью четкой стратегии, которая не просто защитит бизнес, но и обеспечит необходимое соответствие функции информационной безопасности потребностям бизнеса
- ▶ Пересмотрите вашу стратегию информационной безопасности на соответствие актуальным рискам
- ▶ В первую очередь сфокусируйтесь на основах безопасности, вместо покупки новомодных программ или инструментов
- ▶ Выработайте структурированный и прагматичный подход к управлению ИТ-рисками, чтобы сконцентрироваться на основных рисках. Мы считаем, что управление ИТ-рисками или управление рисками и соответствием нормативным требованиям (GRC) может стать ключевой инвестицией для многих организаций
- ▶ Сделайте информационную безопасность неотъемлемой частью работы организации и образом повседневного мышления каждого сотрудника

Дополнительная информация

www.ey.com/GRCinsights



Under cyber attack:
EY's Global Information
Security Survey 2013

www.ey.com/giss2013



Beating cybercrime:
Security Program Management
from the Board's perspective

www.ey.com/spm



Privacy trends 2013:
the uphill climb continues

www.ey.com/privacy2013



Mobile device security:
understanding vulnerabilities
and managing risk

www.ey.com/mobiledevicesecurity



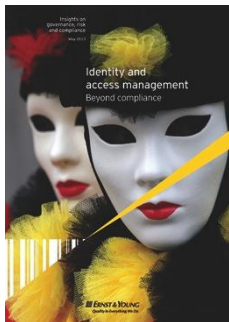
**Protecting and strengthening
your brand:** social media
governance and strategy

www.ey.com/protectingbrand



**Information security in
a borderless world:**
time for a rethink

www.ey.com/infosec_borderless



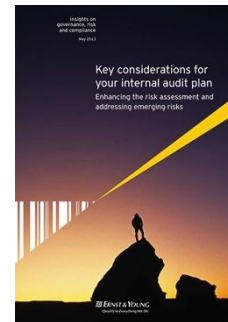
**Identity and access
management (IAM):**
beyond compliance

www.ey.com/iam



Bring your own device: security
and risk considerations for your
mobile device program

www.ey.com/byod



**Key considerations for your
internal audit plan:** enhancing the
risk assessment and addressing
emerging risks

www.ey.com/iaplan

Спасибо за внимание!

Кирилл Домнич, CISA, CISM

Kiryl.Domnitch@by.ey.com

Тел. +375 17 209 4535

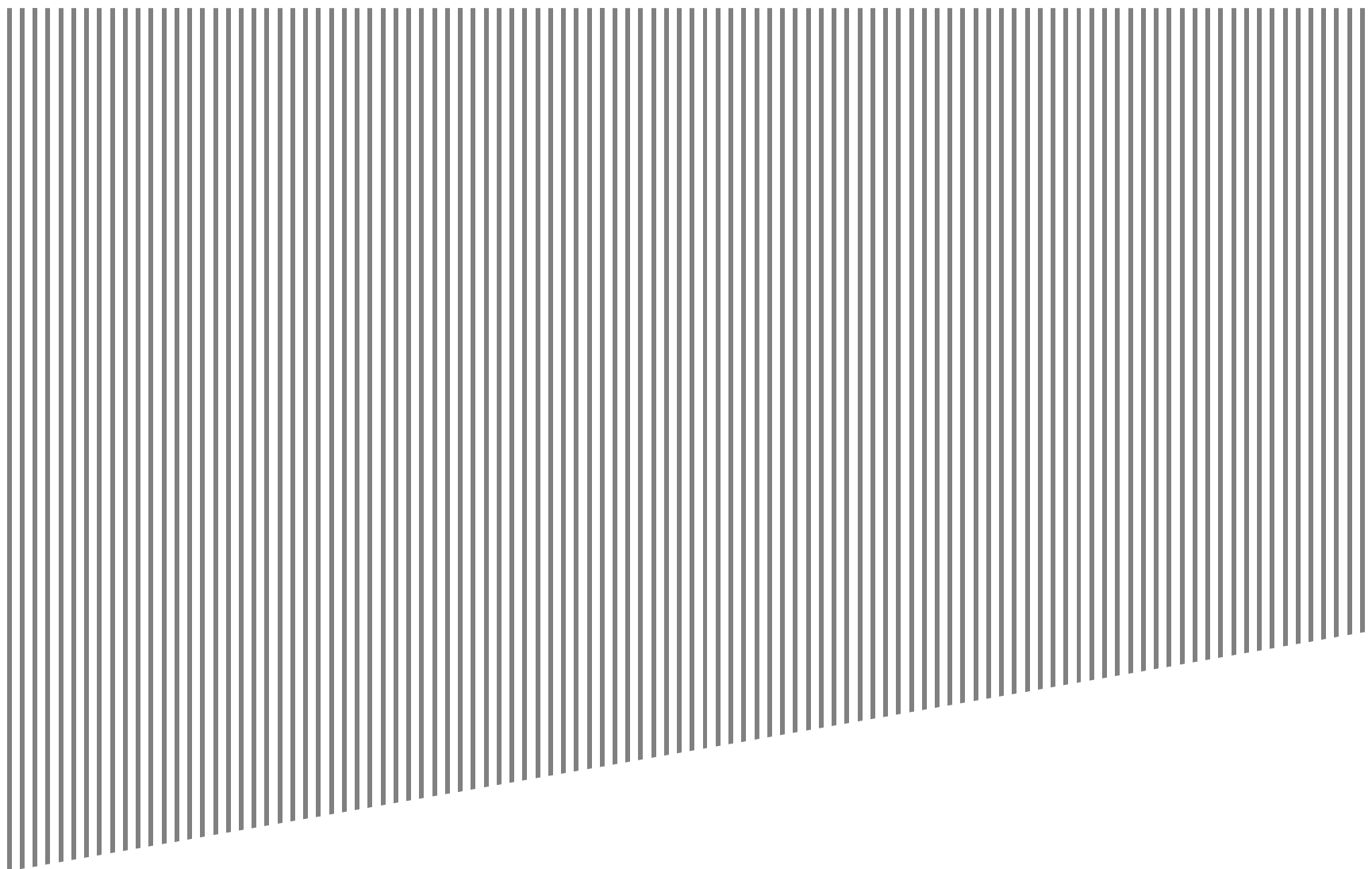
The EY logo consists of the letters 'EY' in a bold, white, sans-serif font. The 'E' and 'Y' are connected at the top. The background of the slide features a landscape with a road leading towards mountains under a sunset sky, with a prominent yellow diagonal stripe.

Building a better
working world

Важная информация

- ▶ Данная презентация содержит лишь общие сведения касательно представленной темы. Информация из этой презентации не должна рассматриваться в качестве исчерпывающей или достаточной для принятия каких-либо решений, а также использоваться для оказания профессиональных консультаций
- ▶ Компания EY не несет ответственности за какие-либо убытки вызванные действием/бездействием касательно вопросов, освещенных в данной презентации
- ▶ Информация в данной презентации дополняется устными пояснениями докладчика и должна рассматриваться только в свете этих устных пояснений
- ▶ Если Вам требуются какие-либо разъяснения, дополнительная информация или конкретная консультация по вопросам, связанным с темой доклада, свяжитесь с нами, и мы будем рады обсудить интересующие Вас вопросы

Консультационные услуги компании EY



Услуги компании EY в области информационных технологий и ИТ-рисков

- ▶ Основные направления
 - ▶ Эффективность ИТ
 - ▶ Аудит ИТ
 - ▶ Информационная безопасность
 - ▶ Управление непрерывностью бизнеса
 - ▶ Управление ИТ-проектами
- ▶ Более 300 консультантов в странах СНГ
- ▶ Глобальная методологическая база
- ▶ Отраслевой и технический опыт
- ▶ Независимость от поставщиков технических решений

Услуги компании EY в области ИТ (1/5)

Эффективность ИТ

- ▶ Обзор текущего состояния ИТ на предмет соответствия требованиям бизнеса, ведущим методологиям и стандартам, выявление возможностей совершенствования ИТ
- ▶ Трансформация ИТ, включая определение целевого состояния ИТ и уровня зрелости ИТ-процессов, разработка инициатив по совершенствованию управления ИТ
- ▶ Разработка и помощь в реализации стратегии ИТ
- ▶ Построение и реинжиниринг ИТ-процессов, включая разработку или актуализацию ИТ-политик и процедур
- ▶ Разработка системы показателей для оценки эффективности ИТ-процессов (KPIs)
- ▶ Сравнительный анализ показателей ИТ с ведущими организациями отрасли

Услуги компании EY в области ИТ (2/5)

Аудит ИТ

- ▶ Оценка состояния ИТ, включая проверку соответствия мировым и региональным стандартам и методологиям (в том числе COBIT, ITIL и др.)
- ▶ Организация работы и оценка эффективности служб внутреннего ИТ-аудита и ИТ-контроля
- ▶ Косорсинг/аутсорсинг внутреннего аудита ИТ
- ▶ Аудит сервисных организаций по международным стандартам (ISAE 3402/SSAE 16, ISO 27001 и др.)
- ▶ Оценка приложений и поддерживающей ИТ-инфраструктуры с точки зрения обеспечения доступности, производительности и безопасности

Услуги компании EY в области ИТ (3/5)

Информационная безопасность

- ▶ Создание системы управления информационной безопасностью, включая разработку необходимых политик, регламентов и процедур
- ▶ Аудит информационной безопасности и проверка соответствия требованиям международных стандартов (ISO 27000, COBIT, ISF, NIST и др.)
- ▶ Разработка стратегии обеспечения информационной безопасности
- ▶ Комплексный анализ уровня защищенности информационных систем

Услуги компании EY в области ИТ (4/5)

Управление ИТ-проектами

- ▶ Независимый контроль качества проектов по внедрению информационных систем
- ▶ Сопровождение проектов по реализации крупномасштабных ИТ-преобразований
- ▶ Помощь в формировании требований к новым системам
- ▶ Помощь в проведении тестирования информационных систем перед их вводом в эксплуатацию

Услуги компании EY в области ИТ (5/5)

Управление непрерывностью бизнеса

- ▶ Реализация и сопровождение проектов разработки и внедрения планов непрерывности бизнеса, в том числе:
 - ▶ анализ воздействия на бизнес сбоев и прерываний в работе ИТ-систем
 - ▶ разработка стратегии обеспечения непрерывности бизнеса, необходимых планов и процедур
 - ▶ разработка требований к резервным решениям, площадям, системам и центрам обработки данных
- ▶ Независимая оценка системы управления непрерывностью бизнеса на соответствие передовой практике, стандартам и законодательным требованиям, включая разработку практических рекомендаций по ее улучшению