Управления рисками ИТ и ИБ в условиях современных вызовов

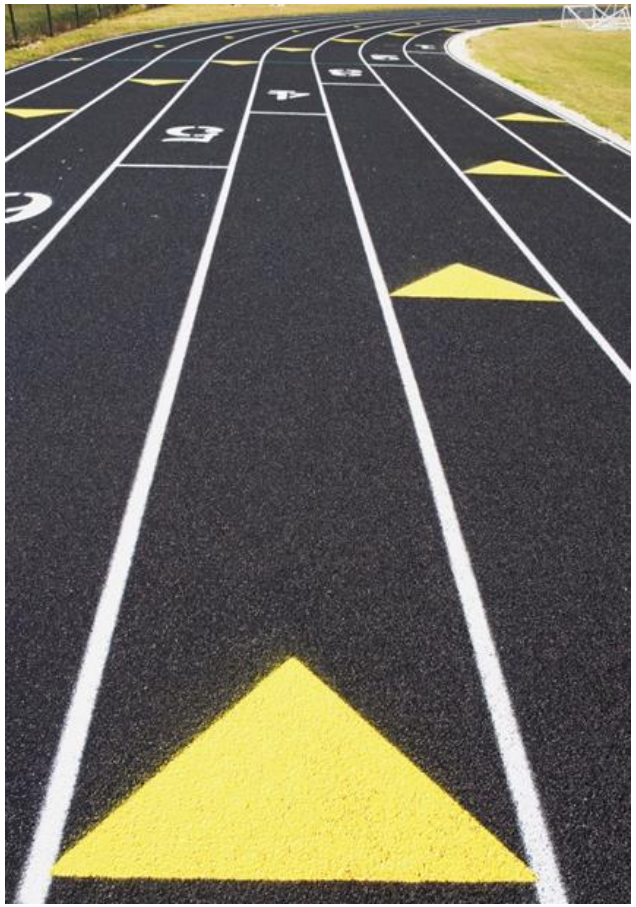
Межбанковский форум по информационной безопасности

20 ноября 2015 года

Building a better working world

Содержание

- Риски ИТ и ИБ
- Тенденции кибер-безопасности
- Примеры управления рисками
  - Использования программного обеспечения
  - Использования «облачных» сервисов



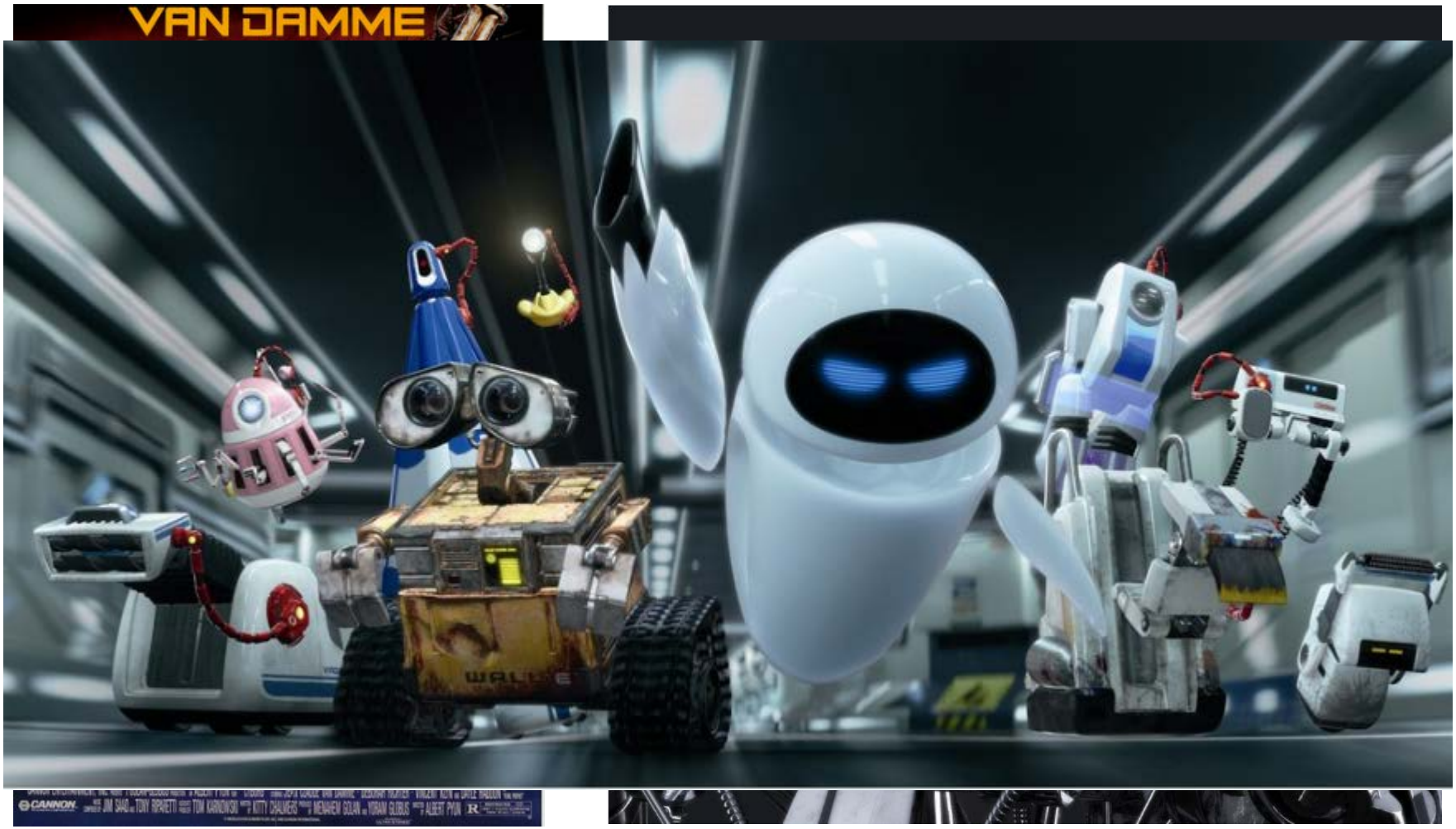
Риски ИТ и ИБ

Понимание области кибер-рисков

Building a better working world

Риски ИТ и ИБ

Понимание области кибер-рисков



Риски ИТ и ИБ
Понимание области киберрисков

- Кибер риски – это подмножество совокупных рисков относящихся одновременно к рискам ИТ и ИБ.

- К ним относятся риски ставшие последствием реализации преднамеренных злоумышленных действий, посредством использования ИТ, и направленных на неавторизованное раскрытие, изменение или разрушение цифровых активов.

Современные вызовы

Building a better working world

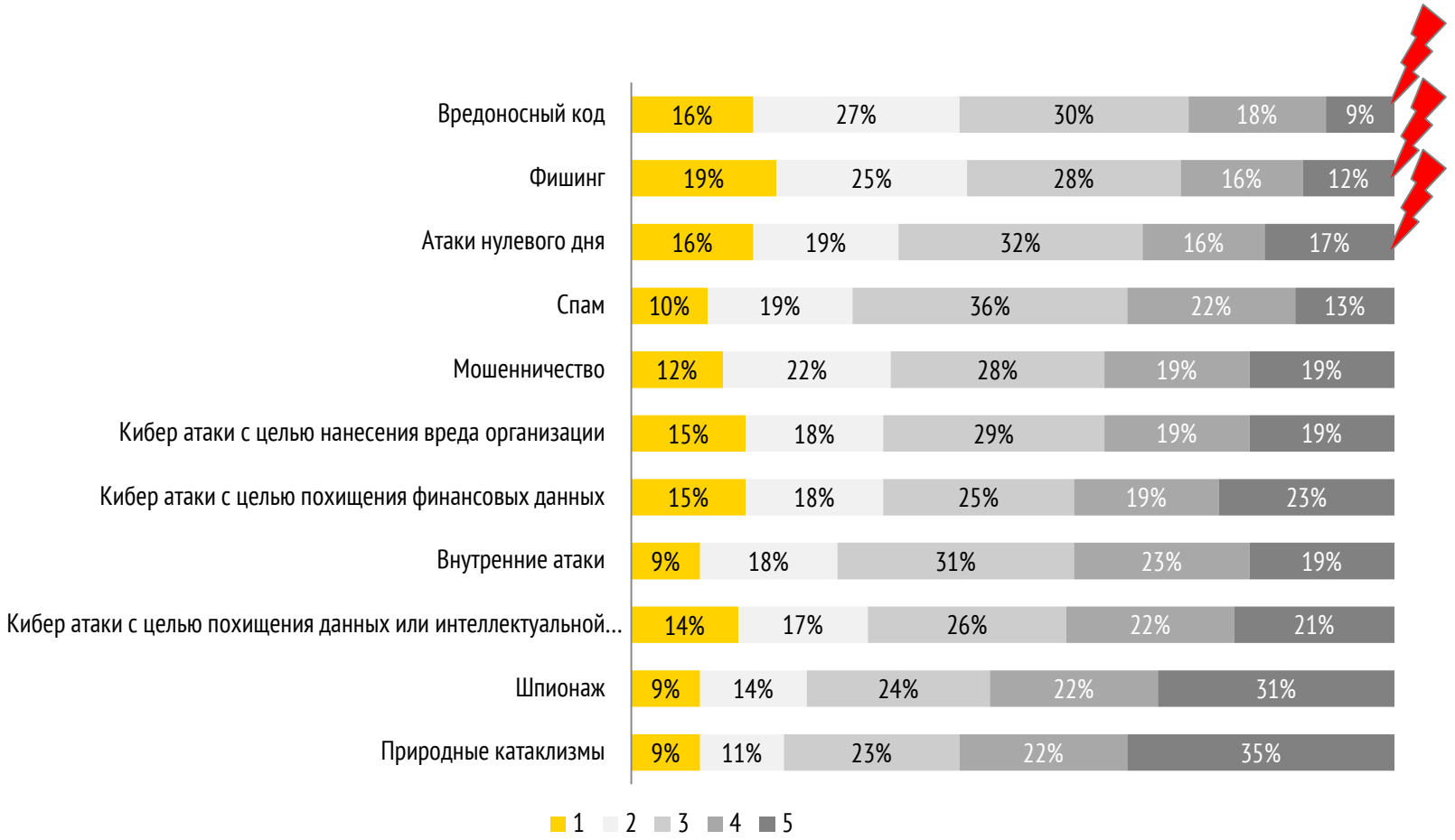
Корпоративные вызовы сегодня

Работа в цифровом мире сопряжена с новыми вызовами и угрозами

- Умные устройства и услуги могут быть причиной непредвиденных последствий и уязвимостей
- Широкая доступность социальных медиа. При этом конфиденциальность и приватность под вопросом.
- Изменения в человеческом поведении, как в лучшую так и в худшую стороны.
- Законодательство и нормативные акты заставляют вносить изменения в процессы, которые могут открыть новые уязвимости и стать целью для атаки.
- Все больше информации хранится в облаке, в результате уровень риска существенно вырастает, а контроль над сложной ИТ экосистемой ограничен.

Текущие тенденции в кибер-безопасности

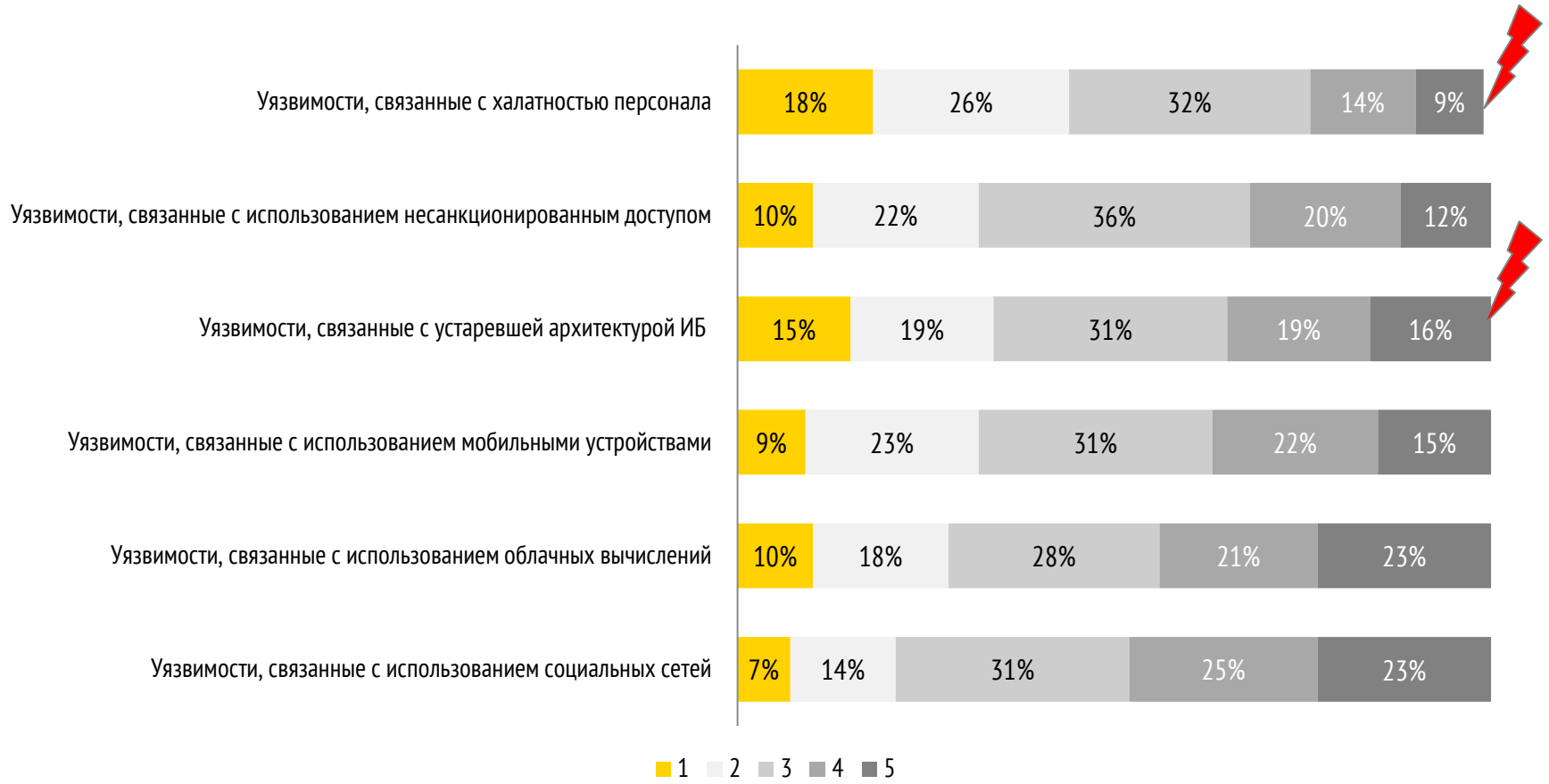
Наиболее критичные угрозы за последние 12 месяцев.



1 – высокий приоритет, 5 - низкий

Текущие тенденции в кибер-безопасности

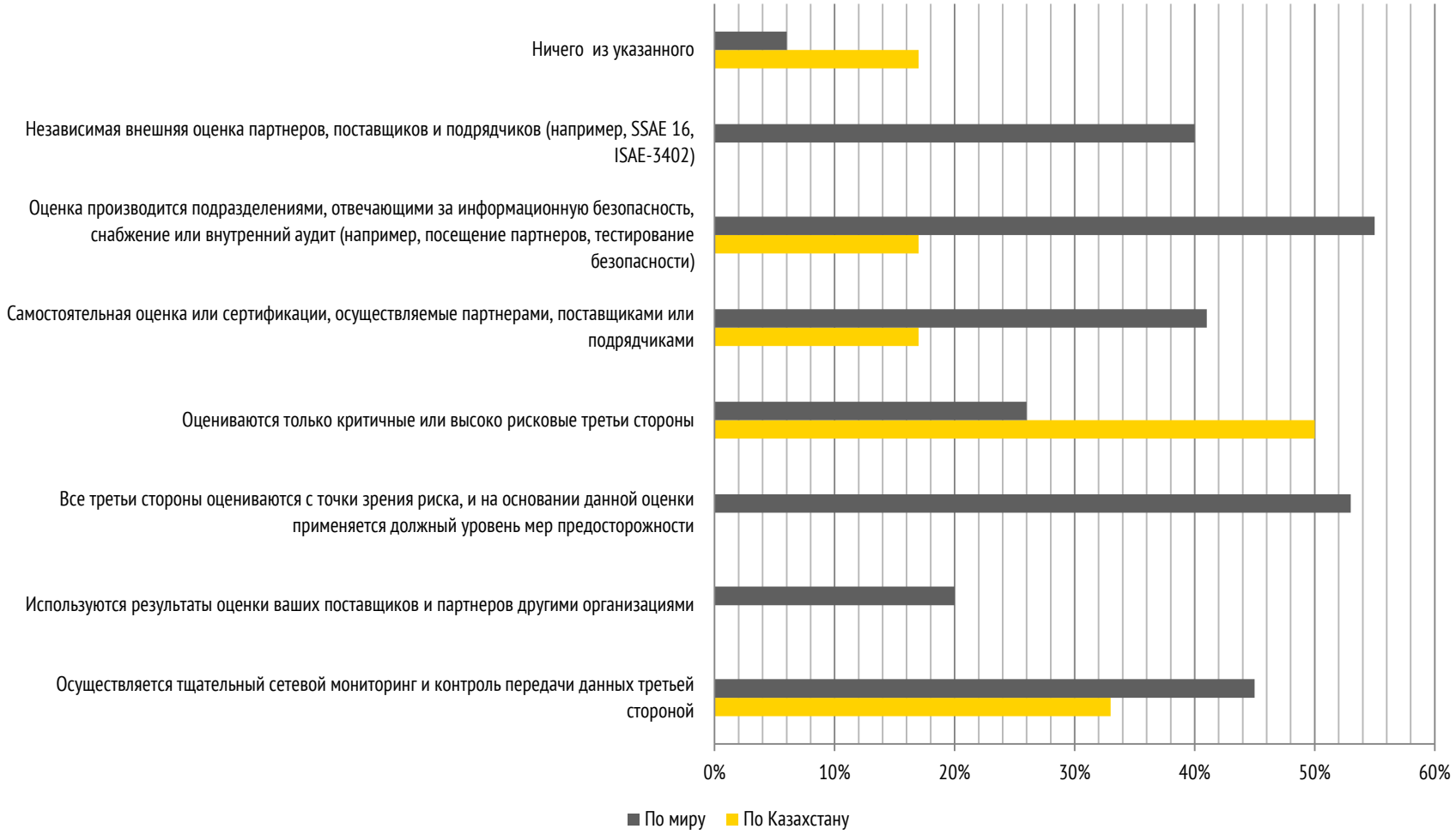
Наиболее критичные уязвимости за последние 12 месяцев.



1 – высокий приоритет, 5 - низкий

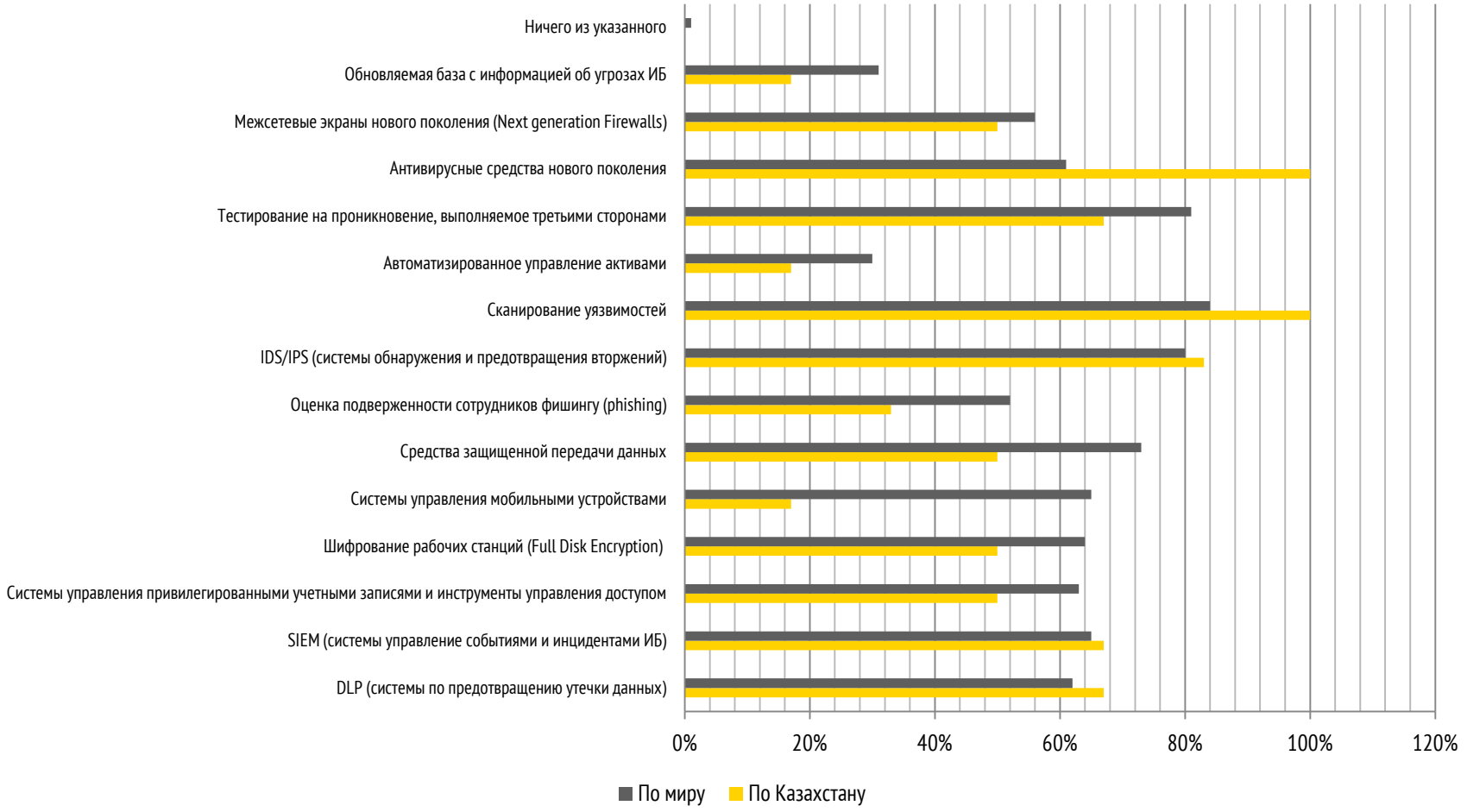
Текущие тенденции в кибер-безопасности

Проверка партнеров, поставщиков и подрядчиков в области ИБ



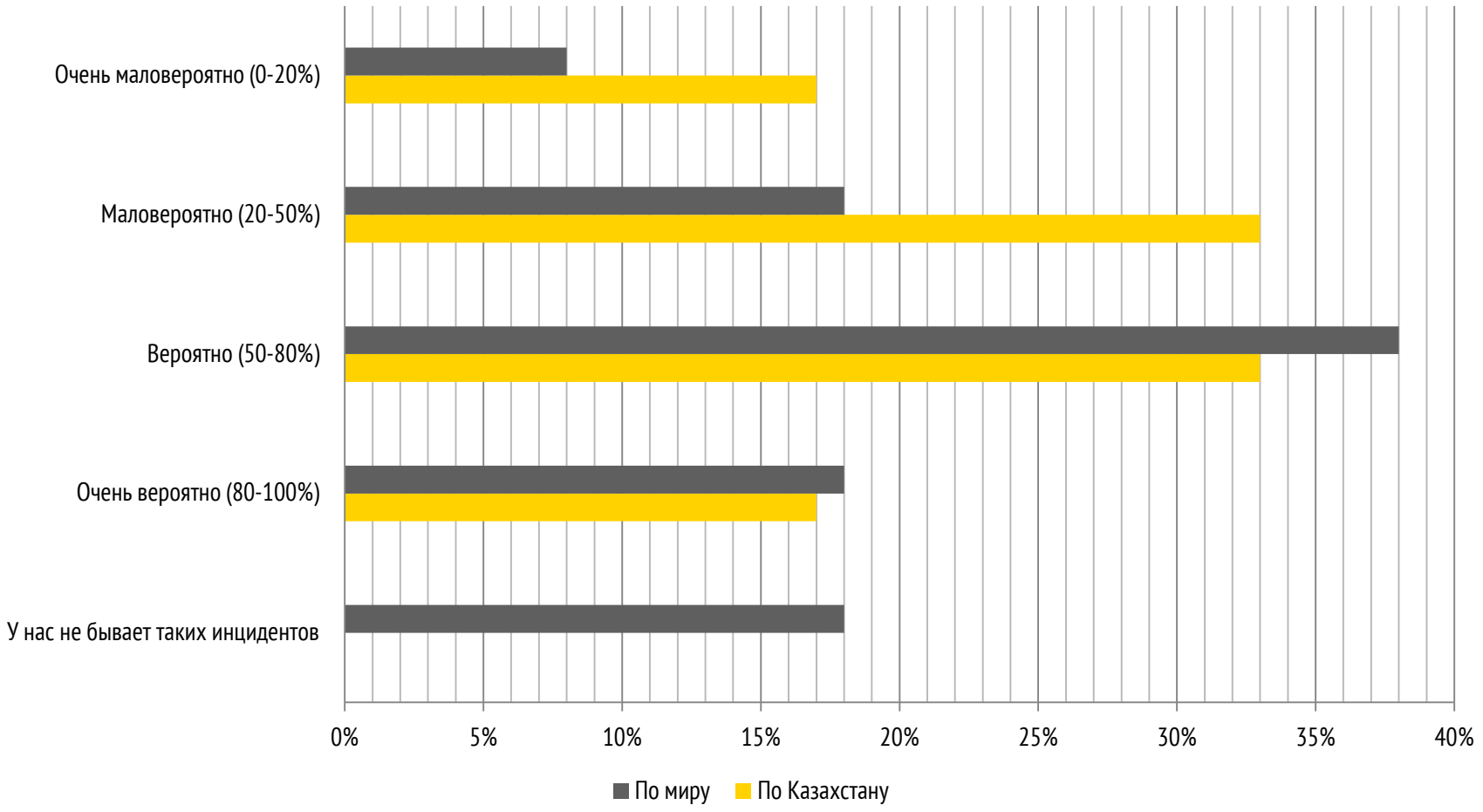
Текущие тенденции в кибер-безопасности

Используемые технологии в области ИБ



Текущие тенденции в кибер-безопасности

Вероятность обнаружения сложной и профессиональной атаки



Примеры управления рисками

Building a better working world

Риски использования ПО

Основные проблемы:

1. Основной рассматриваемый риск при использовании нелицензионного ПО – это риск ИТ: отсутствие технической поддержки.
2. Меры ИБ в данной области ограничиваются снижением рисков использования ПО, не имеющего отношения к работе (игры, мессенджеры и т.п.).
3. Финансовые риски зачастую совсем не рассматриваются (связано с недостаточной прецедентной базой).

Обзор рисков использования программного обеспечения

Основные риски ИБ:

- Наличие широко известных уязвимостей в результате отсутствия регулярных обновлений.
- Внедрение вредоносного программного обеспечения в результате использования ПО из непроверенного источника.

Другие операционные риски:

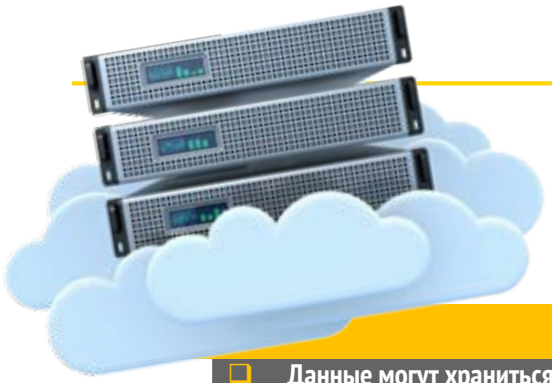
- Штрафные санкции со стороны правообладателя.
- Штрафные санкции со стороны регуляторных органов.
- Репутационные потери.

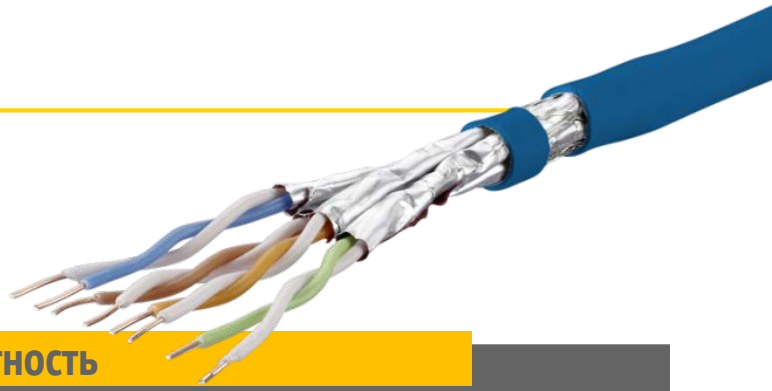
Обзор рисков использования программного обеспечения

Наиболее распространенные подходы к снижению рисков, связанных с использованием ПО:

- Внедрение программы управления используемым программным обеспечением, включающей периодические проверки (аудиты) текущего состояния.
- Использование внешних (облачных) сервисов вместо локального ПО.

Обзор рисков использования «Облаков»





Безопасность и приватность

- Данные могут храниться в Облаке без шифрования, допуская случайное или преднамеренное их разглашение.
- Сложность управления в критических областях, например: в управлении уязвимостями или физической безопасности.
- Слабый логический контроль доступа поставщиком облачных решений.

Данные и технологии

- Существует риск создания разрозненности информации и проблем с ее целостностью, качеством и пониманием.
- Бизнес может обойти ИТ-функции для реализации облачных решений, создав конфликты управление ИТ.
- Облачные вычисления меняют представления о том, как ИТ предоставляет услуги для пользователей.

Регуляторные требования

- Отсутствие прозрачности операций провайдера тормозит анализ их соответствия внешним требованиям.
- Сложность в управлении / хранении журналов создает дополнительные проблемы.
- Данные могут храниться в облаке в юрисдикции, где права объекта данных не защищены.
- Отсутствие нормативной базы для облачных сервисов усиливает риски.

Управление поставщиками

- Отсутствие ясности в понимании обязательств между поставщиком и пользователями организации.
- Отсутствуют распространенные стандарты для взаимодействия с поставщиками облачных решений.
- Существенная зависимость как от провайдера облачного решения, так и от провайдера каналов связи.

Обзор рисков использования «Облаков»

Безопасность и приватность

Проблемы и последствия

- Данные могут храниться в облаке без надлежащего разделения прав клиентов, допуская случайное или преднамеренное разглашение третьим лицам
- Потеря управления в критических областях безопасности
- Слабый логический контроль доступа из-за незрелости IAM облака поставщика

Оценка рисков безопасности	Управление данными	Конфиденциальность	Требования к безопасности	Независимый аудит	Доступ к данным
Разработать надежную модель оценки рисков безопасности, для их последующего выявления и оценки, в том числе рисков ассоциированных с использованием внешнего провайдера. Пересматривать оценку рисков на регулярной основе.	Надежная программа управления данными / информацией поможет сгладить вопросы перехода на Облачные решения. Необходимо заранее определить политики, классифицировать необходимую информацию и приложения, определить требования к шифрованию и местоположению.	Оценить практики провайдера по сбору, хранению, использованию, уничтожению и раскрытию персональной информации (ПИ). Выяснить обстоятельства, при которых провайдер может поделиться или раскрыть хранимую информацию.	Четко сформулировать требования к обеспечению безопасности, определить ответственность и включить строгие требования в контракт.	Убедиться, что договор с поставщиком Облачного решения включает условия прохождения регулярного независимого аудита в вопросах управления информационной безопасностью поставщика и защищенности его Облачной ИТ инфраструктуры.	Разработать структуру для обмена пользовательскими идентификаторами и обеспечением доступа пользователей к чувствительной информации. Определить условия, при которых третьи лица могут иметь доступ к данным.

Обзор рисков использования «Облаков» Данные и технологии

Проблемы и последствия

- Существует риск создания проблем с целостностью, качеством и пониманием информации
- Бизнес может обойти ИТ-функции для реализации облачных решений, делая управление ИТ сложным
- Облачные вычисления резко меняют то, как ИТ предоставляют сервисы

Технологическая стратегия и архитектура	Каталог служб	Управление данными	Предоставление решений	Управление ИТ-службами
Необходимо заранее определить виденье и стратегию Облачных вычислений с учетом долгосрочных перспектив, принципов и стандартов технологической архитектуры, для обеспечения совместимости, интеграции, безопасности и контроля данных размещенных у провайдера.	Для снижения риска неисполнения/обхода внутренних контролей, рассмотреть централизацию облака для всей организации и предложить функциональные службы для пользователей с помощью единого каталога.	Разработать и внедрить модель управления, анализа, повышения качества, целостности и понимания данных. Классифицировать данные, заранее определив их владельцев, местонахождение и политики хранения/архивации.	Традиционный жизненный цикл разработки программного обеспечения (SDLC) должен развиваться в рамках модели цикла интеграции ИТ-услуг, и поддерживать как приложения внутренней разработки, так и решения на базе Облачных вычислений.	Разработать модель и процессы ИТ-операций, чтобы сосредоточиться на широких возможностях управления ИТ-услугами и нетехнологическом управлении

Обзор рисков использования «Облаков»

Регуляторные требования

Проблемы и последствия

- Отсутствие прозрачности операций провайдера тормозит анализ их соответствия законам и правилам
- Сложность в управлении / хранении журналов создает проблемы
- Данные могут храниться в облаке в юрисдикции, где права объекта данных не защищены
- Отсутствие нормативной базы для облачных сервисов усиливает риски

Нарушения	Гарантии	Совместная оценка риска	Расположение данных
Принятие облачных вычислений требует изменений в существующих процессах для обеспечения своевременного выявления, оценки и информирования о любых нарушениях, которое могут повлиять на компрометацию конфиденциальности, целостности и доступности информации.	Методы обеспечения гарантий, принятые «облачным» провайдером должны включать в себя, соответствия требованиям SSAE 16, Webtrust, и т.п. Убедится, что организация ознакомлена с методами гарантирования предоставляемых услуг различными провайдерами.	Внутренние аудиторы, юристы, а также подразделения по управлению рисками и безопасностью должны тесно сотрудничать, чтобы своевременно выявлять возможные регуляторные риски и включить их в перечень мероприятий для дальнейшей обработки.	Включить в контракты с провайдером сервиса Облачных вычислений пункт, оговаривающий где физически будут размещаться данные, и каким методами они будут шифроваться. Убедится ,что необходимые регуляторные требования полностью соблюдаются.

Обзор рисков использования «Облаков»

Управление поставщиками

Проблемы и последствия

- Отсутствие ясности в понимании обязательств между поставщиком и пользователями организации
- Отсутствуют распространенные стандарты для взаимодействия с поставщиками облачных решений.
- Существенная зависимость как от провайдера облачного решения, так и от провайдера каналов связи

Сертификация поставщиков

Установить процесс сертификации провайдеров на основе требований и контроля, необходимого для снижения риска.

Кроме того, использовать процесс для создания сертифицированного списка поставщиков сервисов Облачных вычислений (IaaS, PaaS, SaaS).

Контракты с поставщиками

Необходимо четко определить условия договора включив в него такие пункты, как обязанности сторон, общие данные, ценовые условия, соглашение об уровне обслуживания (SLA), права на проведение независимого аудита, импорт / экспорт данных и т.д. Обязательным требованием является пункты о возможной смене «облачного» поставщика.

Управление поставщиками

Управление поставщиками облачных сервисов необходимо централизовать.

Выбор поставщика

Жизнеспособность мелких поставщиков облачных сервисов может быть проблемой для долгосрочного предоставления сервисов. Неизбежны дополнительные расходы, в случае если потребуется сменить провайдера. Необходимо сосредоточится на проявлении должной осмотрительности перед тем, как выбрать провайдера облачных вычислений.

Спасибо за внимание!

EY в Казахстане

Офис в Алматы

Бизнес-центр «Есентай тауэр»
Проспект Аль-Фараби, 77/7
050060, Алматы
Тел. +7 (727) 258 5960
Факс +7 (727) 258 5961
E-mail: almaty@kz.ey.com

Офис в Астане

Бизнес-центр «Каскад»
Проспект Кабанбай батыра, 6/1
010000, Астана
Тел. +7 (7172) 580 400
Факс +7 (7172)580 410
E-mail: astana@kz.ey.com

Офис в Атырау

Бизнес-центр “Atyrau Plaza",
Ул. Сатпаева, 19
060000, Атырау
Тел. +7 (7122) 996 099
Факс +7 (7122)996 097
E-mail: atyrau@kz.ey.com

Владимир Ремыга

Директор отдела по услугам в области информационных технологий и ИТ-рисков
E-mail: Vladimir.Remyga@kz.ey.com

Юрий Мороз

Старший Менеджер отдела по услугам в области информационных технологий и ИТ-рисков
E-mail: Yuriy.Moroz@kz.ey.com

EY | Assurance | Tax | Transactions | Advisory

Краткая информация о компании EY
EY является международным лидером в области аудита, налогообложения, сопровождения сделок и консультирования. Наши знания и качество услуг помогают укреплять доверие общественности к рынкам капитала и экономике в разных странах мира. Мы формируем выдающихся лидеров, под руководством которых наш коллектив всегда выполняет взятые на себя обязательства. Тем самым мы вносим значимый вклад в улучшение деловой среды на благо наших сотрудников, клиентов и общества в целом.

Мы взаимодействуем с компаниями из стран СНГ, помогая им в достижении бизнес-целей. В 20 офисе нашей фирмы (в Москве, Санкт-Петербурге, Новосибирске, Екатеринбурге, Казани, Краснодаре, Ростове-на-Дону, Тольятти, Владивостоке, Южно-Сахалинске, Алматы, Астане, Атырау, Бишкеке, Баку, Киеве, Ташкенте, Тбилиси, Ереване и Минске) работают 4800 специалистов.

Название EY относится к глобальной организации и может относиться к одной или нескольким компаниям, входящим в состав Ernst & Young Global Limited, каждая из которых является отдельным юридическим лицом. Ernst & Young Global Limited − юридическое лицо, созданное в соответствии с законодательством Великобритании, − является компанией, ограниченной гарантиями ее участников, и не оказывает услуг клиентам. Более подробная информация представлена на нашем сайте: ey.com.

© 2015 ТОО «Эрнст энд Янг – консультационные услуги».
Все права защищены.

ey.com

Информация, содержащаяся в настоящей публикации, предназначена лишь для общего ознакомления и не должна рассматриваться в качестве профессиональных рекомендаций в области бухгалтерского учета, налогообложения или в иных сферах. По всем конкретным вопросам следует обращаться к специалисту по соответствующему направлению.