www.pwc.ru

Управление рисками и кибербезопасность

pwc

Кому и зачем нужно управлять киберрисками

Доверие в эпоху цифровых технологий

Руководители компаний видят прямую взаимосвязь между кибербезопасностью и доверием к их бизнесу

89% **90%**
Перерывы и сбои в работе ИТ-систем

83% **91%**
Взлом систем кибербезопасности, наносящий ущерб бизнес-информации или основным системам организации

81% **93%**
Нарушение конфиденциальности персональных данных и этических норм

75% **88%**
Риски, связанные с использованием социальных сетей

70% **69%**
Отсутствие четкой структуры владения цифровыми активами

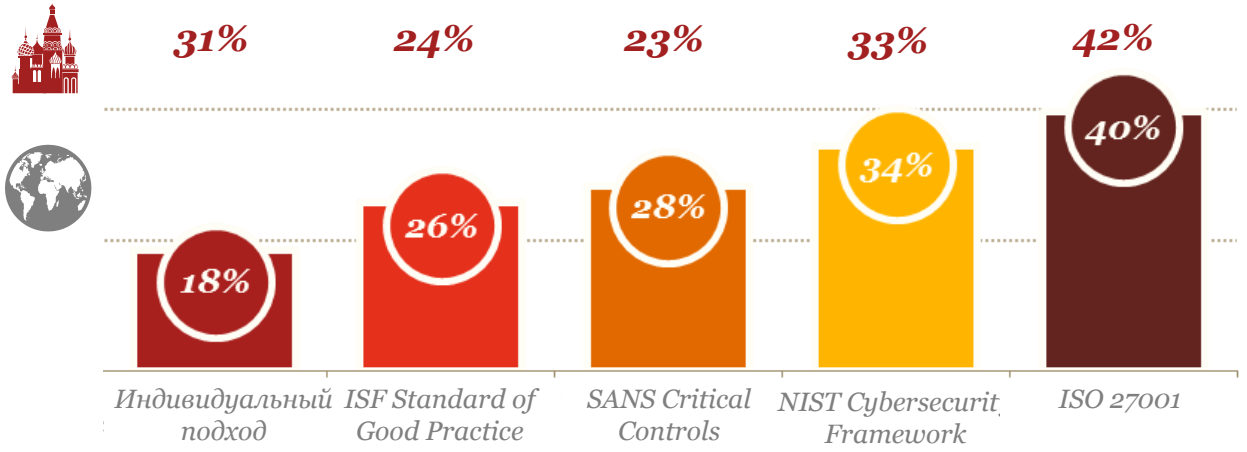
57% **63%**
Отсутствие четкого налогового регулирования цифровых активов

55% **67%**
Искусственный интеллект и автоматизация (включая технологию «блокчейн»)

30% **33%**
Генные технологии (напр., генетически модифицированные зерновые культуры, синтетическая биология)

Фокус на рискориентированное управление

Компаний строят кибербезопасность с использованием инструментов управления рисками



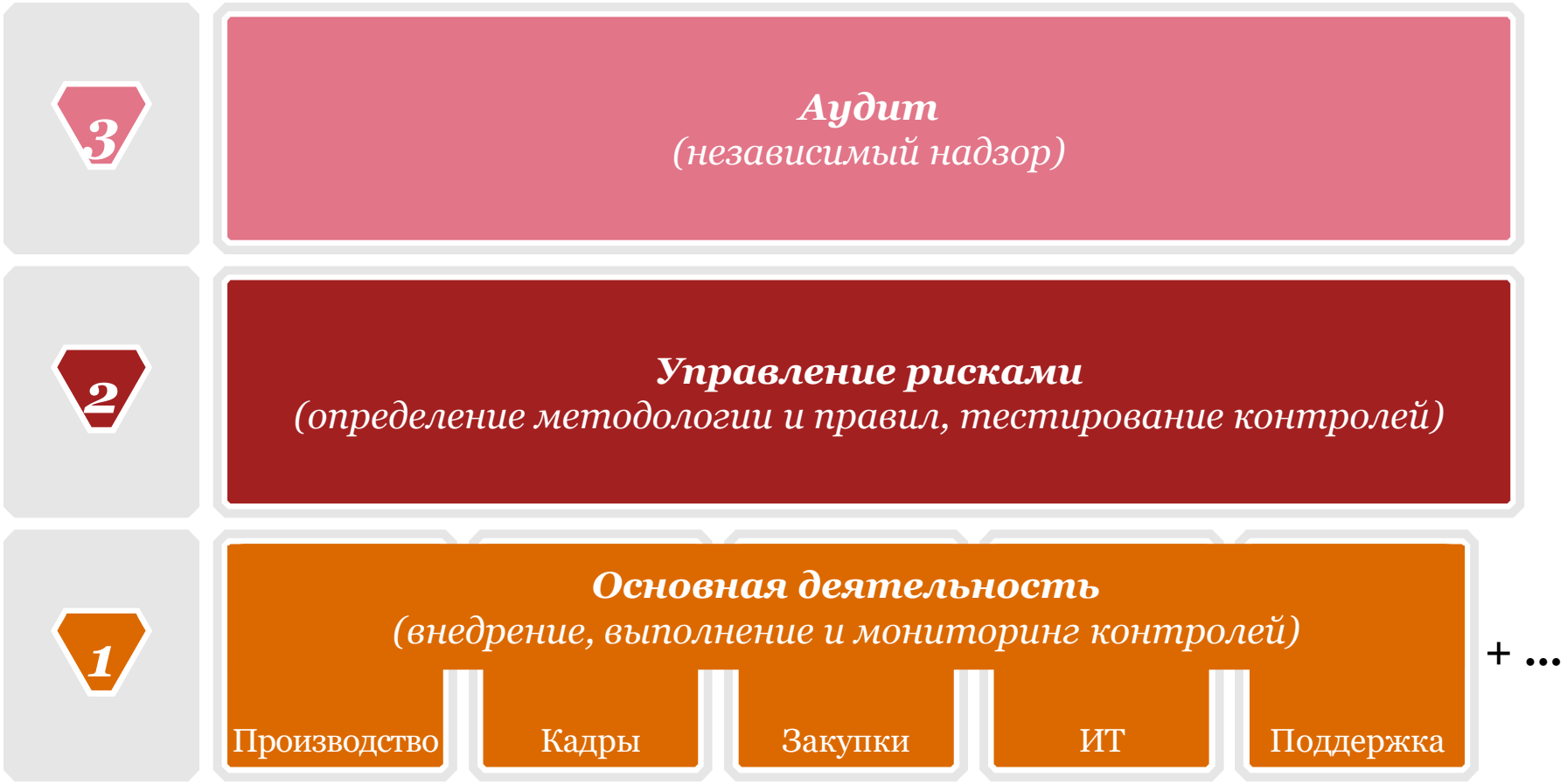
Преимущества от рискориентированного подхода

Управление киберрисками помогает компаниям задавать цели корпоративной программы кибербезопасности и оценивать ее прогресс

Киберриски в системе корпоративного управления

Кибер риски в системе управления корпоративными рисками

Три линии защиты в управлении рисками и контроле



Ожидания бизнеса от системы управления киберрисками

Ключевые аспекты успешного управления киберрисками

- Определены уровень допустимого риска и пороговые значения ущерба.
- Определен приемлемый остаточный риск и лимиты принятия рисков.
- Методика оценки рисков обеспечивает необходимую точность и финансовые значения оценки.
- Установлена прозрачная связь бизнес процессов и критичных активов.
- Новые роли и ответственность распределены между компетентными специалистами.
- Определены допустимые сроки закрытия выявленных рисков
- Определены ключевые индикаторы риска и установлен порядок мониторинга рисков.
- Определено положение киберрисков в системе корпоративного управления рисками.
- Уровни принятия решений соответствуют полномочиям лиц.
- Лица принимающие решения регулярно получают достоверную отчетность о киберрисках.

Управление киберрисками должно позволять

Стратегия

- оценивать влияние кибер угроз и трендов на развитие бизнеса,
- выбирать надежные и эффективные технологии,
- приоритизировать инвестиций в кибербезопасность,
- понимать возможные потери и выгоды.

Тактика

- приоритизировать инициативы кибербезопасности,
- фокусировать усилия на защите наиболее критичных активов,
- предотвращать нарушение деятельности и минимизировать ущерб.

Операции

- поддерживать киберриски на допустимом уровне,
- уверенно обрабатывать изменения и способствовать их внедрения,
- создавать надежные и защищенные продукты и решения.

Проекты

- получить дополнительные конкурентные преимущества,
- минимизировать появление новых угроз и рисков,
- получить пригодный для практического использования результат.

Вопросы?

Роман Чаплыгин

PwC, Директор,

Mob.: +7 (903) 272 1620
E-mail: roman.chaplygin@ru.pwc.com

PwC в России (www.pwc.ru) предоставляет услуги в области аудита и бизнес- консультирования, а также налоговые и юридические услуги компаниям разных отраслей. В офисах PwC в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре, Воронеже, Владикавказе и Уфе работают более 2 500 специалистов. Мы используем свои знания, богатый опыт и творческий подход для разработки практических советов и решений, открывающих новые перспективы для бизнеса.

Под «PwC» понимается сеть PwC и/или одна или несколько фирм, входящих в нее, каждая из которых является самостоятельным юридическим лицом. Глобальная сеть PwC объединяет более 208 000 сотрудников в 157 странах. Более подробная информация представлена на сайте www.pwc.ru/ru/about/structure.jhtml