CONFERENCES

ОЦЕНКА ЭФФЕКТИВНОСТИ И НАДЕЖНОСТИ СМИБ

ИВАНОВ ВЛАД
CISO
Health & Nutrition

Health & Nutrition сегодня

12 заводов

отвечающих самым современным стандартам качества и безопасности

#1

в производстве молочных продуктов

ТОП 5

среди лидеров пищевого сектора

> 5000

сотрудников

1 миллион

тонн сырого молока перерабатывается в год

ЧТО ТАКОЕ – ЭФФЕКТИНОСТЬ ИБ

«Эффективность – делать правильно. Результативность – делать правильные вещи.»

Питер Фердинанд Друкер

Самый влиятельный теоретик менеджмента в XX веке

Количественные метрики эффективности

- [ ] ROI не менее 1
- [ ] Реализованы технологии и процессы ИБ, обеспечивающих выполнение KPI бизнеса
- [ ] Соответствие сервисов ИБ заявленному SLA
- [ ] Удовлетворенность внутреннего клиента

КОЛИЧЕСТВЕННЫЙ АНАЛИЗ
РАСЧЕТ ROI

$$ROI = \frac{\text{Эффект мер ИБ} - TCO}{\text{Совокупные затраты ИБ } (TCO)}$$

3,26m €
Включено в доходную часть бизнес кейса от реализации мер ИБ

1,25
ROI ИБ в 2022 году

Расходы на ТП / подписки / годовые лицензии

HR расходы на сотрудников, сопровождающих данную систему

$$\textbf{TCO} = \text{ИБ OPEX} + \text{ИБ Depreciation} + \text{HR OPEX} + \text{IT costs}$$

CAPEX расходы на ПО/оборудование/разработку

Расходы на содержание системы в части ИТ инфраструктуры

$$\textbf{Эффективность меры ИБ x} = \sum_1^n \left((IR^n - RR^n) * \sum_1^n \left(\frac{\sum_1^{x^n} (SLE^n_{IR^{x^n}} * ARO^n_{IR^{x^n}} - SLE^n_{RR^{x^n}} * ARO^n_{RR^{x^n}})}{\sum_1^n (SLE^n_{IR} * ARO^n_{IR} - SLE^n_{RR} * ARO^n_{RR})} \right) \right)$$

x^n – число мер, закрывающих риск n

IR – присущий риск

RR – остаточный риск

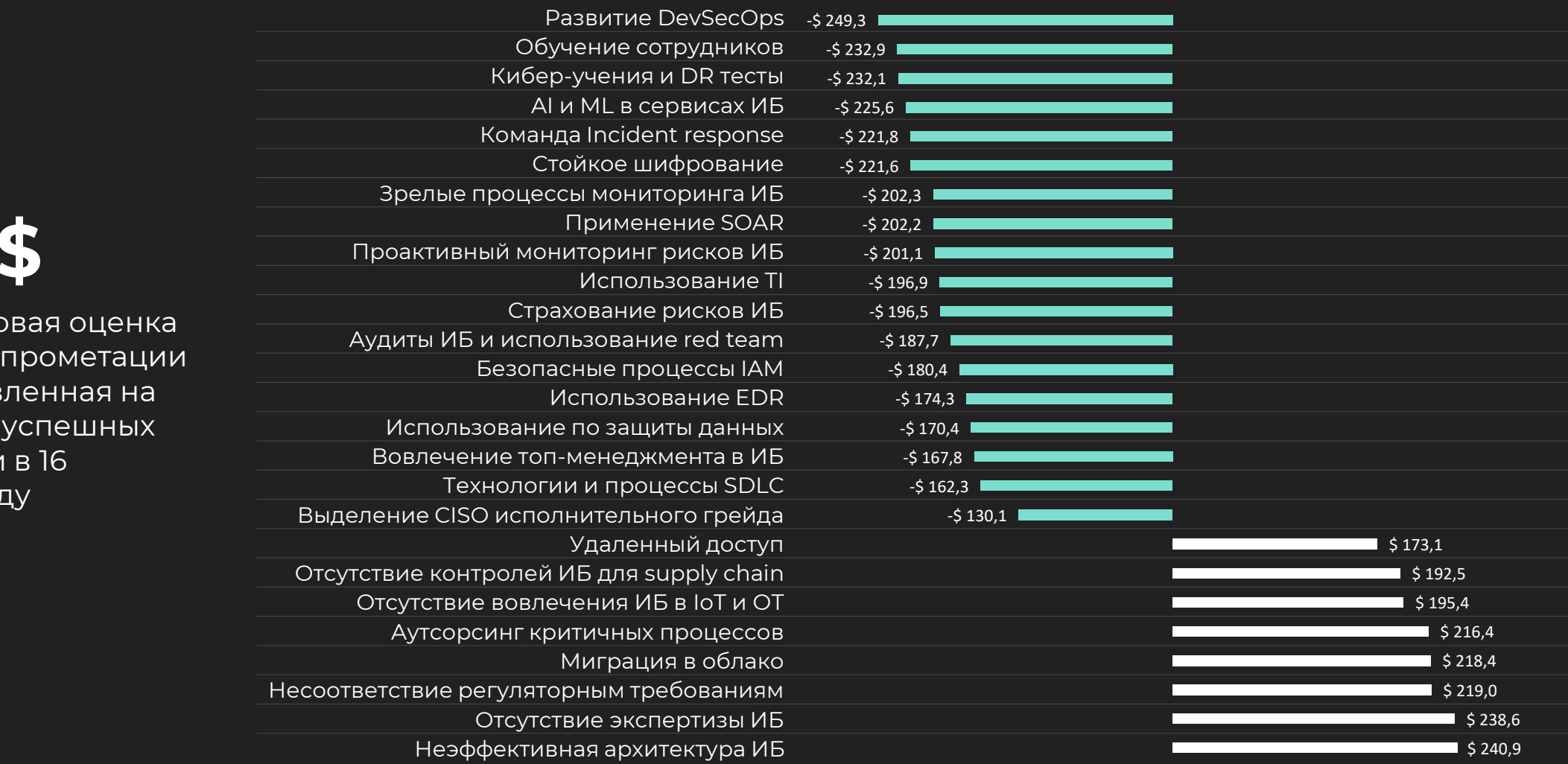
SLE – потери при реализации

ARO – число реализаций риска в год

КОЛИЧЕСТВЕННЫЙ АНАЛИЗ ЭФФЕКТИВНЫЕ КОНТРОЛИ ИБ

4,45M $

Средняя финансовая оценка последствий компрометации компании, составленная на базе анализа 553 успешных атак на компании в 16 странах в 2023 году



Источник: ibm.com

КЛЮЧЕВЫЕ МЕТРИКИ НАДЕЖНОСТИ СМИБ

CONFERENCES

- Mean Time to Detect (MTTD)

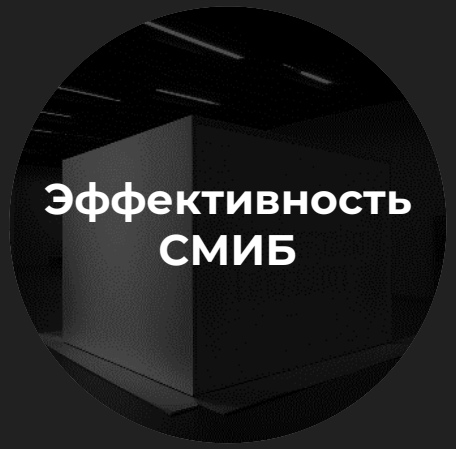
Время между регистрацией события и уведомлением L2

- Mean Time to Response (MTTR)

Время между уведомлением и подтверждением инцидента

- Mean Time to Contain (MTTC)

Время между подтверждением и устранением инцидента



- Среднее время простоя бизнес процессов из-за инцидента ИБ
- Средняя стоимость инцидента ИБ
- Процент систем с критичными уязвимостями / критичных систем с уязвимостями

- Процент сотрудников, прошедших обучение ИБ
- Результаты фишинговых тестов
- Оценка зрелости ИБ партнеров
- Число неподдерживаемых систем
- Число администраторов
- Время деактивации УЗ
- Результаты ARR

ПРИНЦИПЫ ПОСТРОЕНИЯ НАДЕЖНОЙ СМИБ

CONFERENCES

- **Регулярная оценка и приоритезация рисков**
  - Включение в отчетность компании оценки кибер-устойчивости
  - Составление карты ключевых партнеров и цепочек поставок
  - Регулярный пересмотр реестра рисков и статуса реализации мер
  - Ежегодная оценка рисков
  - Учет оценки рисков при формировании бюджета
- **Базовые контроли ИБ внедрены**
  - Оценка безопасности партнеров
  - Дорожная карта развития ИБ
  - Подход “минимальных привилегий”
  - Ежеквартальный отчет менеджменту о статусе KPI
  - Определены минимальные требования к проектам и технологиям
- **Встраивание концепции кибер-устойчивости в бизнес-стратегию**
  - Определены зоны ответственности за кибер-устойчивость
  - Разработана стратегия ИБ с концептом кибер-устойчивости
  - Назначен CISO
  - Назначен ответственный за ИБ в органе управления
  - Проводятся регулярные бенчмарки по ИБ
- **Контроли ИБ поддерживают реализацию бизнес-стратегии**
  - Аудит и тестирования кибер-устойчивости
  - Отслеживание актуальных угроз и их реализаций на рынке
  - Прогнозирование угроз (черные лебеди / серые носороги)
  - Встраивание технологий ИБ в бизнес продукты
  - Контроль актуальности / достоверности отчетности
- **Развивать культуру сотрудников**
  - Включение в общие KPI метрик ИБ
  - Обязательное обучение ИБ для всех сотрудников
  - Демонстрирование руководителями культуры ИБ
  - Сертификация ИБ для критичных ролей
  - Состояние ИБ регулярно доносится до всех сотрудников
  - Контроль инсайдера, анализ и работа с мотивацией
  - Удобство для пользователя механизмов ИБ

ИБ КАК ДВИГАТЕЛЬ РАЗВИТИЯ

CONFERENCES

Контроль запросов (prompt) к AI

Маскирование данных для обучения

Классификация результатов и контроль доступа к выводу AI

AI

Безопасность ключей и алгоритмов

Безопасность алгоритмов и смарт-контрактов

Безопасность узла сети и интерфейсов

Блокчейн

Предотвращение недопустимых событий

Безопасность партнеров

DRP/BCP тестирования

Устойчивость и развитие

ESG

Защита данных как социальная ответственность

Регуляторное соответствие как вектор устойчивого управления компанией

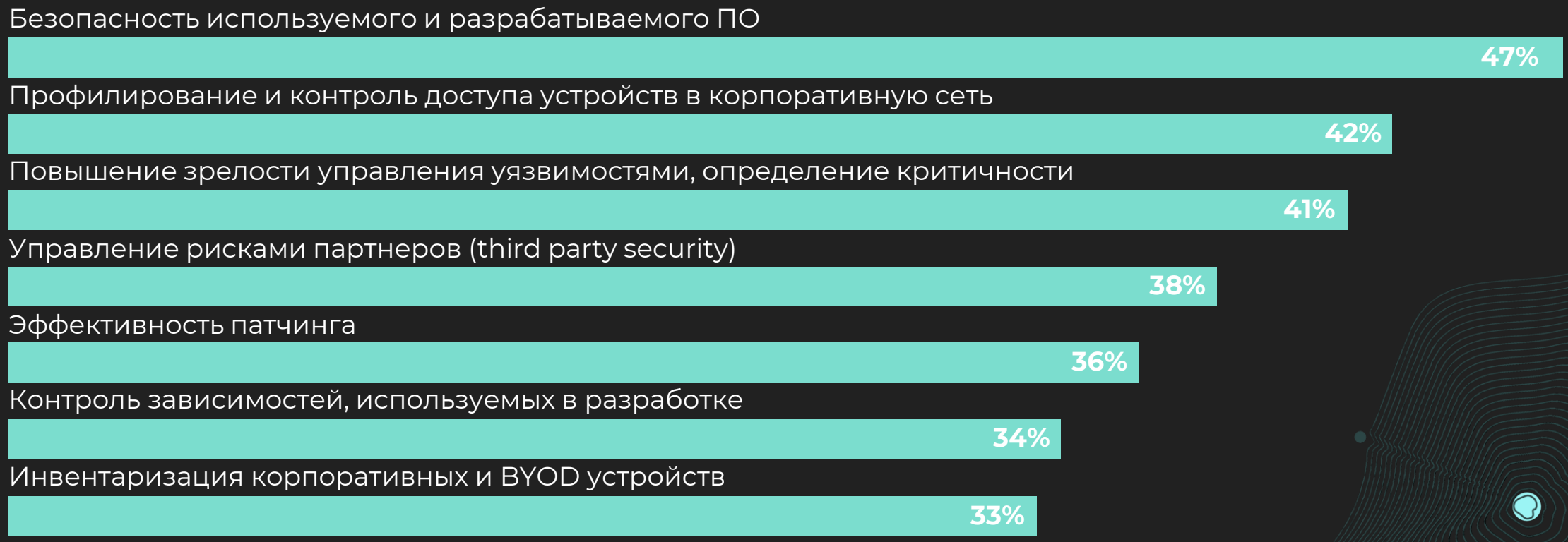
Удаленная работа и продажи

VPN или технологии УД

Контроль активности пользователей и эффективности сотрудников

Управление API

НА ЧЕМ СДЕЛАТЬ АКЦЕНТ В 2025 ГОДУ



Источник: ivanti.com

CONFERENCES

СПАСИБО ЗА ВНИМАНИЕ!

Иванов Влад
vladislav.ivanov@corphn.com