CNews FORUM

CNews FORUM Кейсы
Опыт ИТ-лидеров

КАК **ОПТИМИЗИРОВАТЬ** ЗАТРАТЫ НА ИБ

Влад Иванов

Специализация

- Информационная безопасность
- Стратегия ИБ
- Управление рисками ИБ
- Оценка эффективности
- Предприниматель

Карьера

CISO Health & Nutrition (ранее Danone)

Руководитель BISO в Росбанк

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 в России

1 миллион

тонн сырого молока перерабатывается в год

Ваши затраты на ИБ больше, чем вы считаете

CAPEX расходы на ПО/оборудование/разработку

TCO = ИБ OPEX + ИБ Depreciation + ИБ HR OPEX

Расходы на ТП / подписки / годовые лицензии

HR расходы на сотрудников, сопровождающих данную систему

Ваши затраты на ИБ больше, чем вы считаете

CAPEX расходы на ПО/оборудование/разработку

Непрямые затраты на ИБ, входящие в бюджет ИТ или бизнеса

TCO = ИБ OPEX + ИБ Depreciation + ИБ HR OPEX + non direct ИБ costs

Расходы на ТП / подписки / годовые лицензии

HR расходы на сотрудников, сопровождающих данную систему

Примеры непрямых затрат на ИБ

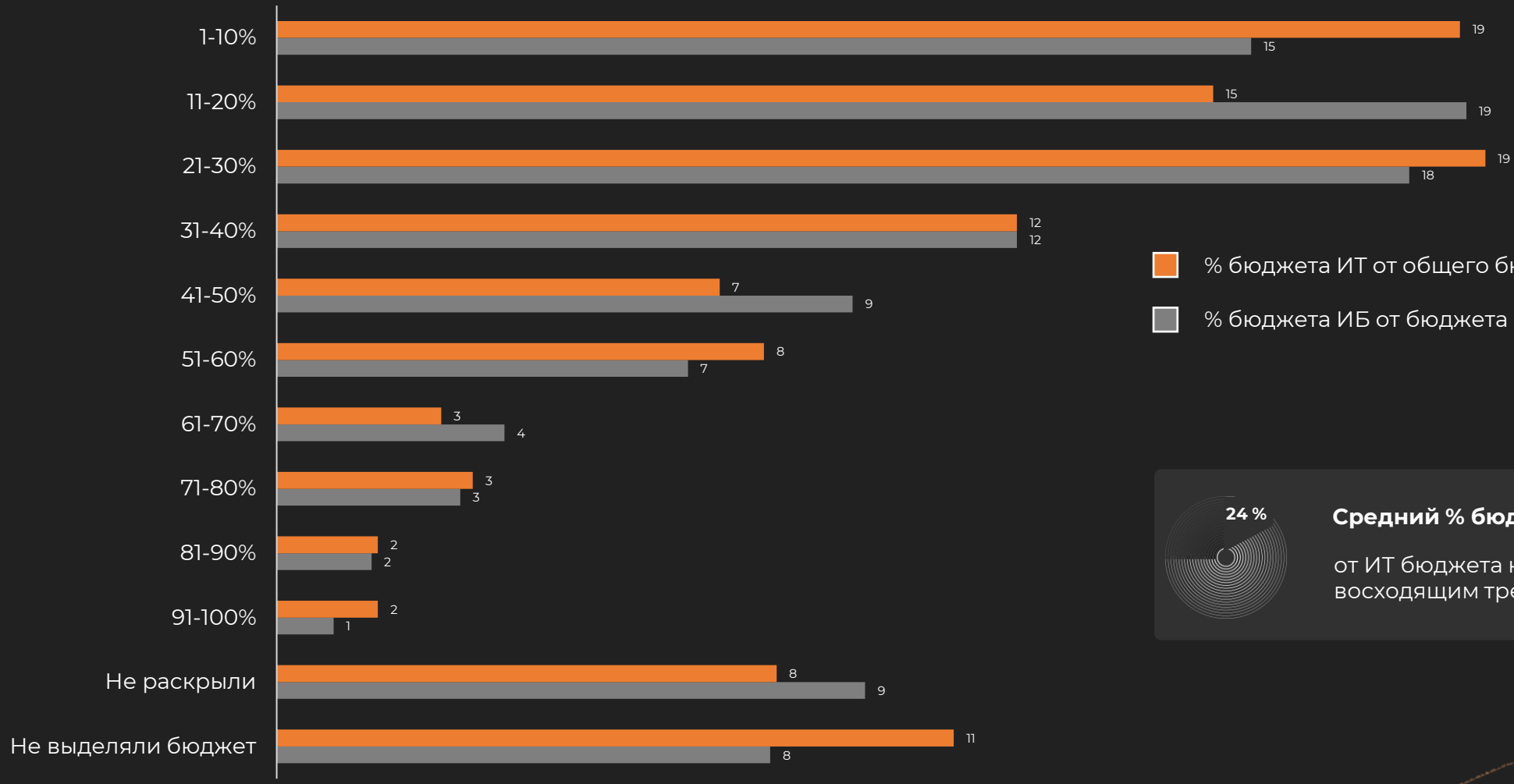
ИТ инфраструктура для ИБ

Рост стоимости ИТ сервисов из-за необходимости учесть нагрузку сервисов ИБ

Необходимость выделения ресурсов в ИТ и бизнесе для учета требований при дизайне и реализации сервисов / продуктов

Увеличение операционной нагрузки на сотрудников и снижение TTM / CSI из-за ограничений ИБ

Структура ИТ и ИБ затрат у других в 2023



Средний % бюджета ИБ в 2023 году

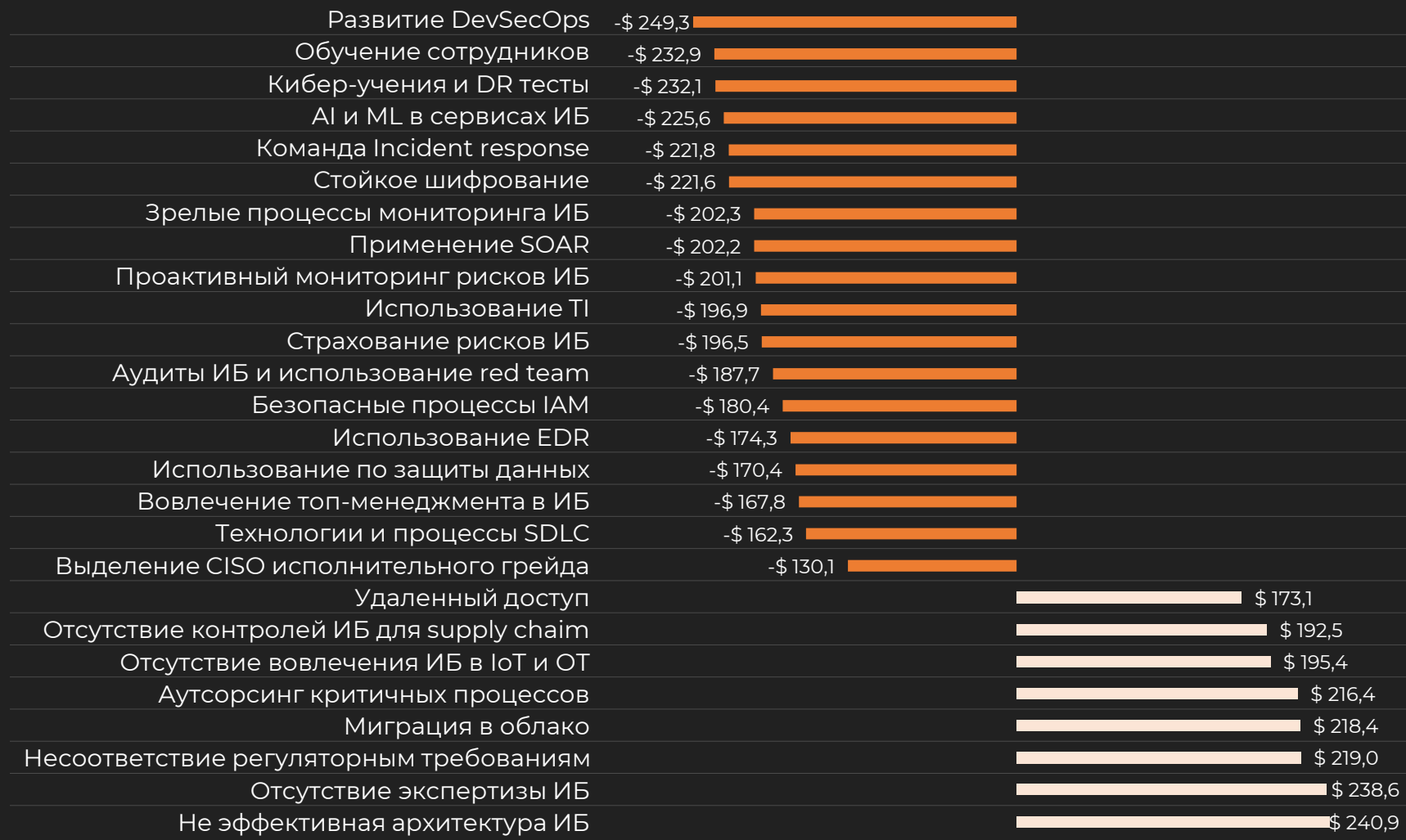
от ИТ бюджета компании, с восходящим трендом 21-27% за 3 года

Источник: nordlayer.com

Способ 1
Инвестировать, исходя из эффективности

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

Способ 1
Расчет эффективности ИБ

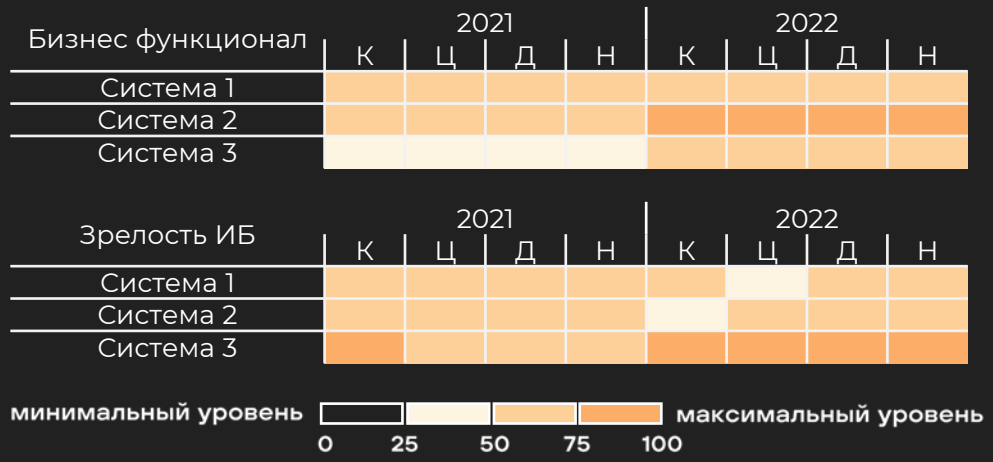
Эффективность меры ИБ x $= \sum_1^n \left((IR^n - RR^n) * \sum_1^n \left(\frac{\sum_1^{x^n} (SLE^n_{IRx^n} * ARO^n_{IRx^n} - SLE^n_{RRx^n} * ARO^n_{RRx^n})}{\sum_1^n (SLE^n_{IR} * ARO^n_{IR} - SLE^n_{RR} * ARO^n_{RR})} \right) \right)$

Расчет IR/RR $= \sum_1^n (1 - \text{Зрелость ИБ}) * \text{функционал}) * \text{медиана}\, IR^n/RR^n)$

1,25
ROI ИБ в 2022 году

3,26m €
Cost avoidance, включенный в БК проекта трансформации

Последствия	Тип риска ИБ	Infra Vuln	NetSec	AMW	Monitoring	Regulatory	Внешний инцидент
€ 14,4 m	Ц						https://www.cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF
€ 6,21 m	К						https://www.bankinfosecurity.com/bec-scam-costs-trading-firm-virtu-financial-69-million-a-14804
€ 0,9 m	Д						https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide
€ 450 m	Н						https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf



x^n – число мер, закрывающих риск n

IR – присущий риск

RR – остаточный риск

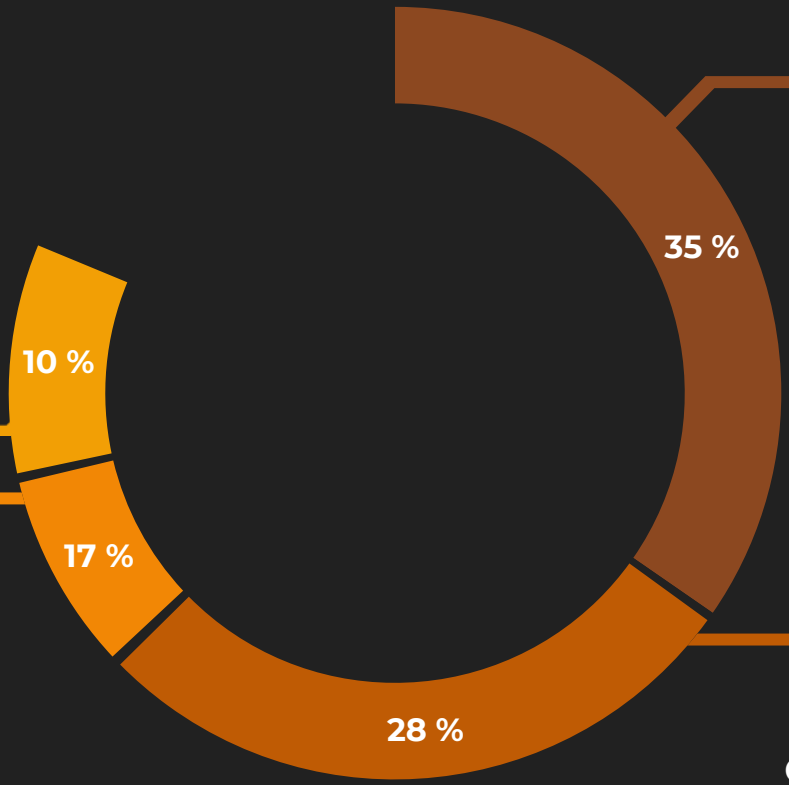
SLE – потери при реализации

ARO – число реализаций риска в год

Способ 2
“Закрывать” ключевые вектора атак

Перебор паролей

и кража учетных записей сотрудников за счет bruteforce или password spraying, возможных из-за ***уязвимых механизмов управления доступом***



Выполнение действий пользователем

путем заражения компании вредоносным ПО или применения атакующими социальной инженерии против ***сотрудников, партнеров, аутстафферов***

Компрометация публичных сервисов

за счет эксплуатации уязвимостей ***доступных из Интернета приложений***, баз данных и иных ресурсов

Модификация или отключение решений ИБ

реализуемая за счет ***некорректной конфигурации или архитектуры СЗИ***

Источник: jetcsirt.su

Способ 3
Работать с недопустимыми событиями

Внешний контекст

5 **КОМПАНИЙ FMCG**
в России за 6 месяцев компрометированы с использованием ransomware

Внутренний контекст

160 **ИНЦИДЕНТОВ**
в день обрабатывает команда ИБ

2 **УСПЕШНЫЕ АТАКИ**
обе локализованы в течении 2х часов без ущерба для компании

Оценка последствий

Атакованная компания	Объект оценки	Применимость
• Восстановление операционной деятельности > 5 дней, полная остановка бизнес процессов	• “X” млн р потерь в продажах за 5 дней • “Y” млн р потерь в “живом” молоке	• BCP только для критичных систем • Среднее покрытие антивирусом – ‘x’% • Среднее покрытие EDR – ‘y’%
• Отсутствие уведомления Роскомнадзора об утечке • Инцидент в КИИ	• Внеплановый аудит • Контроль соответствия 250-У	• Плейбуки ИБ в процессе согласования • Предотвращение утечек за счет компенсирующих мер • Реализация требований 250-У в процессе
• Публикация в государственных и региональных СМИ	• Потеря ключевых партнеров в связи с нарушением NDA	• CPT и brand protection в процессе реализации

Способ 4
Снижать непрямые затраты

Наши контакты и вакансии

hnrus.com

IT_Security@corphn.com