УПРАВЛЕНИЕ

РИСКАМИ И ЭФФЕКТИВНОСТЬЮ

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Health & Nutrition сегодня

12 заводов

отвечающих самым современным стандартам качества и безопасности

#1

в производстве молочных продуктов

ТОП 5

среди лидеров пищевого сектора

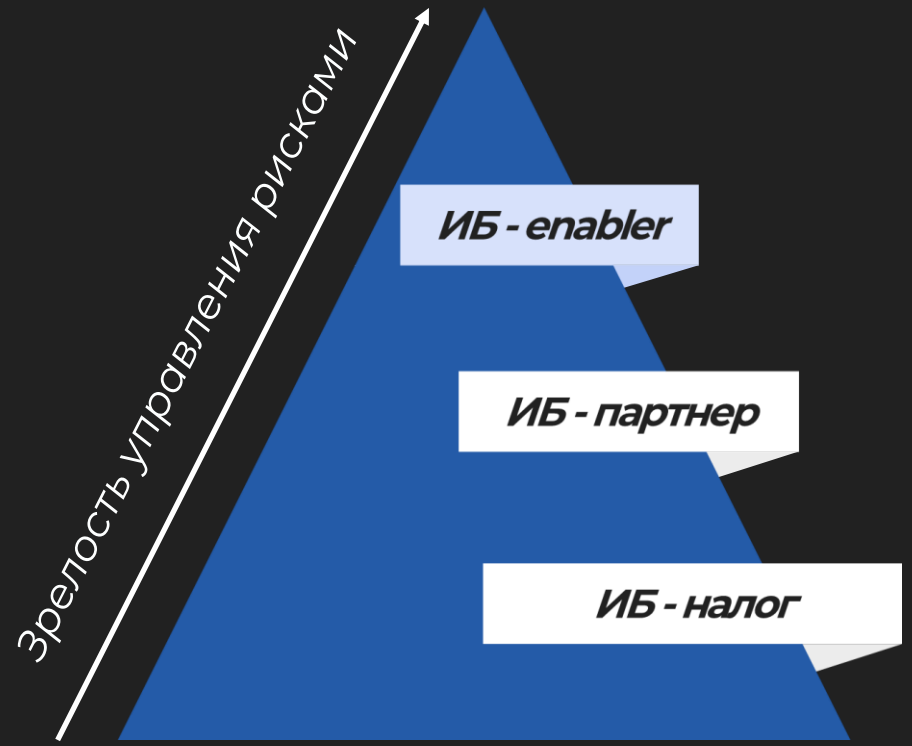
> 5000

сотрудников в России

1 миллион

тонн сырого молока перерабатывается в год

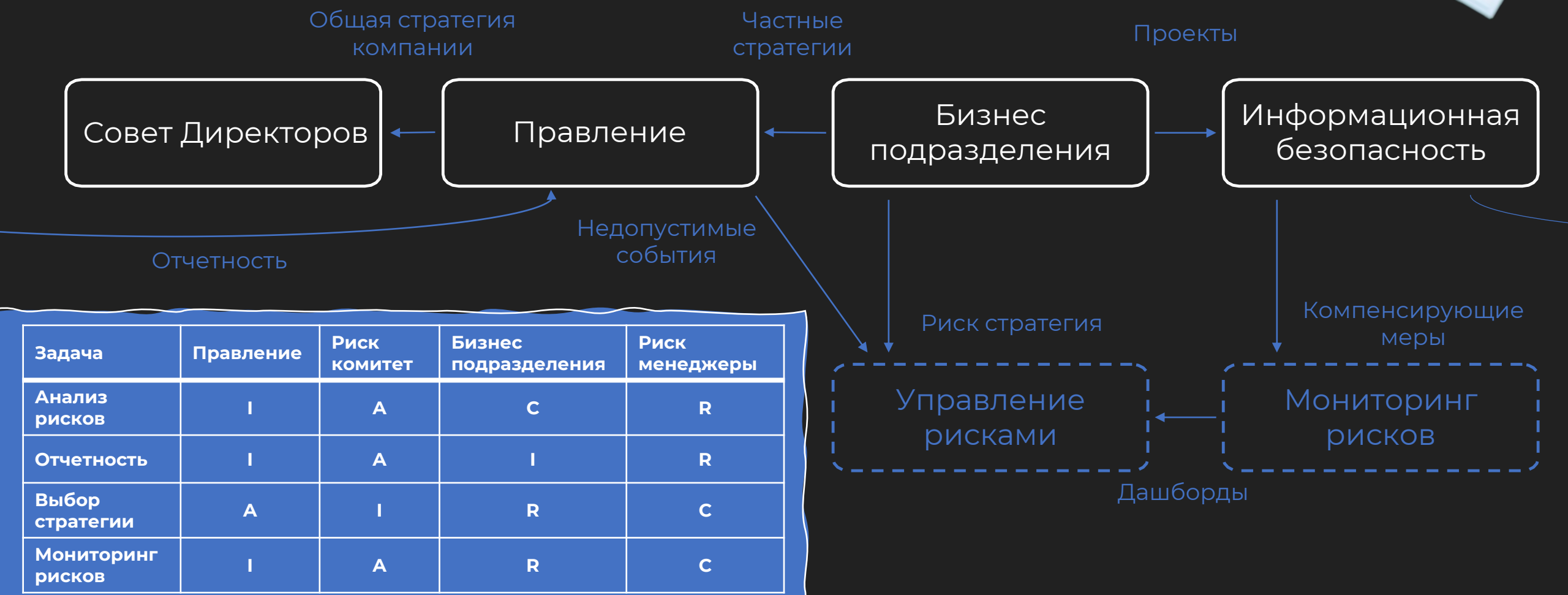
Риски ИБ как драйвер развития функции



Что дает зрелый процесс управления рисками

- Не приходиться латать на последней миле корабль, который идет быстро, но на дно
- Знаем, что значит “кенгуру”
- Существенно меньше споров о бюджете ИБ
- Можем не только тратить, но и зарабатывать

Как инкорпорировать управление рисками ИБ



Задача	Правление	Риск комитет	Бизнес подразделения	Риск менеджеры
Анализ рисков	I	A	C	R
Отчетность	I	A	I	R
Выбор стратегии	A	I	R	C
Мониторинг рисков	I	A	R	C

Методика анализа рисков – процедура оценки

Факторы риска	Угрозы	Объект оценки	Уязвимости	Риск
Внешний контекст • Геополитика • Рынок • Регуляторы • Развитие технологий	Нелегитимный доступ	Сотрудники / аутстафферы	ИТ уязвимости (Infra/OS/APP/DB /Network/Architecture)	Стратегический
Внутренний контекст • Стратегия бизнеса • Ценность ИТ и ИБ • Операционная модель	Недоступность	Процессы	Зависимость компании от поставщиков	Финансовый
Зрелость управления рисками	Нарушение целостности	Инфраструктура	Зависимость от экономической или политической ситуации	Операционный
Зрелость ИТ и ИБ • Мониторинг • Эффективность • Компетенции • Ресурсы	Дополнительный финансовые обязательства	Информация	Появление новых технологий	Регуляторный
	Несоответствие результата бизнес целям (объем, качество, сроки)	Приложения	Зависимость от регуляторных требований	Экологический
	Репутационные потери	Проекты	Низкая операционная культура	
		Компании		

Методика анализа рисков – реестр рисков

Результат оценки				
Категория риска	Утечка информации	Недоступность	Фрод / кибер-преступления	Несоответствие требованиям
Владелец риска				
Дата оценки риска				
Дата согласования оценки				
Категория риска				
Оценка риска	Низкий	Средний	Высокий	Критический
Решение	Принять	Передать	Снизить	Избежать
Оценка риска				
Резюме сценария				
Фактор риска				
Угроза				
Объект оценки				
Уязвимость				
Частота реализации (в год)	<0,01	<0,1	<1	<10
Финансовые последствия	<0,25% EBITDA	<1% EBITDA	<5% EBITDA	>5% EBITDA
Операционные последствия	Несущественная задержка в процессах	Недоступность чувствительных процессах, устраняемая в короткий срок	Среднесрочная приостановка деятельность, требующая существенных ресурсов	Приостановка критических бизнес процессов
Регуляторные последствия	Нет влияния на регуляторное соответвтие	Несоответствие не критичное, влияние на сроки аудита	Несоответствие, приводящее к штрафам или мониторингу	Несоответствие, приводящее к отзыву лицензии или приостановке деятельности
Влияния на имидж	Незначительные публикации, не требующие ответных действий	Публикации в локальных СМИ, жалобы со стороны не ключевых клиентов	Публикации в государственных СМИ, жалобы со стороны ключевых клиентов	Публикации в основных государственных СМИ, потеря ключевых клиентов
Влияние на клиентов (CSI)	<5%	<10%	<20%	>20%
Влияние на стратегию	Незначительное влияние на не стратегические проекты	Краткосрочное влияние на стратегические проекты, требующее незначительных ресурсов для достижения KSI	Среднесрочное влияние на стратегические проекты, требующее вовлечение топ-менеджеров для достижения KSI	Устойчивая и долгосрочная дезорганизация, невозможность выполнить стратегические цели

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

Способ 1
Как посчитать эффективность ИБ

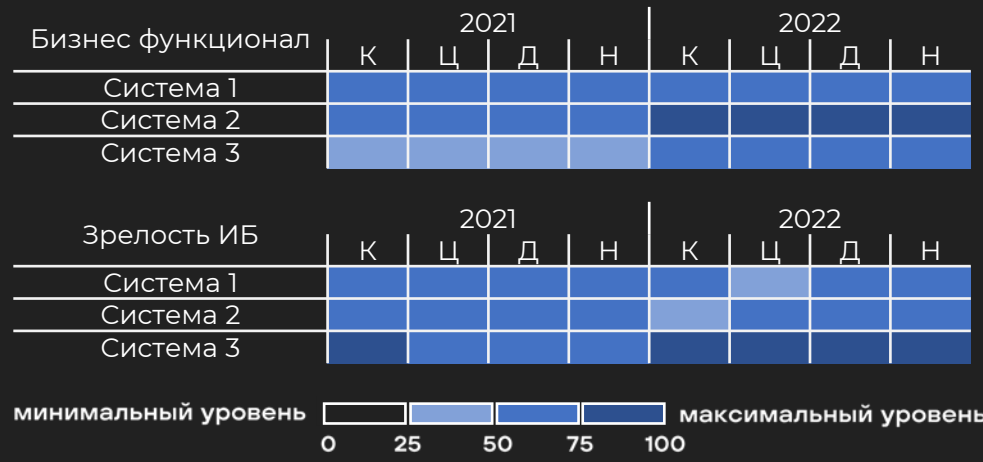
Эффективность меры ИБ x $= \sum_1^n \left((IR^n - RR^n) * \sum_1^n \left(\frac{\sum_1^{x^n} (SLE^n_{IRx^n} * ARO^n_{IRx^n} - SLE^n_{RRx^n} * ARO^n_{RRx^n})}{\sum_1^n (SLE^n_{IR} * ARO^n_{IR} - SLE^n_{RR} * ARO^n_{RR})} \right) \right)$

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

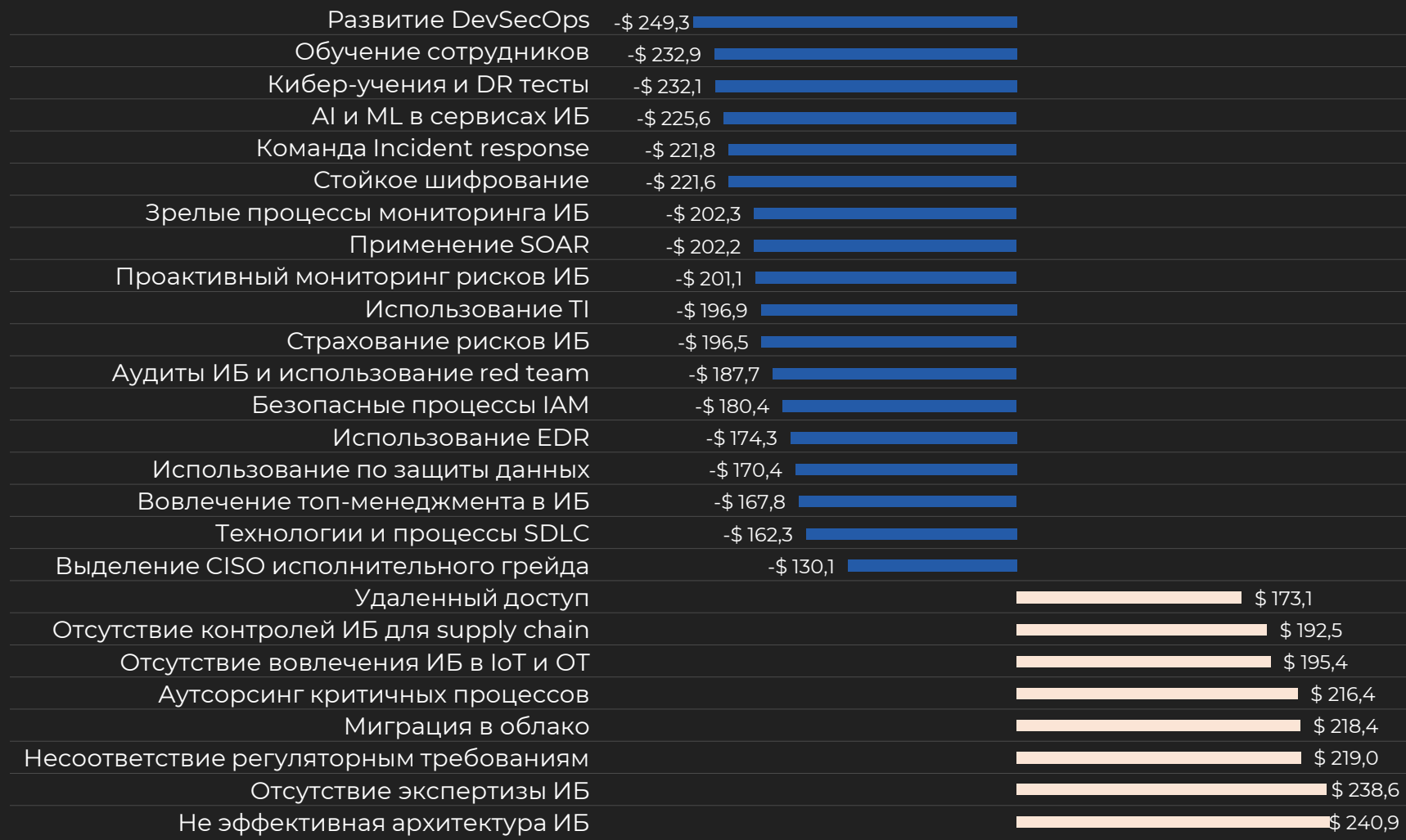
SLE – потери при реализации

ARO – число реализаций риска в год

Способ 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

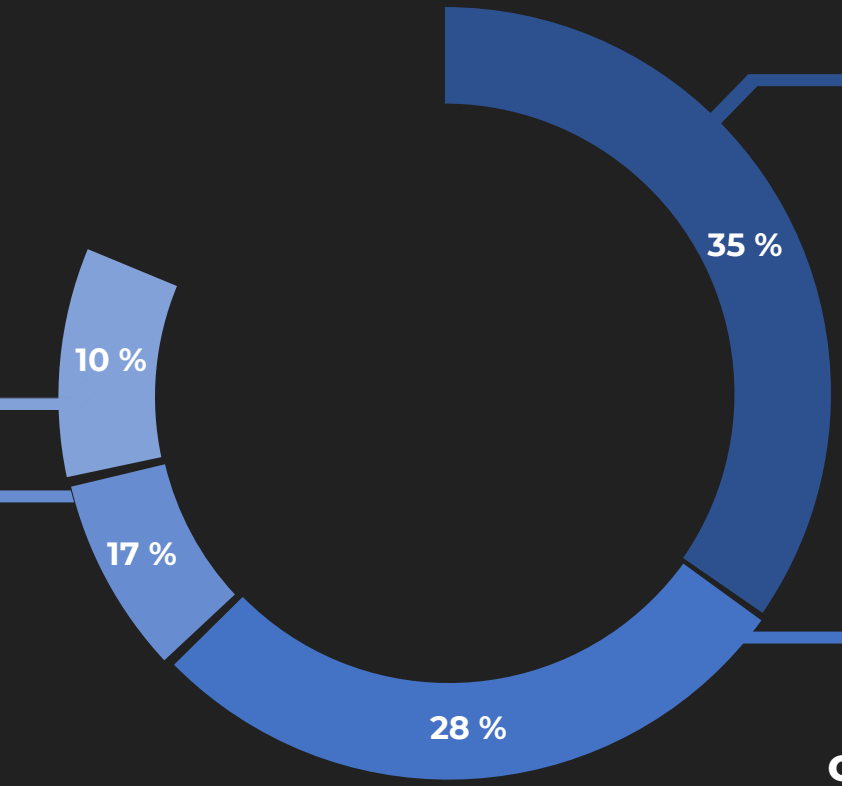
Способ 2
“Закрывать” ключевые вектора атак

Перебор паролей

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

Компрометация публичных сервисов

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



Выполнение действий пользователем

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

Модификация или отключение решений ИБ

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

Источник: jetcsirt.su

Способ 3
Работать с недопустимыми событиями

Внешний контекст

>10 **КОМПАНИЙ FMCG**
в России за 2024 год компрометированы с использованием ransomware

Внутренний контекст

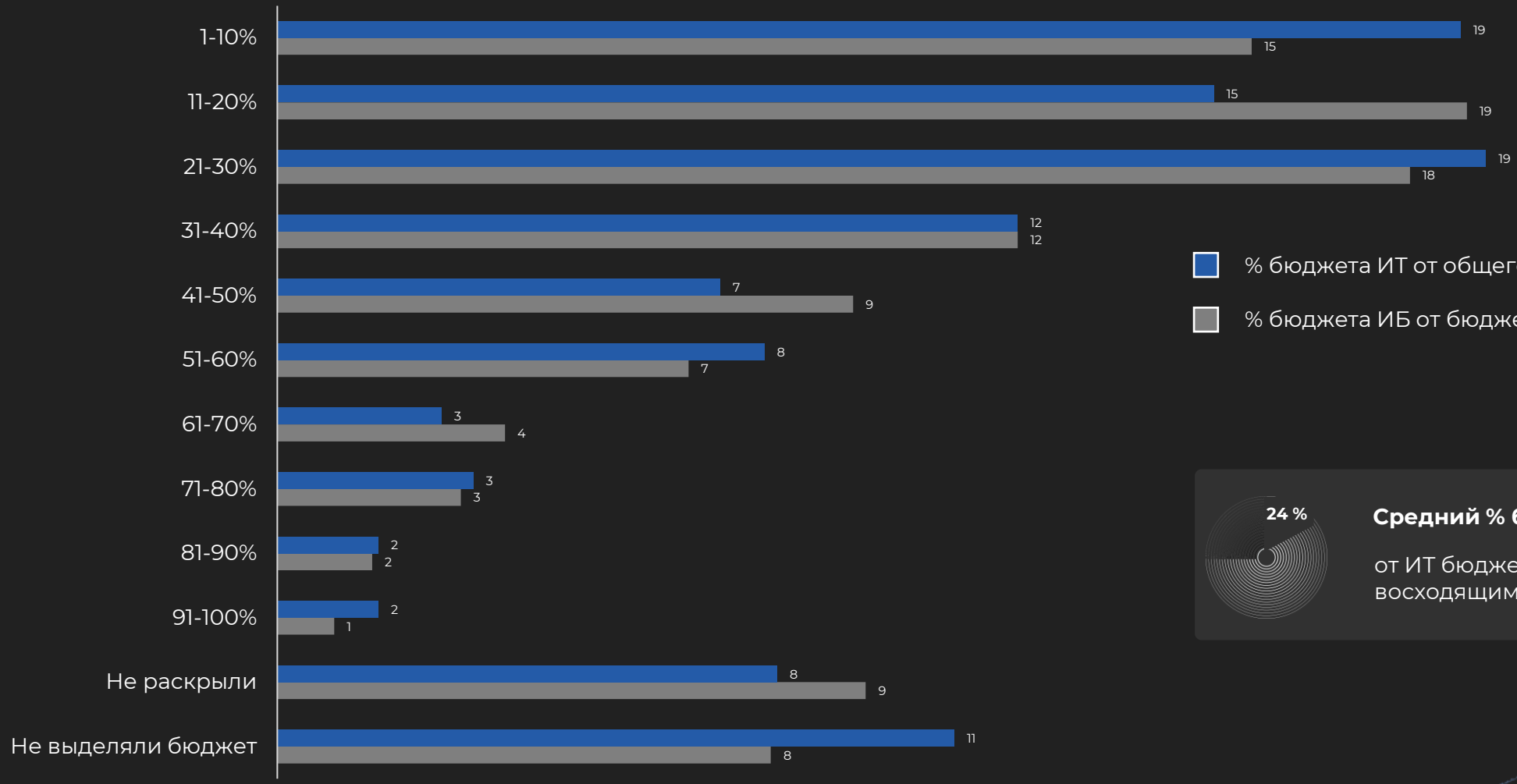
160 **ИНЦИДЕНТОВ**
в день обрабатывает команда ИБ

4 **УСПЕШНЫЕ АТАКИ**
все 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

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

Наши контакты и вакансии

hnrus.com

IT_Security@corphn.com