ЗАЩИТА ДАННЫХ

СОХРАНИТЬ ВСЁ

Экономика защиты данных

Дмитрий Шепелявый,
Технологии Доверия

Переход на экономические показатели эффективности ИБ обусловлены повышением влияния ИБ на бизнес

Драйверы

Прямые требования руководства компании

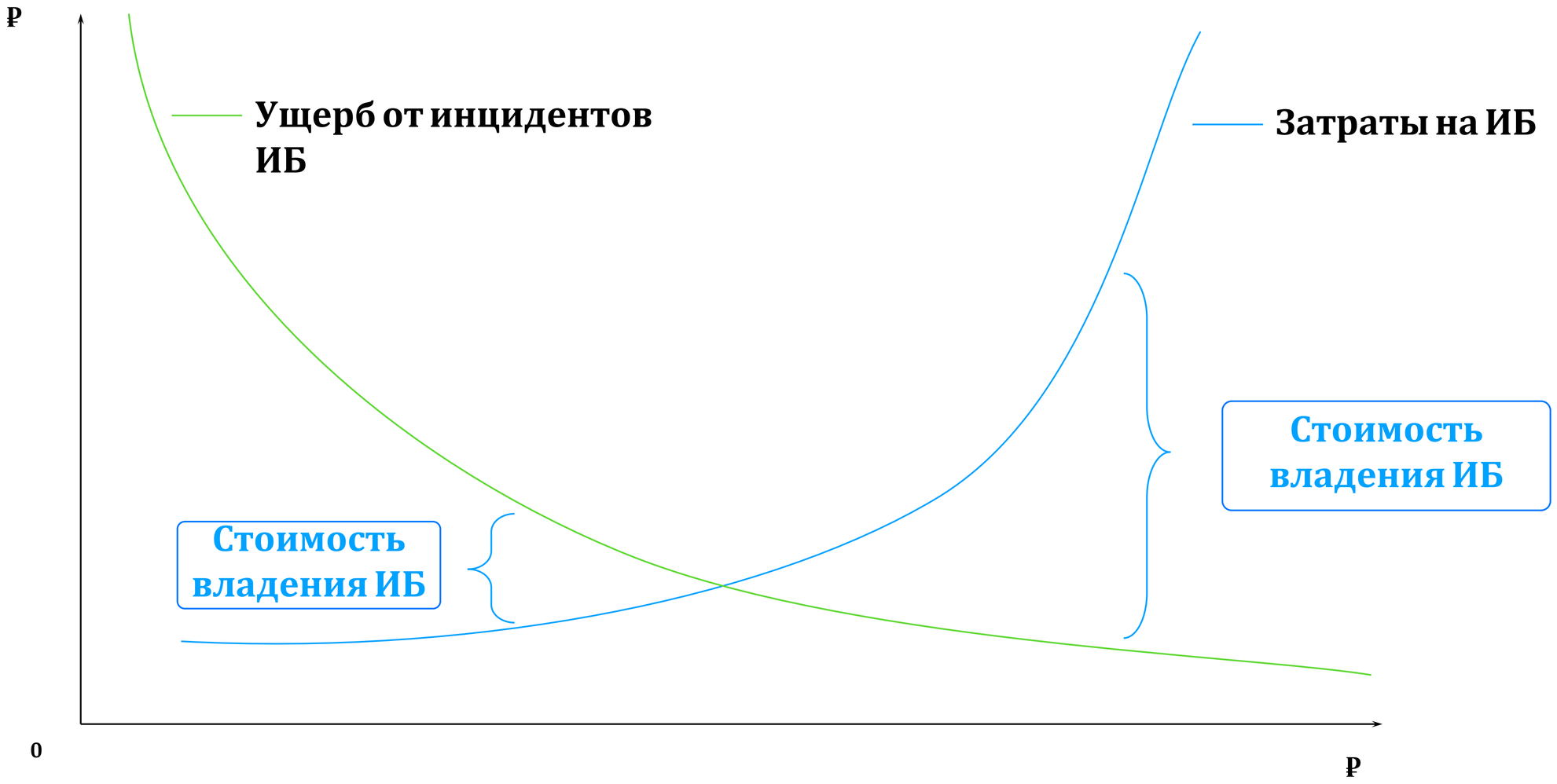
Инвестиции в ИБ ничем не отличаются от прочих инвестиций и требуют аналогичных показателей отдачи

Слабая интегрированность процесса управления киберрисками в процесс управления рисками операционной деятельности

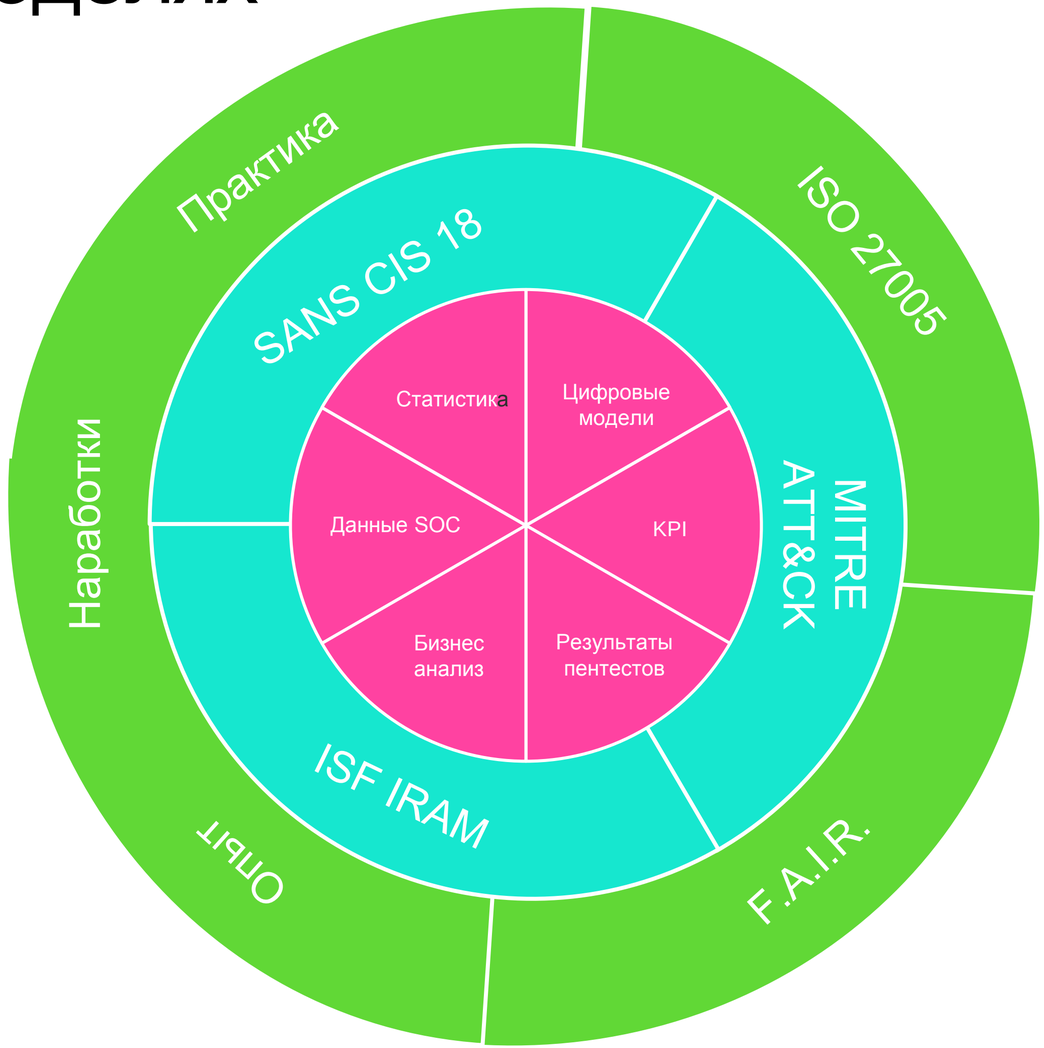
Низкая зрелость отчетности о профиле киберрисков и эффективности контрольной среды

Сложность оценки реальности направленных на нас угроз и достаточности имеющегося уровня защиты

Финансовая задача — найти точку оптимальной стоимости владения ИБ



Подход к управлению ИБ на базе экономических показателей должен базироваться на стандартах и математических моделях

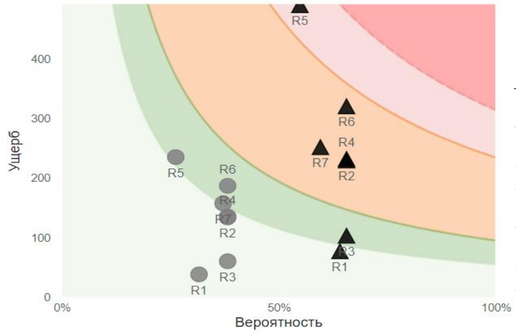


Использование международно признанных методик и стандартов позволяет построить надежный фундамент процесса, дополняя их наработанной практикой и опытом, применимым для российских условий.

- FAIR (Factor Analysis of Information Risk) – методика Value at Risk (VaR), применяемой для моделирования финансовых рисков, адаптированная FAIR Institute для процесса количественной оценки киберрисков. Методика формирует единый подход к управлению киберриском, подходящий как для управляющих менеджеров, так и для сотрудников ИТ и ИБ, позволяя измерять, управлять и создавать отчетность по профилю киберриска.
- ISO 27005 – ключевой компонент серии ISO27000, являющейся международным стандартом по построению СУИБ. Стандарт отписывает лучшую практику дизайна, построения и применения процесса управления киберрисками в организациях любого масштаба.
- SANS CIS18 – методика, разработанная SANS Institute, позволяющая оценивать архитектуру и зрелость компонентов контрольной среды ИБ, выстраивая мост между управляющими фреймворками уровня ISO 27000 и NIST. CIS18 позволяет организациям оценивать киберустойчивость, выявляя наиболее слабые компоненты контрольной среды в триаде «люди, процессы, технологии».
- MITRE ATT&CK – регулярно обновляемый сборник техник и тактик, применяемых реальными агентами киберугрозы. ATT&CK применяется, как общепризнанная база знаний, для разработки моделей угроз и моделирования кибератак.

Процесс управления экономическими показателями ИБ должен быть наглядным и прозрачным для всех участников

Профиль киберриска (executive)



Среднегодовой ожидаемый ущерб (ALE), млн. руб.	Риск аппетит
76.95	✓
229.76	✗
103.06	✓
232.39	✗
491.27	✗
321.01	✗
252.22	✗

Приборная панель демонстрирующая профиль киберриска и динамику его снижения для управляющего звена и директоров

Профиль киберриска (executive)

Метрики площади атаки

Персонал	Привилегированные пользователи	Сотрудники с удаленным доступом	Клиенты системы онлайн платежей
	12,000 ▲	170,000 ▼	100,000 ▼
Пртнеры	Партнеры с доступом к нашим сетям	Партнеры по обмену данными	Программные модули 3х лиц
	150 ▲	800 ▲	50,000 ▲
Системы	Критичные приложения	Приложения доступные из Интернет	Рабочие ставери	Системы снятые с поддержки	IoT (Периферия)
	700 ▲	100 ▲	75,320 ▲	10,000 ▲	20,630 ▲
Облако	Управляемые облачные системы	Используемые облачные сервисы	
	300 ▲	90 ▲	
Данные	User Identity and Credential Repositories	Хранилища критичных данных	Аккаунты в социальных сетях
	1,000 ▲	5,000 ▲	100 ▲
Сети	Пограничные устройства (gateways)	Беспроводные точки доступа	Каналы передачи данных
	55 ▲	1,009,583 ▲	70 ▲

Баланс технологического долга

Эффективность контрольной среды ИБ

Capability	Type	Status	Metrics	Effective ness	Coverage
Аутентификация и автори…	P	11.8%	% внешних критических приложений с много…	12.0% ▼	98.0% ▲
Безопасное подключение…	P	37.0%	% подключений удаленного доступа пользов…	77.0% ▼	48.0% ▲
Безопасное удаление да…	P	15.0%	% больших объектов (LoB), у которых есть ут…	94.0% ▲	16.0% ▼
Безопасность приложени…	P	10.7%	% новых приложений, переведенных на инте…	11.0% ▼	97.0% ▲
Защита конечных точек	P	36.0%	% конечных точек с установленным решение…	80.0% ▼	45.0% ---
Защита от DDoS-атак	P	36.3%	% критически важных внешних систем, защит…	79.0% ▼	46.0% ▼
Культура безопасности и …	P	90.0%	% людей, которые не прошли более одного …	90.0% ▲	100.0% ▲
Предотвращение потери …	P	7.6%	% пользователей, использующих средства у…	8.0% ▼	95.0% ▲
Сетевая безопасность (вк…	P	13.0%	% производственных систем (приложений), п…	93.0% ▼	14.0% ▼

Комплексное представление о площади атаки и эффективности контрольной среды ИБ (метрики)

Профиль киберриска (executive)

Risk Posture
How well are we securing ourselves?

Reset

Enterprise Residual Cyber Risk

Accidental Leakage of Customer Information	Theft of Confidential Business Information	Theft of Customer Information	Disruption to Business Operations	Disruption to Online Services	Theft of Funds	Loss of Digital Trust
H Trend: ▲	H Trend: ---	M Trend: ---	H Trend: ---	H Trend: ---	H Trend: ---	M Trend: ---

Threat Exposure

Threat Category	Exposure	Prevent	Detect/ Correct
Accidental Insider Leak	H ▲	2.0	3.2
External Cyber Attack	M ▲	2.0	1.9
Malicious Insider Cyber Attack	H ▲	1.8	1.9
Supply Chain Compromise	M ▲	2.2	1.9
Denial of Service Attack	H ▲	2.1	1.9
External Information Manipulation	M ▼	2.3	2.4
Customer Compromise	H ▲	1.8	3.1

Key Capabilities

Ref	Capability	Type	Current (Maturity)	Current (Derived)	Target (Maturity)	Metrics	Effective ness	Coverage
ASM.2	Vulnerability Management …	P	3.0	3.3	4.0	% of open critical vulnerabilities identified more than 30 days old	7.0% ▼	90.0% ▼
ASM.3	AppSec / DevSecOps (SA…	P	2.0	1.5	4.0	% of new apps promoted into live pen tested with all sec findings fixed	75.0% ---	70.0% ▲
ASM.4	Asset Management (Attack…	P	2.0	1.5	4.0	% of endpoints not in the asset inventory	10.0% ▲	73.0% ▼
IAM.1	Privileged Access Manage…	P	2.0	1.5	4.0	% privileged accounts on boarded into PAM solution with regular passwor…	92.0% ▲	61.0% ▼
IAM.2	Identity Governance	P	2.0	1.3	4.0	% of critical apps where all access is certified at least every 6 months	90.0% ---	54.0% ▲
IAM.3	Authentication & Authorisat…	P	2.0	1.3	3.5	% of externally facing critical apps with multi-factor authentication	87.0% ▲	43.0% ▼
IIP.1	Data Loss Prevention	P	2.0	1.3	4.0	% of user endpoints with DLP solution installed	96.0% ---	36.0% ▲
IIP.2	Data Encryption	P	2.0	1.3	4.0	% of critical apps with all sensitive fields / records encrypted	81.0% ▲	46.0% ▲
IIP.3	Data Backup & Recovery	C	3.0	3.3	4.0	% of critical apps (BCM / DR) tested	10.0% ---	88.0% ▼
IIP.4	Secure Data Disposal	P	3.0	3.3	3.5	% of LoBs that have an approved data destruction process and have the …	90.0% ---	96.0% ▼
IS.1	Network Security (inc. Seg…	P	3.0	3.3	4.0	% of network devices not located on dedicated VLANs	9.0% ▲	90.0% ---
IS.2	Endpoint Protection	P	3.0	3.3	4.5	% of endpoints with an EPP solution installed	10.0% ▲	93.0% ▼
IS.3	DDOS Mitigation / Protection	P	2.0	1.3	4.0	% of critical external facing systems protected by a DDoS mitigation soluti…	55.0% ---	69.0% ▲
IS.4	Email / Web Access & Filte…	P	3.0	3.3	4.0	% of systems / end users being scanned by web proxies	90.0% ---	91.0% ▲
IS.5	Secure Connectivity (inc. R…	P	2.0	1.5	4.0	% of remote user access connections with key controls implemented	93.0% ▲	71.0% ▼
SGL.1	Security Culture & Training	P	4.0	3.0	4.5	% of employees targeted in a phishing campaign who reported the phishi…	5.0% ▲	44.0% ▼
SGL.2	Cyber Crisis Management	C	2.0	1.0	4.5	% outstanding findings from post incident reports (for major incidents)	9.0% ▲	18.0% ▲
SRC.1	Supply Chain Risk Manage…	P	2.0	2.0	3.5	% of critical suppliers with outstanding issues still to resolve	98.0% ▲	76.0% ▼
TDR.1	Incident Response	C	4.0	3.5	4.5	% deviation from target time bhv SOC engagement and containment	9.0% ▼	80.0% ▲
TDR.2	Continuous Monitoring (inc…	D	3.0	3.5	4.0	% of all systems with logs enabled and capturing events into SIEM tool	95.0% ---	1000.0…
TDR.3	Anomaly Analysis & Detect…	D	4.0	4.3	4.5	% of endpoints with an EDR solution installed	90.0% ▼	90.0% ▼
TDR.4	Threat Intelligence	D	2.0	1.3	3.5	% of incidents where the criticality has been informed by threat intelligence	96.0% ---	40.0% ---
TDR.5	Digital Brand Protection	P	3.0	2.3	4.0	% of company social media accounts in compromise monitoring tool	80.0% ---	50.0% ▲

Интерактивная карта зависимостей рисков, агентов угрозы, элементов контрольной среды и метрик, позволяющая получить ценные инсайты

Профиль киберриска (executive)

Категория угроз

Случайная инсайдерская утечка	Внешняя кибератака	Вредоносная инсайдерская кибератака	Компрометация цепочки поставок	Атака "отказ в обслуживании"	Манипулирование внешней информацией	Customer Compromise Компромисс с клиентом
64.1%	63.6%	61.1%	61.8%	54.9%	54.5%	59.6%

Сценарий

Ref	Threat Scenario	Вероятность инициации атаки	Вероятность успешной атаки
TS1	Потеря данных онлайн-хранил…	71.0%	67.8%
TS2	Потеря данных электронной по…	59.3%	55.1%
TS3	Потеря данных устройства	78.2%	65.9%
TS4	Атака программ-вымогателей	25.3%	63.0%
TS5	Постоянное вторжение в сеть	79.6%	61.9%
TS6	Компрометация внутреннего п…	39.6%	62.2%
TS7	Компрометация внешнего прил…	74.6%	59.5%
TS8	Компрометация корпоративной…	40.5%	58.8%
TS9	Порча сайта	62.7%	57.0%
TS10	Компрометация со стороны пр…	81.1%	61.1%
TS11	Компрометация непривилегиро…	62.2%	
TS12	Кибер нарушение со стороны п…	50.3%	60.7%
TS13	Компрометация бэкдора поста…	91.2%	61.1%
TS14	Компрометация данных постав…	32.8%	8.8%
TS15	Компрометация стороннего пр…	7.7%	59.3%
TS16	Компрометация SaaS/ PaaS	44.0%	61.0%
TS17	Инфраструктурные DDoS	1.3%	56.4%
TS18	Прикладные DDoS	51.0%	55.0%
TS19	DoS-атака перехвата DNS	37.8%	56.4%
TS20	Сквоттинг домена	67.0%	54.5%
TS21	Взлом учетной записи в социа…	48.4%	54.5%
TS22	Брэндджекинг	11.6%	54.5%

Жизненный цикл атаки (kill chain)

Ref	Capability	Type	Уязвимость	Начальный доступ	Распространение	Воздействие	Сила
TDR.1	Реагирование на инцидент	C					6.9%
SGL.2	Управление кибер-кризисом	C					88.0%
IIP.3	Резервное копирование и вос…	C					17.1%
TDR.4	Аналитика угроз	D					29.8%
TDR.3	Анализ и обнаружение анома…	D					29.9%
TDR.2	Мониторинг конфигурации (вк…	D					30.0%
TDR.5	Цифровая защита бренда	P					29.7%
SRC.1	Управление рисками цепочки …	P					12.6%
SGL.1	Культура безопасности и обуч…	P					90.0%
IS.5	Безопасное подключение (вк…	P					37.0%
IS.4	Электронная почта/доступ в и…	P					36.7%
IS.3	Защита от DDoS-атак	P					36.3%
IS.2	Защита конечных точек	P					36.0%
IS.1	Сетевая безопасность (вкл. с…	P					13.0%
IIP.4	Безопасное удаление данных	P					15.0%
IIP.2	Шифрование данных	P					19.2%
IIP.1	Предотвращение потери дан…	P					7.6%
IAM.3	Аутентификация и авторизация	P					11.8%
IAM.2	Управление идентификацией	P					10.9%
IAM.1	Управление привилегированн…	P					10.0%
ASM.4	Управление активами (Повер…	P					9.6%
ASM.3	Безопасность приложений и …	P					10.7%
ASM.2	Управление уязвимостями (вк…	P					8.8%

Визуализация возможностей реализации различный сценариев событий риска для ключевых агентов угрозы

ЗАЩИТА ДАННЫХ

СОХРАНИТЬ ВСЁ

Благодарю за внимание!