Как держать руку на пульсе всех процессов СУИБ, имея лишь один инструмент - SGRC

Николай Казанцев,
CEO SECURITM

securitm.ru

Николай Казанцев

CEO SECURITM.ru

В ИБ с 2010, работал в Лаборатории противодействия промышленному шпионажу, Администрации Санкт-Петербурга, Начальником отдела ИБ в фарм-компании ПОЛИСАН

ECCouncil CEH, Comptia Security+,
Медаль ФСТЭК за заслуги в области защиты информации

SECURITM решает проблему деградации систем защиты

Меры
Учет организационных и технических мероприятий

Задачи
Таск-менеджер для операционной работы

Риски
Управление ИБ на базе риск-ориентированного подхода

Каталоги
БДУ ФСТЭК, MITRE ATT@CK

RPA
Robotic process automation - автоматизация задач

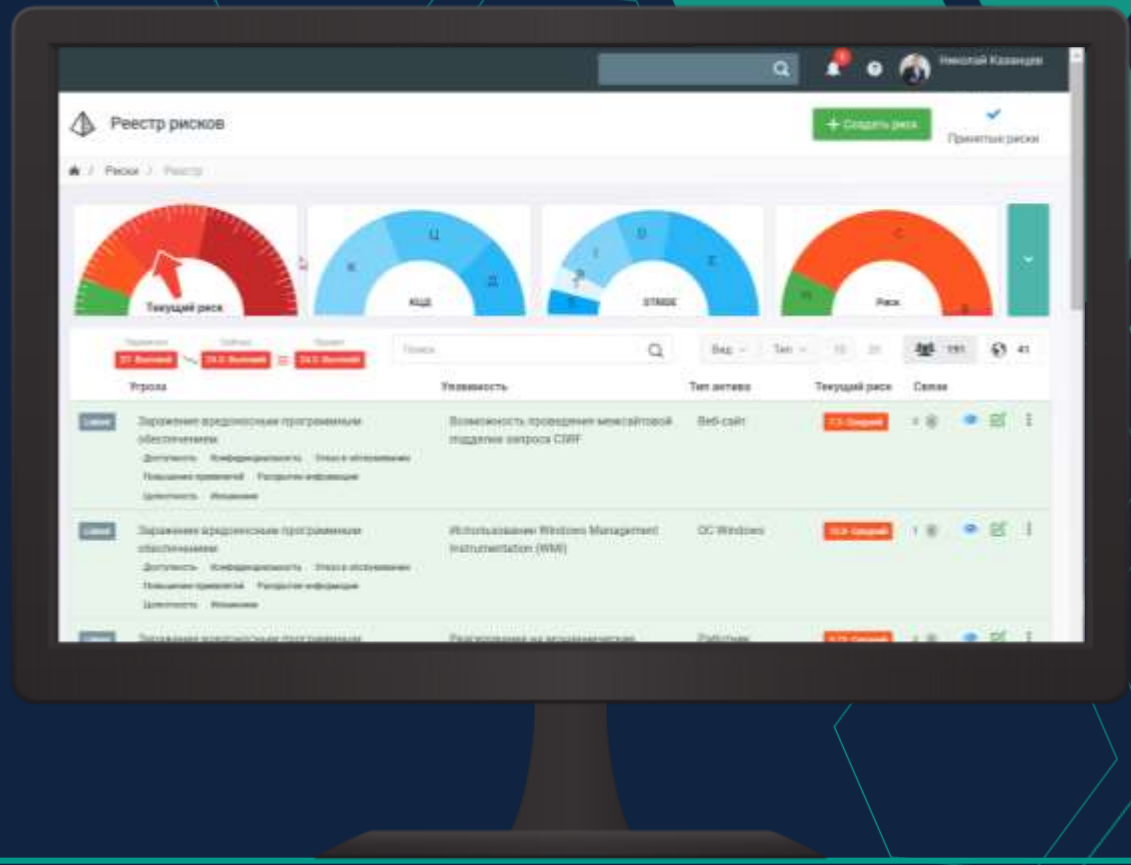
Метрики
Конструктор метрик для процессов ИБ

Опросы
Сбор сведений с работников и контрагентов, Service Desk

Уязвимости
Агрегатор отчетов от сканеров безопасности

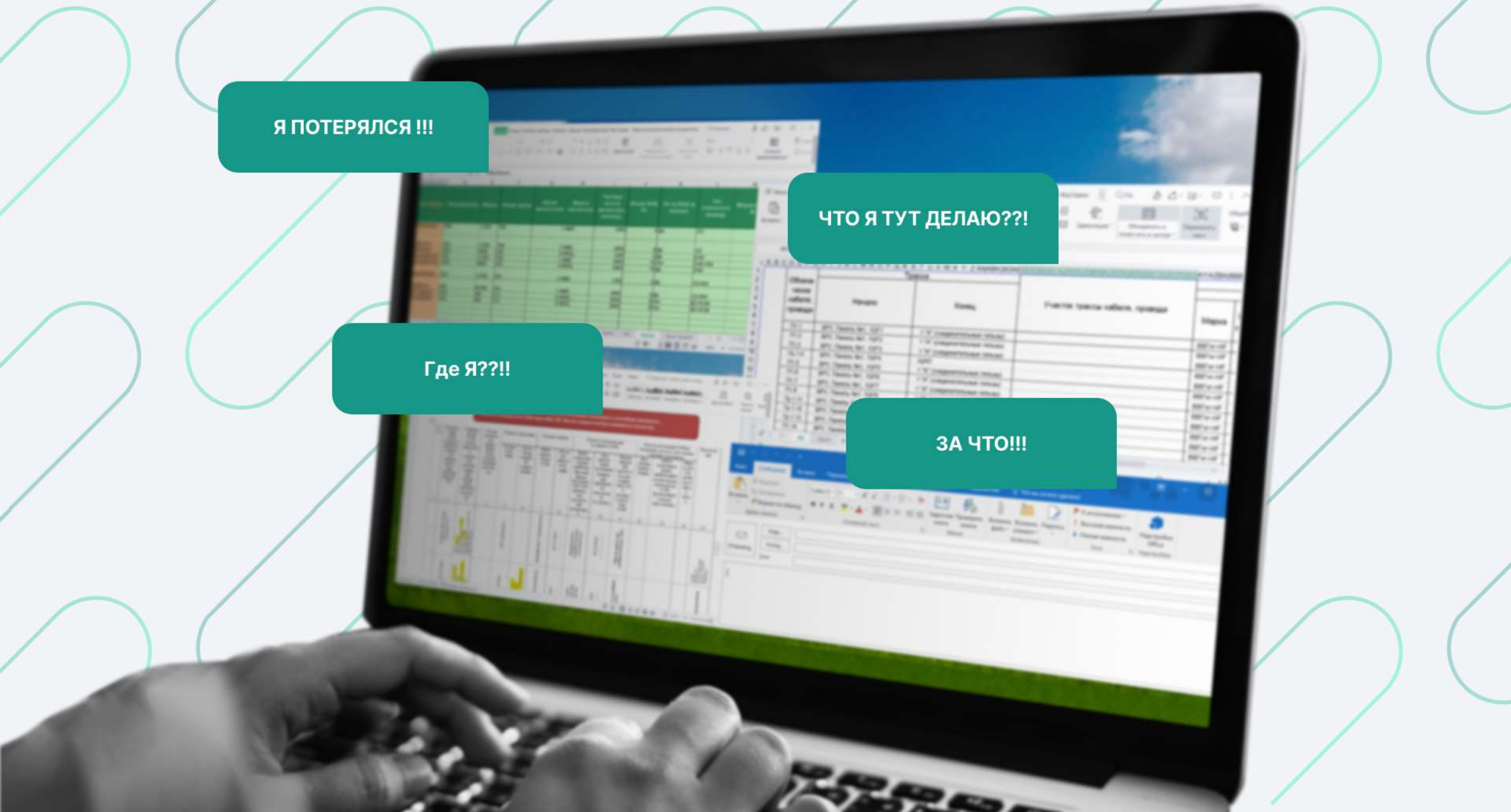
Требования
Соответствие требованиям регуляторики и стандартов по ИБ

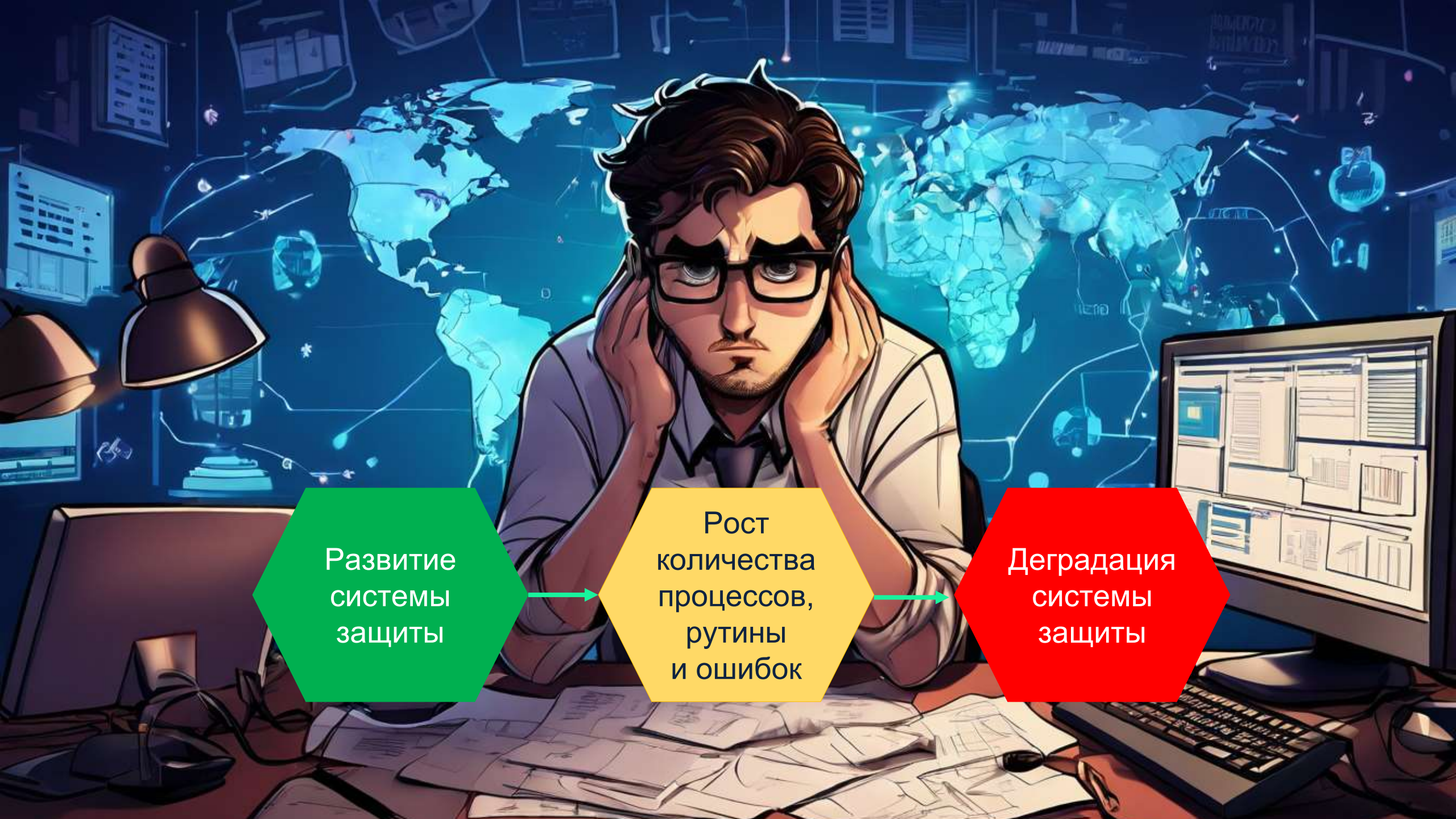
Активы
Учет и управление любыми типами активов



SECURITM

Открытая цена | Открытая база | Community версия | Социальная платформа


Я ПОТЕРЯЛСЯ !!!
ЧТО Я ТУТ ДЕЛАЮ??!
Где Я??!!
ЗА ЧТО!!!


Развитие системы защиты
Рост количества процессов, рутины и ошибок
Деградация системы защиты

SGRC решает проблему деградации систем защиты.

Выгоды

- ✓ **Отсутствие зависимости** от человеческого фактора благодаря цифровизации знаний и процессов
- ✓ **Минимизация затрат** на безопасность за счет обоснованного распределения ресурсов
- ✓ **Снижение ручного труда** службы безопасности через автоматизацию рутинных операций
- ✓ **Повышение защищенности компании** благодаря правильной оценке рисков безопасности

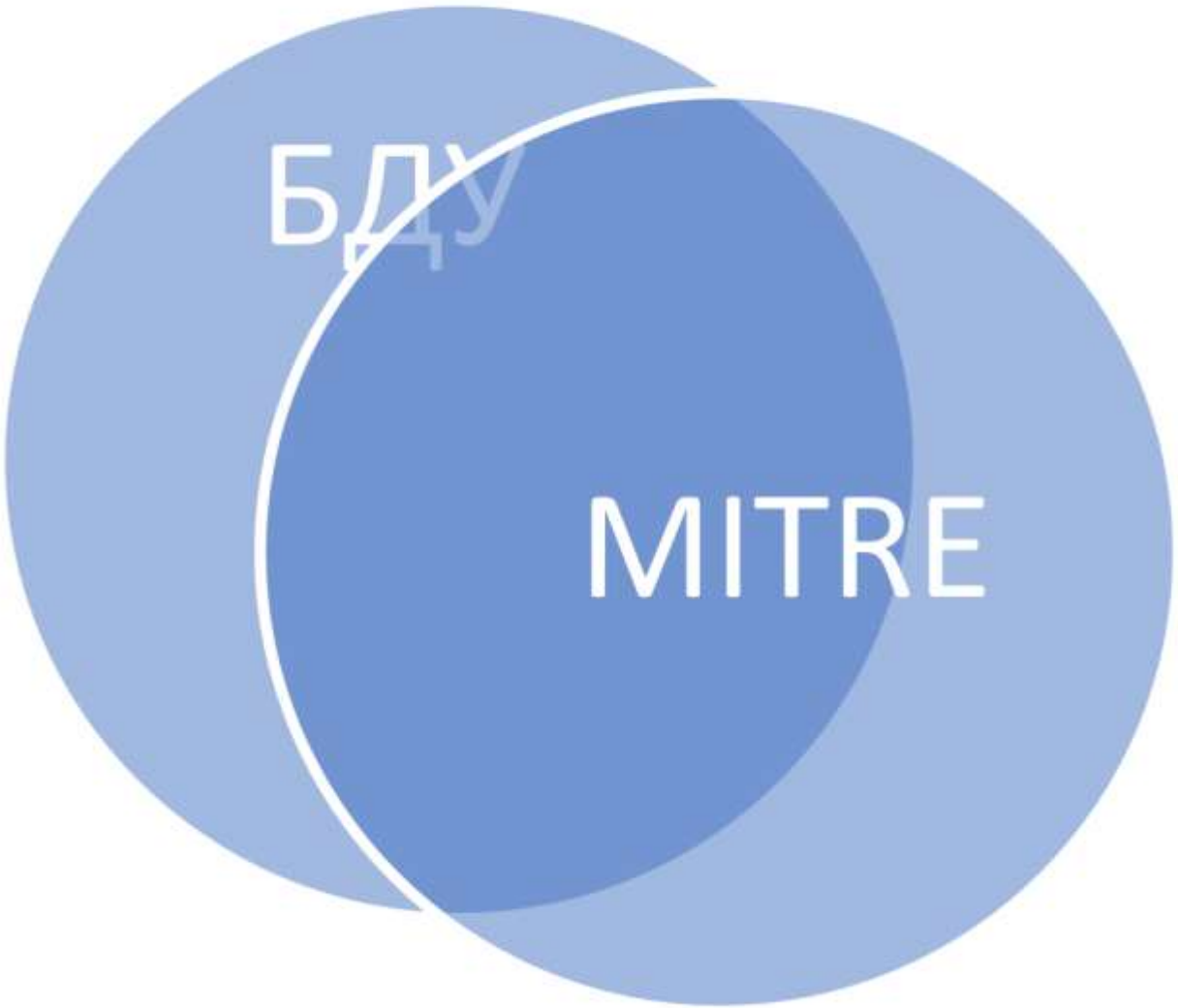
Для продаж – CRM, для производства – ERP, **для безопасности –** SGRC


Нормативы
Каталоги
SGRC
Контент
Интеграции


Каталоги


Что
Каталоги угроз
• БДУ ФСТЭК
• MITRE Attack
Каталоги уязвимостей
• CVE
• БДУ ФСТЭК
• НКЦКИ
Каталоги ПО
• CPE
Зачем
Управление рисками
Управление уязвимостями VM

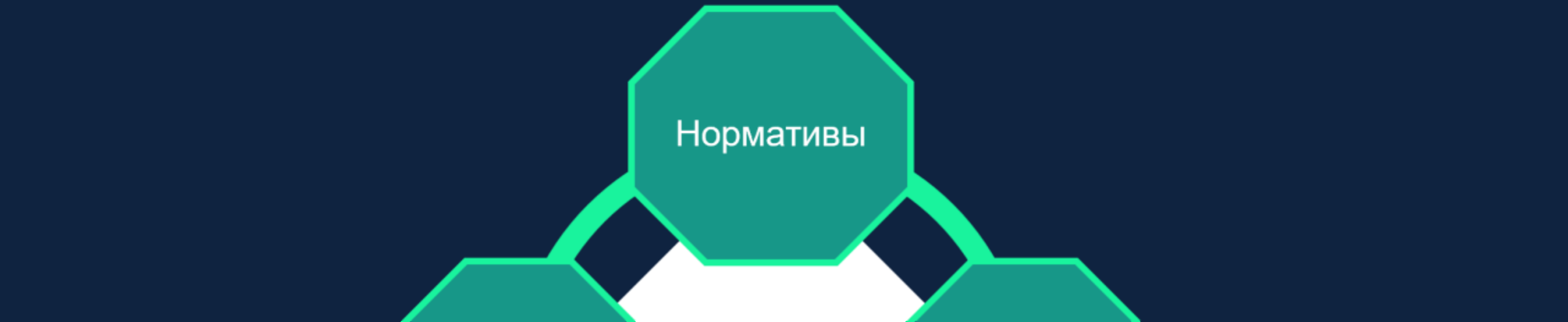

Каталоги



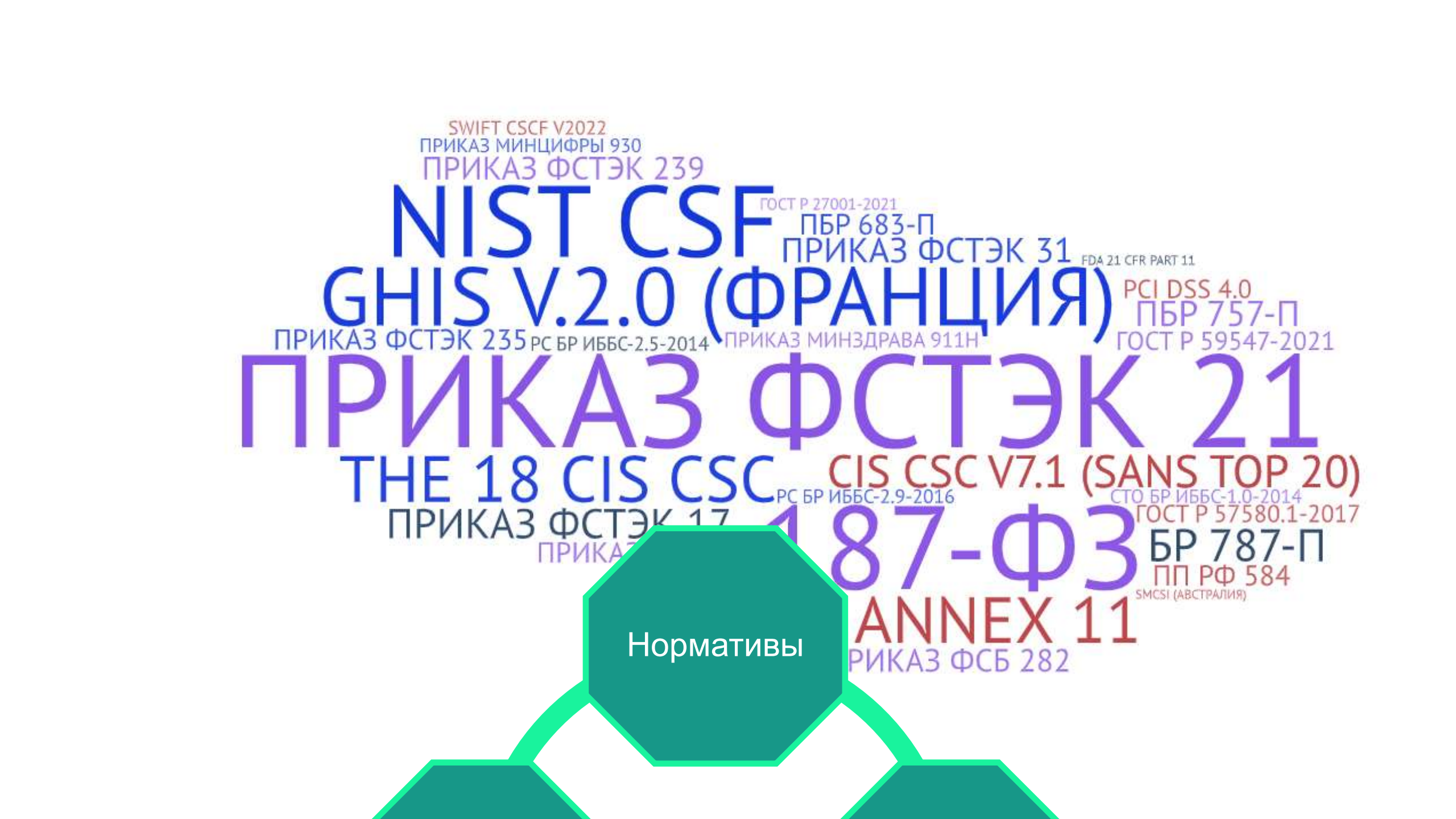
Маппинг БДУ ФСТЭК и MITRE ATT&CK

- **43%** объектов уникальны
- **57%** пересечений

Каталоги


Нормативы


Что
Зачем
База регуляторики по ИБ
Корреляция всех требований
Контроль соответствия требованиям
Кросс-комплаенс
Нормативы

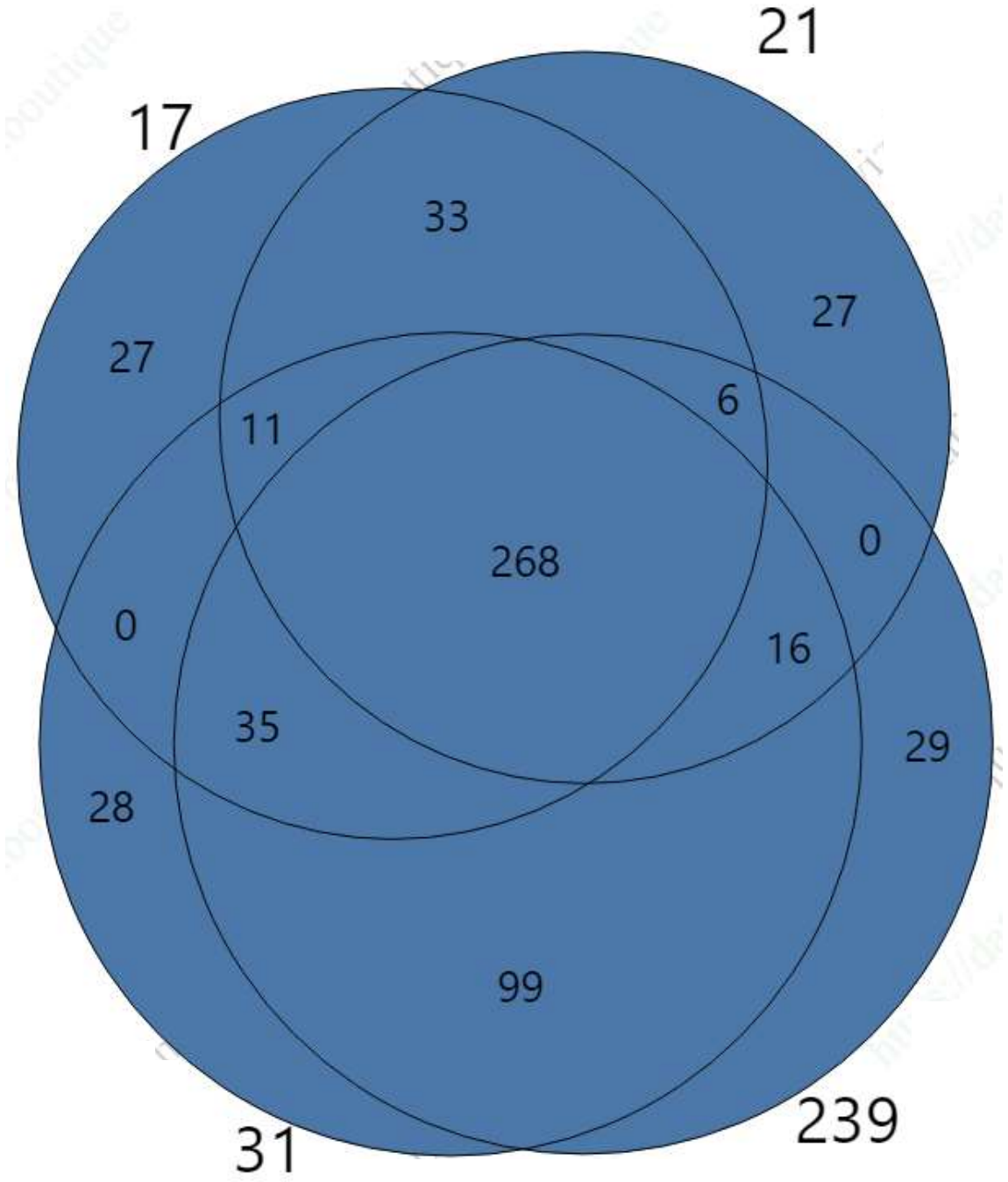

SWIFT CSCF V2022
ПРИКАЗ МИНЦИФРЫ 930
ПРИКАЗ ФСТЭК 239
NIST CSF
ГОСТ Р 27001-2021
ПБР 683-П
ПРИКАЗ ФСТЭК 31
FDA 21 CFR PART 11
GHIS V.2.0 (ФРАНЦИЯ)
PCI DSS 4.0
ПБР 757-П
ПРИКАЗ ФСТЭК 235
РС БР ИББС-2.5-2014
ПРИКАЗ МИНЗДРАВА 911Н
ГОСТ Р 59547-2021
ПРИКАЗ ФСТЭК 21
THE 18 CIS CSC
CIS CSC V7.1 (SANS TOP 20)
РС БР ИББС-2.9-2016
СТО БР ИББС-1.0-2014
ГОСТ Р 57580.1-2017
ПРИКАЗ ФСТЭК 17
187-ФЗ
БР 787-П
ПП РФ 584
SMCSI (АВСТРАЛИЯ)
ANNEX 11
ПРИКАЗ ФСБ 282
Нормативы

Документ	gost-57580-1-2017-part9	gost-57580-1-2017-part8	sto-br-ibbs-10-2014	cis-csc-8	polozhenie-banka-rossii-787-p	gost-57580-1-2017-part7	fstec-21	iso-27001	guideline-for-a-healthy-information-system	iso27001-annex-a	cis-csc-7	pci-dss-v4-0-ru	fstec-17	strategies-to-mitigate-cyber-security-incidents	cscf-v2022	fstec-31	polozhenie-br-757p	polozhenie-br-779p	polozhenie-br-683p	nist-csf-en	rs-dr-ibbs-25-2014	fstec-239
gost-57580-1-2017-part9		0	0	0	8	0	3	0	6	25	0	30	2	3	5	3	6	7	1	0	0	4
gost-57580-1-2017-part8	0		0	0	0	0	5	0	9	10	0	35	5	1	5	20	20	0	3	0	0	19
sto-br-ibbs-10-2014	0	0		0	25	1	0	0	59	114	0	140	0	9	29	2	19	23	11	0	0	3
cis-csc-8	0	0	0		8	1	1	0	60	122	106	114	1	44	15	4	1	8	1	76	0	2
polozhenie-banka-rossii-787-p	8	0	25	8		6	10	0	1	15	8	15	6	2	5	12	1	1	2	18	2	14
gost-57580-1-2017-part7	0	0	1	1	6		206	0	106	147	0	241	202	50	38	214	7	6	5	0	0	224
fstec-21	3	5	0	1	10	206		0	31	62	1	97	94	32	45	39	7	10	4	1	0	41
iso-27001	0	0	0	0	0	0	0		3	1	0	4	0	0	1	0	0	0	0	35	0	0
guideline-for-a-healthy-information-system	6	9	59	60	1	106	31	3		40	53	23	20	22	18	37	3	1	0	35	0	37
iso27001-annex-a	25	10	114	122	15	147	62	1	40		204	158	64	11	36	75	7	13	4	285	40	71
cis-csc-7	0	0	0	106	8	0	1	0	53	204		79	1	47	19	4	0	7	0	125	0	2
pci-dss-v4-0-ru	30	35	140	114	15	241	97	4	23	158	79		91	12	67	111	5	10	11	140	21	115
fstec-17	2	5	0	1	6	202	94	0	20	64	1	91		27	37	87	4	6	2	0	0	78
strategies-to-mitigate-cyber-security-incidents	3	1	9	44	2	50	32	0	22	11	47	12	27		11	32	0	2	0	29	0	32
cscf-v2022	5	5	29	15	5	38	45	1	18	36	19	67	37	11		39	0	5	1	51	4	39
fstec-31	3	20	2	4	12	214	39	0	37	75	4	111	87	32	39		9	14	6	0	0	100
polozhenie-br-757p	6	20	19	1	1	7	7	0	3	7	0	5	4	0	0	9		1	9	1	5	7
polozhenie-br-779p	7	0	23	8	1	6	10	0	1	13	7	10	6	2	5	14	1		2	23	2	16
polozhenie-br-683p	1	3	11	1	2	5	4	0	0	4	0	11	2	0	1	6	9	2		1	0	7
nist-csf-en	0	0	0	76	18	0	1	35	35	285	125	140	0	29	51	0	1	23	1		0	0
rs-dr-ibbs-25-2014	0	0	0	0	2	0	0	0	0	40	0	21	0	0	4	0	5	2	0	0		0
fstec-239	4	19	3	2	14	224	41	0	37	71	2	115	78	32	39	100	7	16	7	0	0	

Требования приказов ФСТЭК

Приказ	Требования
№21	107
№17	113
№31	149
№239	145

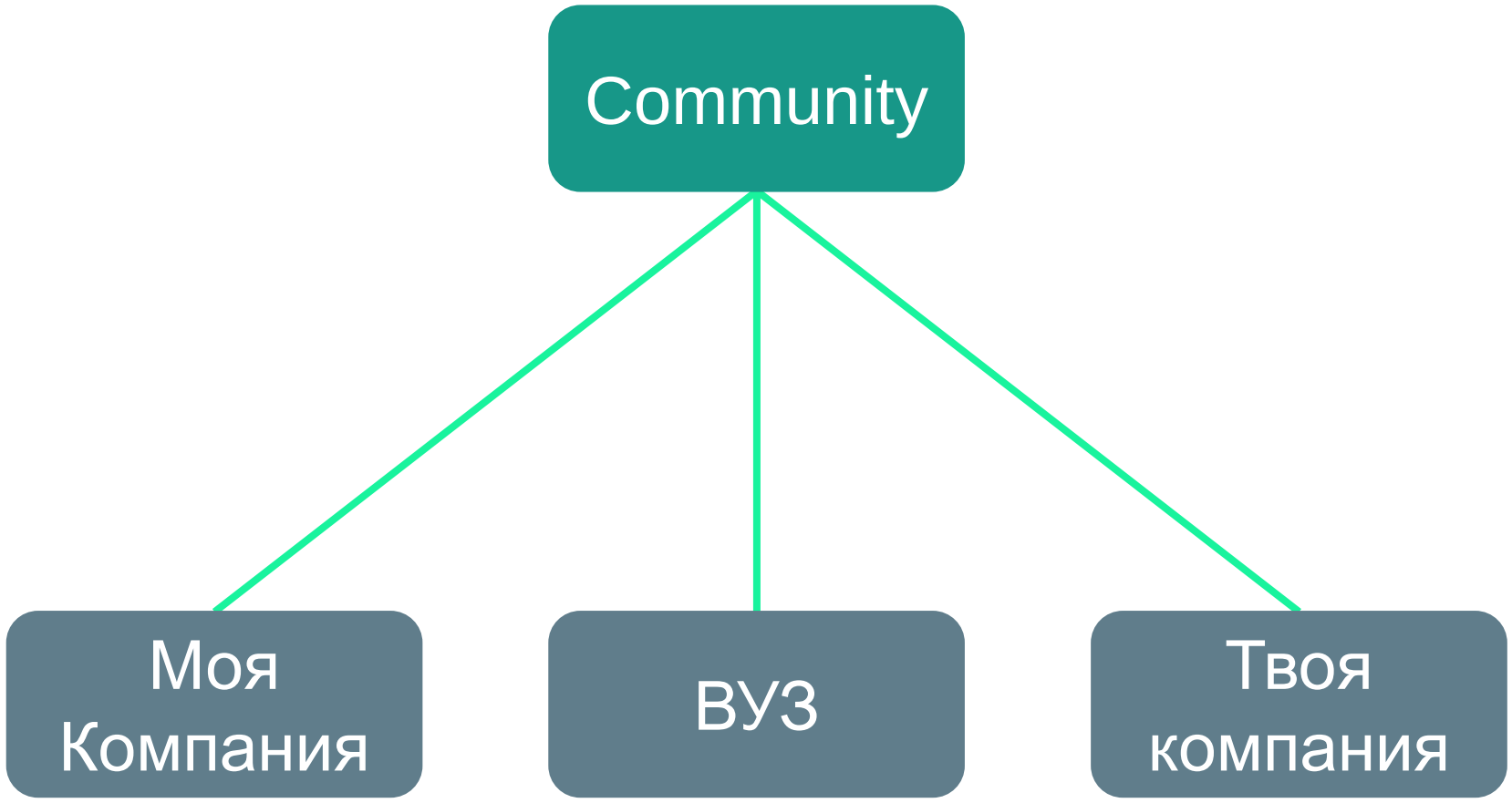
- 20%-25% требований **уникальны**
- 75-80% требований **повторяются** хотя бы раз
- 46% - 62% **одинаковы** во всех приказах

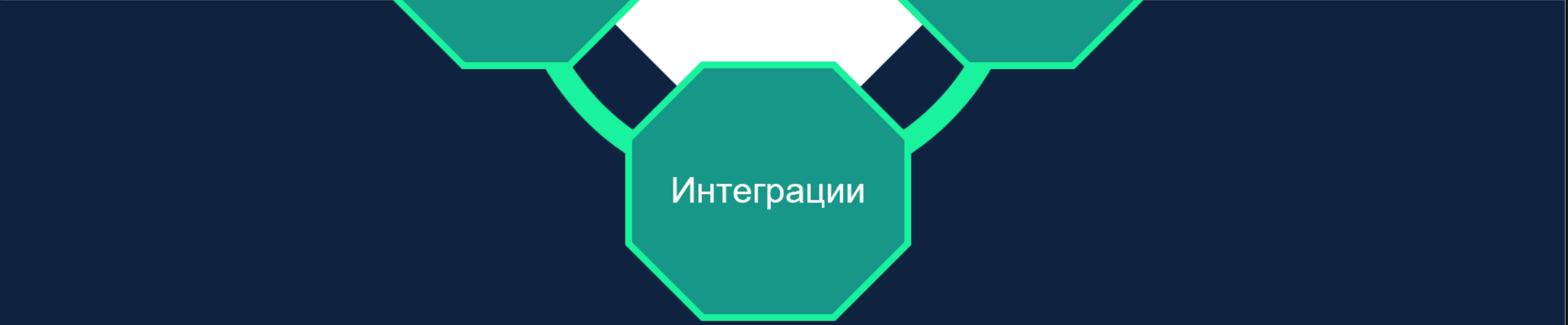



Контент

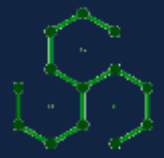
Что	Зачем
База рисков и мер	Быстрый старт СУИБ
Community доступ	Обмен опытом


Контент


Community
Моя Компания
ВУЗ
Твоя компания


Интеграции

Чем больше систем,
тем сложнее их контролировать







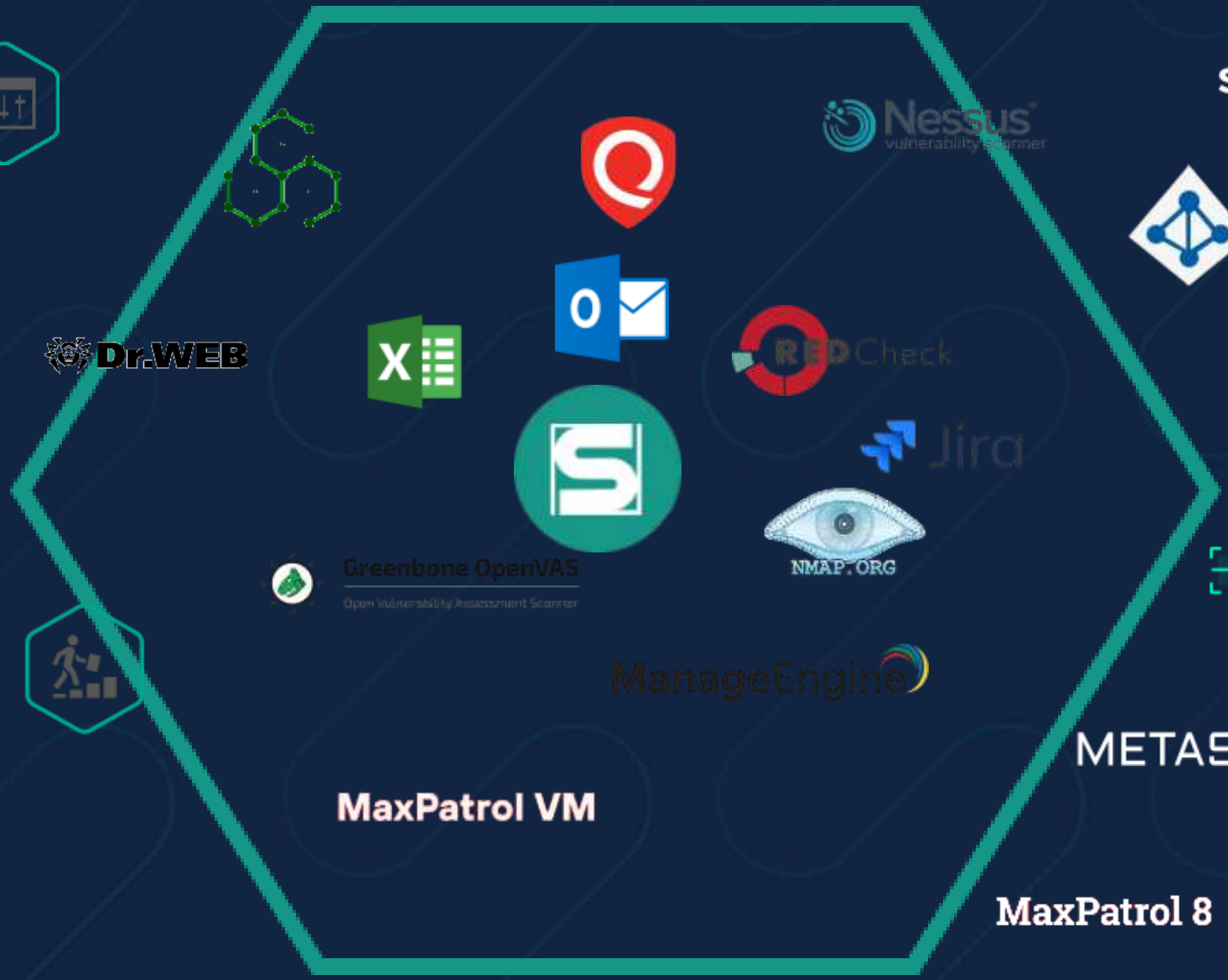






SCAN FACTORY
XSpider
Vulns.io VM
MaxPatrol VM
MaxPatrol 8

Системы важные для служб безопасности можно объединить в SGRC



staffcop

ZABBIX

Dr.WEB

Cloud Advisor

netbox labs

SCAN FACTORY

Vulns.io VM

METASCAN
by vulnspace

XSpider

MaxPatrol 8

SECURITM


Нормативы
Каталоги
SGRC
Контент
Интеграции


AUTOMATION
SGRC
SGRC

SGRC – это не просто инструмент, это стратегическое решение, которое помогает объединить все грани ИБ в единую Систему

t.me/SECURITM

Николай Казанцев
nk@securitm.ru
securitm.ru