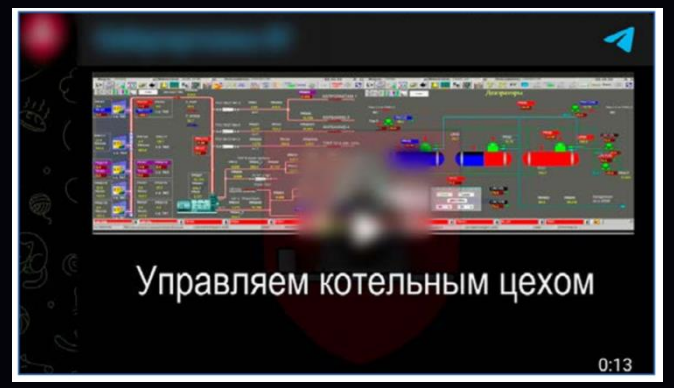
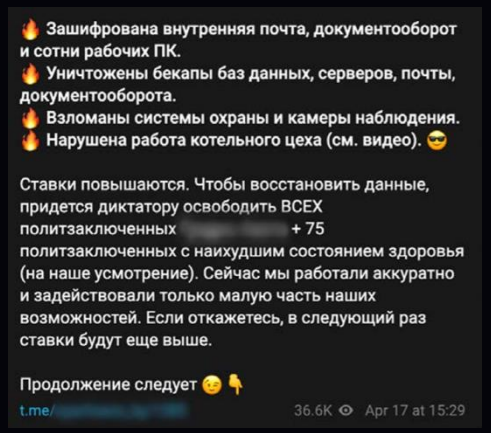
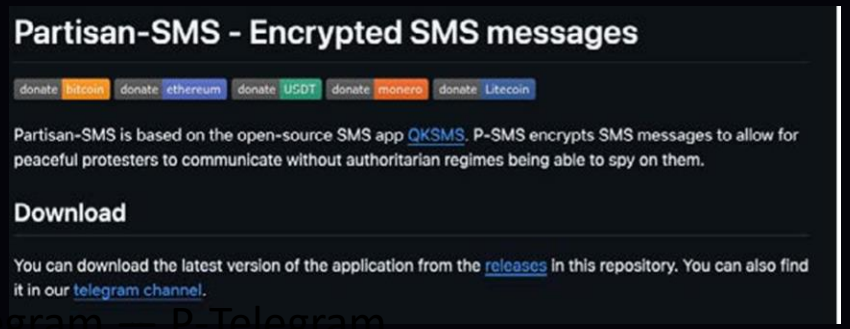
аудит защищенности промышленного предприятия

информзащита

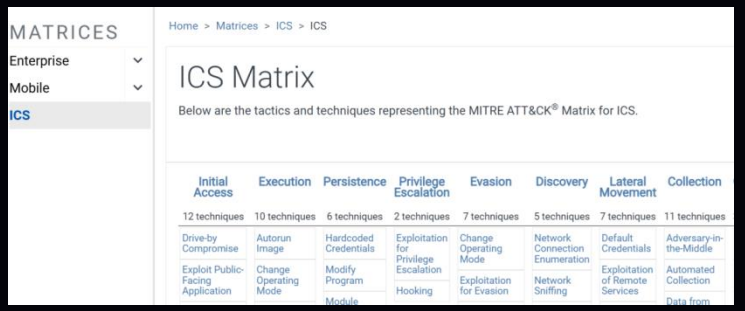
атаки на промышленные сети

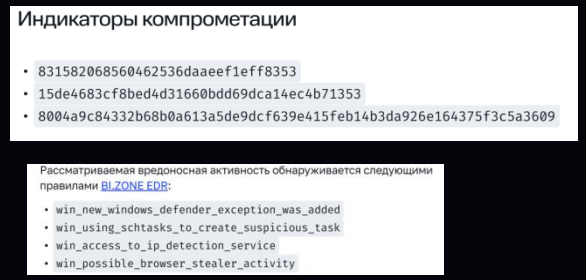






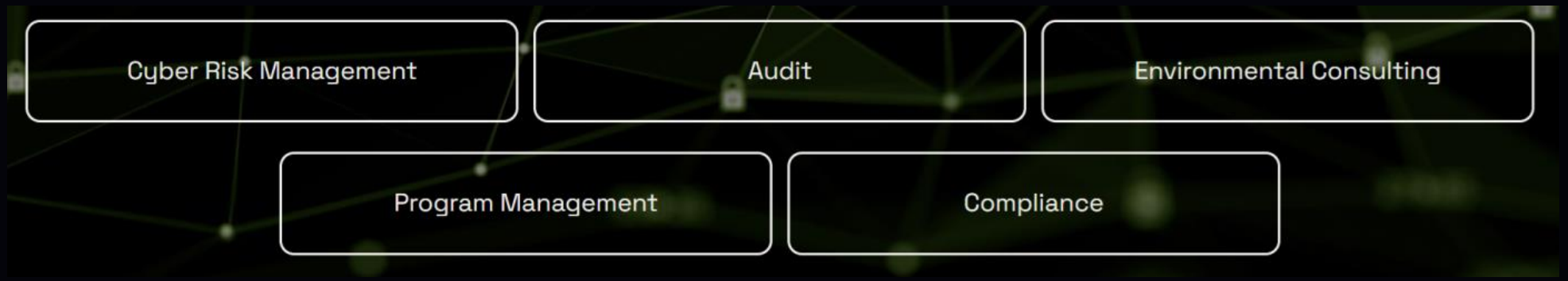
Хактивизм Кибер-Партизаны, Belarussian Cyber Partisan Telegram — P-Telegram P-SMS





- Modbus
- EtherNet/IP
  Ethernet Industrial Protocol.
- PROFINET
- PROFIBUS
- Modbus.
- Bacnet
- ……

Международный взгляд



причины аудитов

- Оценка соответствия требованиям ФЗ-187.
- Оценка соответствия требованиям Приказам ФСТЭК, ФСБ и отраслевым требованиям.
- Смена собственника. Оценка актива и в том числе по ИТ и ИБ для производственного сегмента предприятия.
- Смена ИТ/ИБ руководства.
  Подготовка к новой Стратегии.
- Подготовка к новым проектам.

что требуется

Оценка соответствия требованиям

Оценка уровня зрелости

Оценка защищенности

Подготовка рекомендаций

Подготовка Технического задания или Дорожной карты

Инвентаризация, проверка закупки, предпроектное обследование

объекты аудитов

- Компании, предприятия, цеха, производственные площадки, здания
- АСУ ТП, ЧПУ, объект энергетики, транспортные узлы, судовые установки
- ИТ, ИС, ИБ
- Персонал ИТ, ИБ

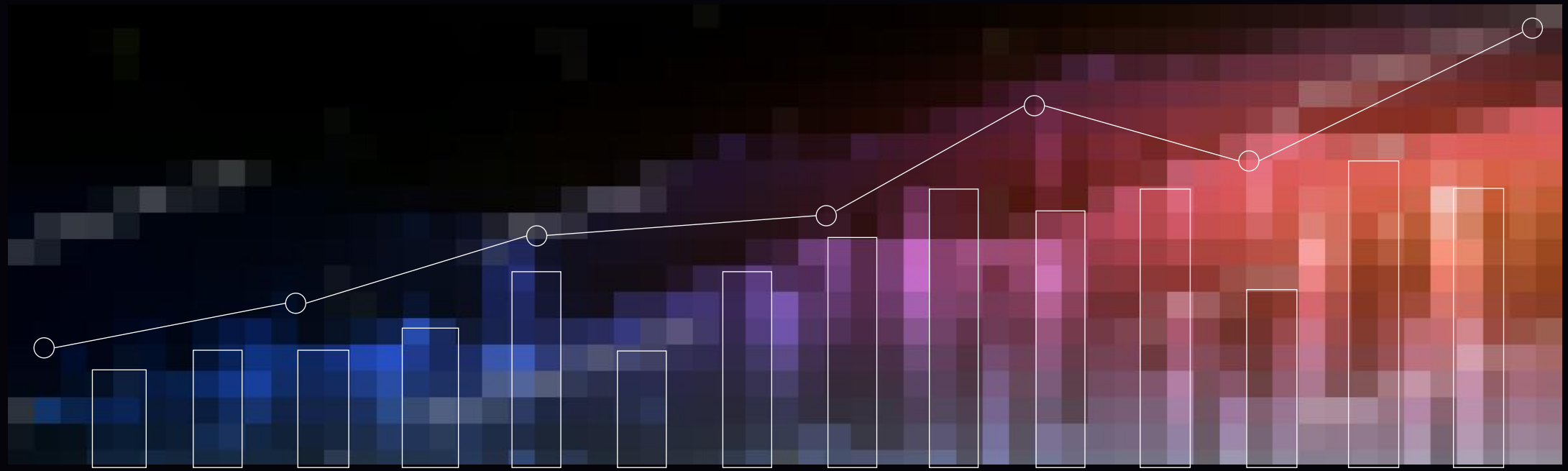
формы проведения аудита

Очное

Заочное

Комплексное

Инструментальное



методики аудита и их применимость

источники требований для аудита

Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Приказ ФСТЭК России от 21 декабря 2017 г. №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Постановление Правительства РФ от 14 ноября 2023 г. № 1912 "О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации"

отчетные материалы

Диаграммы оценки уровня развития процессов

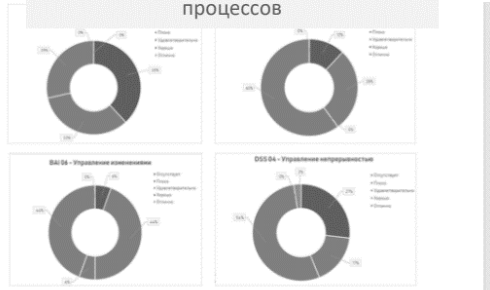
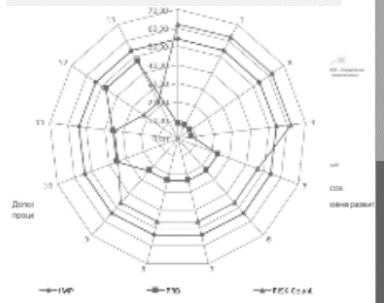
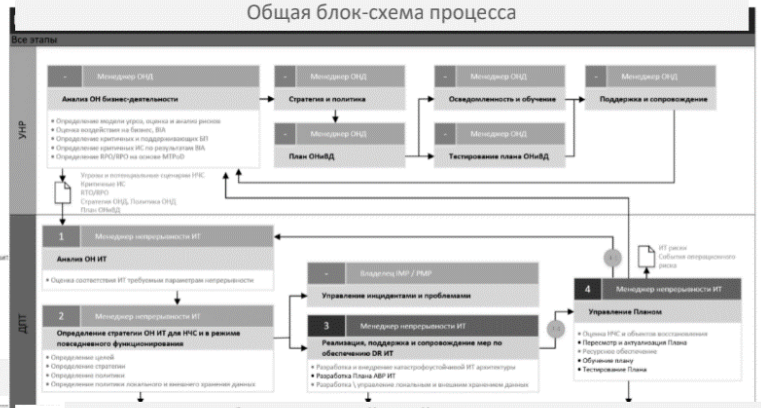


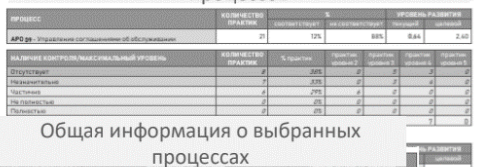
Диаграмма текущего и целевого уровня развития процессов



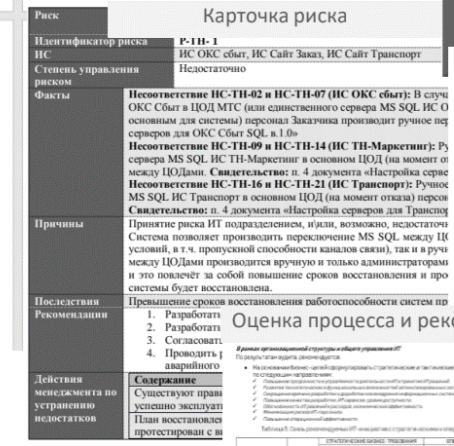
Общая блок-схема процесса



Сводная информация о выполнении практик процессов

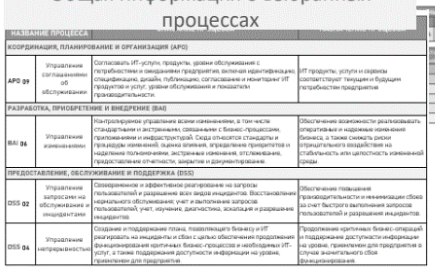


Карточка риска

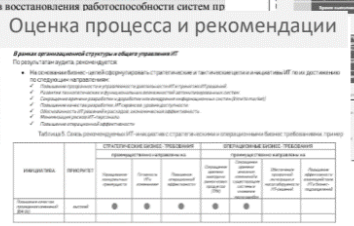


Детальная блок-схема действий персонала при выполнении DRP

Общая информация о выбранных процессах



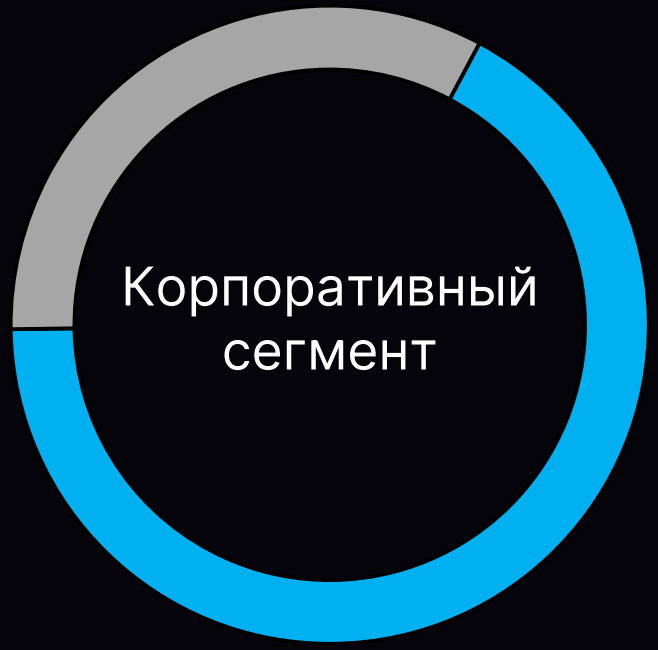
Оценка процесса и рекомендации

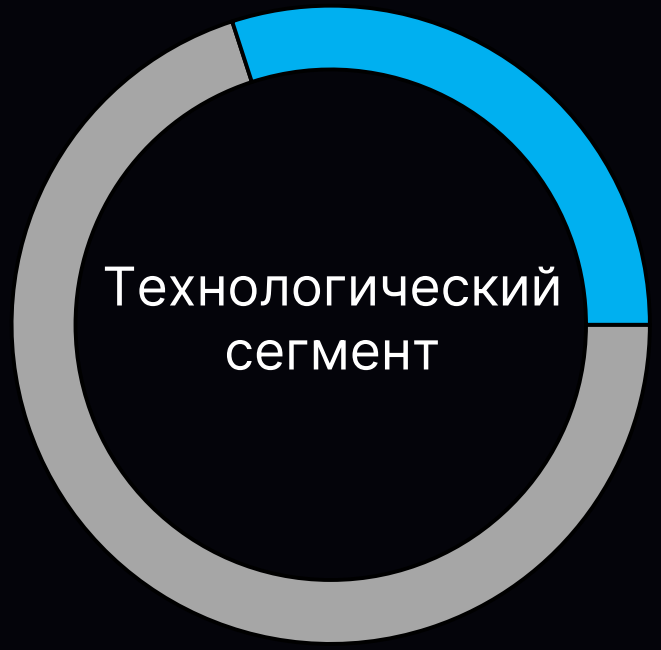


оценка регламентации мер ИБ

67 %
регламентировано

33 %
не регламентировано



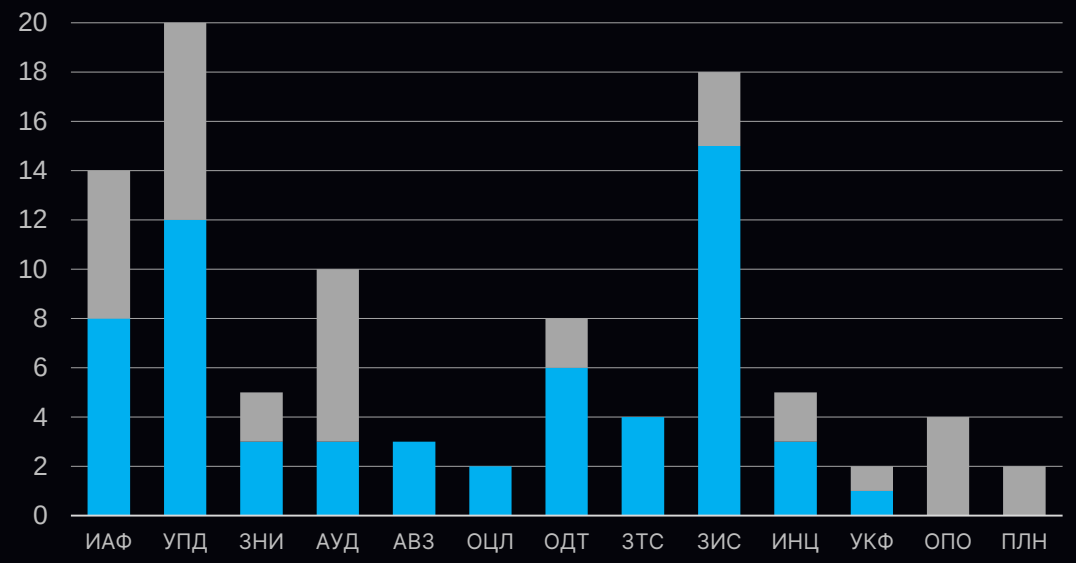


23 %
регламентировано

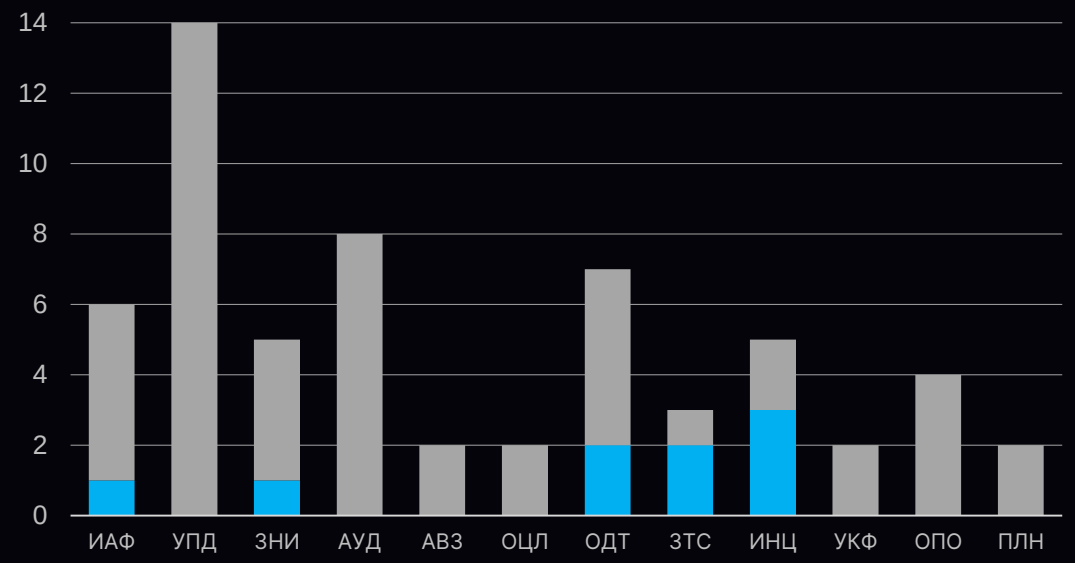
77 %
не регламентировано

оценка реализации мер ИБ

Корпоративный сегмент



Технологический сегмент



- мера защиты выполняется

- мера защиты не выполняется

ключевые недостатки и рекомендации (корпоративный сегмент)

№	Недостатки	Рекомендации
1	Проблемы использования СЗИ иностранного производства	
2	Отсутствие средств централизованного мониторинга безопасности	
3	Антивирусная защита	
4	Факты установки нелигитимного ПО	
5	Невыполнение установки обновлений безопасности	
6	Резервное копирование	

ключевые недостатки и рекомендации (технологический сегмент)

№	Недостатки	Рекомендации
1	Избыточность прав доступа	
2	Пароли привилегированных УЗ длительное время не меняются	
3	Низкий контроль портов ввода-вывода	
4	Низкая защита от вредоносного ПО в изолированных сетях	
5	Не для всех объектов обеспечена возможность восстановления в случае нештатных ситуаций	
6	Не выполняется анализ уязвимостей	

представление результатов проекта

- Отчётные документы
- Презентация для Руководства
- Рабочая сессия для технических руководителей и специалистов

Игорь Рыжов

заместитель директора Центра промышленной безопасности, Информзащита