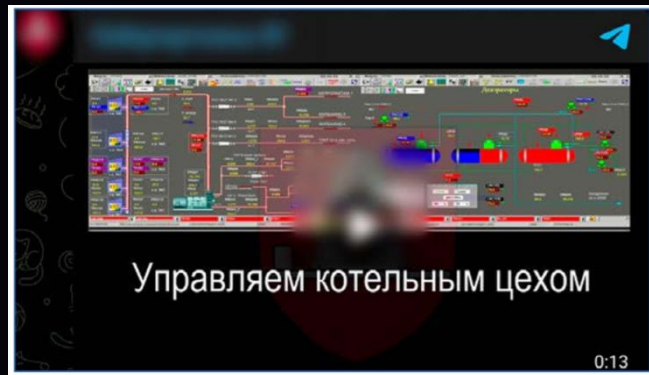


# аудит защищенности промышленного предприятия



информзащита

# атаки на промышленные сети



🔥 Зашифрована внутренняя почта, документооборот и сотни рабочих ПК.  
 🔥 Уничтожены бекапы баз данных, серверов, почты, документооборота.  
 🔥 Взломаны системы охраны и камеры наблюдения.  
 🔥 Нарушена работа котельного цеха (см. видео). 😊

Ставки повышаются. Чтобы восстановить данные, придется диктатору освободить ВСЕХ политзаключенных + 75 политзаключенных с наихудшим состоянием здоровья (на наше усмотрение). Сейчас мы работали аккуратно и задействовали только малую часть наших возможностей. Если откажетесь, в следующий раз ставки будут еще выше.

Продолжение следует 🤔👉  
 t.me/... 36.6K 👁 Apr 17 at 15:29

### Partisan-SMS - Encrypted SMS messages

[donate bitcoin](#) [donate ethereum](#) [donate USDT](#) [donate monero](#) [donate Litecoin](#)

Partisan-SMS is based on the open-source SMS app [QKSMS](#). P-SMS encrypts SMS messages to allow for peaceful protesters to communicate without authoritarian regimes being able to spy on them.

#### Download

You can download the latest version of the application from the [releases](#) in this repository. You can also find it in our [telegram channel](#).

Хактивизм

Кибер-Партизаны, Belarussian Cyber Partisan

Telegram — P-Telegram

P-SMS

MATRICES

Home > Matrices > ICS > ICS

### ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques
Drive-by Compromise Exploit Public-Facing Application	Autorun Image Change Operating Mode	Hardcoded Credentials Modify Program Module	Exploitation for Privilege Escalation Hooking	Change Operating Mode Exploitation for Evasion	Network Connection Enumeration Network Sniffing	Default Credentials Exploitation of Remote Services	Adversary-in-the-Middle Automated Collection Data from

MITRE ATT&CK

Тактика	Техника	Процедура
Initial Access	Phishing	NOVA распространяется через фишинговые письма
Execution	User Execution: Malicious File	Выполнение кода NOVA начинается после запуска пользователем вредоносного файла
	Command and Scripting Interpreter: PowerShell	Загрузчик NOVA вызывает PowerShell для выполнения команд (в частности, для добавления в исключения Microsoft Defender)
Defense Evasion	Impair Defenses: Disable or Modify Tools	NOVA имеет функциональность по отключению командной строки, редактора реестра, диспетчера задач и других системных компонентов, а также для добавления себя в исключения AV

### Индикаторы компрометации

- 831582068560462536daaeef1efff8353
- 15de4683cf8bed4d31660bdd69dca14ec4b71353
- 8004a9c84332b68b0a613a5de9dcf639e415feb14b3da926e164375f3c5a3609

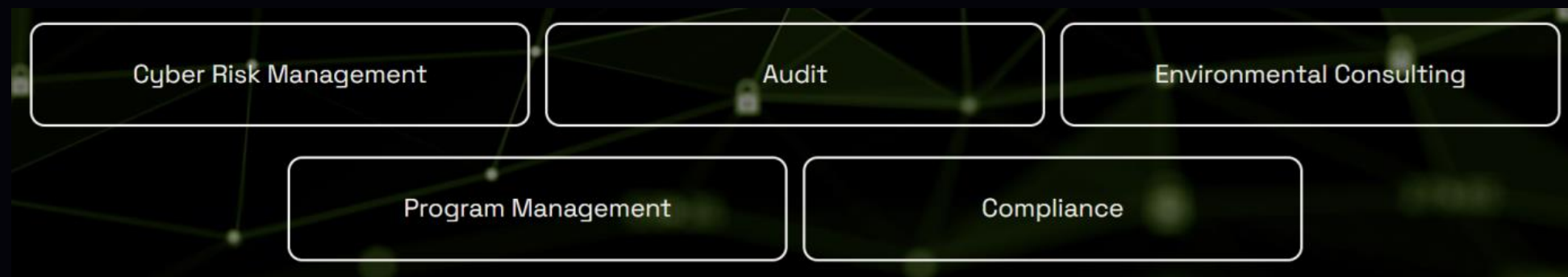
Рассматриваемая вредоносная активность обнаруживается следующими правилами [BI\\_ZONE EDR](#):

- win\_new\_windows\_defender\_exception\_was\_added
- win\_using\_schtasks\_to\_create\_suspicious\_task
- win\_access\_to\_ip\_detection\_service
- win\_possible\_browser\_stealer\_activity

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

# Международный взгляд

---



# причины аудитов

---



- ▶ Оценка соответствия требованиям Ф3-187.
- ▶ 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



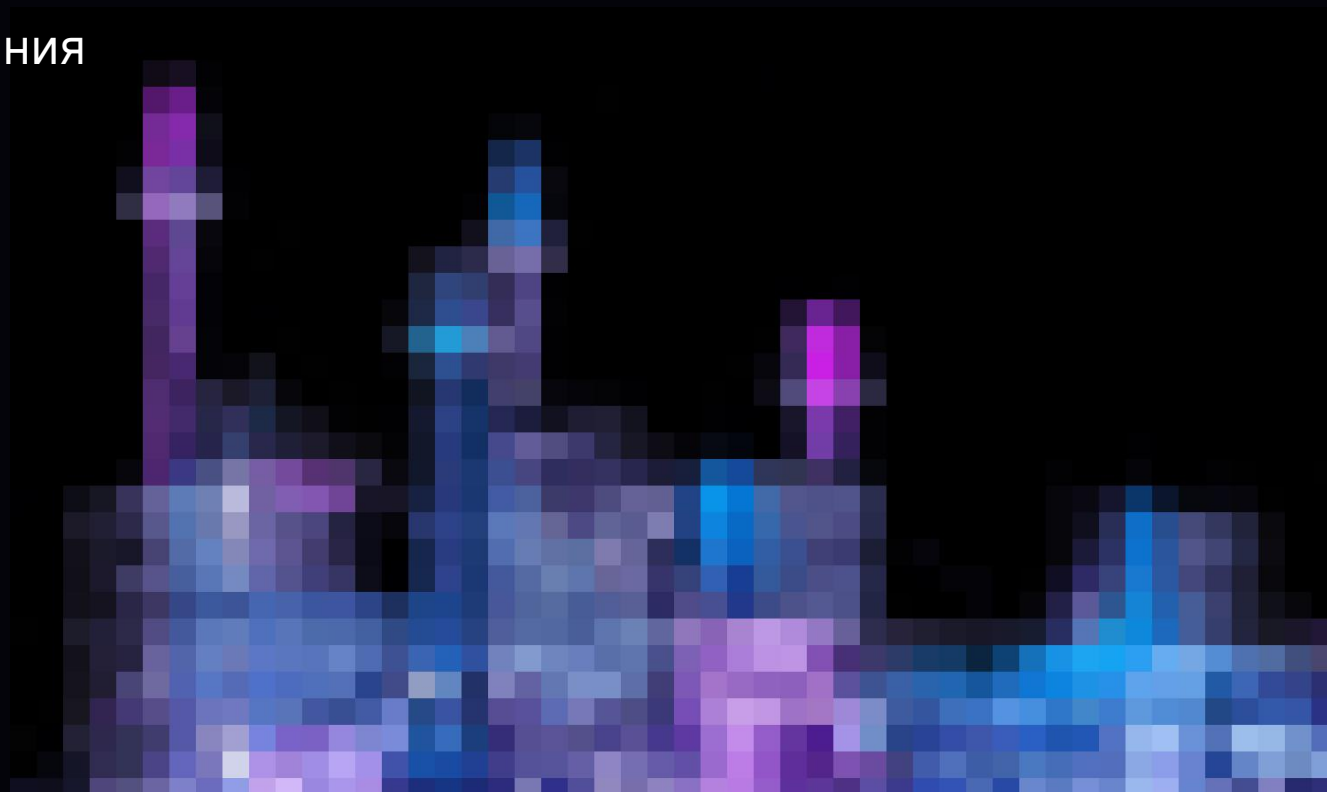
Инвентаризация, проверка закупки,  
предпроектное обследование

# 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

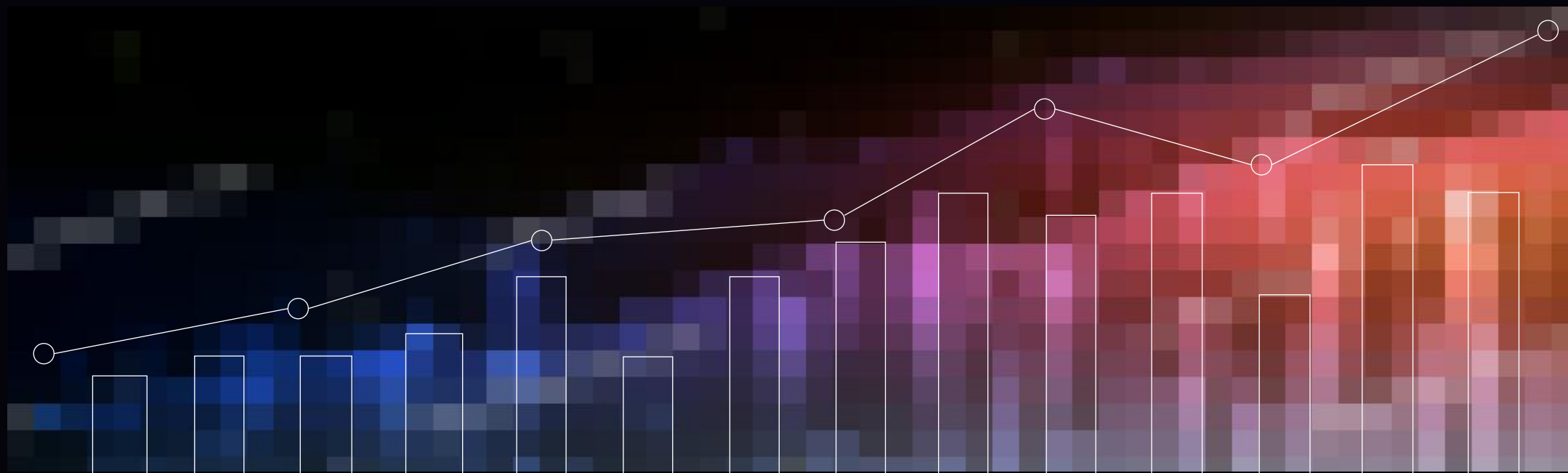


Очное

Заочное

Комплексное

Инструментальное



# методики аудита и их применимость

---



ГОСТ/  
ISO



СОБИТ



TOGAF



Методики  
вендоров



Методики  
регуляторов,  
внутренние  
методики

# 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

Рисунок 2. Оценка уровня выполнения практик контроля для выбранных ИТ-процессов

### Диаграмма текущего и целевого уровня развития процессов

### Общая блок-схема процесса

### Сводная информация о выполнении практик процессов

ПРОЦЕСС	КОЛИЧЕСТВО ПРАКТИК	%	УРОВЕНЬ ЗАВЕРШЕНИЯ
ИТ-инфраструктура	12	100%	100%
ИТ-сервисы	12	100%	100%
ИТ-управление	12	100%	100%

### Карточка риска

**Идентификатор риска:** Р-11-1  
**ИС:** ИС ОКС сбыт, ИС Сайт Заказ, ИС Сайт Транспорт  
**Степень управления риском:** Недостаточно

**Факты:** Несоответствие ИС-ТН-02 и ИС-ТН-07 (ИС ОКС сбыт): В случае ОКС Сбыт в ЦОД МТС (или единственного сервера MS SQL ИС О основным для системы) персонал Заказчика проводит ручное перенос серверов для ОКС Сбыт SQL в 1.0.  
 Несоответствие ИС-ТН-09 и ИС-ТН-14 (ИС ТН-Маркетинг): Ручной сервер MS SQL ИС ТН-Маркетинг в основном ЦОД (на момент отъезда ЦОДов). Свидетельство: в 4 документа «Настройка сервера MS SQL ИС Транспорт в основном ЦОД (на момент отъезда) персонал Свидетельство: в 4 документа «Настройка серверов для Транспорт».

**Причины:** Принятие риска ИТ подразделением, и, или, возможно, недостаточная Система позволяет проводить перенос сервера MS SQL между ЦОД условий, в т.ч. пропускной способности каналов связи), так и в ручную между ЦОДами производится вручную и только администраторами и это позволяет за собой повышение сроков восстановления и про системы будет восстановлена.

**Последствия:** Превышение сроков восстановления работоспособности систем при аварии.

**Рекомендации:**

1. Разработать
2. Разработать
3. Согласовать
4. Проводить аварийного

### Детальная блок-схема действий персонала при выполнении DRP

### Общая информация о выбранных процессах

НАИМЕНОВАНИЕ ПРОЦЕССА	УРОВЕНЬ ЗАВЕРШЕНИЯ
ИТ-инфраструктура	100%
ИТ-сервисы	100%
ИТ-управление	100%

### Оценка процесса и рекомендации

**Результат:** Оценка процесса ИТ-инфраструктуры, ИТ-сервисов, ИТ-управления.

**Рекомендации:**

1. Обновить документацию по ИТ-инфраструктуре, ИТ-сервисам, ИТ-управлению.
2. Обновить документацию по ИТ-инфраструктуре, ИТ-сервисам, ИТ-управлению.
3. Обновить документацию по ИТ-инфраструктуре, ИТ-сервисам, ИТ-управлению.
4. Обновить документацию по ИТ-инфраструктуре, ИТ-сервисам, ИТ-управлению.

# оценка регламентации мер ИБ

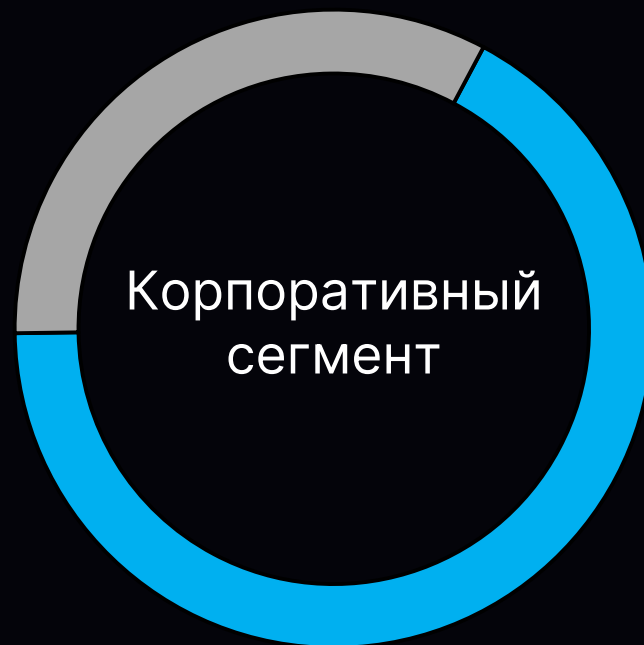


67%

регламентировано

33%

не регламентировано



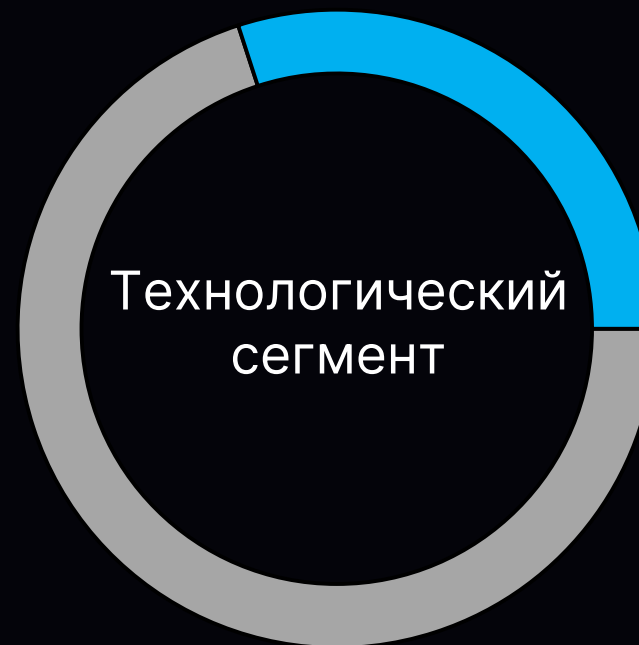
Технологический  
сегмент

23%

регламентировано

77%

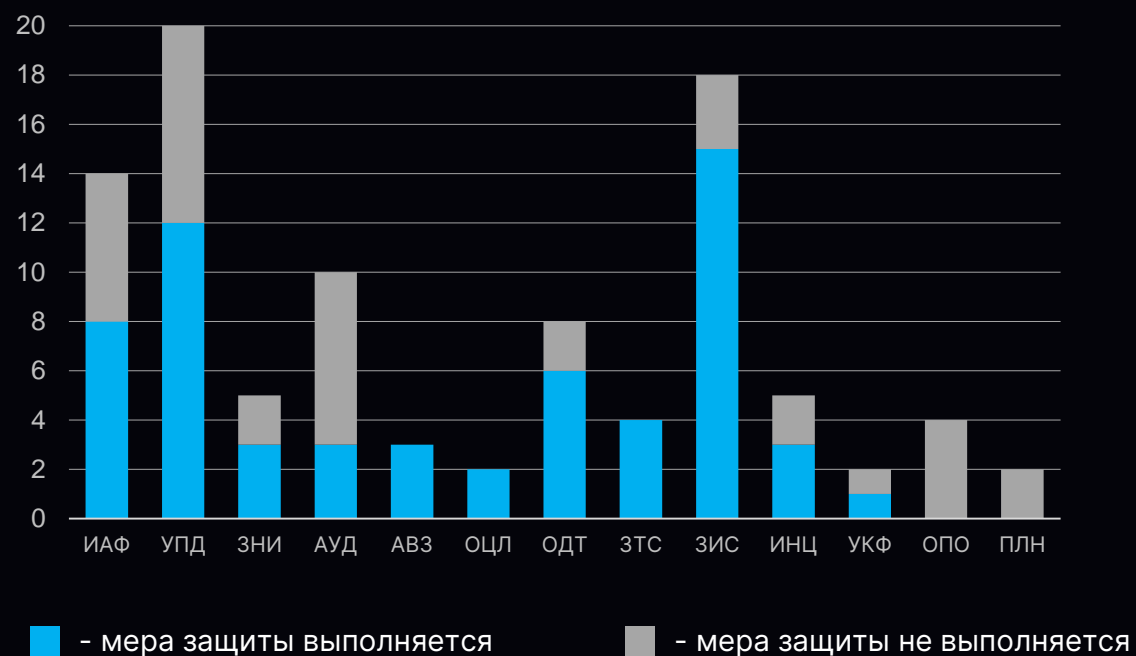
не регламентировано



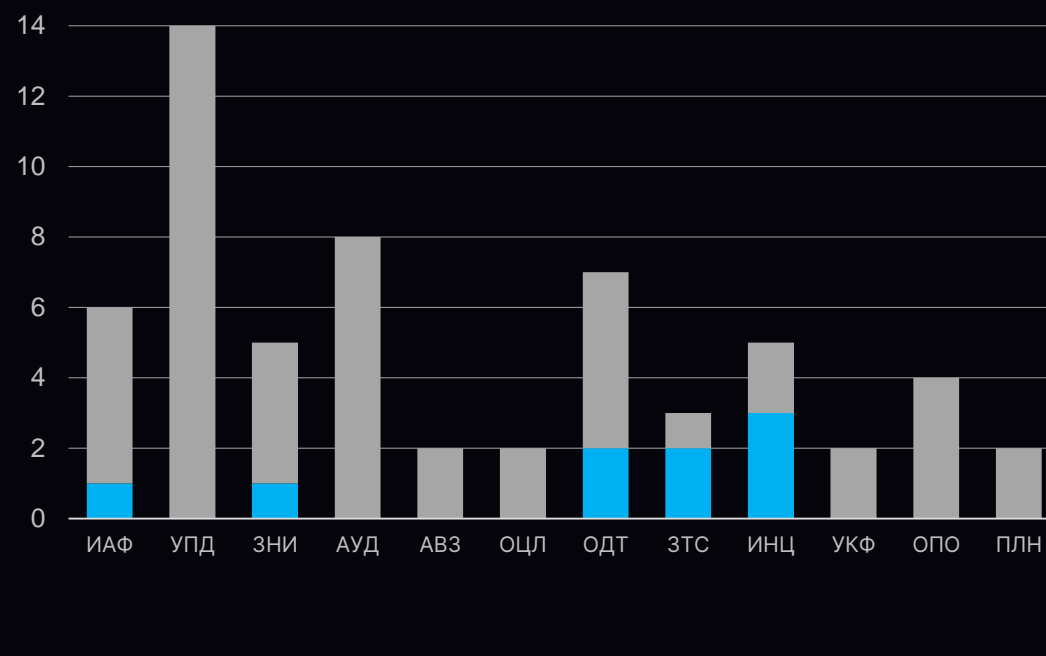
# оценка реализации мер ИБ



## Корпоративный сегмент



## Технологический сегмент



# 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 нелегитимного 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

---



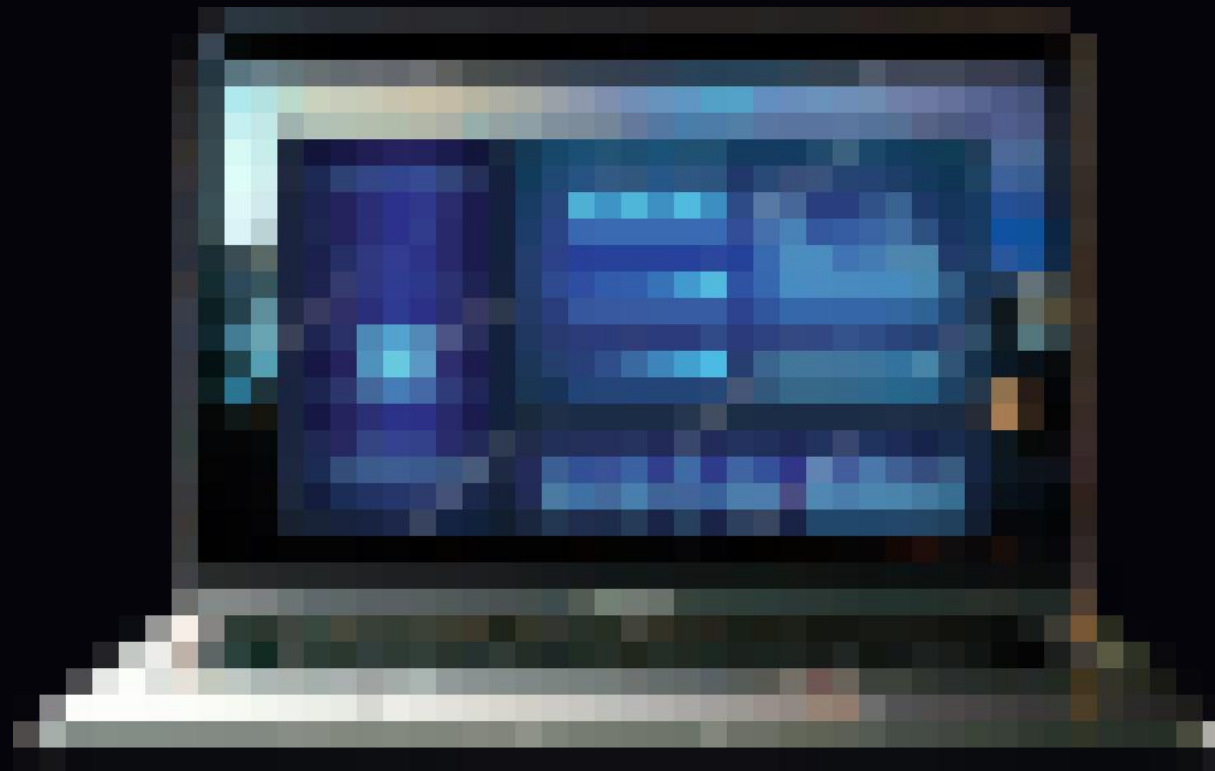
Отчётные документы



Презентация для Руководства



Рабочая сессия для  
технических руководителей  
и специалистов





# Игорь Рыжов

заместитель директора Центра промышленной безопасности, Информзащита