

**Практикующее сообщество по внутреннему аудиту (СВА)**  
**АУДИТ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: от теории к практике**  
**ВЕБИНАР**

**Ресурсы и планирование аудита в сфере информационных технологий**



**Профессор Франк Ям**  
**Председатель и Исполнительный директор - Focus Strategic Group Inc**

## □ **Принятие новых условий жизни**

- COVID-19
- Влияние на функции внутреннего аудита
- Цифровизация всех аспектов жизни

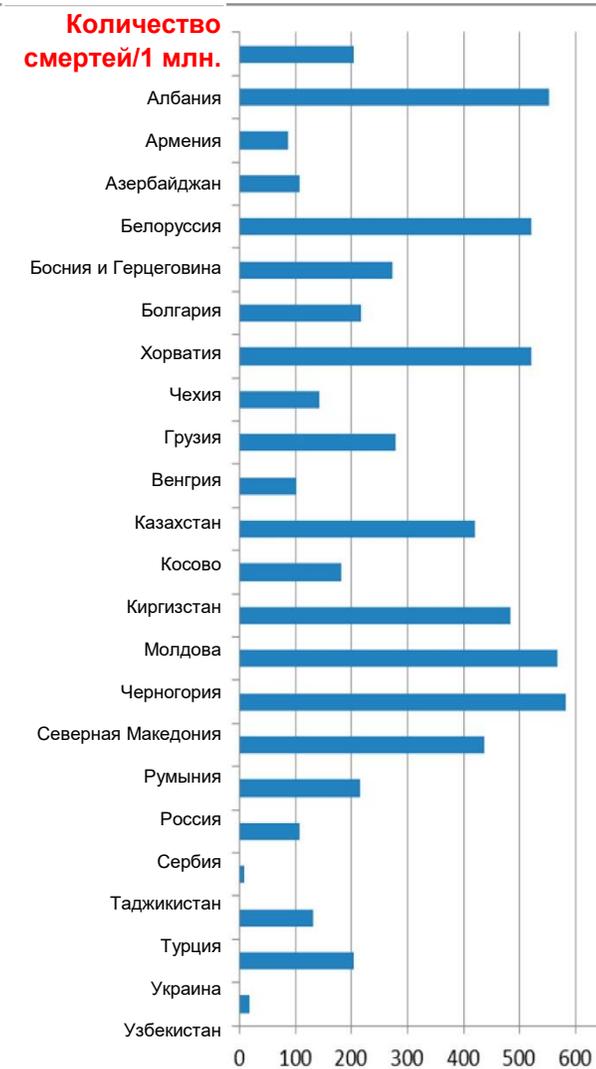
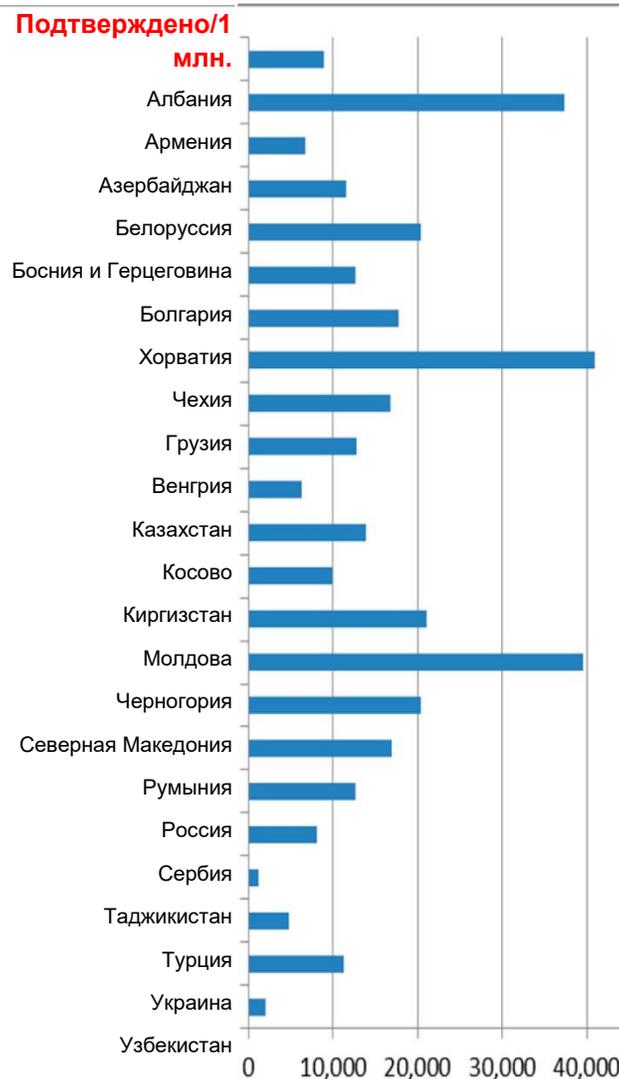
## □ **Ресурсы аудита в сфере информационных технологий**

## □ **Планирование аудита в сфере информационных технологий**

# НОВЫЕ УСЛОВИЯ ЖИЗНИ

## После COVID-19

Страна	Население	Подтверждено/1 млн.	Количество смертей / 1 млн.
<a href="#">Албания</a>	<a href="#">2 876 641</a>	<b>8 969</b>	<b>205</b>
<a href="#">Армения</a>	<a href="#">2 965 275</a>	<b>37 281</b>	<b>552</b>
<a href="#">Азербайджан</a>	<a href="#">10 172 439</a>	<b>6 743</b>	<b>87</b>
<a href="#">Белоруссия</a>	<a href="#">9 448 180</a>	<b>11 574</b>	<b>108</b>
<a href="#">Босния и Герцеговина</a>	<a href="#">3 273 270</a>	<b>20 336</b>	<b>520</b>
<a href="#">Болгария</a>	<a href="#">6 929 071</a>	<b>12 601</b>	<b>274</b>
<a href="#">Хорватия</a>	<a href="#">4 095 903</a>	<b>17 784</b>	<b>218</b>
<a href="#">Чехия</a>	<a href="#">10 716 269</a>	<b>40 948</b>	<b>520</b>
<a href="#">Грузия</a>	<a href="#">3 986 347</a>	<b>16 697</b>	<b>142</b>
<a href="#">Венгрия</a>	<a href="#">9 651 311</a>	<b>12 730</b>	<b>279</b>
<a href="#">Казахстан</a>	<a href="#">18 858 176</a>	<b>6 283</b>	<b>101</b>
<a href="#">Косово</a>	<a href="#">1 810 366</a>	<b>13 934</b>	<b>421</b>
<a href="#">Кыргызстан</a>	<a href="#">6 563 032</a>	<b>9 806</b>	<b>181</b>
<a href="#">Молдова</a>	<a href="#">4 030 509</a>	<b>21 016</b>	<b>484</b>
<a href="#">Черногория</a>	<a href="#">628 095</a>	<b>39 588</b>	<b>567</b>
<a href="#">Северная Македония</a>	<a href="#">2 083 343</a>	<b>20 419</b>	<b>582</b>
<a href="#">Румыния</a>	<a href="#">19 190 198</a>	<b>16 889</b>	<b>437</b>
<a href="#">Россия</a>	<a href="#">145 957 452</a>	<b>12 586</b>	<b>216</b>
<a href="#">Сербия</a>	<a href="#">8 724 381</a>	<b>8 072</b>	<b>107</b>
<a href="#">Таджикистан</a>	<a href="#">9 614 381</a>	<b>1 192</b>	<b>9</b>
<a href="#">Турция</a>	<a href="#">84 668 717</a>	<b>4 749</b>	<b>132</b>
<a href="#">Украина</a>	<a href="#">43 636 591</a>	<b>11 225</b>	<b>205</b>
<a href="#">Узбекистан</a>	<a href="#">33 644 633</a>	<b>2 061</b>	<b>18</b>
<b>Среднее</b>	<b>19 283 677</b>	<b>15 369</b>	<b>277</b>



# НОВЫЕ УСЛОВИЯ ЖИЗНИ

## Влияние COVID-19 на функции внутреннего аудита

4



### COVID-19 AND INTERNAL AUDIT

Preparing for the New Normal in 2020 and Beyond

Deborah F. Kretchmar, CIA

The Institute of  
Internal Auditors

INTERNAL AUDIT  
FOUNDATION

AUDITBOARD

Основные вопросы, которым уделяется недостаточно внимания в годовых планах проведения аудита:

### 1) Кибербезопасность

- Организации разрешили сотрудникам **работать из любого места мира**, полагаясь на процессы и средства контроля в отношении киберрисков, которые, возможно, недостаточно изучены.

### 2) Информационные технологии

- Почти 60% добавили **новые технологии** и безопасность данных.

### 3) Отношения с третьими сторонами

- Менее половины (48%) использовали ресурсы ВА в рамках отношений с третьими сторонами.

**ОДНАКО РЕЧЬ ИДЕТ НЕ ТОЛЬКО О COVID-19.**

# НОВЫЕ УСЛОВИЯ ЖИЗНИ

## Цифровизация всех аспектов жизни

5

### Аспекты, касающиеся организаций:

- ❑ Сотрудники работают в разных местах.
- ❑ Действует гибкий график работы.
- ❑ Наблюдается смещение графиков.
- ❑ СИЗ предоставляются персоналу (и даже клиентам и гостям).
- ❑ К приоритетным задачам относятся: (1) обеспечение безопасности каждого; (2) применение методов СЕМ и лучшего современного опыта.
- ❑ Новые стратегии и инициативы (в том числе в сфере технологий).
- ❑ Возможное увольнение сотрудников.



### Аспекты, касающиеся внутренних аудиторов:

- ❑ Удаленный аудит (с использованием средств телеконференцсвязи, демонстрации экрана, видеоконференцсвязи, совместного доступа к файлам)
- ❑ Изменение требуемых навыков в результате цифровой трансформации
- ❑ Безработица и экономический спад приведут к увеличению рисков, связанных с мошенничеством (следовательно, приоритеты аудита должны изменяться)

# Ресурсы для аудита в сфере информационных технологий

## Кто нам потребуется?

6



**КЛЮЧ** к успеху заключается в формировании групп, которые смогут успешно действовать в непредсказуемом будущем.

Поэтому **необходимо постоянно совершенствоваться!**

Источник: Видео «Какие навыки потребуются аудитору в будущем?» (CA - A/NZ)

# Ресурсы для аудита в сфере информационных технологий

## Кто нам потребуется?

7

- Искусственный интеллект
- Машинное обучение
- Большие данные
- Роботизированная автоматизация процессов (RPA)
- Блокчейн
- DevSecOps
- Динамичность / SCRUM
- Цифровая трансформация
- Экосистема
- Графический пользовательский интерфейс приложений и качество пользовательского взаимодействия (UI / UX)
- Проектное мышление
- Облачные вычисления
- SaaS (программное обеспечение как услуга), IaaS (вычислительная инфраструктура как услуга), PaaS (платформа как услуга)
- VPN
- API
- SDK
- Квантовые вычисления
- Нанотехнологии
- Революционные технологии
- Разделение обязанностей

### ЦИФРОВЫЕ / ТЕХНОЛОГИЧЕСКИЕ ТЕНДЕНЦИИ



### КУЛЬТУРНЫЕ ТЕНДЕНЦИИ



### ВЛИЯНИЕ НА БИЗНЕС И ИТ-СЛУЖБУ

Бимодальные ИТ | Теневые ИТ | Подход, основанный на выстраивании отношений | Динамичность и гибкость | Общеорганизационное сотрудничество | Повышение квалификации | Новые риски

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ = ПРЕОБРАЗОВАНИЕ БИЗНЕС-МОДЕЛИ + ТЕХНОЛОГИЧЕСКИЕ ИННОВАЦИИ (СВОЕВРЕМЕННЫЕ)

ЦИФРОВИЗАЦИЯ С RPA = УСОВЕРШЕНСТВОВАНИЕ БИЗНЕС-ПРОЦЕССОВ + ИХ АВТОМАТИЗАЦИЯ (ЭФФЕКТИВНОСТЬ И РЕНТАБЕЛЬНОСТЬ)

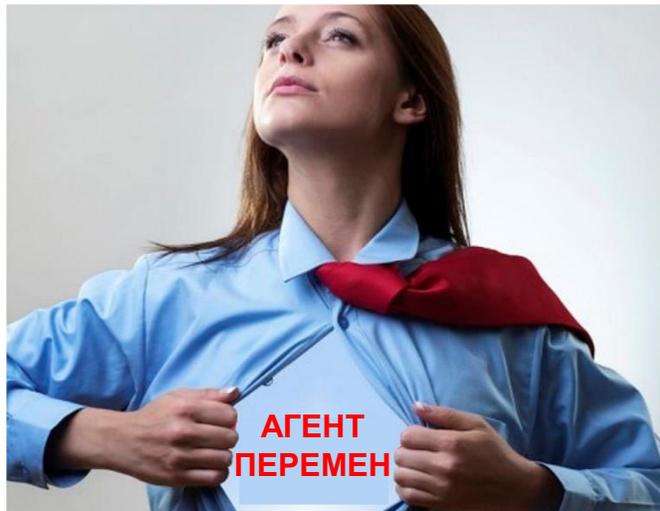
**Специалист, который разбирается в вопросах, связанных с использованием информационных технологий в бизнесе**

- Zoom
- Webex (Cisco)
- Teams (MS)
- Meet (Google)
- KOL
- Интернет вещей
- Виртуальная / дополненная реальность
- 5G
- Финансовые технологии, технологии регулирования, образовательные технологии, технологии в сфере здравоохранения
- Криптовалюта
- Электронные кошельки
- Электронные платежи
- QR-коды
- Дроны
- Чат-боты
- 3D-печать
- Портативные электронные устройства
- Гигномика
- Умный город / правительство
- Поколение Миллениума

## Кто?

### ■ Штатные аудиторы

- Острая необходимость в повышении квалификации и профессиональной переподготовке
- Возможность командирования
- Обмен опытом

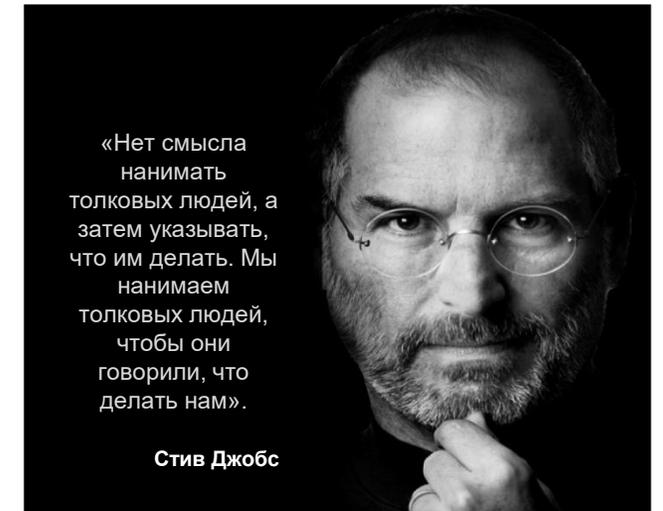


### ■ Сотрудничество

- Вопросы соответствия
- Внутренний контроль
- Управление рисками
- Безопасность
- Конфиденциальность
- Расследование случаев мошенничества
- Внешний аудит

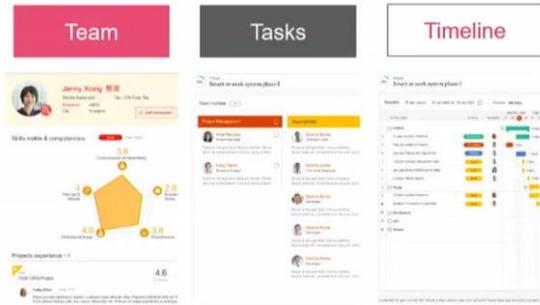
### ■ Совместная работа

- Технические вопросы
- На периодической основе, при необходимости
- Передача знаний



# Ресурсы для проведения аудита в сфере информационных технологий

## Как?



Управление аудитом

RPA / CAATs

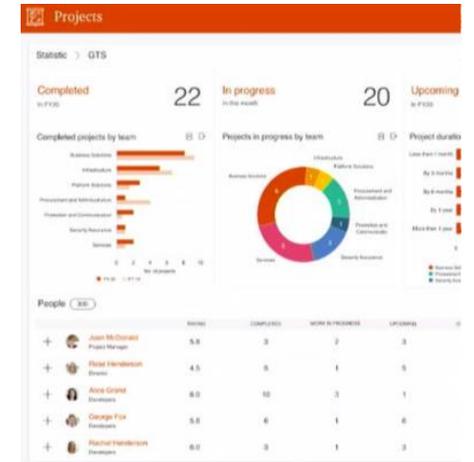
Управление работой с клиентами

Управление портфелем

Управление проектами

Управление рисками (и планирование)

Управление документацией



# Планирование аудита в сфере информационных технологий



Элемент системы управления	Примеры портфеля аудита в сфере информационных технологий	Потенциальный источник *
Процессы	Процессы COBIT® 2019	Цели управления и руководства COBIT 2019 <sup>13</sup>
Организационные структуры	Сторонние поставщики, дочерние предприятия, подразделения предприятия	Система планирования ресурсов предприятия (ERP), документация структуры предприятия, организационные диаграммы
Принципы, политики, процедуры	Конфиденциальность, законодательство, нормы и прочие требования по обеспечению соответствия	Юридическая служба, служба обеспечения конфиденциальности, служба безопасности, органы управления, службы управления рисками и обеспечения безопасности (GRC)
Информация	Отчеты о результатах проведения аудита в сфере информационных технологий	Требования комитета по аудиту
Культура, этика и поведение	Выполнение аудиторских рекомендаций, новые IT-инициативы	Сроки выполнения рекомендаций службы внутреннего аудита и руководства; выполненные рекомендации
Люди, навыки и компетенции	Тренинг, обеспечиваемый в связи с аудитом в сфере информационных технологий; тренинг, который должен быть организован в связи с проведением аудита в сфере информационных технологий; тренинг, связанный с информированностью о вопросах, касающихся проведения аудита в сфере информационных технологий	рекомендации Планы тренинга, планы личного развития
Услуги, инфраструктура и приложения	Приложения, базы данных, веб-сайты, операционные системы, виртуальные машины и т.п.	Реестр IT-активов

Источник: Журнал Ассоциации аудита и контроля информационных систем (ISACA) - 1 мая 2019 года - «Разработка плана проведения аудита в сфере информационных технологий с учетом задач информационных и смежных технологий (COBIT) 2019 года».

# Планирование аудита в сфере информационных технологий

## Годовое планирование

11

- Возможность применения подхода, основанного на **динамичном управлении портфелем**
  - Использование подхода, предусматривающего определение приоритетов на краткосрочную перспективу
  - Регулярный пересмотр / обновление плана проведения аудита (с целью отражения изменений в рисках и необходимости обеспечения гарантий)
- Обеспечение **повышенной гибкости** плана проведения аудита:
  - Попытки содействия при реализации **новых проектов / инициатив**
  - Это лучшее время для выстраивания отношений и подтверждения важности внутреннего аудита
- **Сотрудничество с основными заинтересованными лицами** (включая КА) для понимания любых новых и/или повышенных рисков, а также для оценки того, как лучше всего обеспечить гарантии
- Увеличение количества встреч с основными заинтересованными лицами по вопросам, касающимся хода выполнения задач в рамках деятельности. Использование (по возможности) видеозвонков **для формирования отношений и установления доверия.**



# Планирование аудита в сфере информационных технологий

## Годовое планирование – Предлагаемые приоритетные направления

12

### (1) Кибербезопасность (программы-вымогатели, кибершантаж)

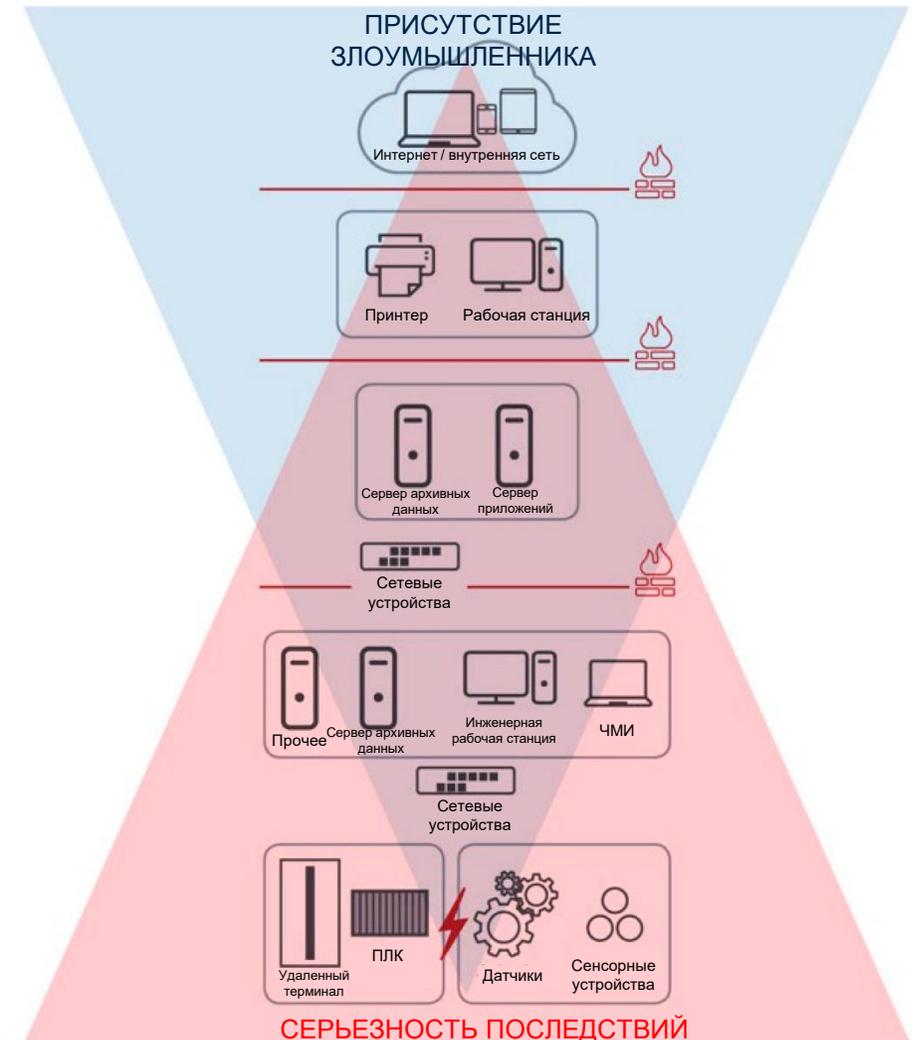
- Средства контроля доступа пользователей
- Резервирование и восстановление данных
- Нормативные требования, касающиеся защиты данных (GDPR и т.п.)



**Программа-вымогатель** – не позволяет вам получить доступ к вашим данным.



**Кибершантаж** - угроза передачи ваших данных другим лицам.



# Планирование аудита в сфере информационных технологий

## Годовое планирование – Предлагаемые приоритетные направления

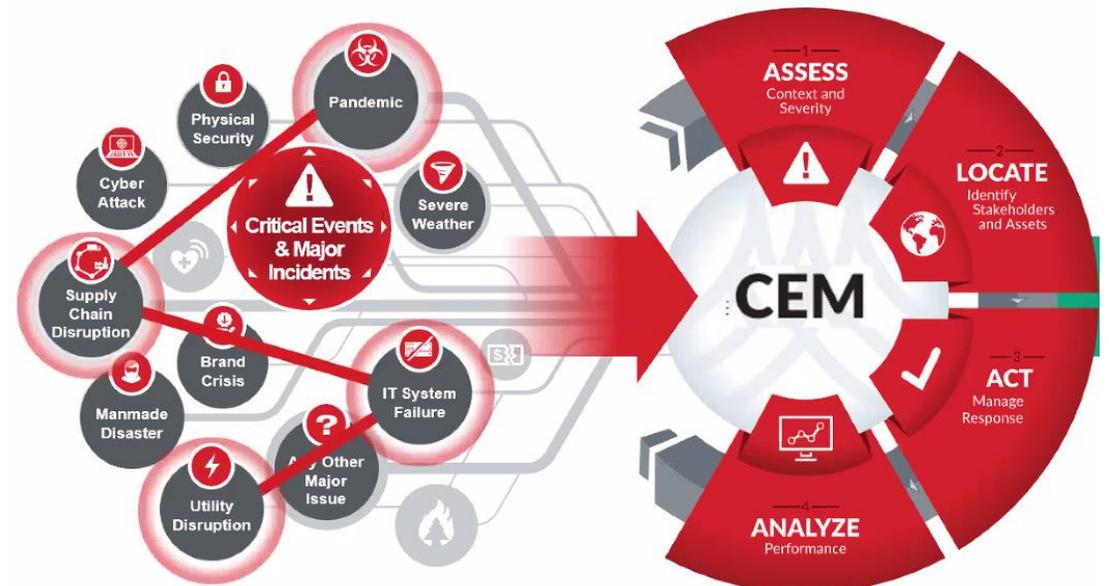
13

### (2) Бесперебойность бизнес-процессов

- Аварийное восстановление (CEM)
- Разделение основных групп (в случае карантинных мер)
- Анализ цифровых возможностей: от заключения сделок до взаимодействия с клиентами
- Повторный анализ ВИА и пессимистичных сценариев
- Планы управления мультимедиа

### (3) Пересмотр процессов в сфере информационных технологий, которыми НЕ управляют информационные технологии

### (4) Пересмотр действующих политик и основных принципов



### Предлагаемые приоритетные направления:

- ❑ Возможность удаленного аудита
- ❑ Наличие электронной документации (+возможность сканирования бумажных документов)
- ❑ Удаленный сквозной контроль (тщательные обсуждения), актуализация информации о ходе выполнения задач и предоставление отчета о результатах
- ❑ Наличие новых технологий для выполнения работы, например, Microsoft Teams, Zoom или Skype для проведения виртуальных встреч / семинаров (рекомендуется вести запись подобного взаимодействия для наличия соответствующих свидетельств, которые могут использоваться при проведении внутреннего аудита)
- ❑ Развитие аналитики с целью расширения покрытия и учета аномальных значений
- ❑ Регулирование контроля (во время периодов неопределенности работники ищут обходные пути в отношении существующих средств контроля)
- ❑ Рост рисков, связанных с мошенничеством

# Полезные ресурсы для проведения аудита в сфере информационных технологий

## NIST Cyber Security Framework



### OWASP TOP 10 INTERNET OF THINGS 2018

- Weak, Guessable, or Hardcoded Passwords**  
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.
- Insecure Network Services**  
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...
- Insecure Ecosystem Interfaces**  
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
- Lack of Secure Update Mechanism**  
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.
- Use of Insecure or Outdated Components**  
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.
- Insufficient Privacy Protection**  
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
- Insecure Data Transfer and Storage**  
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
- Lack of Device Management**  
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
- Insecure Default Settings**  
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
- Lack of Physical Hardening**  
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

50  
page

NIST Special Publication 800-82

## Guide To Industrial Control Systems (ICS) Security

www.50page.com

# Что дальше?

## □ **Аудиторы**

- Оценка ваших навыков (по сравнению с теми, которые потребуются в будущем)

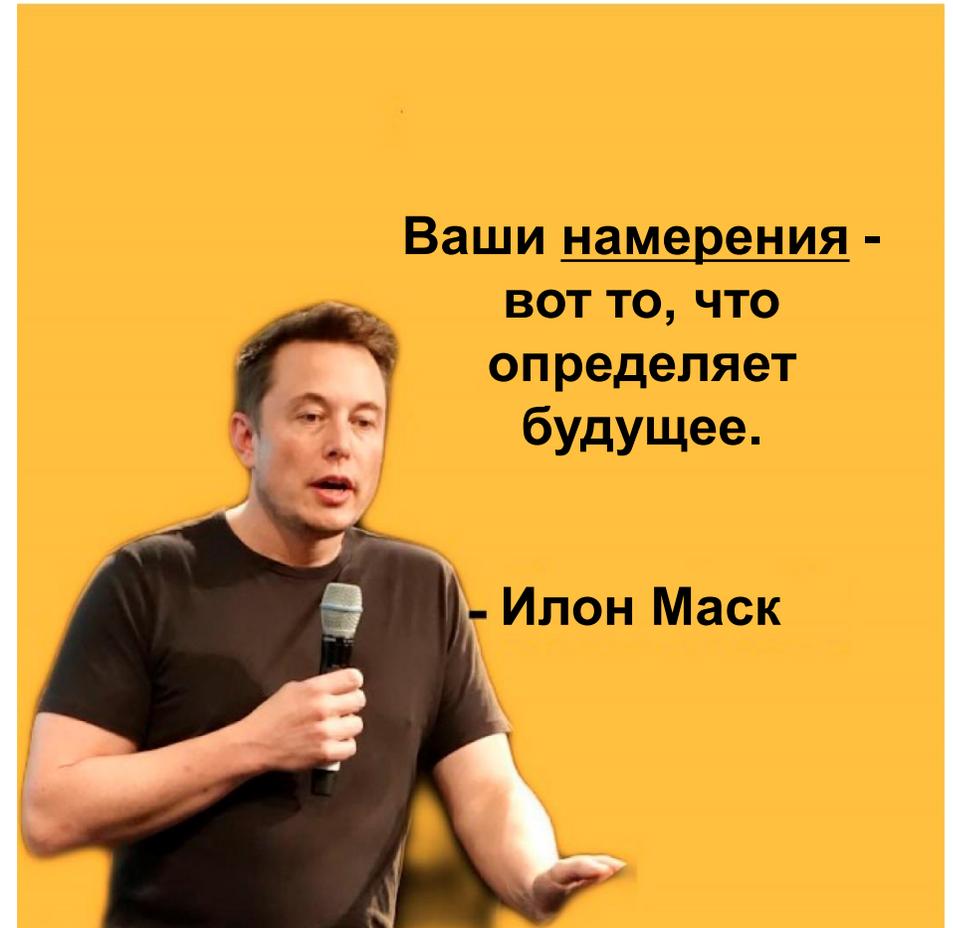
## □ **Руководители аудиторской проверки**

- Вложение средств в роботизированную автоматизацию процессов и искусственный интеллект
- Наем и поддержка сотрудников, разбирающихся в цифровых технологиях

## □ **Правительства / организации**

- Подготовка к кардинальным переменам в работе и распределении трудовых ресурсов
- Принятие технологий и цифровой трансформации
- Приоритетное внимание вопросам, связанным с графическим пользовательским интерфейсом приложений и качеством пользовательского взаимодействия

## **Никто не знает, каким будет цифровое будущее**



**Ваши намерения -  
вот то, что  
определяет  
будущее.**

**- Илон Маск**

**СПАСИБО ЗА ВНИМАНИЕ!**

---