



19 октября 2021 | конференция

11:00 — 16:00

Управление инцидентами: SOAR, IRP, SOC

Оптимизация взаимодействия с внешним SOC: финансы, юридические аспекты, коммуникации

Ксения Темникова, кандидат экономических наук,

- доцент кафедры «Информационная безопасность» факультета информационных технологий Московского политехнического университета,
 - эксперт по ESG-стратегии,
 - заместитель генерального директора по стратегии и развитию ООО «Профконсалт ИСМ»,
 - член СРО «НАКД»,
 - член Ассоциации независимых директоров,
 - член Национального реестра профессиональных корпоративных директоров,
 - консультант, ведущий аудитор системы управления непрерывности бизнеса (ISO 22301:2019); систем управления информационной безопасностью (ISO/IEC 27001:2013), систем управления противодействием коррупции (ISO 37001:2016), комплаенс (ISO 37301:2021)
-

Фокус внимания

Как сократить трудозатраты и расходы на комплексный мониторинг ИБ?

Как обеспечить непрерывность бизнеса



Как проактивно защитить всю организацию, снизить вероятности ошибок, риски возникновения ИБ-инцидентов и времени на реагирование и расследование, нивелировать экономический ущерб от недоступности ресурсов и потери конфиденциальной информации?

SOC –

- команда профессионалов
- набор процессов, структурированных под Вашу организацию

За какими данными «охотятся» злоумышленники?

- конфиденциальная информация, включая информацию, касающуюся ESG-факторов
- другая информация

Содержание

- В чем проблема
- Как найти решение
- Что будет, если не разрабатывать ESG-стратегию?
- «Дорожная карта»: финансы, юридические аспекты, коммуникации

ESG

Environmental (окружающая среда)
Social (социальный)
Governance (корпоративное управление)





1

В чем проблема?

В каких условиях внешней среды
осуществляется взаимодействие с
внешним SOC в настоящее время?

Устойчивое развитие и ESG: общемировой тренд

75%

инвесторов
заинтересованы
в ответственном
инвестировании

90%

Миллениалов
планируют
увеличить свои
вложения с учетом
концепции
ответственного
инвестирования в
ближайшие 5 лет

94%

Ценных бумаг
компаний,
ориентированных
на ESG, показали
более высокую
доходность в 2020
году, чем базовые
индексы

600

рейтингов и
рэнкингов,
относящихся к
Целям устойчивого
развития (ЦУР) и
ESG*

120

Публичных
стандартов для
раскрытия
корпоративной
ESG-информации

«Затраты на аналитические продукты и рейтинги в области ESG за последние два года выросли на 20%, а в мире этот показатель уже приближается почти к миллиарду долларов. Это очень значительная сумма»**.

Источники:

* <https://www.sustainability.com/thinking/rate-the-raters-2020/>

** <https://www.finversia.ru/publication/experts/konflikty-reitingov-102514>

Рост популярности ответственного инвестирования

- **75%** инвесторов заинтересованы в ответственном инвестировании (Morgan Stanley Institute for Sustainable Investing).
- **90%** миллениалов планируют увеличивать свои вложения с учетом концепции ответственного инвестирования в ближайшие 5 лет (Morgan Stanley Institute for Sustainable Investing).
- **94%** ценных бумаг компаний, ориентированных на ESG, показали более высокую доходность в 2020 году, чем базовые индексы (BlackRock).
- **100%** - прирост инвестиций в ESG в 2020 году (ETF Database).
- **36%** - прирост количества инвесторов, разделяющих принципы ответственного инвестирования ООН (UN PRI), только за 6 месяцев 2021 года
- **¾ из 300** опрошенных PwC инвесторов, включая пенсионные фонды и страховые компании, заявили, что к 2022 году прекратят инвестировать в традиционные фонды, заменив их вложениями в ESG-продукты.



Первая

Основные сведения ▾

Кампании ▾

Цели ▾

Участвуйте! ▾

Партнерства ▾

Мультимедиа ▾

Ресурсы ▾

Цели в области устойчивого развития

Цели в области устойчивого развития являются своеобразным призывом к действию, исходящим от всех стран — бедных, богатых и среднеразвитых. Он нацелен на улучшение благосостояния и защиту нашей планеты. Государства признают, что меры по ликвидации бедности должны приниматься параллельно усилиям по наращиванию экономического роста и решению целого ряда вопросов в области образования, здравоохранения, социальной защиты и трудоустройства, а также борьбе с изменением климата и защите окружающей среды.

Источник:

<https://www.un.org/sustainabledevelopment/ru/sustainable-development-goals/>

Цели в области устойчивого развития

Приоритизация Целей устойчивого развития (ЦУР) ООН и внедрение их в стратегию развития компании

Например, 5 целей из 17

Важно сформировать матрицу стандартов, применимых для достижения [Целей в области устойчивого развития](#), включающую международные стандарты



Показатели устойчивого развития предприятий промышленности:

–перечень показателей устойчивого развития, используемыми зарубежными промышленными предприятиями;

–перечень факторов, влияющих на внедрение показателей устойчивого развития;

–этапность внедрения показателей устойчивого развития промышленными предприятиями.

- стандарты Российской Федерации в сфере технического регулирования и стандартизации (например, ГОСТ Р ИСО 37101–2018, ISO 37101:2016, ИСО 37120:2014, ИСО/ТС 37151:2015, ИСО 13065:2015, ИСО 10795:2011, ИСО 14064-1:2006, ИСО 26000:2010, ИСО 15392:2008, ИСО 14001:2015, ИСО/ТС 37150:2014, ИСО 73:2009, ИСО 82:2014 и другие);
- правовые акты Российской Федерации, регулирующие сферу устойчивого развития;
- проекты законодательных инициатив, связанных с устойчивым развитием, климатическими изменениями, требованиями к нефинансовой отчетности предприятий промышленности;
- прочая информации из прочих открытых источников.

Глобальные вызовы vs. Глобальные возможности.
Как ESG тренды меняют мировую экономику?



ESG – это совокупность характеристик, критериев и стандартов, при следовании которым организация участвует в решении экологических, социальных и управленческих вопросов.

Проблема

Жесткие требования в отношении экологизации и декарбонизации экономической деятельности

ESG

Жесткие требования в отношении применения факторов ESG при принятии инвестиционных решений со стороны участников финансового рынка

Система взаимоотношений с потребителями и поставщиками

- заключение международных контрактов с учетом требований о «прослеживаемости»
- соблюдение принципов ESG по всей цепочке поставок
- разработка и внедрение системы мониторинга и измерения удовлетворенности потребителей
- ESG-аудит поставщиков
- ESG-маркетинг

Требуется ответственное ведение бизнеса и соблюдение принципов устойчивого развития и ESG в рамках **всей цепочки создания ценностей**

Неподготовленность компаний к работе в новых условиях конкурентной среды усложняет/препятствует заключению контрактов и доступу к финансированию

Отсутствие «общих правил игры» в новой экономической реальности

Быстрый темп вхождения в процессы ESG-трансформации

IR

- доступ к долгосрочному финансированию (важно информировать инвесторов не только о стоимости компании в текущий момент, но и о создании долгосрочной стоимости компании)
- Руководство для эмитента: как соответствовать лучшим практикам устойчивого развития

2

Как найти решение?

Финансы

Юридические аспекты

Коммуникации

Как найти решение?

Интересы внутренних
заинтересованных сторон

ESG

Интересы внешних
заинтересованных сторон

Целеполагание

Проведение ESG-сессии

**Разработка и развертывание корпоративной
ESG-стратегии**

переосмысление стратегии развития компании с
учетом современных тенденций в мире и в России,
а также для разработки и осуществления комплекса
мероприятий по ESG-трансформации

Разработка и осуществление комплекса
мероприятий по ESG-трансформации, включая
подготовку и переподготовку кадров

Первоочередные практические шаги

- Приоритизация Целей устойчивого развития (ЦУР) ООН и внедрение их в стратегию развития компании
- Идентификация и институционализация ESG-качеств предприятия
- Соответствие действий компании меняющимся требованиям международных стандартов и актуальной международной практике
- Разработка внутренних документов. Обучение персонала
- Оценка лидерского ESG-потенциала компании. Получение ESG-рейтинга.
Разработка дорожной карты мероприятий по повышению позиций компании в ESG-рейтингах
- Подготовка отчетности, включая применимую «дорожную карту» для осуществления необходимых изменений. ESG-показатели в системе корпоративной отчетности. Цифровая отчетность ESEF: актуальные требования и перспективы

Продукт или
экосистема
продукта

Диагностический
ESG-аудит
поставщиков

Умные данные
для принятия
управленческих
решений.
Автоматизация
контроля ESG-
параметров.
Информационная
безопасность

ESG-сессия

Основные этапы проведения стратегической ESG-сессии



Каждая минута коллективной работы помогает продвигаться к цели

Время

ESG

- ESG-стратегия как способ действий в ситуации, когда для прямого достижения основной цели недостаточно наличных ресурсов и как важный элемент управления
- ESG-факторы как идеология стратегии развития компании



З

Работа с документами

Финансы

Юридические аспекты

Коммуникации

Международные стандарты (выборка)

- ISO 14001 Environmental management systems — Requirements with guidance for use (серия стандартов ISO 14000)
- ISO 45001 Occupational health and safety management systems — Requirements with guidance for use (серия стандартов ISO 45000)
- ISO 37001:2016 Anti-bribery management systems — Requirements with guidance for use
- ISO 37301:2021 Compliance management systems — Requirements with guidance for use
- ISO 26000:2010 Guidance on social responsibility
- ISO 50001:2018 – ENERGY MANAGEMENT (серия стандартов ISO 50000)

Внедрение международных стандартов способствует соблюдению интересов акционеров, повышению доверия со стороны деловых партнеров, соблюдению принципов ESG, успешному развитию компаний на мировом рынке

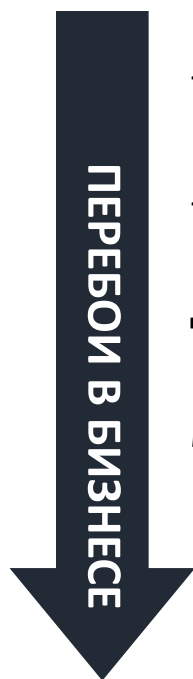
Международные стандарты (выборка)

- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (серия стандартов ISO 270XX);
- ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements;
- ISO 31000 – ISO 31000:2018 Risk management — Guidelines (Менеджмент рисков. Принципы и руководящие указания)
- IEC 31010 – IEC 31010:2019 Risk management — Risk assessment techniques
- ISO GUIDE 73 – ISO GUIDE 73:2009 Risk management — Vocabulary (Словарь терминов по управлению рисками)
- COSO – «Концептуальные основы управления рисками организации: интеграция со стратегией и управлением деятельностью» COSO 2017 г.

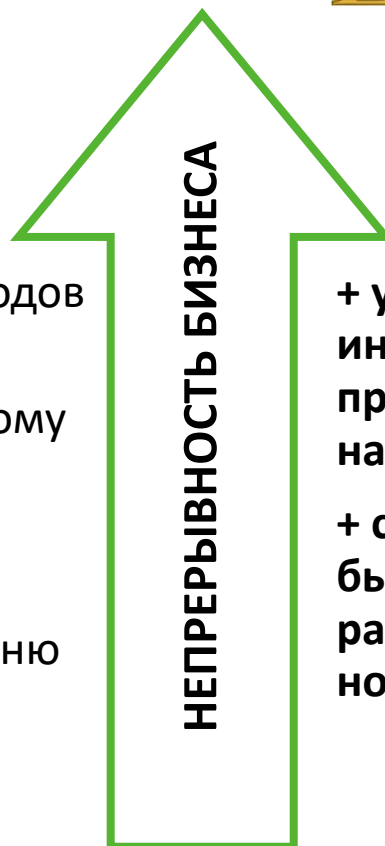
ESG и непрерывность бизнеса

ESG

Как обеспечить
непрерывность
бизнеса



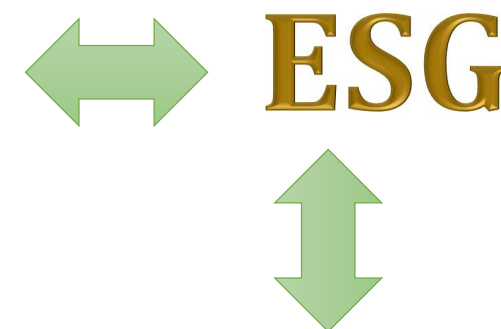
- потеря клиентов, доходов и репутации
- неготовность к быстрому восстановлению деятельности
- несоответствие международному уровню



- + устойчивость к инцидентам любой природы и направленности
- + способность быстро восстанавливать работоспособность до нормального уровня

ESG и непрерывность бизнеса

- Стратегия и планирование непрерывности бизнеса
- Анализ воздействия на бизнес (BIA). Определение RTO и PRO.
- Оценка рисков. Модели и сценарии угроз
- План обеспечения непрерывности бизнеса (BCP) и план восстановления бизнеса (DRP)
- Разработка плана, ключевые факторы успеха и внедрение плана
- Программа повышения осведомленности сотрудников
- Обучение сотрудников, оценка осведомленности сотрудников
- Учения
- Тестирование плана обеспечения непрерывности бизнеса (BCP) и плана восстановления бизнеса (DRP). Типы тестирования
- Оценка текущего состояния и разработка дорожной карты для достижения целевого состояния.



**Провести аудит
непрерывности бизнеса
намного экономичнее,
чем устранять
последствия сбоев**

ESG и непрерывность бизнеса

Согласно BCI Horizon Scan:

- главной причиной нарушения деятельности за последний год были инциденты, связанные со здоровьем сотрудников;
- кибератаки остаются негативным фактором, однако организации сводят их воздействие к минимуму (основными угрозами в предстоящем году по-прежнему считаются кибератаки, экстремальные погодные условия и перебои в работе IT-систем и телекоммуникаций);
- наибольшие средние издержки организаций связаны с нарушением деятельности вследствие изменений нормативно-правовой базы.

Источник: <https://reports.weforum.org/global-risks-report-2020/executive-summary/>

Результаты сравнительного анализа непрерывности бизнеса:

- больше организаций теперь имеют систему менеджмента непрерывности бизнеса, сертифицированную по ISO 22301 (20,5%, что на 6,5 процентных пункта больше, чем в 2018 году);
- организации, которые сообщают о сертификации по ISO 22301, также сообщили **о меньшем количестве инцидентов за последние 12 месяцев**;
- многие организации предпочитают использовать несколько стандартов, а не пройти сертификацию по одному стандарту.

Методологическая основа

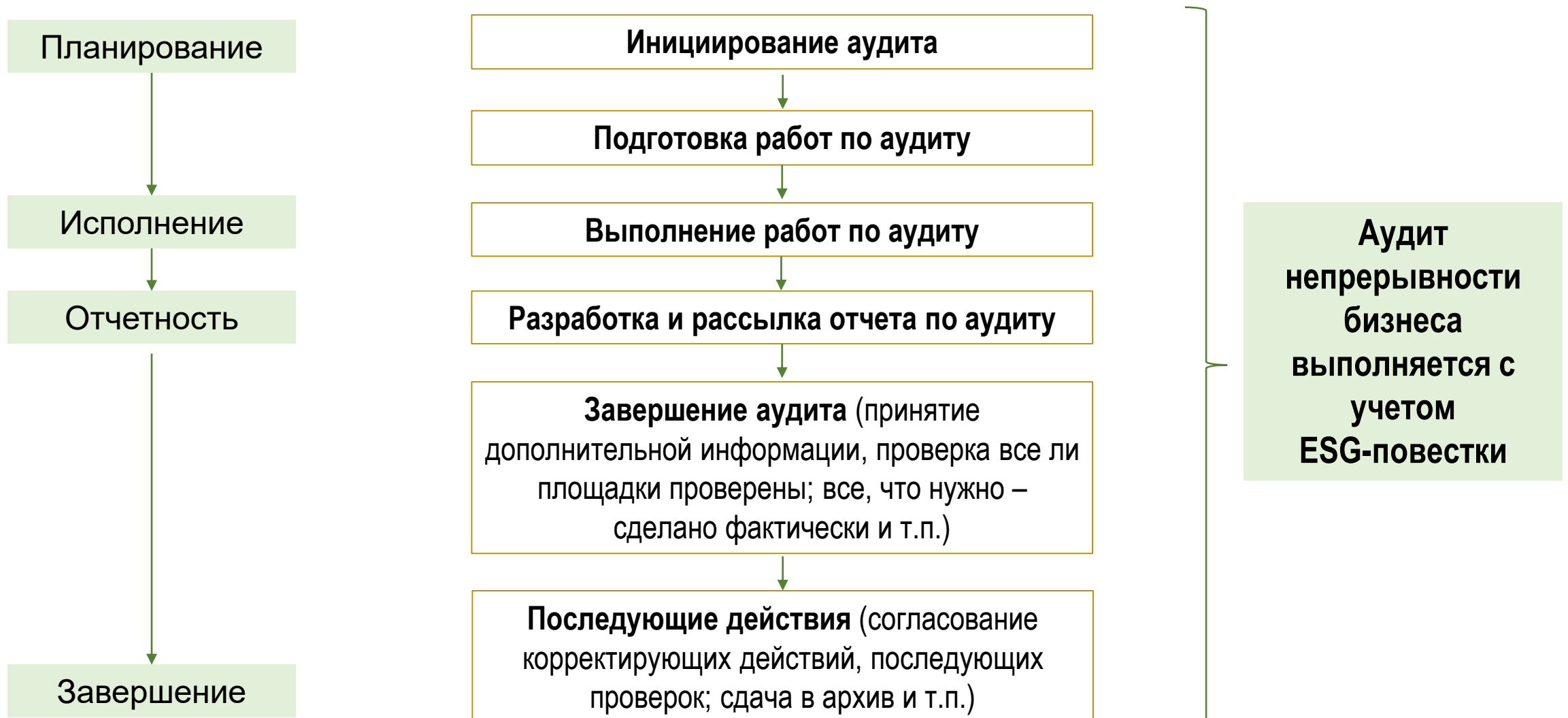
- ISO 19011:2018 Guidelines for auditing management systems
- ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements
- ISO 22300:2021 Security and resilience — Vocabulary
- ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 20000-1:2011 Information technology — Service management — Part 1: Service management system requirements
- ISO 28000:2007 Specification for security management systems for the supply chain
- ISO 31000:2018 Risk management — Guidelines
- и другие стандарты, руководства, своды правил, библиотеки, документы

**Аудит проводится
в соответствии с
международными
стандартами**

**Используется новое
поколение стандартов
в области управления
непрерывностью
бизнеса**

**Используются лучшие
практики управления
непрерывностью
бизнеса**

Основные действия при аудите



Программа обучения «ESG-стратегия»

- Программа разработана в трех вариантах:
 - 16 часов;
 - 40 часов;
 - 72 часа.
- Срок обучения и график проведения занятий – по согласованию.
- Форма обучения – смешанная, очное обучение дополняется электронным ресурсами. С учетом санитарно-эпидемиологической обстановки и производственной необходимости применяется очная и/или дистанционная форма обучения.

4

Что будет, если...

Финансы

Юридические аспекты

Коммуникации

Что будет, если не разрабатывать ESG-стратегию?

1

Компания будет утрачивать доверие деловых партнеров, так как конкуренты не только разрабатывают и внедряют **ESG-стратегии**, оцифровывают управление системой менеджмента, но и внедряют **автоматизированные системы контроля ESG-параметров**, соответствия требованиям международных стандартов.

Отставание от конкурентов будет нарастать быстрыми темпами

Компания не сможет подтвердить лидерство, заботу о клиентах (например, что компания предоставляет более качественные по сравнению с конкурентами услуги и заботится о защите информации своих клиентов). Это особенно актуально для компаний, выходящих на международный рынок

Что будет, если не разрабатывать ESG-стратегию?

2

Будут все более остро проявляться **внутренние проблемы и противоречия** (особенно связанные принятием управленческих решений, активным развитием динамических межмашинных цифровых инфраструктур, стремительно растущим объемом данных, подвергающихся обработке, **с оценкой влияния ESG-параметров**, систем менеджмента на экономические показатели компании и др.), которые в конечном счете **снижат экономическую эффективность компании, ее инвестиционную привлекательность.**

Что будет, если не разрабатывать ESG-стратегию?

3

Критического значения достигнет плохая взаимосвязь между корпоративными информационными системами и документами, описывающими **системные процессы, влияющие на соблюдение необходимых ESG-параметров**, что может приводить к системным ошибкам.

Как развивать корпоративное управление?
Роль ESG-комитета в Совете директоров?
Наблюдательный совет как драйвер ESG-повестки?

Цена ошибки при принятии управленческих решений?

Для киберфизических систем **критически важно не допустить перехвата управления и навязывания чужих алгоритмов управления**. Этот тезис относится, прежде всего, к информационной безопасности предприятий, которые внедряют (внедрили) **программы цифровизации**.

Что будет, если не разрабатывать ESG-стратегию?

4

Будет нарастать разрыв между высококвалифицированными специалистами в области оцифровки управления системой менеджмента, информационной безопасности, автоматизации производства и общим низким уровнем информированности специалистов по внедрению систем менеджмента о разнообразии цифровых решений, прикладных инструментов, которые можно применять для реализации требований систем менеджмента, мониторинга, развития внутреннего аудита и постоянных улучшений.

Как повлияет на формирование и развитие команд и их эффективность?

Как повлияет на системы менеджмента и позиции компании в ESG-рейтингах?

Как повлияет на ESG-показатели в системе корпоративной отчетности? (цифровая отчетность ESEF: актуальные требования и перспективы)



5

«Дорожная карта»

Финансы

Юридические аспекты

Коммуникации

Финансы

Фокус внимания:
Как сократить
трудозатраты и
расходы на
комплексный
мониторинг ИБ?

Общая стратегия развития предприятия и
Стратегия взаимодействия с внешним
SOC: раздел «Финансы»

Бизнес-планирование с учетом рисков ИБ

Ключевые показатели эффективности (KPI)

Доходы предприятия

Расходы предприятия

Серия практических семинаров по бизнес-
планированию с учетом рисков ИБ

Другие вопросы

Юридические аспекты

Фокус внимания:

Как проактивно защитить всю организацию, снизить вероятности ошибок, риски возникновения ИБ-инцидентов и времени на реагирование и расследование, нивелировать экономический ущерб от недоступности ресурсов и потери конфиденциальной информации?

Общая стратегия развития предприятия и
Стратегия взаимодействия с внешним SOC: раздел
«Юридические аспекты»

Организация договорной работы: пересмотр
предмета договора, раздела об ответственности

Режим коммерческой тайны

Юридические аспекты страхования рисков ИБ

Обзор судебной практики

Другие вопросы

Коммуникации

Как сократить трудозатраты и расходы на комплексный мониторинг ИБ?

Как проактивно защитить всю организацию, снизить вероятности ошибок, риски возникновения ИБ-инцидентов и времени на реагирование и расследование, нивелировать экономический ущерб от недоступности ресурсов и потери конфиденциальной информации?

Общая стратегия развития предприятия и
Стратегия взаимодействия с внешним SOC: раздел
«Коммуникации»

Внутренние коммуникации

Внешние коммуникации

Повышение осведомленности сотрудников,
клиентов

Методы коммуникации в области ИБ

Другие вопросы

Ксения Темникова

Моб. тел.: +7(985)564-15-00

E-mail: 5577ksenia@gmail.com

Спасибо за внимание !
