Конференция
Управление инцидентами: SOAR, IRP, SOC как ответ на новые вызовы 6 апреля 2022

Управление инцидентами. Что важно знать об информационной безопасности в контексте ESG-повестки

Ксения Темникова, кандидат экономических наук,

- эксперт по ESG-стратегии
- руководитель Международного центра компетенций по устойчивому развитию (ESG) АСПОЛ
- заместитель председателя комитета по ESG СРО «Национальная ассоциация корпоративных директоров»
- консультант, ведущий аудитор систем управления информационной безопасностью (ISO/IEC 27001:2013), систем управления непрерывности бизнеса (ISO 22301:2019); систем управления противодействием коррупции (ISO 37001:2016), комплаенс (ISO 37301:2021)
- доцент кафедры «Информационная безопасность» Московского политехнического университета

Содержание

- Проблематика управления инцидентами
- Задачи достижения целей устойчивого развития, соответствия ESG-повестке

  Какие вызовы? Как найти решение?

  Что важно знать об информационной безопасности в контексте ESG-повестки?

Кейс 1

Кейс 2

Кейс 3

1

Проблематика управления инцидентами

Задачи и опыт управления инцидентами

- Построение систем анализа, управления и реагирования на инциденты
- Сбор и анализ ИБ-событий (Security Information and Event Management, SIEM)
- Платформы кибербразведки (Threat Intelligence Platform)
- Управление ИБ-инцидентами (Incident Response Platforms, IRP)
- Системы безопасности и автоматического реагирования (Security Orchestration, Automation and Response, SOAR)
- Аналитическое хранилище (Security Data Lake)

Управление инцидентами:

SOAR, IRP, SOC решения **ускоряющие разбор** ИБ-инцидентов

Проблематика

- Большой объем информации, который нужно обработать
- Возрастающая сложность управления инцидентами
- Понятие «инцидент» в разных системах менеджмента
- Кадровый голод
- Текучка кадров
- Высокая эмоциональная, психологическая нагрузка
- Требования инвесторов
- Требования потребителей
- Новые вызовы

Особенности управления инцидентами:

- работа «внутреннего SOC»
- коммерческий SOC
- переход от «внутреннего SOC» к сервисной модели

Аутсорсинг

- SOC
- Cloud провайдеры

- Кто, кому и в какое время может/должен передавать информацию?
- На какой предмет обмениваться информацией?
- Процессы передачи информации. Как контролировать?
- Аудит первой стороны? Аудит второй стороны? Аудит третьей стороны?
- Как налагать ответственность? Для этого есть юридические основания?
- Как проверить хранение данных? Как проверить доступ к информации?
- Какие меры по защите
- Какие политики применяются в компании? Политика ИБ и НБ?
- Есть ли система управления информационной безопасностью?

Удаленная работа

- Размытие периметра
- Защищенный доступ
- Многофакторная аутентификация
- Утечка данных
- Фишинговые сообщения
- Целевые фишинговые атаки на ТОП-менеджеров
- Социальная инженерия

- **BYOD** - добровольные программы «принеси свое устройство» (bring your own device)

- **Zero Trust** - Электронная среда является средой нулевого доверия, поэтому бизнес стал переходить на системы защиты от сетевых угроз Zero Trust Network Access (ZTNA)

2

Задачи достижения целей устойчивого развития, соответствия ESG-повестке

Какие вызовы? Как найти решение?

Что важно знать об информационной безопасности в контексте ESG-повестки?

Качество процессов управления

В 2015 году Генеральная Ассамблея ООН приняла Декларацию об устойчивом развитии общества на период **до 2030 года**, в которой определены 17 целей устойчивого развития (ЦУР)

Вслед за декларацией вступила в силу и стратегия Международной организации по стандартизации (ISO) на период **до 2030 года**

Цели в области устойчивого развития

Цели в области устойчивого развития ООН представляют собой 17 глобальных целей, принятые всеми 193 странами-членами ООН в рамках «Повестки дня в области устойчивого развития на период до 2030 года»

Документ: Цели в области устойчивого развития / ООН: Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года Резолюция Генеральной Ассамблеи 25 сентября 2015 г.
Подробнее: https://www.un.org/sustainabledevelopment/ru/

ESG

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

Цифровая предиктивная модель

Цифровой двойник

Открытость данных

ESG-рейтинги (рэнкинги)

ESG-стратегии

SOAR, IRP, SOC решения ускоряющие разбор ИБ-инцидентов по всей цепочке создания ценности

Вызовы

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

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

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

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

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 институциализация 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

Compliance

Требования законодательства Российской Федерации, в том числе:

- Федеральный закон от 27 июля 2006 г. N **152-ФЗ** "О персональных данных" (с изменениями и дополнениями)
- Федеральный закон от 26 июля 2017 г. N **187-ФЗ** "О безопасности критической информационной инфраструктуры Российской Федерации"

Нормативные акты и рекомендации Банка России

Требования внутренних нормативных актов	• Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/EC (Общий Регламент о защите персональных данных) General Data Protection Regulation (**GDPR**)
Требования контрактов	• международный стандарт **PCI DSS**

Текущая ситуация

- Пересмотр цепочек поставок
- Импортозамещение
- Быстрое внедрение изменений в компаниях (в ряде случаев без должной подготовки)
- Политика вендоров
- Высокая плотность и сложность атак
- Встраивание в библиотеки

- Управление рисками
- Должная осмотрительность
- Цифровой след

Мероприятия

- Идентификация информационных активов
- Все ли риски корректно идентифицированы?
- Переоценка информационных активов и рисков
- Системное взаимодействие: **ИТ-ИБ-Compliance**
- Защита периметра
- Защита персональных данных
- Защита от вредоносного кода
- Контроль действий привилегированных пользователей
- Мониторинг и логгирование
- SDLC (Secure Development Life Cycle)
- Обеспечение **непрерывности и устойчивости**
- **Обучение пользователей + системная проверка знаний и навыков (тестирование, учения и др.)**
- Другие мероприятия

Управление инцидентами:

SOAR, IRP, SOC решения **ускоряющие разбор** ИБ-инцидентов

Аудит

Стандартизация

Разработка стратегии

Международные стандарты, проекты, руководства

- **GRI стандарты Глобальной инициативы по отчетности**
- **SASB совет по стандартам учета в области устойчивого развития**

Ожидается появление нового стандарта

- CDP проект по раскрытию информации об углероде
- TCFD руководство по раскрытию финансовой информации, связанной с изменением климата
- Другие стандарты

Большое количество стандартов

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.

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)
- ISO 19011:2018 Guidelines for auditing management systems
- ISO 28000:2022

Раскрытие информации

Рекомендации Банка России по раскрытию публичными акционерными обществами нефинансовой информации, связанной с деятельностью таких обществ, и другие проекты Банка России по стимулированию раскрытия ESG-факторов

Концепция развития публичной нефинансовой отчетности, утвержденная Распоряжением Правительства РФ от 05.05.2017 N 876-р.

Выводы и рекомендации

- Информационная безопасность и непрерывность пронизывают всю ESG-повестку (не только G), причем по всей цепочке создания ценности (необходимо знать как обеспечивается информационная безопасность, включая управление инцидентами у поставщиков, потребителей и других деловых партнеров)
- Фокус внимания:
  - ✓ умные данные для принятия управленческих решений
  - ✓ автоматизация контроля ESG-параметров, ESG-стратегия как электронная модель
  - ✓ раскрытие информации
- Требуется пересмотр подходов к
  - ✓ идентификации информационных активов
  - ✓ идентификации и оценке рисков информационной безопасности
  - ✓ выявлению и использованию возможностей
  - ✓ повышению осведомленности персонала компании и поставщиков
  - ✓ планированию и проведению аудита информационной безопасности
- Необходимо уточнение задач управления инцидентами и углубленное изучение опыта применения SOAR, IRP, SOC решений ускоряющих разбор ИБ-инцидентов по всей цепочке создания ценности

Темникова Ксения Николаевна

Экономист, юрист, специалист в области международных отношений

кандидат экономических наук

Ведущий аудитор по системам менеджмента в соответствии с международными стандартами ISO, эксперт в области устойчивого развития, непрерывности бизнеса, разработке стратегий.

Тел. +7(495) 697-44-45
E-mail: temnikova@aspolrf.ru

Спасибо за внимание !