Трубная Металлургическая Компания

Москва 2023 г.

Актуальные вопросы комплексной защиты металлургического Предприятия в рамках взаимодействия подразделений информационной и экономической безопасности

История. 1

В период становления коммерческой безопасности в России, основное развитие процессов защиты бизнеса основывалось на усилиях в области экономической безопасности и финансовой аналитики. В рамках должной осмотрительности активно совершенствовались процессы проверки партнёров и контрагентов, в то время как, информационная безопасность присутствовала обособленно, делая основной упор на методологию и соответствие законодательным требованиям.

Развитие. 2

С начала нулевых годов картина серьёзно поменялась: массовое внедрение современных средств защиты информации, контроля движения данных и выявления утечек (DLP), появление принципиально новых классов СЗИ с уникальными возможностями (SIEM\UEBA\NGFW\IDS.IPS\NTA.NDR) серьёзно расширили возможности подразделений информационной безопасности.

Компании стали применять более современные методы обработки данных, включая Bigdata, Data since, ИИ для целей максимизации прибыли в рамках электронной коммерции.

Появились новые ИТ- профессии, стали востребованы новые навыки и знания от персонала, включая подразделения безопасности.

Совершенствование. 3

В текущих условиях на вооружении подразделений безопасности появились новые эффективные web- сервисы проверки партнёров/контрагентов (Контур.Фокус/Спарк-Интерфакс и т.д.).

Активное развитие приняли средства бизнес- аналитики (Power BI/Qlik), появились российские аналоги.

Объекты защиты. 4

Одновременно, сильно расширился пул объектов защиты, информационных системы, содержащих критические данные:

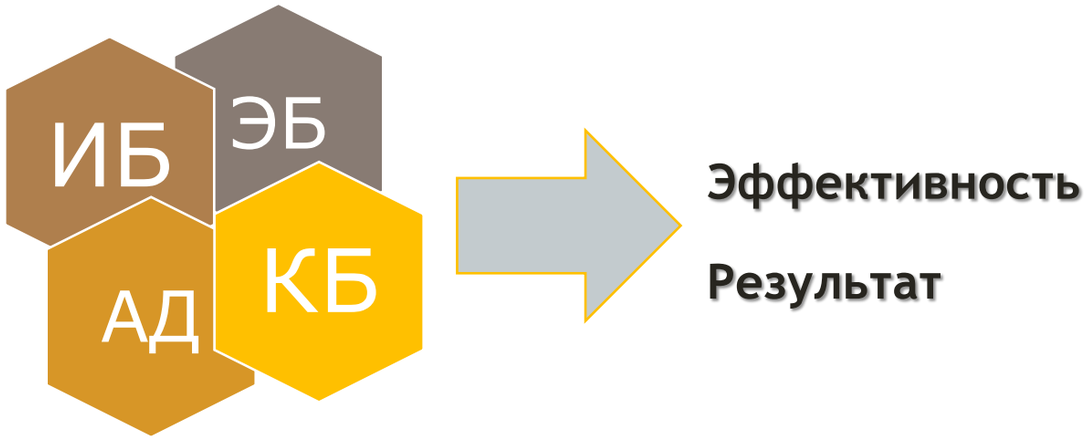
1. Персональные данные
2. Коммерческая тайна и «ноу-хау»
3. Биометрия
4. Объекты КИИ
5. Инсайдерская информация
6. Банковская тайна
7. Врачебная тайна
8. Платёжная информация

Взаимодействие. 5

Развитие технологий и массовая цифровизация породила новые угрозы и вызовы. Работать по устаревшим канонам и парадигмам жёсткого разделения по направлениям, стало не эффективно!

Появились новые точки соприкосновения:

1. Информационной безопасности
2. Экономической безопасности
3. Объектовой безопасности
4. Кадровой безопасности



Синергия. 6

Основная цель комплексной безопасности по минимизации ущерба и защите собственности Предприятия привела к новым моделям взаимодействия подразделений, где роль специалистов информационной безопасности в реализации мер предотвращения экономического ущерба, резко возросла!

В тоже время, востребованность ИТ-навыков у работников экономической безопасности и аналитики стали обязательными!

Новые возможности. 7

Одним из эффективных инструментов по предотвращению экономических потерь в рамках снабжения e-commerce, выявлению признаков сговора и недопустимых способов ведения закупочных процедур – стал инструмент **«Антифрод»**, адаптированный под потребности Предприятия и эффективно управляемый Службой экономической безопасности ПАО «ТМК».

Мы впервые из Российских Предприятий металлургии смогли адаптировать одну из платформ систем класса «Антифрод» под особенности производственного предприятия, получив экономический эффект, более 150 млн. рублей за непродолжительный период эксплуатации

Актуальные вопросы взаимодействия. 8

Общие зоны взаимодействия ЭБ и ИБ в текущих условиях сложившейся обстановки:

1. Участие в проверки зарубежных партнёров, где от подразделений ИБ требуется помощь в формировании достоверного цифрового профиля потенциального поставщика в целях выявления прямого или косвенного мошенничества (особенно на территории АТР).
2. Участие в выявлении признаков сговора поставщиков на цифровых платформах.
3. Участие в выявлении некондиционного ИТ- оборудования и программного обеспечения, способного нанести потенциальный вред производственным процессам, особенно в сегменте АСУТП (КИИ)

Какие угрозы предотвращаем. 9

1. Минимизация или исключение рисков кибер- атак на цепочку поставок в рамках закупочной деятельности (особенно оборудования и компонентов зарубежного производства).

2. Минимизация рисков нарушения эксплуатации производственного высокотехнологичного оборудования (включая располагающегося в сегментах АСУТП).

Начальник Управления
информационной безопасности СЭБ
ПАО «ТМК»

Севостьянов Александр
Владимирович, 16.03.2023

**Узнай больше
о компании ТМК**

**ТМК eTrade
Интернет-магазин труб**

**Премиальные резьбовые
соединения ТМК UP**