ОТРАСЛЕВОЙ ЦЕНТР КОМПЕТЕНЦИЙ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ПРОМЫШЛЕННОСТИ

Оценка состояния выполнения законодательства субъектом КИИ (метрики зрелости)

Эксперт Отраслевого центра компетенций
по ИБ в промышленности

Христолюбова Анна Анатольевна

НПП "Гамма"

ФГУП «НПП «ГАММА»
ЕКАТЕРИНБУРГСКИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР
12 июля 2023 г.

Кратко об основах…

Устойчивое функционирование КИИ при проведении в отношении неё компьютерных атак

(КИИ = объекты критической информационной инфраструктуры)

КРИТЕРИЕМ ОТНЕСЕНИЯ К ОДНОЙ ИЗ СФЕР ЯВЛЯЕТСЯ ПРОЦЕСС, НО НЕ РЕЗУЛЬТАТ

МЕРЫ В ОТНОШЕНИИ КОНКРЕТНОГО ТИПА ОБЪЕКТА ВОЗДЕЙСТВИЯ (ИС, АСУ, ИТКС), НО НЕ СУБЪЕКТА КИИ

ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД (ВЕДЕНИЕ РЕЕСТРА ОБЪЕКТОВ КИИ)

ФАКТИЧЕСКАЯ ЭКСПЛУАТАЦИЯ ОБЪЕКТА vs. ЗАКОННОЕ ПРАВО ВЛАДЕНИЯ

См.: ст.1 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Информационная инфраструктура

См.: ГОСТ Р 52653-2006 Информационно-коммуникационные технологии в образовании. Термины и определения

Оценка состояния субъекта КИИ

ОТРАСЛЕВОЙ ЦЕНТР КОМПЕТЕНЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОСТИ

«Система безопасности объекта КИИ»≠ «Состояние безопасности субъекта КИИ»

Состояние безопасности субъекта КИИ

ПРАВОВЫЕ МЕРЫ

ОРГАНИЗАЦИОННЫЕ МЕРЫ

ТЕХНИЧЕСКИЕ МЕРЫ

Подсистема безопасности ЗОКИИ

СИСТЕМА БЕЗОПАСНОСТИ ОБЪЕКТА КИИ {N}

ОРГАНИЗАЦИОННЫЕ МЕРЫ

ТЕХНИЧЕСКИЕ МЕРЫ

Подсистема безопасности ЗОКИИ

СИСТЕМА БЕЗОПАСНОСТИ ОБЪЕКТА КИИ {N+1}

ОРГАНИЗАЦИОННЫЕ МЕРЫ

ТЕХНИЧЕСКИЕ МЕРЫ

См.: п. 2 и п. 34 Приказа 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»

Информационные риски vs. Комплаенс-риски

РЕАЛИИ

Последствия для устойчивого выпуска продукции наступают при любом воздействии на элементы информационной инфраструктуры , которые задействованы в процессе производства

- Нарушение оперативной деятельности (как собственной, так и третьих сторон)
- Нарушение планов и конечных сроков
- Репутационные потери
- Гражданско-правовая ответственность

НОРМАТИВНЫЕ ТРЕБОВАНИЯ

Мерой безопасности КИИ являются последствия от компьютерных атак (количество и интенсивность мероприятий определяется не угрозами, а количеством ущерба)

- Уголовная ответственность
- Административная ответственность
- Дисциплинарная ответственность

Способы оценивания

Понять состояние дел на текущий момент…
оценить…
изменить поведение

КЛАССИФИКАЦИЯ, КАТЕГОРИРОВАНИЕ, АТТЕСТАЦИЯ

МЕТРИКИ, ФРЭЙМВОРКИ, КАТАЛОГИ, ЧЕК-ЛИСТЫ

АУДИТ НА СООТВЕТСТВИЕ СТАНДАРТАМ, «ЛУЧШИЕ ПРАКТИКИ»

ЭКСПЕРТНАЯ ОЦЕНКА

Наборы метрик

ОТРАСЛЕВОЙ ЦЕНТР КОМПЕТЕНЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОСТИ

Метрика «К»

- Легитимность решений постоянно действующей комиссии по категориро-ванию объектов КИИ

Метрика «П»

- Правильность оформления перечня объектов КИИ, подлежащих категориро-ванию

Метрика «tП»

- Соблюдение сроков направления перечня объектов КИИ, подлежащих категориро-ванию, в адрес ФСТЭК России

Метрика «tК»

- Соблюдение сроков категориро-вания объектов КИИ, внесенных в перечень

Метрика «tС»

- Соблюдение сроков направления сведений об объектах КИИ, которые прошли процедуру категориро-вания

Метрика «С»

- Правильность заполнения сведений об объектах КИИ

Метрика «Т»

- Выполнение требований трудового законода-тельства Российской Федерации

Метрика «Д»

- Выполнение требований делопроиз-водства и архивного хранения

Степень зрелости выполнения требований

ОТСУТСТВУЮЩАЯ
«Мы не субъекты КИИ!»

- Руководитель организации не осознает последствия
- Специалисты ошибочно трактуют требования законодательства.
- Решение принято безосновательно (без анализа всех аспектов деятельности организации и соответствующих информационных систем).

НАЧАЛЬНАЯ
«Мы субъекты КИИ. Надо что-то делать…»

- Комиссия по категорированию объектов КИИ не создана или называется по-другому (задачи по категорированию объектов КИИ не в компетенции комиссии).
- Подготовлены проекты документов, но не утверждены
- Перечень объектов КИИ отсутствует или подготовлен без учета процессов

УПРАВЛЯЕМАЯ
«Работа проделана большая, но …»

- Перечень объектов КИИ содержит не все ключевые элементы информационной инфраструктуры организации
- Изменения в документы не вносятся
- Требования по ИБ на этапе проектирования ИС, АСУ, ИТКС не предъявляются
- Ответственный работник не назначен

УЛУЧШАЕМАЯ
Создание (поддержание) системы обеспечения безопасности

- Имеется установленная политика ИБ, которая реализуется
- Изменения вносятся своевременно
- Требования по ИБ вносятся в технические задания на создание ИС, АСУ, ИТКС
- Четко определены функциональные обязанности специалистов

ОТРАСЛЕВОЙ ЦЕНТР КОМПЕТЕНЦИЙ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ПРОМЫШЛЕННОСТИ

Пройдите оценку степени зрелости самостоятельно

Инструмент самооценки позволяет оценить текущую степень зрелости выполнения законодательства по КИИ в вашей организации, проявить «тонкие» места в организации системы обеспечения безопасности КИИ и начать совершенствовать ее уже сегодня

Отраслевой центр компетенций по ИБ в промышленности Минпромторга России

ОТРАСЛЕВОЙ ЦЕНТР КОМПЕТЕНЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОСТИ

https: //ock.gammaural.ru

t.me/ockgammaural

Взаимодействие с Отраслевым центром компетенций

ОТРАСЛЕВОЙ ЦЕНТР КОМПЕТЕНЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОСТИ

- В рамках проведения мониторинга субъектам КИИ в части сроков предоставления, актуальности и достоверности сведений о результатах присвоения объектам критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий

Получение консультаций в ходе мониторинга от экспертов Отраслевого центра по интересующим вопросам

- В рамках индивидуальных обращений за получением консультаций от экспертов Отраслевого центра компетенций по ИБ в промышленности
- «Личный кабинет субъекта КИИ»
- Методические и справочные материалы
- Доступ к «лучшим практикам» и опыту коллег

e-mail: info@gammaural.ru
mikdv@gammaural.ru
Тел. (343) 362-40-04
(343) 374-86-39
ock.gammaural.ru

- В рамках проведения регулярных форумов (конференций) под эгидой Отраслевого центра компетенций по ИБ в промышленности
- Проведения семинаров под индивидуальные задачи субъектов КИИ
- Обучение в соответствии с требованиями регуляторов.

Очные встречи с экспертами Отраслевого центра компетенций на мероприятиях и индивидуальных семинарах

ЛЮБАЯ ПРОБЛЕМА ИМЕЕТ РЕШЕНИЕ!