Изменения законодательства в области обеспечения безопасности значимых объектов критической информационной инфраструкутры Российской Федерации

ТОРБЕНКО Елена Борисовна

Начальник управления ФСТЭК России

Оценка уровня реализации категорирования объектов КИИ

В 2024 г. рассмотрено сведений о более чем **30 000** объектов КИИ

Направлено более **1300** требований о выполнении законодательства в области ОБ КИИ

Обеспечена актуализация сведений о более чем **2500** объектах КИИ

Разработаны методические указания, регламентирующие отраслевые особенности категорирования объектов критической информационной инфраструктуры

Разработаны перечни типовых отраслевых объектов критической информационной инфраструктуры

Во всех 14 сферах, попадающих под действие Федерального закона № 187-ФЗ

Внесение изменений в Правила категорирования объектов КИИ РФ, а также перечень показателей критериев значимости объектов КИИ РФ и их значений

(постановление Правительства РФ от 8 февраля 2018 г. №127)

✓ ***Постановление Правительства РФ от 19 сентября 2024 г. № 1281***

- Исключено понятие «перечень объектов критической информационной инфраструктуры, подлежащих категорированию»

Типовые межотраслевые нормы времени на работы по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

(приказ Министерства труда и социальной защиты Российской Федерации от 30 января 2024 г. № 31нДСП)

- Определяют нормы трудозатрат на все виды работ, предусмотренных законодательством в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

  - ✓ нормы времени на категорирование объектов КИИ
  - ✓ нормы времени на построение системы безопасности и реализация мероприятий по обеспечению безопасности ЗОКИИ
  - ✓ нормы времени на обеспечение безопасности ЗОКИИ в ходе их эксплуатации
  - ✓ нормы времени на планирование мероприятий по обеспечению безопасности ЗОКИИ
  - ✓ нормы времени на обеспечение безопасности ЗОКИИ при выводе их из эксплуатации
  - ✓ нормы времени на подготовку предложений по организации обучения и повышения уровня осведомленности работников, эксплуатирующих, обеспечивающих функционирование, и иных работников, участвующих в обеспечении безопасности ЗОКИИ, по вопросам обеспечения безопасности ЗОКИИ
  - ✓ нормы времени на контроль состояния безопасности ЗОКИИ

Внесение изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

(в приказ ФСТЭК России от 25.12.2023 № 239 приказом ФСТЭК России от 28 августа 2024 г. № 159)

22.2. Меры по обеспечению защиты значимых объектов от атак, направленных на отказ в обслуживании, должны приниматься в отношении значимых объектов, имеющих интерфейсы и сервисы, к которым должен быть обеспечен постоянный доступ из информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), и должны предусматривать:…

26.2. Организационные меры, направленные на защиту значимых объектов от атак, направленных на отказ в обслуживании, должны предусматривать:…

26.3. Программно-аппаратные средства, используемые для осуществления контроля, фильтрации и блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, должны быть расположены на территории Российской Федерации.

Планируемые изменения в НПА в области ОБ КИИ

- ✓ *По результатам проведенного мониторинга правоприменения*
- ✓ *По результата принятия во втором чтении законопроекта № 581689-8 «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»*

- ***Правила категорирования объектов критической информационной инфраструктуры Российской Федерации***
- ***Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений***
- ***НПА в области обеспечения безопасности критической информационной инфраструктуры***

Оценка обеспечения безопасности объектов КИИ

По результатам государственного контроля выявлено более **800** нарушений

В более **40%** имелась реальная угроза нарушения устойчивого функционирования ЗО КИИ

Составлено протоколов об административных правонарушениях:

статья 13.12.1 ***31*** *дело*

статья 19.7.15 ***123*** *дела*

Типовые нарушения:

- несоответствие фактического состава значимых объектов КИИ сведениям, включенным в реестр значимых объектов КИИ
- Некатегорирование объектов КИИ, соответствующих типовому перечню
- отсутствие контроля за действиями организаций-подрядчиков, которым разрешен доступ к ПО и ПАК значимых объектов КИИ
- непроведение мероприятий по выявлению и анализу уязвимостей на значимых объектах КИИ, наличие уязвимого ПО на значимых объектах КИИ
- отсутствие компенсирующих мер, обеспечивающих блокирование угроз безопасности информации
- отсутствие обновления антивирусных баз
- администрирование осуществляется с рабочих мест, находящихся в корпоративных сетях, имеющих выход в Интернет, без реализованных мер обеспечения безопасности

Спасибо за внимание!

ТОРБЕНКО Елена Борисовна