Особенности реализации законодательства ОБ КИИ Реализация технических мер по повышению защищенности

ТОРБЕНКО Елена Борисовна

Начальник управления ФСТЭК России

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 24 декабря 2021 г. № 2431**
- ✓ **Постановление Правительства РФ от 19 августа 2022 г. № 1463**
- ✓ **Постановление Правительства РФ от 20 декабря 2023 г. № 2036**

Совершенствование законодательства

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации

- п. 19.1. Актуализация сведений
- п. 19.2. Мониторинг представления актуальности и достоверности сведений
- п. 19.3. Привлечение к мониторингу подведомственных организаций

- п. 10. Исходными данными для категорирования являются:
  ж) перечни типовых отраслевых объектов КИИ *(с 21 марта 2023 г.)*

- Уточнены показатели критериев значимости объектов КИИ РФ и их значения

Совершенствование законодательства

Показатели критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения

№3.Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств

№5.Отсутствие доступа к государственной услуге, оцениваемое:
б) во времени с момента приема запроса о предоставлении гос. услуги

№8.Возникновение ущерба субъекту критической информационной инфраструктуры, который является …, организацией оборонно-промышленного комплекса, …

№9.Возникновение ущерба бюджету РФ... - значения показателей

№10 - 10.5 показатели для организаций банковской сферы и иных сфер финансового рынка

№13. Снижение показателей государственного оборонного заказа, оцениваемое:
б) в увеличении времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции)

Вступление в силу

Требования
по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации
(приказ ФСТЭК России от 25.12.2017 № 239)

29.2. СЗИ (не встроенные) должны соответствовать *6* или более высокому уровню доверия.

29.3. Прикладное ПО, планируемое к внедрению в рамках создания, модернизации, реконструкции, ремонта ЗО и обеспечивающее выполнение его функций, должно соответствовать следующим требованиям по безопасности:

- 29.3.1. Требования по безопасной разработке ПО
- 29.3.2. Требования к испытаниям по выявлению уязвимостей в ПО
- 29.3.3. Требования к поддержке безопасности ПО

29.4. Выполнение требований, оценивается на этапе проектирования ЗО на основе анализа материалов и документов, представляемых разработчиком

Типовые нарушения выявленные в ходе ГК

Требования. Приказ 235

18. Для ЗО КИИ должны применяться сертифицированные на соответствие требованиям по безопасности СЗИ или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

Требования. Приказ 239

12.7. В ходе приемочных испытаний ЗО и его подсистемы безопасности должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности настоящим Требованиям, а также требованиям технического задания на создание значимого объекта и (или) технического задания (частного технического задания) на создание подсистемы безопасности значимого объекта.

Типовые нарушения выявленные в ходе ГК

- ✓ **Фактический состав ЗОКИИ не соответствует внесенным в реестр ЗО КИИ**
- ✓ **Архитектурные уязвимости ЗОКИИ**

Типовые нарушения выявленные в ходе ГК

- ✓ **Не рассматриваются в качестве ОКИИ системы, обеспечивающие технологические процессы субъекта**
- ✓ **Не учитывается взаимодействие с другими объектами критической информационной инфраструктуры** *(п.14.2 Правил)*
- ✓ **Занижаются размеры ущерба от нарушения функционирования ОКИИ**

Основные меры по обеспечению безопасности значимых объектов КИИ

- Создание подразделений (назначение специалистов)
- Приведение в соответствие организационно-распорядительных документов
- Разработка планов по внедрению технических мер ОБ КИИ
- Проведение оценки эффективности системы ОБ КИИ

Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Реализация технических мер обеспечения безопасности

- ✓ Идентификация и аутентификация (ИАФ)
- ✓ Управление доступом (УПД)
- ✓ Аудит безопасности (АУД)
- ✓ Предотвращение вторжений (компьютерных атак) (СОВ)
- ✓ Антивирусная защита (АВЗ)
- ✓ Обеспечение целостности (ОЦЛ)
- ✓ Обеспечение доступности (ОДТ)
- ✓ Защита технических средств и систем (ЗТС)

Осуществление государственного контроля

основными недостатками являются

- отсутствие оценки защищенности значимых систем и сетей
- наличие критических уязвимостей
- недостатки в парольной защите
- отсутствие граничных межсетевых экранов

наиболее вероятные векторов атаки

- граничные маршрутизаторы
- устаревшие и/или слабые учетные записи
- сервисы электронной почты
- съемные носители информации

Первоочередные меры

- ✓ Устранение уязвимостей
- ✓ Защита периметра
- ✓ Защита ОС
- ✓ Защита от внутренних нарушителей
- ✓ Работа с подрядчиками
- ✓ Безопасное использование e-mail

Порядок обновлений

Меры безопасности периметра

Инвентаризация внешних устройств и минимизация количества открытых портов

Применение VPN и многофакторной аутентификации для удаленного подключения

Отказ от незащищенных протоколов управления на сетевом оборудовании

Исключение использования анонимных учетных записей на сетевом оборудовании

Осуществление доступа в интернет через шлюзы или прокси-серверы

Использование DNS, размещенных на территории РФ

Цепочки поставок

Использовать системы обнаружения вторжений или анализаторы трафика в точках сопряжения

Реализовать контроль действий и возможность экстренного отключения сессии и отката действий подрядчиков

Установить подрядчикам обязанность обеспечивать ОБ КИИ

Использовать защищенные каналы передачи данных

Использовать персонифицированные учетные записи с двухфакторной аутентификацией

Электронная почта. Внутренние нарушители

- Запретить на сетевом уровне взаимодейст-вие с иностранными IP-адресами
- Запретить *open relay*
- Отключить удаленный доступ к критичным узлам, сетям
- Активировать механизмы проверки подлинности домена-отправителя
- Ограничить расширения вложений
- Реализовать запись действий привилегиро-ванных пользователей
- Создать почтовый адрес для пересылки подозритель-ных писем
- Не допускать пересечений прав администра-тора и работников

Изменения законодательства

КОАП

Статья 19.7.15 Непредставление сведений, предусмотренных законодательством в области ОБ КИИ РФ

1. Ответственность за непредставление или представление недостоверных сведений

2. Ответственность за повторное непредставление сведений

Статья 13.12.1 Нарушение требований в области ОБ КИИ РФ

Спасибо за внимание!

ТОРБЕНКО Елена Борисовна