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 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

(приказу 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 ЗО КИИ
  - ✓ нормы времени на обеспечение безопасности ЗО КИИ в ходе их эксплуатации
  - ✓ нормы времени на планирование мероприятий по обеспечению безопасности ЗО КИИ
  - ✓ нормы времени на обеспечение безопасности ЗО КИИ 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 ЗО КИИ, по вопросам обеспечения безопасности ЗО КИИ
  - ✓ нормы времени на контроль состояния безопасности ЗО КИИ

Защита от атак «отказ в обслуживании»

- ✓ Требования (приказ №239) - мера ЗИС 34
- ✓ Рекомендации исх. № 240/84/2582 от 30 сентября 2022 г.

Изменения в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239 *(проект)*

❖ Предусматривают:

- Меры по обеспечению защиты ЗО КИИ от атак, направленных на отказ в обслуживании, имеющих интерфейсы и сервисы, которые должны быть постоянно доступны из информационно-телекоммуникационной сети «Интернет»
- Организационные меры, направленные на защиту значимых объектов от атак, направленных на отказ в обслуживании

Устранение уязвимостей и обновление

Проблема:

- Затруднено получение обновлений
- Существует вероятность компрометации обновлений
- Незрелость процессов устранения уязвимостей у разработчиков

<u>Недостаток:</u>

- *Отсутствие реализации компенсирующих мер при невозможности устранения уязвимости*

Решение:

- ✓ Руководство по организации процесса управления уязвимостями в органе организации) *(утверждена ФСТЭК России 17 мая 2023 г.)*
- ✓ Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств *(утверждена ФСТЭК России 28 октября 2022 г.)*
- ✓ Методика тестирования обновлений безопасности программных, программно-аппаратных средств *(утверждена ФСТЭК России 28 октября 2022 г.)*

Цепочки поставок – действия подрядчиков

Подготовка изменений в НПА в части установления дополнительных требований по обеспечению информационной безопасности в организациях, выполняющих работы по заказам субъектов КИИ

Рекомендации исх. № 240/80/729 от 27 марта 2022 г.

Установить подрядчикам обязанность реализовывать мероприятия по обеспечению безопасности обслуживаемых объектов и защите информации заказчика работ
Реализовать контроль действий подрядчика
Реализовать возможность экстренного отключения сессии и отката действий подрядчиков
Использовать системы обнаружения вторжений или анализаторы трафика в точках сопряжения с системами подрядчика
Для взаимодействия использовать только защищенные каналы передачи данных
Использовать персонифицированные учетные записи для работников подрядчика

Особенности АСУ ТП

- ✓ Цели нарушителя:
  - уничтожение данных;
  - модификация данных;
  - вызов отказа в обслуживании.
- ✓ В зависимости от техник, применяемых нарушителями, возникают события ИБ:
  - отказ в обслуживании;
  - несанкционированный доступ;
  - модификация (подмена) данных;
  - нарушение функционирования АСУ ТП или ее отдельных частей;
  - нарушение функционирования (работоспособности) технических (инженерных) средств и систем.
- ✓ Особенности построения в АСУ ТП
  - Использование промышленных протоколов передачи технологической информации, в которых не предусмотрены механизмы защиты передаваемой информации (HART,Profibus, Modbusи др.)
  - Отсутствие (слабость) механизмов идентификации и аутентификации в промышленных программно-аппаратных средствах
  - Применение промышленных программно-аппаратных средств, исключающих возможность установки программных СЗИ
  - Ограничения, существующие в рамках регламента ТП, на проведение обновлений (на периодичность обновлений) программного обеспечения
  - Расположение отдельных компонентов АСУ ТП и (или) линий связи за пределами контролируемых зон
  - Наличие открытых для доступа общих сетевых ресурсов

Спасибо за внимание!

ТОРБЕНКО Елена Борисовна