Особенности реализации законодательства в области ОБ ЗО КИИ, в том числе реализация технических мер по повышению защищенности объектов КИИ

АНДРЕЕВ Игорь Юрьевич

Начальник отдела 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)

- п. 10. Исходными данными для категорирования являются:

  ж) перечни типовых отраслевых объектов КИИ *(с 21 марта 2023 г.)*

это типы систем, которые могут иметься у СКИИ с учетом его видов деятельности;

это системы, которые должны быть включены в Перечень объектов, подлежащих категорированию (при их наличии);

*это **НЕ** перечень значимых объектов КИИ*

Типовые перечни:

здравоохранение	ракетно-космическая промышленность
транспорт	атомная энергия
связь	оборонная промышленность
энергетика	горнодобывающая промышленность
ТЭК	металлургическая промышленность
банковская сфера	химическая промышленность

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 20 декабря 2022 г. № 2036***

- п. 19.1. Направление измененных сведений не позднее 20 рабочих дней
- п. 19.2. Мониторинг представления актуальности и достоверности сведений
- п. 19.3. Привлечение к мониторингу подведомственных организаций

Внесение изменений в Требования к созданию систем безопасности значимых объектов критической инфраструктуры и обеспечение безопасности объектов критической информационной инфраструктуры

(приказ ФСТЭК России от 21 декабря 2017 г. № 235)

✓ ***приказ ФСТЭК России от 20 апреля 2023 г. №69***

- Приведены в соответствие положениям Указа Президента Российской Федерации от 1 мая 2022 г. № 250
- Исключено требование к сроку переподготовки руководителя структурного подразделения по безопасности
- Изменены требования к образованию штатных работников:
  - *профессиональное образование по направлению ИБ (среднее или высшее)*
  - *высшее профессиональное образование с прохождением повышения квалификации по направлению ИБ*
- Срок прохождения обучения по программам повышения квалификации снижен до 3 лет
- На работников со средним профессиональным образованием возлагаются отдельные функции в соответствии с полученной такими работниками специальностью
- Определены действия субъекта КИИ в случае невозможности обеспечения применяемых СЗИ технической поддержкой со стороны производителей

Внесение изменений в Порядок ведения реестра значимых объектов критической инфраструктуры Российской Федерации

(приказ ФСТЭК России от 6 декабря 2017 г. № 227)

- ✓ ***приказ ФСТЭК России от 1 сентября 2023 г. №177***

- Добавлена 14-я сфера – *государственная регистрация прав на недвижимое имущество и сделок с ним*
- Уточнен порядок внесения изменений в сведения о ЗО КИИ при их объединении или разделении

Оценка обеспечения безопасности объектов КИИ

Проведен гос. контроль в сферах:

Энергетика
Химическая пром.
Горнодобывающая пром.
Металлургическая пром.
Транспорт
Связь
Оборонная пром.

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

Составлено в 2023 г. протоколов об административных правонарушениях:

статья 13.12.1
***26** дел*

статья 19.7.15
***138** дел*

Типовые нарушения:

- Не реализовано обновление антивирусных баз
- Не настроены средства антивирусной защиты
- Администрирование осуществляется с рабочих мест, находящихся в корпоративных сетях, имеющих выход в Интернет, без реализованных мер обеспечения безопасности
- Не проведены мероприятия по выявлению, анализу и устранению уязвимостей на значимых объектах КИИ
- Применяется уязвимое ПО без принятых компенсирующих мер обеспечения безопасности

Устранение уязвимостей и обновление

Проблема:

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

Руководство по организации процесса управления уязвимостями в органе (организации)
(утверждена ФСТЭК России 17 мая 2023 г.)

оценка уязвимостей

Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств
(утверждена ФСТЭК России 28 октября 2022 г.)

устранение уязвимостей

Методика тестирования обновлений безопасности программных, программно-аппаратных средств
(утверждена ФСТЭК России 28 октября 2022 г.)

Недостаток:

- *Отсутствие реализации компенсирующих мер при невозможности устранения уязвимости*

Защита от атак «отказ в обслуживании»

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

Подготовка изменений в НПА в части установления требований по обеспечению защищенности от несанкционированных воздействий типа «отказ в обслуживании»

Канальный уровень:

- Заключить договор с провайдером на предоставление соответствующей услуги

Прикладной уровень:

- исключить неиспользуемые сетевые интерфейсы и протоколы;
- не размещать в одной сети общедоступные ресурсы и ресурсы, обеспечивающие выход в «Интернет»;
- размещать общедоступные ресурсы во внешнем облаке провайдера

- исключить прямое подключение ЗО КИИ к ССОП;
- резервирование каналов обмена информации ЗО КИИ с ССОП
- использовать серверное оборудование, способное выдержать большие нагрузки при обработке TLS-трафика прикладных запросов;
- настроить межсетевые экраны в части сокращения таймаутов

- не размещать в общедоступных ресурсах сервисы по UDP-протоколу или осуществить их перевод на TCP-протокол;
- вывести сервисы с UDP-протоколом в отдельную подсеть;
- обеспечить защиту от атак на таблицу состояний и ограничения по количеству одновременных соединений с одного IP-адреса;
- организовать фильтрацию трафика на прикладном уровне

- проводить регулярную инвентаризацию общедоступного IP-адресного пространства, с целью своевременного реагирования на подмену или компрометацию

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

Вовлеченность персонала в процессы ОБ КИИ

- Кто относится к силам ОБ КИИ?
  - *работники, ответственные за ОБ ЗО КИИ;*
  - *работники, эксплуатирующие ЗО КИИ;*
  - *работники, обеспечивающие функционирование, сопровождение, обслуживание, ремонт ЗО КИИ;*
  - *иные работники, участвующие в ОБ ЗО КИИ.*
- Проведение организационных мероприятий, направленных на повышение уровня знаний работников по вопросам ОБ ЗО КИИ
  - *доведение новых угроз безопасности;*
  - *доведение и разъяснение изменений в ОРД;*
  - *разъяснение методов социальной инженерии.*
- Проведение тренировок с персоналом СКИИ по вопросам ОБ ЗО КИИ и ИБ
  - *отработка планов реагирования на компьютерные инциденты;*
  - *отработка реализации мер ОБ ЗО КИИ;*
  - *отработка взаимодействия подразделений СКИИ.*
- Доведение положений ОРД по ОБ ЗО КИИ (в части касающейся).

Проблемные вопросы по результатам гос. контроля

- ✓ Уязвимость цепочек поставок
- ✓ Неготовность к защите от атак «отказ в обслуживании»
- ✓ Наличие не устраненных уязвимостей и не принятие компенсирующих мер
- ✓ Архитектурные уязвимости
- ✓ Отнесение АСУ ТП к ОКИИ
- ✓ Вовлеченность персонала в процессы ОБ КИИ
- ✓ Не производится обновление баз/сигнатур
- ✓ Наличие неучтенных/незащищенных подключений
- ✓ Не реализован контроль МНИ и мобильных систем
- ✓ Использование слабых паролей
- ✓ Не проводится анализ защищенности периметра
- ✓ Проведение испытаний (приемки) несертифицированных СЗИ

Спасибо за внимание!

АНДРЕЕВ Игорь Юрьевич