



Новое измерение нашего мира – цифровое – все больше влияет на реальность не только через умы людей, но и через окружающую нас технику – от бытовых устройств до систем жизнеобеспечения, транспорта, производств. И несанкционированное воздействие на них, что умышленное, что случайное, может привести к самым разным последствиям – от небольшого ущерба до техногенных катастроф.

Данное пособие посвящено одной из самых актуальных на данный момент областей информационной безопасности – защите критической информационной инфраструктуры.

В пособии обоснована необходимость комплексного обеспечения безопасности национальной критической информационной инфраструктуры на основе требований Федерального закона №1 87-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года. Предложены подходы к формированию требований по обеспечению безопасности объектов критической информационной инфраструктуры; систематизированы основные мероприятия по их защите и даны практические рекомендации.

Введение

Часть I. Основные требования и рекомендации по обеспечению безопасности критической информационной инфраструктуры Российской Федерации

1.1. Основные организационно-нормативные документы по защите национальной критической инфраструктуры

- 1.1.1. Основные понятия и определения в области информационных технологий и технологий защиты информации
- 1.1.2. Соотношение понятий «автоматизированная система» и «информационная система»
- 1.1.3. Охраняемая законом информация
- 1.1.4. Типы и формы представления информации в ходе ее обработки, объекты информатизации, каналы утечки информации
- 1.1.5. Руководящие и нормативные документы по защите критической инфраструктуры Российской Федерации
 - 1.1.5.1. Основные положения государственной политики по защите критически важной инфраструктуры РФ
 - 1.1.5.2. Федеральные законы РФ, указы Президента РФ
 - 1.1.5.3. Руководящие и методические документы, стандарты РФ по обеспечению ИБ АСУТП и КСИИ
 - Документы по защите информации в ключевых системах информационной инфраструктуры
 - Стандарты РФ по кибербезопасности сетей и систем
- 1.1.6. Система технической защиты информации в РФ. Структура и направления деятельности
 - 1.1.6.1. Государственная система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам
 - 1.1.6.2. Лицензирование деятельности по защите информации
 - 1.1.6.3. Сертификация средств защиты информации
 - 1.1.6.4. Аттестационные испытания
 - 1.1.6.5. Оценка соответствия

1.2. Защита критически важных и потенциально опасных объектов

- 1.2.1. Критически важные объекты
- 1.2.2. Виды и классификация КВО, категорирование объектов
- 1.2.3. Потенциально опасный объект
- 1.2.4. Соотношение понятий КВО и ПОО
- 1.2.5. Распределение КВО и ПОО по федеральным округам
- 1.2.6. Субъекты топливно-энергетического комплекса. Основные функции и взаимодействие в области безопасности

- 1.3. Антитеррористическая защищенность критически важных объектов**
 - 1.3.1. Безопасность в чрезвычайных ситуациях. Основные понятия и определения
 - 1.3.2. Антитеррористическая защищенность. Основные понятия и определения
 - 1.3.3. Необходимость комплексного подхода к антитеррористической защищенности
 - 1.3.4. Категорирование и паспорт безопасности КВО
 - 1.3.5. Требования к обеспечению безопасности объектов
 - 1.3.6. Взаимодействие службы безопасности, служб эксплуатации и сопровождения в части физической защиты объектов информатизации
 - 1.3.7. Особенности эксплуатации категорированных объектов информатизации
 - 1.3.8. Типы и виды ответственности за невыполнение (нарушение) требований по противодействию терроризму на объектах
- 1.4. Защита национальной критической информационной инфраструктуры**
 - 1.4.1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ
 - 1.4.2. Подзаконные акты
 - 1.4.3. Категорирование объектов КИИ
 - 1.4.3.1. *Критерии категорирования и категории значимости объектов КИИ*
 - 1.4.3.2. *Полномочия, права и обязанности субъектов КИИ*
 - 1.4.3.3. *Система безопасности значимого объекта КИИ*
 - 1.4.3.4. *Оценка безопасности КИИ*
 - 1.4.3.5. *Государственный контроль в области обеспечения безопасности значимых объектов КИИ*
 - 1.4.3.6. *Ответственность за нарушение требований Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним иных нормативных правовых актов*
 - 1.4.4. Порядок действий при категорировании объектов критической информационной инфраструктуры
 - 1.4.5. Ключевые системы информационной инфраструктуры
- 1.5. Особенности защиты критически важных объектов ТЭК**
 - 1.5.1. Субъекты защиты информации критически важных объектов ТЭК
 - 1.5.2. Взаимодействие критически важных объектов между собой с помощью систем связи
- 1.6. Первоочередные мероприятия по защите АСУТП**
 - 1.6.1. Аудит АСУ на соответствие требованиям информационной безопасности
 - 1.6.2. Разработка системы менеджмента информационной безопасности АСУ
 - 1.6.3. Разработка проектов основных организационно-распорядительных документов
 - 1.6.4. Роль и место службы информационной безопасности в организации
 - 1.6.4.1. *Основные задачи, решаемые службой ИБ организации*
 - 1.6.4.2. *Система должностей, ответственных за обеспечение ИБ в организации*
 - 1.6.5. Особенности взаимодействия подразделения эксплуатации АСУТП со службами безопасности
 - 1.6.6. Планирование мероприятий по обеспечению ИБ в АСУТП КВО и ПОО
 - 1.6.7. Формирование требований к системе защите АСУТП КВО, ПОО
 - 1.6.7.1. *Техническое проектирование системы защиты АСУ. Техническое задание. Разработка раздела «Информационная безопасность»*
 - 1.6.7.2. *Выбор мер защиты информации в АСУ*
 - 1.6.8. Внедрение системы защиты АСУ и ввод ее в эксплуатацию
 - 1.6.9. Эксплуатация системы защиты АСУ
 - 1.6.10. Вывод из эксплуатации системы защиты АСУ
 - 1.6.11. Ответственность за невыполнение (нарушение) требований по обеспечению безопасности информации, обрабатываемой в АСУ КВО
- 1.7. Основные квалификационные требования к сотрудникам в части защиты АСУТП**
 - 1.7.1. Актуальность требований к персоналу в 3 части защиты АСУТП
 - 1.7.2. Важность учета требований безопасности к персоналу на этапе проектирования АСУТП

- 1.7.3. Организационно-нормативная основа формирования требований по защите АСУТП
- 1.7.4. Система квалификационных требований к персоналу в области безопасности АСУТП
 - 1.7.4.1. *Квалификационный справочник должностей руководителей, специалистов и других служащих (общепромышленной)*
 - 1.7.4.2. *Квалификационный справочник должностей руководителей, специалистов и других служащих организаций электроэнергетики*
 - 1.7.4.3. *Квалификационные характеристики должностей работников организаций атомной энергетики*
 - 1.7.4.4. *Квалификационные характеристики должностей руководителей специалистов организаций воздушного транспорта*
 - 1.7.4.5. *Национальные (государственные) стандарты*
 - 1.7.4.6. *Профессиональные стандарты*
 - Специалист в области информационных технологий на атомных станциях (разработка и сопровождение программного обеспечения)
 - Специалист по диспетчерско-технологическому управлению нефтегазовой отрасли
 - Специалист по администрированию сетевых устройств информационно-коммуникационных систем
- 1.7.5. Требования к персоналу в части технической защиты информации
 - 1.7.5.1. *Квалификационный справочник должностей руководителей, специалистов и других служащих (общепромышленной)*
 - 1.7.5.2. *Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации*
 - 1.7.5.3. *Квалификационный справочник должностей руководителей, специалистов и других служащих организаций электроэнергетики*
 - 1.7.5.4. *Квалификационные характеристики должностей работников организаций атомной энергетики*
 - 1.7.5.5. *Профессиональные стандарты*
- 1.7.6. Требования к лицензиатам в части технической защиты информации
- 1.7.7. Квалификационные требования к инженерному составу в области безопасности АСУТП
- 1.7.8. Разрешительные документы, необходимые для работы, связанной с обеспечением безопасности АСУТП
- 1.7.9. Обучение и проверка навыков у персонала в области обеспечения безопасности АСУТП
 - 1.7.9.1. *Обучение и проверка знаний персонала как этап создания АС*
 - 1.7.9.2. *Учебные программы повышения квалификации и переподготовки в области обеспечения безопасности АСУТП*
- 1.7.10. Сертификация специалистов по кибербезопасности АСУТП
- 1.8. Основные квалификационные требования к сотрудникам в части защиты объектов КИИ

Часть II. Проблема обнаружения аномального функционирования КИИ Российской Федерации

- 2.1. Состояние проблемы обнаружения вторжений и аномального функционирования критической информационной инфраструктуры
- 2.2. Возможные постановки задач обнаружения аномального поведения с последующим самовосстановлением критической информационной инфраструктуры
- 2.3. Пример построения ведомственного сегмента обнаружения, предупреждения и нейтрализации компьютерных атак СОПКА
- 2.4. Перспективные модели и методы упреждения компьютерного нападения на национальную критическую информационную инфраструктуру

Заключение

Приложения

Приложение 1. Словарь терминов по теме «Безопасность КИИ РФ»

Приложение 2. Перечень сокращений

Приложение 3. Перечень основных нормативно-правовых документов по защите КИИ РФ