244 стр. PDF 2018 г.

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.

1.3. Антитеррористическая защищенность критически важных национальных 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 Российской Федерации

- 1.5.1. Субъекты защиты информации критически важных национальных объектов
- 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 персоналу 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