Петербургский государственный университет
путей сообщения Императора Александра I

Кафедра «Электрическая связь»

Анализ современных нормативно-методических требований по обеспечению информационной безопасности телекоммуникационных систем Цифровой железной дороги

Лектор:
д.в.н., проф. Привалов А.А.

Санкт-Петербург
2019

Рассматриваемые вопросы:

1. Нормативно-правовые основы информационной безопасности в РФ

2. Стандарты информационной безопасности: "Общие критерии".

3. Стандарты информационной безопасности распределенных систем.

Зарубежные нормативные документы

ISA SP99: «Integrating Electronic Security into the Manufacturing and Control Systems Environment»
«Интеграция средств электронной безопасности в производственные системы и системы управления»

ISA SP99: «Security Technologies for Manufacturing and Control Systems»
«Технологии обеспечения безопасности для производственных систем и систем управления»

IEC 62443 «Security for industrial process measurement and control – Network and system security»
«Безопасность в промышленных системах измерения и управления – Безопасность сетей и систем»

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Standards
Стандарты по защите критической инфрастуктуры от NERC

NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations»
Меры обеспечения безопасности федеральных информационных систем и организаций

NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security»
Руководство по безопасности промышленных систем управления

Guidance for Addressing Cybersecurity in the Chemical Sector
Руководство по кибербезопасности в химической отрасли

EC 61784-4 «Digital data communications for measurement and control – Profiles for secure communications in industrial networks»
«Цифровые системы передачи данных для целей измерения и управления – Методы защиты связи в промышленных сетях»

NIST PCSRF Security Capabilities Profile for Industrial Control Systems
«Профиль возможностей по безопасности для промышленных систем управления»

Отечественные нормативные документы

Законы РФ
Указы президента
Постановления правительства

- № 256-ФЗ «О безопасности объектов ТЭК»
- № 458 «Об утверждении правил по обеспечению безопасности и антитеррористической ..»
- № 459 «Об утверждении Положения об исходных данных для проведения...»
- № 460 «Об утверждении Правил актуализации паспорта безопасности объекта ТЭК...»
- Указ Пр. № 31 «О создании государственной системы обнаружения...»

Ведомственные документы

- «Базовая модель угроз безопасности информации в КСИИ»
- «Методика определения актуальных угроз безопасности информации в КСИИ»
- «Общие требования по обеспечению безопасности информации в КСИИ»
- «Рекомендации по антитеррористичес-кой защищенности объектов...»
- «Рекомендации по обеспечению безопасности информации в КСИИ»
- «Методические рекомендации по организации контроля состояния обеспечения ИБ в КСИИ РФ»
- «Положение о Реестре КСИИ»
- СТО ГАЗПРОМ серии 4.2
- «Методические рекомендации по отнесению информационных систем, функционирующих в составе КВО...»
- «Методические рекомендации по форми-рованию аналитического прогноза...»
- «Методические рекомендации по форми-рованию аналитического прогноза...»
- №587 «Об утверждении перечня работ, связанных с обеспечением безопасности..»
- №592 «Об утверждении перечня объектов ТЭК, обеспечение безопасности которых..»
- «Методические рекомендации по анализу уязвимости производственно-технологического процесса»
- № Пр-803 «Основные направления государственной политики в области обеспечения АСУ ТП»
- № Пр-1753 «Основы государственной политики РФ в области международной информационной безопасности ...»
- №31 «Об утверждении требований к обеспечению защиты информации..»
- Информационное сообщение №240/22/2748ъ «По вопросам обеспечения безопасности информации в ключевых системах информационной структуры..»

Сравнение отечественных и зарубежных нормативных документов

Отечественные стандарты не определяют решения таких проблем, как:

- управление промышленными беспроводными сетями;
- влияние стандартных СЗИ на временные параметры;
- обновление баз данных СЗИ;
- совмещение различных протоколов и устройств между собой.

Аналогичные проблемы регулируются иностранными стандартами, например:

- промышленные беспроводные сети, управление параметрами и обновлениями системы: *ISA/IEC 62443 Security for Industrial Automation and Control Systems, NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security», NIST 800-48 Guide to Securing Legacy.*
- вопросы безопасности коммуникационных протоколов и систем взамодействия:
  IEC 62351 Security Standards.

Стандарты информационной безопасности: "Общие критерии".

- Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам.
- "Общие критерии" являются стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.
- "Общие критерии" содержат два основных вида требований безопасности:
  - функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
  - требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.
- Угрозы безопасности в стандарте характеризуются следующими параметрами:
  - источник угрозы;
  - метод воздействия;
  - уязвимые места, которые могут быть использованы;
  - ресурсы (активы), которые могут пострадать.
- Для структуризации пространства требований в "Общих критериях" введена иерархия класс – семейство – компонент – элемент.
- **Классы** определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).
- **Семейства** в пределах класса различаются по строгости и другим тонкостям требований.
- **Компонент** – минимальный набор требований, фигурирующий как целое.
- **Элемент** – неделимое требование.

Стандарты информационной безопасности распределенных систем

«Рекомендации X.800» "Оранжевая книга"

- **Стандарты** информационной безопасности предусматривают сервисы безопасности: аутентификация; аутентификация источника; управление доступом; конфиденциальность; конфиденциальность трафика; целостность соединения; целостность вне соединения; неотказуемость.
- **Механизмы** безопасности: шифрование; электронная цифровая подпись; механизм управления доступом; механизм контроля целостности данных; механизм аутентификации; механизм дополнения трафика; механизм управления маршрутизацией; механизм нотаризации (заверения).
- **Администрирование средств безопасности** включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании.
- Администратор средств безопасности решает следующие задачи:
  - администрирование информационной системы в целом;
  - администрирование сервисов безопасности;
  - администрирование механизмов безопасности.

Литература:

1. Конституция РФ.
2. Галатенко В. А. Стандарты информационной безопасности. - М: Интернет-Университет Информационных Технологий - ИНТУИТ. РУ, 2016.
3. Карпов Е. А., Котенко И. В., Котухов М. М., Марков А. С., Парр Г. А., Рунеев А. Ю. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И. В.Котенко. - СПб.: ВУС, 2014.
4. *www.iso.ch* – Web-сервер Международной организации по стандартизации.
5. *Www.infotecs.ru/gts/* – Сервер Государственной технической комиссии при Президенте Российской Федерации.
6. Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2015.
7. *www.jetinfo.ru*.

СПАСИБО ЗА ВНИМАНИЕ