КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИЧЕСКОМ КОМПЛЕКСЕ УКРАИНЫ

Гриб О. Г.[1)], Белов Н. С. [2)], Иерусалимова Т.С.[1)]
[1)]***Национальный технический университет «Харьковский политехнический институт» ул. Фрунзе, 21, г. Харьков, Украина, 61002***
[2)] ***ООО «НМУ «ЭЮМ», ул. Каштановая, 33, г. Харьков, Украина, 61036***

В современных энергетических предприятиях применяются различные SCADA-системы для диспетчерского управления сложными автоматизированными системами управления технологическими процессами (АСУ ТП):IntellutioniFix, SIMATICWinCC, Alstomи др.

На 2016 г. Украина является высоко информатизированным государством, более 12 млн. пользователей сети Internet, как физических лиц, так и юридических. Многие предприятия представляют собой реляционную структуру, что приводит к передачи данных через глобальную сеть Internet.

Это приводит также к росту киберпреступлений. Если же для физических лиц это в основном кража личных данных, финансовых средств, то на предприятиях кибервзлом может грозить от останова производства до экологической катастрофы. Поэтому каждое предприятие проводит меры по защите своего киберпространства.

Для этого разделим безопасность на два вида: сетевую и физическую.

В сетевой безопасности применяется стандарт AAA. Стандарт установления подлинности, разрешения и учета (Authentication, authorization, and accounting) применяется в отношении пользовательского доступа и учета трафика для всего сетевого оборудования. В нем определяется, кто или что имеет доступ, к каким сетевым ресурсам, используются списки правил и безопасности управления доступа для фильтрации входящего и исходящего трафиков. Стандарт AAA используют следующие протоколы:

- SNMPv3 – (SimpleNetworkManagementProtocol) протокол сетевого управления предоставляет важные особенности безопасности: Конфиденциальность — шифрование пакетов для предотвращения перехвата несанкционированным источником; Целостность — целостность сообщений, для предотвращения изменения пакета в пути, включая дополнительный механизм защиты от повторной передачи перехваченного пакета; Аутентификация – чтобы убедиться, что сообщение пришло из правильного источника.
- RADIUS – (RemoteAuthenticationinDial-InUserService) протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между

центральной платформой и оборудованием. RADIUS-сервер является интерфейсом взаимодействия с телекоммуникационной системой/сервером (напримермаршрутизатором или коммутатором) и может реализовывать для такой системы следующие сервисы: управление учётной записью пользователя; сбор и анализ статистической информации о сессиях пользователя и всей обслуживаемой системы; проверку учётных данных пользователя (в том числе шифрованных) по запросу обслуживаемой системы; Выдача разрешения к той или иной услуге.

- TACACS+ – (TerminalAccessControllerAccessControlSystemplus) – сеансовый протокол. Поддерживает установление трёх различных типов сеансов AAA.

Для обеспечения физической безопасности необходимо соблюдать следующие меры:

- Коммуникационные, серверные шкафы запирать на ключ;
- Отключать не нужные сетевые порты на устройствах и коммутаторах;
- Занести в коммутаторы списки разрешенных MAC и IP – адресов;
- Диспетчерские места, сервера сбора и передачи технологической информации необходимо выносить в отдельную независимую технологическую сеть, как и информационную, так и электрическую.

Как мы видим физическая безопасность связана на прямую с человеческим фактором.

Сетевая безопасность реализуется в сетевом оборудовании таких компаний как CiscoиHP.

Большинство энергетических предприятий используют на данный момент для обмена данными телефонные линии по дозвону и старые протоколы передачи данных, которые не защищены от внешнего воздействия, поэтому вопрос о кибербезопасности энергетического комплекса Украины носит первостепенный характер.

Список литературы

1. ShailendraFuloria, Ross Anderson. The Protection of Substation Communications. Computer Lab, Cambridge University.
2. Brunner C. IEC 61850& Smart Grids. PAC WorldMagazine. September 2013.
3. Указ президента України №514/2009 від 08.07.2009 р. «Про Доктрину інформаційної безпеки України».