своевременно реагировать на изменение внешних условий (увеличение, уменьшение водопритока) и технического состояния оборудования, но и осуществлять обоснованное планирование эксплуатации и технологического обслуживания оборудования системы шахтного водоотлива.

Литература.

1. Шевчук С.П. Повышение эффективности водоотливных установок: Учеб.пособие/С.П.Шевчук. – К.: УМК ВО, 1990. – 104 с.

2. Гейер В.Г. Шахтные вентиляторные и водоотливные установки: Учебник для вузов./ Гейер В.Г., Тимошенко Г.М. – М.: Недра, 1987. – 304 с.

3. Попов В.М. Рудничные водоотливные установки. – 2-е изд. перераб. и доп./ Попов В.М. – М.: Недра, 1983. – 304 с.

4. Груба В.И. Технические средства автоматизации в горной промышленности: Учебное пособие / В.И. Груба, Э.К. Никулин, А.С. Оголобченко. Под общей редакцией докт. техн. наук, проф. В.И. Грубы. – К.: ИСМО, 1998. – 373 с.

Проценко О.Г.
Наук. керівник к.т.н. Брєжнєв Є.В.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»

Анализ обеспечения информационной безопасности SMART grid систем

В последние годы во всем мире наблюдается повышенный интерес к разработке и имплементации концепции энергосистем нового поколения, получившей название SMART (*Self Monitoring Analysis and Reporting Technology)* Grid. В основе этой концепции лежит идея

модернизации существующих и разработке новых «интеллектуальных», адаптивно-активных энергосистем с упором на широкое использование информационно-коммуникационных и компьютерных технологий, что позволяет достичь большей гибкости, безопасности, надежности и экономичности по сравнению с традиционными энергосетями.

Модернизация энергосистем подразумевает использование существующих информационных и коммуникационных технологий. Очевидно, что в таком случае функциональная и информационная безопасность Smart Grid будет зависеть также и от проблем, связанных с используемыми технологиями. Под функциональной безопасностью следует понимать невозможность системы причинить вред жизни человека, его здоровью или окружающей среде. Информационная безопасность в свою очередь подразумевает невозможность окружающей среды использовать систему непредусмотренным способом. Для традиционных энергосетей обеспечение безопасности носит первостепенный характер. Поскольку для Smart Grid систем коммуникационные сети являются критическим компонентом, информационная безопасность системы оказывается тесно связанной с функциональной безопасностью. Вмешательство (преднамеренное или случайное) в работу телекоммуникаций сети может послужить причиной возникновения угрозы работе отдельных компонентов, либо всей системы, что в свою очередь может быть причиной серьёзных аварий, наносящих вред жизни человека и окружающей среде.

В различных источниках существующие проблемы информационной безопасности описаны достаточно подробно [1-3]. Поскольку телекоммуникационная составляющая Smart Grid разрабатывается на основе существующих протоколов передачи данных, таких как

IPv4 и IPv6, большое влияние на информационную безопасность всей системы оказывают именно их уязвимости. В качестве наиболее общих проблем можно отметить следующие:

- осуществление DoS/DDoS атак;
- использование вредоносного программного обеспечения;
- подмена личности пользователя системы;
- похищение пароля пользователя системы;
- внедрение и прослушивание.

Разрешение данных проблем в будущем поможет повысить информационную безопасность сети. Однако стоит отметить, что вопрос обеспечения функциональной безопасности системы в целом как результат обеспечения информационной безопасности в существующих работах не рассматривался. На данный момент обеспечение функциональной безопасности Smart Grid практически копирует приемы для традиционных энергетических сетей. Поскольку обеспечение связанности узлов SMART grid системы будет одной из ключевых задач проектирования, использование телекоммуникационных технологий для построения интеллектуальных энергосистем должно учитывать связь между информационной безопасностью каналов передачи данных и возможными последствиями несанкционированного доступа и вмешательства в работу системы.

С нашей точки зрения, обеспечение функциональной безопасности Smart Grid невозможно без учёта её взаимосвязи с информационной безопасностью. Использование традиционных методов обеспечения информационной безопасности рассматривает информационную сеть как обособленную сущность. Новые методы обеспечения информационной безопасности телекоммуникационных сетей, предполагаемых к

использованию в Smart Grid, должны учитывать не просто возможность потери, утечки или искажения данных системы, но и влияние таких событий на функциональную безопасность.

Література.

1. Line M.B. Cyber Security Challenges in Smart Grids [Text] / Maria B. Line, Inger Anne Tøndel, Martin G. Jaatun // The second International Conference on Innovative Smart Grid Technologies, Manchester, Dec 5 – 7, 2011, UK.

2. Genge B. Developing Cyber-Physical Experimental Capabilities for the Security Analysis of the Future Smart Grid [Text] / Béla Genge, Christos Siaterlis // The second International Conference on Innovative Smart Grid Technologies, Manchester, Dec 5 – 7, 2011, UK.

3. Fuloria S. Towards a security architecture for substations [Text] / Shailendra Fuloria, Ross Anderson // The second International Conference on Innovative Smart Grid Technologies, Manchester, Dec 5 – 7, 2011, UK.