УДК 004.056.57

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ В АПК

***Меликов Алексей Владимирович**, доцент кафедры автоматизации и роботизации технологических процессов имени И.Ф.Бородина, ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева*

***Аннотация.** Представлены современные проблемы информационной безопасности в электроэнергетической области в сфере АПК. Подводится вывод о необходимости построения системы защиты, зиждущейся на принципах обеспечения, целостности и доступности самого технологического процесса и автоматизированных систем управления. Приводится обоснование целесообразности применения технологии «Блокчейн» в сфере кибербезопасности в электроэнергетике.*

***Ключевые слова:** информационная безопасность, кибербезопасность, проблемы, электроэнергетика, технология «Блокчейн».*

При выборе средств защиты информации для электроэнергетической отрасли требуется понимать, что основным активом является не информация, а технологический процесс. При разработке систем обеспечения информационной безопасности в электроэнергетике речь идет не о «дежурной» защите от утечек данных, а о защите от нарушения технологического процесса за счет реализации киберугроз [1].

При нарушении технологического процесса в АПК ущерб сразу не восстанавливается, будь то компенсация денежных средств. Помимо прямых потерь, учитывающих (не учитывающих) упущенную выгоду от нереализованной продукции, есть реальные потери численности поголовья скота, неурожая, восстановление которых требует время. На пример, ущерб от «простого» отключения электроэнергии птицефабрики в Белой Калитве в 2018 г. «стоил» 12 млн. рублей и 3 месяцев на восстановление. В 2005 г. прямые потери Петелинской птицефабрики от отключения электроэнергии составили 14 млн. руб., погибли 278,5 тыс. голов птицы [2]. А что говорить, если вопрос касается технологического процесса на объекте стратегического назначения?

Специфическое (в том числе устаревшее) программное обеспечение и протоколы передачи данных (в их числе и протоколы с отсутствующими функциями и механизмами безопасности), негативное отношение разработчиков к дополнительным средствам защиты, требования к скорости передачи данных, неприменение обновлений программ и улучшений аппаратного обеспечения являются распространенными проблемами в защите автоматизированных систем управления технологическими процессами [3].

Широко используемым протоколом передачи данных в электроэнергетике является семейство стандарта МЭК/IEC 60870-5-101/104, при разработке которого вопросам кибербезопасности не уделялось должного внимания. Полноценное использование возможностей современных протоколов, типа IEC 60870 и новее, на отечественных объектов электроэнергетики мало распространено. Разработчики автоматизированных систем управления технологическими процессами часто используют собственные нестандартизированные протоколы передачи данных. Аналогичный подход наблюдается и в вопросах выбора программного обеспечения – встроенные механизмы информационной безопасности могут не отвечать современным требованиям защиты данных (или вовсе отсутствовать).

Для разработчиков технологических систем главным показателем качества является надежность, однако ресурсы на тестирование продуктов совместно со средствами защиты выделяются редко. Отсутствие процесса обновлений, улучшения аппаратной части еще одна распространенная проблема в защите автоматизированных систем управления технологическими процессами. В большинстве случаев технологическая сеть изолирована от Интернет, а собственная система обновлений не внедрена; их установка зачастую связана с рисками сбоев, недопустимыми на электроэнергетических объектах. В дополнении к этому, технологические системы в электроэнергетике чувствительны к характеристикам каналов передачи данных, т.е. применение дополнительных средств защиты может значительно снизить скорость реакции на управляющее воздействие, что также недопустимо в большинстве случаев.

Среди угроз, потенциально возможных в электроэнергетике в АПК, помимо известных «внутренних» атак в криптографии, уместно выделить 3 вида: атака посредника, DDoS-атака и манипулирование данных [4]. Вмешательство «специалиста», преследующего злые умыслы, может осуществляться в протокол передачи данных посредством подключения к каналу между контрагентами с целью удаления или искажения информации. Или он может превысить допустимое возможное число обращений к серверу, обрабатываемых одновременно, с целью ограничения пропускной способности сетевого ресурса. «Специалист» также желает манипулировать данными системы, осуществляю подмену информации. Отсюда, при построении системы защиты от подобных атак требуется учитывать принципы обеспечения, целостности и доступности самого технологического процесса и автоматизированных систем управления.

а) б)

Архитектуры информационных сетей

а) модель «Клиент-Сервер», б) «Блокчейн»

Такие принципы заложены в технологию «Блокчейн» [5], при работе которой в противовес единому контролирующего органа в системе создается много отдельных узлов, каждый из которых ведет свой журнал транзакций; и каждая производимая транзакция сверяется со всеми журналами узлов, входящих в систему; а сами транзакции упаковываются специальным образом «закрывающиеся» блоки. Основное преимущество этой технологии в сравнении с традиционной базой данных заключается в архитектуре информационной сети, представленной на рисунке.

Для взлома технологии «Блокчейн» «специалист» вынужден одновременно взламывать 1000 компьютеров вместо 1 сервера. Данные в «Блокчейне» практически невозможно удалить, потому что их придется удалять со всех узлов. При использовании этой технологии подмена (или удаление) информации невозможна, поскольку опубликованный пользователем «открытый» ключ в зашифрованном виде «распознается» всеми узлами сети. Следовательно, ключ-подделка выявится сразу. Еще один плюс распределенной сети состоит в том, что «специалист» одновременно не сможет атаковать все ее узлы. При построении клиент-серверной сети становится возможной атака намеренной перегрузки сервера большим количеством запросов, которые он не в состоянии обработать. С помощью «Блокчейн» достигается надежная защита от ошибок персонала, злонамеренных действий сотрудников и «специалиста», желающего «быть» в системе, направленных на вольное/невольное искажение данных. При попытке подмены информации (хоть на 1 бит), транзакция будет отклонена системой, так как контрольные хэш-суммы, рассчитывающиеся как функции от исходных данных, не совпадут.

Применение технологии «Блокчейн» в электроэнергетической области позволит продавцу и покупателю электроэнергии проводить денежные средства без посредников по защищенному каналу связи в надежной сети. На платформе «Блокчейн» также предусмотрено использование «умных контрактов» для соблюдения баланса спроса и предложения электроэнергии на рынке.

Библиографический список

1. Ярушевский, Д. Особенности информационной безопасности в электроэнергетике / Д. Ярушевский // официальный сайт «ДиалогНаука» [Электронный ресурс]. – Режим доступа: https://www.dialognauka.ru/press-center/article/14322/.
2. Информационный портал «obzor.city» [Электронный ресурс]. – Режим доступа: https://obzor.city/news/9957/.
3. Кондратенко, А. Информационная безопасность в электроэнергетике. Отраслевые нюансы / А. Кондратенко, Д. Прохоров // Электронный журнал «Connect». № 3, 2012 [Электронный ресурс]. – Режим доступа: https://elvis.ru/ upload/iblock/0f2/ib_energy.PDF.
4. Юшкова, Е.Е. Проблемы информационной безопасности в сфере электроэнергетики Архангельской области и возможные пути ее решения / Е.Е. Юшкова, Е.С. Юшков, Е.А. Малицкая // Гайдаровские чтения «Цифровые технологии в управлении регионом». – Арх.: САФУ им. М.В. Ломоносова, 2018. – С. 17-34.
5. Тапскотт Д. Технология Блокчейн: то, что движет финансовой революцией сегодня / Д. Тапскотт, А. Тапскотт. [Текст] / пер. с англ. К. Шашковой, Е. Ряхиной. – М.: Эксмо, 2017. – 550 с.

УДК 517.925.7+523.566

ПОВЫШЕНИЕ БЫСТРОДЕЙСТВИЯ ВЕРТИКАЛЬНОГО МАНЕВРИРОВАНИЯ ДИРИЖАБЛЕЙ СЕЛЬСКОХОЗЯЙСТВЕННОГО НАЗНАЧЕНИЯ

Белов Дмитрий Владимирович, *инженер ОАО «Московский Высоковольтные Сети»*

Андреев Сергей Андреевич, *доцент кафедры автоматизации и роботизации технологических процессов имени И.Ф.Бородина, ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева*

Аннотация. *Выявлены недостатки известных способов нагрева гелия в дирижаблях. Предложено заменить локальный нагрев гелия одновременным нагревом всего объема рабочего пространства за счет пропускания электрического тока по виткам нагревательного прибора, удерживаемого кронштейнами. Внутреннюю поверхность оболочки предложено оснастить отражателями тепловой энергии, а управление нагревательным прибором осуществлять по соотношению температур гелия и окружающей среды, а также сигнала с задатчика высоты полета.*

Ключевые слова: *дирижабль, вертикальное маневрирование, гелий, нагревательный прибор, отражатель тепловой энергии, кронштейн, задатчик высоты полета.*