DOI: 10.25586/RNU.V9187.18.11.P.119 УДК 681. 51.037

А.И. Гладышев, В.К. Кузнецов

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНЦЕПЦИИ МОНИТОРИНГА СИСТЕМ ЭЛЕКТРОСНАБЖЕНИЯ

Рассматриваются проблемы информационной безопасности системы мониторинга электрооборудования и меры защиты от деструктивных воздействий на процесс мониторинга системы электроснабжения.

Ключевые слова: *система электроснабжения, концепция мониторинга, информационная безопасность, деструктивное воздействие, рабочий процесс, техническое состояние, измерительная информация*

A.I. Gladyshev, V.K. Kuznetsov

INFORMATION SECURITY ISSUE THE CONCEPT OF MONITORING SUPPLY SYSTEM

The problems of information security of electrical equipment monitoring system and measures of protection against destructive effects on the process of monitoring the power supply system are considered.

Keywords: *power supply system, monitoring concept, information security, destructive impact, working process, technical condition, measuring information*

Введение

Автоматизированному управлению технологическими комплексами систем электроснабжения (СЭС) промышленного назначения и специальных объектов нет альтернативы. Возрастание степени управляемости указанных систем оказывает прямое влияние на повышение их интеллектуализации – свойства, обеспечивающего новый уровень качества и надежности электроснабжения, безопасности эксплуатации СЭС [1].

Необходимым компонентом эффективного управления СЭС является осуществляемый в реальном масштабе времени автоматизированный мониторинг параметров режима и технического состояния электроагрегатов СЭС, включаемый в контур обратной связи автоматизированной системы управления технологическим процессом (АСУ ТП) электроснабжения.

Система взглядов на мониторинг СЭС, или концепция мониторинга СЭС, в форме совокупности общих требований к последнему лежит в основе планирования системы мониторинга, определяющего ее цели, облик и взаимодействие с другими модулями системы автоматизированного управления СЭС.

Далее мы остановимся на одном из аспектов рассматриваемой концепции – информационной безопасности системы мониторинга СЭС.

Особенности информационных атак на АСУ ТП

Целями атак являются: перехват управления технологическим процессом, внедрение средств отсроченного дистанционного воздействия на него, получение информации об особенностях производства и уязвимостях технологии управления [2–5].

Планируемые как специальные операции информационные атаки учитывают особенности функционирования информационно-коммуникационной сферы СЭС. Они могут осуществляться, в частности, посредством программ-эксплойтов в виде таргетированных атак – прицельных деструктивных воздействий на ранее выявленные уязвимости. Отмечается особенность использования другого типа инструментов – программ-вымогателей: атакуя АСУ ТП, они часто нацеливаются не на шифрование файлов, а на прерывание технологического процесса. Прогнозируется нарастание интенсивности массированных атак, осуществляемых в автоматизированном режиме суперкомпьютерами. Через доступные промежуточные узлы информационно-коммуникационной сети ведутся так называемые транзитивные атаки. Скрытное осуществление – характерный признак атак. К примеру, в атаке предприятия Ирана по обогащению урана с использованием червя stuxnet последний сработал спустя несколько лет латентного существования, остановив производственный процесс.

СЭС рассматриваемого класса используют технологию промышленного Интернета вещей (IIoT) пока далеко не повсеместно. Вместе с тем неуязвимыми не остаются даже физически изолированные промышленные системы, не подключенные к Интернету, но использующие, например, беспроводную связь [6].

Один из возможных механизмов распространения уязвимости систем мониторинга связан с использованием современных датчиков. Наличие микропроцессора у контроллера интеллектуального датчика превращает его в отдельный вычислительный узел, что влечет повышенную опасность передачи заражения датчика другим звеньям цепи управления с риском разрушительного влияния на технологический процесс.

Некоторые основные направления построения безопасной информационно-технологической инфраструктуры системы мониторинга СЭС

В качестве основных признаков безопасной информационно-технологической инфраструктуры АСУ ТП в работах [2; 6] указываются целостность, стабильность и непрерывность технологического процесса.

На этапе становления дистанционного контроля СЭС в качестве главных угроз ее функциональной устойчивости рассматривался несанкционированный физический доступ к оборудованию, разведывательная деятельность в форме визуального наблюдения и вербовки сотрудников. Вопросы информационной безопасности прорабатывались преимущественно в плане защиты информационных каналов от хищений информации, ошибочных или преднамеренных действий операторов, проникновения иностранных технических разведок.

Ныне информационно-коммуникационная сфера промышленных СЭС превращается в арену конфликтного противоборства, в котором участвуют информационные системы стороны-агрессора, располагающей широким набором дистанционно используемых средств деструктивного воздействия, и противодействующей стороны, выстраивающей рациональные стратегии поведения в указанном конфликте.

Чрезвычайно высокая цена «игры» – информационного конфликта в сфере управления СЭС, – а также отмеченная выше критическая значимость мониторинга СЭС для устойчивости технологического процесса электроснабжения определяют актуальность выработки технических и управленческих решений, обеспечивающих информационную безопасность системы мониторинга СЭС .

Анализ подходов к обеспечению информационной безопасности АСУ ТП и других автоматизированных систем обработки информации [5–10] позволяет сформулировать некоторые общие принципы построения безопасной системы мониторинга СЭС.

1. *Включение требований к информационной безопасности компонентов системы мониторинга в перечень общих технических требований при ее проектировании.*

При создании ранних версий системы дистанционного контроля СЭС определяющими факторами были масштаб и функциональное назначение агрегатов СЭС, согласование функциональных параметров и электромагнитная совместимость устройств, снижение затрат. С расширением спектра информационных угроз при выборе структуры и конфигурировании системы мониторинга СЭС, проектировании ее компонентов разработчики и производители не могут ограничиться лишь функциональными аспектами.

2. *Использование опыта обеспечения информационной безопасности автоматизированных систем.*

Правомерность интерпретации системы мониторинга, осуществляющей технологический процесс получения, обработки, передачи и хранения первичной измерительной информации как одной из разновидностей автоматизированных систем обработки информации определяет возможность переноса накопленного опыта построения безопасной информационно-технологической инфраструктуры системы мониторинга.

3. *Разработка адаптируемого к изменению угроз комплекса технических, программных и организационных мер прогнозирования, предупреждения и отражения информационных атак*, включающего:

– системные (технические) решения – обоснование требований к безопасности аппаратных компонентов, обеспечение изоляции среды полевых устройств, соблюдение правил сегментации и настройки сетевого оборудования, использование межсетевых экранов, защита каналов передачи информации;

– программные средства – выбор конфигурации программных средств, антивирусная защита, настройки операционной системы и системного ПО, криптографическая защита информации, контроль целостности ПО;

– организационные и административные меры – ограничение и периодический пересмотр текущих доступов к компонентам и управляющим интерфейсам, строгая парольная политика, включение в документы, регламентирующие процесс работы системы, наряду с техническими рекомендациями также раздела обеспечения информационной безопасности, внедрение инновационных технологий прогнозирования и диагностирования атак.

4. *Учет потенциальной возможности эффекта срыва защиты в процессе эксплуатации системы.*

Указанный эффект возможен из-за негативного взаимовлияния различных средств защиты при некоторых сочетаниях их параметров.

5. *Концентрация усилий на формировании облика и взаимодействий со средой системы мониторинга при ее концептуальном проектировании, а также на поиске свежих инженерных (схемотехнических) решений при техническом проектировании компонентов системы мониторинга.*

Методологической основой работ по созданию безопасной системы мониторинга на указанных этапах являются определяющий характер ранних стадий жизненного цикла для формирования свойств системы и канонический принцип «информационная безопасность системы есть функция ее архитектуры».

Заключение

1. Нарушение в результате информационных атак процесса автоматизированного мониторинга СЭС может быть отнесено к критическим факторам ввиду риска потери управляемости базового процесса электроснабжения.

2. В условиях нарастания остроты информационных конфликтов и разнообразия поражающих воздействий в информационно-коммуникационной сфере информационная безопасность непрерывного процесса наблюдения за параметрами режима

и технического состояния электроагрегатов приобретает статус одного из наиболее важных аспектов концепции мониторинга СЭС.

3. Достижение информационной безопасности системы мониторинга СЭС требует разработки комплекса технических решений, программных средств и организационных мер в диапазоне от обоснования требований к безопасности аппаратных компонентов и конфигурации программных средств до работы с персоналом и обслуживания системы.

4. Средства информационной безопасности системы мониторинга и ее элементов наравне со средствами реализации функциональных требований обязаны быть предусмотренными на этапе проектирования системы мониторинга СЭС и не должны встраиваться в готовую систему.

5. С целью рационального использования накопленного опыта выработку комплекса технических и управленческих решений, направленных на построение безопасной информационно-технологической инфраструктуры системы мониторинга СЭС, целесообразно осуществлять в парадигме информационной безопасности автоматизированных систем обработки информации.

Литература

1. *Вариводов В.Н., Коваленко Ю.А.* Интеллектуальные электроэнергетические системы // Электричество. 2011. № 9. С. 4–9.

2. *Корнев А.В.* Кибербезопасность: взвешенный подход // Автоматизация в промышленности. 2017. № 7. С. 41–46.

3. *Петренко С.А., Ступин Д.Д.* Национальная система раннего предупреждения о компьютерном нападении: науч. моногр. / под общ. ред. С.Ф. Боева. Ун-т Иннополис. Иннополис: Издат. дом «Афина», 2017. 440 с.

4. *Войтов М.Л.* Рост числа атак на промышленные системы // Автоматизация в промышленности. 2016. № 12. С. 59–60.

5. От информационной безопасности к кибербезопасности / П.Д. Зегжда [и др.]. СПб.: Изд-во Политехн. ун-та, 2017. 322 с.

6. *Литвинов Е.М.* Безопасность АСУ ТП // Автоматизация в промышленности. 2017. № 7. С. 33–35.

7. *Некрасов А.В.* Системы мониторинга на объектах электроэнергетики / А.В. Некрасов // Автоматизация в промышленности. 2014. № 11. С. 22–23.

8. *Юрьева Р.А., Виксин И.И., Мурадов А.Р.* Подход к обнаружению новых атак на киберфизические системы // Автоматизация в промышленности. 2018. № 2. С. 58–62.

9. *Лифшиц И.И., Неклюдов А.В.* Гибридная методика оценки безопасности информационных технологий // Автоматизация в промышленности. 2017. № 7. С. 36–41.

10. *Колосок И.Н., Гурина Л.А.* Определение показателя уязвимости к кибератакам задачи оценивания состояния // Электротехника. 2017. № 1. С. 52–59.

References

1. *Varivodov V.N., Kovalenko Yu.A.* Intellektual’nye elektroenergeticheskie sistemy // Elektrichestvo. 2011. № 9. S. 4–9.

2. *Kornev A.V.* Kiberbezopasnost’: vzveshennyy podkhod // Avtomatizatsiya v promyshlennosti. 2017. № 7. S. 41–46.

3. *Petrenko S.A., Stupin D.D.* Natsional’naya sistema rannego preduprezhdeniya o komp’yuternom napadenii: nauch. monogr. / pod obshch. red. S.F. Boeva. Un-t Innopolis. Innopolis: Izdat. dom “Afina”, 2017. 440 s.

4. *Voytov M.L.* Rost chisla atak na promyshlennye sistemy // Avtomatizatsiya v promyshlennosti. 2016. № 12. S. 59–60.

5. Ot informatsionnoy bezopasnosti k kiberbezopasnosti / P.D. Zegzhda [i dr.]. SPb.: Izd-vo Politekhn. un-ta, 2017. 322 s.

6. *Litvinov E.M.* Bezopasnost' ASU TP // Avtomatizatsiya v promyshlennosti. 2017. № 7. S. 33–35.

7. *Nekrasov A.V.* Sistemy monitoringa na ob"ektakh elektroenergetiki // Avtomatizatsiya v promyshlennosti. 2014. № 11. S. 22–23.

8. *Yur'eva R.A., Viksin I.I., Muradov A.R.* Podkhod k obnaruzheniyu novykh atak na kiberfizicheskie sistemy // Avtomatizatsiya v promyshlennosti. 2018. № 2. S. 58–62.

9. *Lifshits I.I., Neklyudov A.V.* Gibridnaya metodika otsenki bezopasnosti informatsionnykh tekhnologiy // Avtomatizatsiya v promyshlennosti. 2017. № 7. S. 36–41.

10. *Kolosok I.N., Gurina L.A.* Opredelenie pokazatelya uyazvimosti k kiberatakam zadachi otsenivaniya sostoyaniya // Elektrotekhnika. 2017. № 1. S. 52–59.