УДК 681.3.01

А.Е. Бекмачев

Исследование утечки конфиденциальной информации по цепям питания и заземления

Проанализированы потенциальные угрозы информационной безопасности обособленных объектов, на которых суммарная мощность электрической нагрузки в сети соизмерима с мощностью источника электроэнергии, т.е. в условиях «критической нагрузки». Показана возможность съема информации о технологических циклах на объекте с помощью находящихся в свободном обращении приборов. Предложены технические способы противодействия несанкционированному сбору информации.
Ключевые слова: угроза, конфиденциальность, защита информации, несанкционированный доступ к информации, прибор.

Информационная безопасность отдельно стоящего промышленного объекта или объекта, составляющего часть распределенной на территории инфраструктуры, имеет существенную зависимость от схемы его энергоснабжения.

В случае, когда объект не имеет автономной системы электропитания или находится в конце длинной линии электропередачи, возникает ситуация критической нагрузки (КН) – такое состояние местной электрической сети, когда она длительное время подвержена пиковым нагрузкам или большую часть времени эксплуатируется в режимах, сопоставимых с аварийными. Это происходит из-за превышения расчетных нагрузок, когда суммарная мощность электроприемников объекта сравнима с мощностью источника.

В такой ситуации возникает потенциальная угроза съема информации, в том числе и дистанционного, о рабочих циклах и технологических процессах этот объекта. Наиболее простой способ получения указанной информации – мониторинг силовых фидеров, подводимых к объекту от электросетей общего пользования и цепей заземления. По характеру, длительности, повторяемости, гармоническим составляющим помех, вносимых электроустановками объекта в сеть, можно судить о его функциональном назначении, скорости приведения систем в активное состояние, составе оборудования. Для эффективного противодействия несанкционированному мониторингу необходимо позаботиться об электромагнитной совместимости (ЭМС) объекта.

ЭМС в большой степени определяется качеством электроэнергии (КЭ) обособленного объекта. Качество электроэнергии является существенным фактором обеспечения ЭМС. Этот фактор в отличие от других факторов обеспечения ЭМС, таких как выбор сигналов, аппаратуры приема и обработки информации, которые заданы проектировщиками соответствующих систем, может обеспечиваться средствами операторов, эксплуатирующих организации [1]. Одними из основных показателей качества электроэнергии (ПКЭ) являются: установившееся отклонение напряжения δU_y, размах изменения напряжения δU_t, длительность провала напряжения Δt_n [3].

Это параметры, которые можно регистрировать находящимися в свободном обращении приборами контроля ПКЭ даже без проникновения в охраняемую зону обособленного объекта.

Анализ полученных таким образом данных, особенно при привязке по времени к другим, внешним событиям, позволяет судить о технологических процессах и назначении объекта.

В качестве примера объекта, подверженного КН, можно рассмотреть типичную площадку объекта радиосвязи, которым может быть: радиорелейная станция, подсистема контроля и управления системы навигации, базовые станции подвижной радиосвязи. Пример такого объекта приведен на рис. 1 [2].

Эксперимент по исследованию качества местной электрической сети (МЭС) был проведен с использованием щитового регистратора Н393 и программно-аппаратного комплекса «Прорыв-КЭ». В первом случае преимуществом является мгновенное получение «твердой копии», во втором – возможность архивирования ПКЭ по нескольким каналам с последующим параметрическим анализом с установкой контрольных точек и автоматизированная обработка с выдачей отчетов по различным ключевым показателям.

Исследование основных показателей качества электроэнергии проводилось на КТП 250-6/0,4 на стороне низкого напряжения – 0,4 кВ.

В результате установлено, что действующие ПКЭ имеют следующие значения за сутки:

Среднее значение напряжения $U_{ср} = 209$ В.

Максимальное значение напряжения $U_{max} = 218$ В.

Минимальное значение напряжения $U_{min} = 194$ В.

Установившееся отклонение напряжения $\delta U_у = 5{,}3\%$ при норме 5%.

Размах изменения напряжения $\delta Ut = 3{,}6\%$ при норме 2,7% на интервале 60 мин.

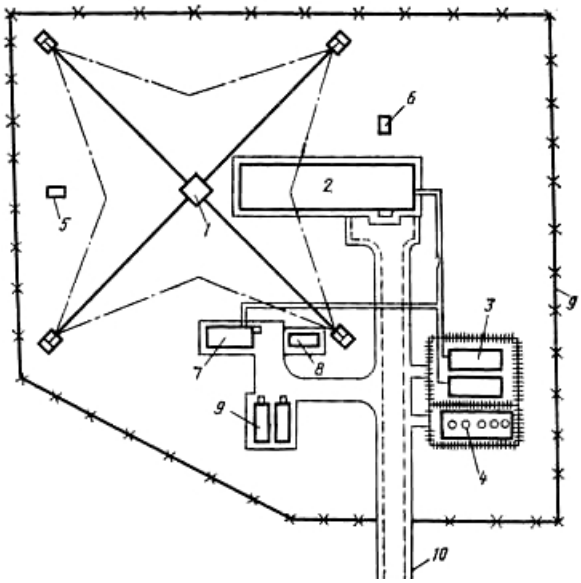

Рис. 1. Генеральный план площадки обособленного объекта радиосвязи: *1* – антенная мачтовая опора; *2* – техническое здание; *3* – склад; *4* – склад горюче-смазочных материалов; *5* – трансформаторная подстанция; *6* – котельная; *7* – помещение для мотопомпы; *8* – резервуар с водой на случай пожара; *9* – ограждение; *10* – подъездная автодорога

Это означает, что исследованная сеть перегружена и длительные промежутки времени – от 0,5 до 8,5 ч – работает на пониженном относительно нормального допустимого напряжении, при этом длительность провалов напряжения составляет от 10 до 60 с. Величина отклонения напряжения от максимально допустимой также превышает разрешенные пределы.

На рис. 2 приведены показания «Прорыв-КЭ» – часовая запись изменения амплитуды напряжения на нагрузке. Видна сильная асимметрия потребления по фазам и значительный размах изменения параметра.

Рис. 2. Запись экрана отображения прибора «Прорыв-КЭ»: амплитуда напряжения по 3 фазам за 60 мин

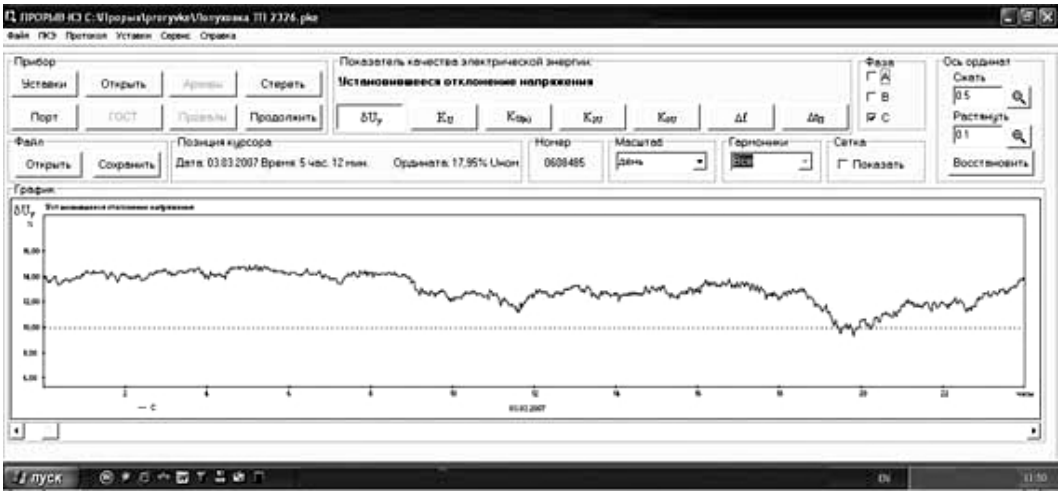

Рис. 3. Запись экрана отображения прибора «Прорыв-КЭ»: суточная диаграмма значения установившегося отклонения напряжения δUу

Суточная диаграмма значения установившегося отклонения напряжения $\delta U_{\text{у}}$ демонстрирует стандартные минимумы и максимумы нагрузки сети в зависимости от сезона и времени суток, а также периоды продолжительной перегрузки сети и моменты выброса реактивной мощности (рис. 3).

Таким образом, установлено, что основными факторами, влияющим на образование КН в исследованной сети, являются коммутация мощных электроприборов, затяжные пуски, генерация реактивной мощности. Эффективной мерой повышения качества МЭС и, как следствие, предотвращения утечки конфиденциальной информации по цепям питания и заземления является централизованная установка силовых (косинусных) конденсаторов типа КС1, КС2; конденсаторных установок типа УКЛ, УКН, УКТ, ККУ; тиристорных компенсаторов реактивной мощности типа ТКРМ, варисторных ограничителей перенапряжения типа ОПН и т.п.

Другими способами снижения нагрузки на сеть служат применение на месте потребления электроэнергии стабилизаторов напряжения, автотрансформаторов, дополнительных автономных источников электропитания, а также широкое внедрение устройств плавной коммутации нагрузки в соответствии с имеющимися потребителями электроэнергии [4, 5].

Литература

1. Кучумов Л.А. Потери мощности в электрических сетях и их взаимосвязь с качеством электроэнергии: учеб. пособие / Л.А. Кучумов, Л.В. Спиридонова. – Л.: Изд. ЛПИ, 1985. – 92 с.

2. Мордухович Л.Г. Системы радиосвязи: Курсовое проектирование. учеб. пособие для вузов / Л.Г. Мордухович, А.П. Степанов. – М.: Радио и связь,1987. – 192 с.

3. ГОСТ 13109-97. Электрическая энергия. Совместимость технических средств электромагнитная. – М.: ИПК Изд-во стандартов,1998.

4. Тиристоры. Технический справочник / Под ред. В.А. Лабунцова. – М.: Энергия, 1971. – 157 с.

5. Алиев И.И. Справочник по электротехнике и электрооборудованию. – М.: Высшая школа, 2000. – 255 с.

Бекмачев Александр Егорович
Ижевский государственный технический университет, инженер
Эл. адрес: sam@mail.ru

A.E. Bekmachev

Research of loss of confidential infirmation on food chains and grounding

Analyzed the potential threats to information security of stand-alone facilities where the total power of the electrical load on the network is commensurate with the power source of electricity,such conditions are also defined as «critical load». The possibility of monitoring the information about the cycles in the facility with the help of the freely available measurement units has shown. The technical means to counter the unauthorized collection of information offered.

Keywords: threat, confidentiality, information security, unapproved access to information, device.