ВЛАДИСЛАВ ЧЕПИНОГО,
управляющий директор ООО «Коммуникации»

Системы оперативно-технологической связи и оповещения на предприятиях и необходимость их защиты от несанкционированного доступа

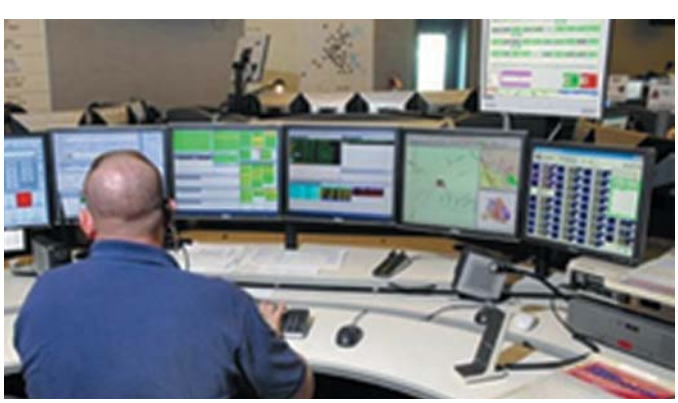
Перед современным производством стоит немало важных и первостепенных задач. Мировая промышленность развивается быстрыми темпами: появляются новые научные разработки в области технологических процессов, применяется усовершенствованное производственное оборудование. Но, несмотря на это, количество техногенных и экологических катастроф продолжает расти.

Участки и цеха, на которых работа связана с воспламеняющимися, окисляющимися, горючими, взрывчатыми и токсичными веществами, представляют опасность для предприятия и окружающей природной среды. Таким образом, промышленная безопасность на опасных производствах выходит на первый план.

Своевременное обеспечение предприятий оперативно-технологической связью и оповещением – залог безопасности жизни и здоровья работников предприятия. Диспетчерская и двухсторонняя громкоговорящая связь позволяет минимизировать последствия аварии или предотвратить ее вовсе, избежать травматизма и человеческих жертв, разрушений и неполадок в работе, дает возможность оперативно управлять персоналом, обеспечив доступ к связи для каждого работника.

Оборудование оперативно-технологической связи, устанавливаемое на производствах, представляет собой сложную спроектированную систему, которая может быть исполнена в различных конфигурациях, исходя из технологических особенностей предприятия.

Установленный на объекте коммутатор представляет собой стандартный телекоммуникационный «шкаф» с оборудованием, к которому подключены различные устройства и который принимает сигналы управления от других систем информационно-технологического обеспечения. Для начальников и диспетчеров устанавливаются многоклавишные настольные диспетчерские пульты связи и управления. Непосредственно на объектах имеются всепогодные или взрывозащищенные промышленные переговорные устройства, сигналы



с которых дублируются на выносные рупорные громкоговорители и оптические сигнальные устройства.

Вся система оперативно-технологической связи включает в себя более десятка наименований, что говорит о сложности и трудоемкости процесса проектирования.

Производители оборудования, зарекомендовавшие себя на рынке связи, осуществляют контроль производства своей продукции, тщательно тестируют каждую позицию. По опыту наших зарубежных коллег оборудование, предназначенное для установки во взрывоопасных зонах, проходит испытания независимыми лабораториями в течение двух лет, прежде чем начинается серийное производство.

Оборудование систем связи должно выдерживать большие перепады температур, надежно работать в условиях повышенной запыленности, наличии химически агрессивных сред и взрывоопасных зон. Поэтому при выборе производителя следует обращать внимание на такие факторы, как класс защиты, уровень влагозащищенности и пыленепроницаемости.

Однако, помимо надежности диспетчерских пультов, громкоговорителей и переговорных устройств, установленных на участках, внимание нужно обратить также на «мозг» системы. А именно, на программное обеспечение (ПО), устанавливаемое на центральном коммутаторе. ПО позволяет реализовать весь спектр функций диспетчерской, двусторонней громкоговорящей, командно-поисковой, селекторной связи и оповещения.

Вся система оперативно-технологической связи включает в себя более десятка наименований, что говорит о сложности и трудоемкости процесса проектирования

Так же на базе ПО создается ряд дополнительных возможностей системы. Например, функция удаленного доступа. Еще в 2007–2008 годах при внедрении системы диспетчерской, громкоговорящей связи и оповещения на ОАО «ЛУКОЙЛ-Нижегороднефтеоргсинтез» возник вопрос сервисного обслуживания оборудования без фактического присутствия на территории предприятия. И тогда был разработан «модуль удаленного доступа», который позволяет при помощи IP-адреса подрядчика осуществлять управление системой. Таким образом, система, установленная в любой точке мира, теперь может обслуживаться из центрального офиса компании-производителя.

Тем временем современность бросает все новые вызовы. Создаются угрозы безопасности, которые требуют определенных методов защиты. Повысившаяся в последнее время угроза террористических атак (примером может служить нападение на атомные электростанции в Бельгии) заставляет промышленные предприятия усиливать меры безопасности.

Защита самой системы связи от внешних атак становится все более актуальной. Кибератаки на системы оперативно-технологичесвой связи и оповещения могут привести не только к остановке производства, но и создать серьезную опасность для сотрудников предприятия и окружающих территорий.

Вернемся к недавнему происшествию в Бельгии. При планировании атаки на АЭС «Тианж» террористы убили сотрудника службы безопасности с целью похищения у него пропуска работника станции. Фактически злоумышленники, проникнув на территорию АЭС, смогли бы вывести из строя систему оповещение о тревоге, подключившись к управлению технологической связи. Или же, наоборот, запустить сообщение с ложной информацией, вызвав панику у персонала. Это позволит отвлечь внимание службы охраны и реализовать более крупное разрушение.

Практика зарубежных производителей акцентирует внимание на защите информации в сетях беспроводной передачи данных и сетях международного доступа. Компьютерные ПО

защищают антивирусные программы, телефонные системы – программы специальных кодировок. С целью защиты систем оперативно-технологической связи и оповещения был разработан «SWMS. Модуль защиты программного обеспечения от несанкционированного доступа к системам связи». Схема функционирования модуля SWMS схожа с компьютерной технологией «антивируса» и на данный момент является инновационной для систем связи. Принцип работы заключается в создании дополнительного защитного барьера при подключении к оборудованию, установленному на предприятии.

Еще одним поводом, подтверждающим необходимость ограничения доступа к ПО систем связи, является недобросовестность некоторых подрядчиков. На этапе пусконаладочных работ в целях экономии собственных средств некоторые подрядчики нанимают дешевую рабочую силу. Неквалифицированный персонал производит неверные настройки системы уже на этапе ее установки на объект заказчика. Вероятность возникновения чрезвычайных ситуаций на опасных производствах велика (взрывы, пожары, выброс вредных химических и радиоактивных веществ и т. д.). Некорректно настроенная система связи и оповещения может дать сбой в самый необходимый момент, что понесет за собой жертвы, внеплановый ремонт оборудования и финансовые потери.

Надежность работы оборудования оповещения является важнейшим условием по обеспечению безопасности

Надежность работы оборудования оперативно-технологической связи и оповещения является важнейшим условием по обеспечению безопасности, от которого зависят жизни людей. Поэтому ПО систем связи должно быть защищено от некомпетентных «специалистов». Установленная защита от несанкционированного доступа позволяет программировать систему только уполномоченным подрядчикам, имеющим код доступа.

Стоит отметить еще одну причину, доказывающую необходимость защиты систем связи на предприятии. Фактически персонал предприятия, изменив настройки системы, может организовать ложное срабатывание сигнала тревоги и вызвать незапланированную эвакуацию. Остановка технических процессов, несомненно, влечет за собой финансовый ущерб для предприятия. Модуль SWMS предотвращает доступ сотрудников, непричастных к работе с системами громкоговорящей связи, и позволяет организовать полноценный контроль за функционированием оповещения, тем самым предупреждая саботаж рабочего процесса, влекущий за собой простой оборудования на производстве.

Каждое промышленное предприятие является объектом повышенной опасности. Безопасность – важное условие в организации рабочего процесса. Защищенность систем оперативно-технологической связи и оповещения от злоумышленников и некомпетентных специалистов на опасных объектах является необходимым условием обеспечения промышленной безопасности. Некорректно работающее оборудование связи приводит к сбоям в работе предприятия, гарантируя серьезный ущерб производству.

Российские компании-производители занимают передовые позиции в мире по разработкам в области промышленной безопасности. ●