



Комплексный подход к обеспечению безопасности стационарных платформ и плавучих буровых установок

И.В. Войтенко, М.Е. Белецкий (ЗАО «Хоневелл»)

Представлен подход к созданию комплексной системы обеспечения безопасности стационарных платформ и плавучих буровых установок на основе интегрированных решений Honeywell.

Ключевые слова: интегрированная система безопасности, морские платформы, террористическая угроза, видеонаблюдение, система контроля доступа, радиолокационная станция ближнего действия, тепловизоры.

В настоящее время большое внимание уделяется проектам по освоению углеводородных ресурсов арктического шельфа и прибрежных районов. Крупнейшие компании ведут и планируют строительство значительного числа морских объектов для разведки, добычи и транспортировки углеводородов в Арктике, в том числе: плавучие и стационарные буровые установки различных типов, добычные морские плавучие и гравитационные установки, морские выносные причалы и хранилища, береговая инфраструктура (обеспечение снабжения платформы, доставка персонала) и др.

Все это увеличивает угрозу рисков, в том числе незаконных и террористических актов для буровых платформ и других производственных объектов. Буровая платформа как объект критически важной инфраструктуры состоит из сотен эксклюзивных конструкций, включая сервисные объекты (вертолетная площадка, зоны технического обслуживания, командный центр и др.). Вывод из строя одного из них может привести к остановке всего операционного цикла добычи, разработки и транспортировки нефти и газа.

Морские платформы и комплексы расположены в нескольких километрах от побережья. Существует несколько основных типов платформ: стационарная, свободно закрепленная ко дну, полупогружная, мобильная морская платформа с выдвигаемыми опорами (рис. 1). Капитальные затраты и человеческие ресурсы на строительство платформы чрезвычайно высоки — порядка 500 млн. долл. в США и 4 года работы. Однако объемы ежесуточной добычи тоже могут быть огромными — до 250 тыс. баррелей нефти или 14 млн. долл. США. Один морской комплекс может добывать нефть с 24 скважин, и этот гигантский объем

нефти проходит весь производственный цикл на одном объекте в открытом море.

В последнее время все больше специалистов по антитеррористической безопасности обращают внимание на высокую потенциальную опасность терактов, направленных против объектов водной инфраструктуры и, в частности, морских платформ [1, 2]. Морская платформа — единственный объект нефтепромышленного хозяйства, атака на который может быть произведена с воздуха, поверхности и под водой. Наибольшую угрозу для критической инфраструктуры на сегодня представляют действия диверсионных групп террористических, преимущественно международных, организаций. Мегапроекты по освоению и добыче углеводородных ресурсов арктического шельфа ставят серьезнейшие задачи по обеспечению безопасности морских объектов и другой инфраструктуры. В эти задачи входит обеспечение транс-



Рис. 1. Различные типы морских платформ и объектов оффшорной инфраструктуры (www.kaigyoshien-ring.com)



Рис. 2. Различные модели РПС, тепловизионных и всепогодных камер

портной безопасности акватории, оперативное автоматическое обнаружение объектов, контроль за их перемещением на акватории, в том числе на дальних дистанциях.

В качестве основных источников угроз для морского объекта рассматривают, прежде всего, злоумышленников, использующих специальное подводное снаряжение (пловцы-диверсанты), малые подводные лодки и маломерные суда. Незваные гости (например, рыбаки или Гринпис), внутренняя кража и саботаж подрядчиков и персонала создают дополнительные риски для безопасности. Эти риски увеличиваются, если идет эвакуация персонала из за погодных условий. Эти риски сохраняются пока платформа не войдет в рабочий ритм и работники не вернуться на вахту. Морские месторождения обычно расположены в значительной удаленности от береговой полосы, и служба безопасности или полиция не имеют оперативного доступа на такого рода объекты.

Террористы чрезвычайно последовательны и применяют все свои навыки и опыт для выявления пробелов в защите морской платформы и разрабатывают детальный план, использующий недостатки системы безопасности в полной мере. Обычно большинство нападений в открытом море происходят поздним вечером или рано утром, когда бдительность персонала на самом низком уровне и видимость судна с платформы практически равна нулю при определенных погодных условиях. Фактор неожиданности является самым сильным элементом стратегии злоумышленников.

В разработке практического плана охраны платформы важнейшим элементом является возможность раннего обнаружения потенциальной атаки [3]. Это является самым эффективным с точки зрения затрат подходом по предотвращению физической атаки или высадки злоумышленников на платформу. Сегодня используются различные подходы для обеспечения безопасности: ночное патрулирование палубы платформы, прожектора подсветки платформенных зон, сетка под напряжением и обмен сообщениями между танкерами и платформой по текущей обстановке.

Интегрированное решение

Большим преимуществом является управление всеми системами безопасности с единой платформы автоматизации и централизованное отслеживание

обстановки в целом. Интеграция отдельных систем в масштабе всей морской инфраструктуры снижает нагрузку на персонал, объединяет разрозненные данные о происшествии и оперативно выводит их на пульт оператора в удобном и читаемом виде.

Honeywell Building Solutions (HBS) разработала интегрированное решение по безопасности для пространств вокруг морских буровых установок и мест хранения углеводородов, предоставляющее широкие возможности по интеграции систем контроля доступа, безопасности, цифрового видеонаблюдения, пожарной сигнализации, защиты периметра платформы и акватории, обнаружения вторжений, сетевой инфраструктуры и систем автоматизации процессов. Решение HBS позволяет составить полную картину обстановки на объекте, контролировать ее и незамедлительно оповещать оператора и службу безопасности платформы, береговые службы реагирования. Скорость, с которой реагирует работник на сигнал тревоги системы безопасности, является показателем эффективности самой системы и уже сама по себе является сдерживающим фактором для потенциальных террористов или злоумышленников.

Интегрированное решение по обеспечению безопасности позволит внедрить многоуровневую стратегию безопасности с единой системой управления всеми физическими системами на объекте, повышая осведомленность на корпоративном уровне и возможность оперативно развивать систему в соответствии с последними тенденциями и прогнозами.

Комплексная интегрированная система безопасности морского объекта состоит из нескольких подсистем.

Радиолокационная станция (РПС) ближнего действия

Стратегия террористов организовывать свои атаки под покровом ночи, когда бдительность персонала притуплена, указывает на самые слабые стороны в системе безопасности морских платформ. Люди склонны постоянно отвлекаться, и после часа напряженного наблюдения их глаз «замыливается», и они делают ошибки. При низкой освещенности или полной темноте первое «выявление» нарушителей может случиться, когда они уже на палубе платформы.

РПС ближнего действия (рис. 2) отображает маломерные цели на многокилометровом удалении

(до 30 км) от охраняемого объекта. Возможно совместное использование РЛС и морских камер, что обеспечивает видеофиксацию нарушителя в зоне особой значимости и его автоматического ведения. С обнаруженным судном может быть установлен контакт по приемопередающей радиостанции, и в случае молчания команда готова работать по тревожному регламенту. Это позволяет персоналу принять контрмеры, такие как: звуковой сигнал тревоги на платформе, оповещение головного офиса компании и службы по борьбы с угрозами (береговые и т.д.), освещение платформы и подозреваемого в нарушении объекта, инициация других процедур реагирования. Во многих случаях раннее обнаружение позволяет отпугнуть потенциальных нарушителей.

Всепогодные и многоцелевые поворотные камеры и охлаждаемые тепловизоры кругового обзора

После идентификации и определения приоритета угрозы запускаются автоматические реакции. Обычно в таких случаях за угрозой следит отдельная камера ТВ-системы. Система видеонаблюдения с двумя типами камер может быть полностью интегрирована с РЛС и системами управления безопасностью для визуальной оценки обнаруженных целей. Радиолокационные системы видеонаблюдения состоят из комбинации лазерной камеры день/ночь и тепловизора (рис. 2). Использование двух видов камер оптимизирует визуальную оценку в различных погодных условиях. Например, камеры с лазерной подсветкой позволяют засекать движение человека на расстоянии 1500 метров, распознавать человека на расстоянии 1000 м, распознавать лицо на расстоянии 450 м в любое время суток. Если густой туман мешает обычным камерам, в дело вступают тепловизоры.

При перемещении объекта камера следует за ним. Видеозапись на высокой кадровой частоте начинается вместе со слежением. Если цель определяется как "безопасная", то оператор подтверждает получение сигнала тревоги и РЛС продолжает отслеживать объект. В случае потенциально опасной цели оператор начинает реализацию заранее определенного плана реагирования.

Предварительная запись сохраняется в системе и содержит буферные кадры, полученные до возникновения угрозы. Записи ТВ-системы имеют цифровую подпись и могут быть использованы в суде в качестве доказательства. Интеграция системы радарного видеонаблюдения с другими системами и автоматическое выполнение задач обеспечивают высокий уровень безопасности объекта за гораздо меньшую стоимость, чем традиционные методы обеспечения безопасности.

Digital Video Manager (DVM)

Система DVM позволяет захватывать и записывать тревожное событие, производить его анализ. DVM оснащен передовой системой хранения видеоданных

для быстрого и удобного доступа к архиву записей с любого рабочего места. Данные могут храниться в «облаке», что исключает вероятность его удаления после нападения на платформу. Новые возможности записи и воспроизведения в сочетании с улучшенным интерфейсом также содействуют быстрому выявлению потенциальной угрозы и реагированию персонала службы безопасности прежде, чем случится правонарушение или будет причинен вред морской платформе.

В систему встроены интеллектуальные модули диагностики, которые анализируют работу системы безопасности, чтобы помочь операторам быстро обрабатывать отчеты об активности в кадре, они также выполняют диагностику системы, проверяют ее производительность и состояние. Видеоаналитика ограничивается только полем обзора камеры.

DVM R500 является также интегральной составляющей системы управления объектами инфраструктуры Honeywell Enterprise Buildings Integrator (EBI), которая объединяет все аспекты решений безопасности, в том числе видеонаблюдение, системы контроля доступа и охранной сигнализации. Это дает головной компании единую точку доступа ко всей необходимой информации и ресурсам для контроля, управления и защиты морской платформы и акватории возле нее. В результате руководители службы безопасности получают оптимизированную видеoinформацию и интеллектуальное управление видеонаблюдением, что позволяет им более эффективно и действенно использовать свой персонал и ресурсы. Также в единую систему управления можно интегрировать гидроакустические станции, объемные и магнитометрические средства подводного обнаружения, инженерные системы отказа в доступе и обеспечения безопасности подводной части акватории, состоящие из устройств обнаружения вторжения и (полу)автоматических средств обороны (представляют собой различные виды заграждений и выбираются индивидуально в зависимости от типа поставленной задачи и предполагаемого нарушителя).

Система управления доступом

Эффективная и надежная система управления доступом является необходимым требованием любой морской платформы. Ее основная цель заключается в предотвращении подрывной деятельности, например, саботажа и любых других действий, которые могут принести ущерб платформе. Морской буровой комплекс должен быть оборудован мультизонами с разграниченным уровнем доступа персонала в каждую из них. Все сигналы тревоги (отказ в доступе, проникновение и двери «открытые слишком долго» и пр.) должны быть немедленно обработаны и по ним должно быть вынесено решение. Зоны, требующие более высокого уровня безопасности, должны быть оснащены дополнительными камерами для визуальной оценки тревожного события.

Заключение

Оффшорные проекты по добыче углеводородов могут стать мишенью международных террористических организаций независимо от политического строя и экономической ситуации в стране. В ответ на эту угрозу энергетические компании должны принять решительные меры по обеспечению безопасности и сохранности своих капиталоемких оффшорных активов.

Компания Honeywell Building Solutions, располагающая последними разработками в области автоматизации, видеонаблюдения и сигнализации и использующая единый пользовательский интерфейс для обслуживающего персонала и работников службы безопасности, предлагает комплексную систему

по управлению безопасностью, позволяющую эффективно решать растущие проблемы безопасности в эксплуатации морских платформ.

Список литературы

1. Федяев С.Л., Козлов С.А., Маркевич П.А. Обзор технических средств активного противодействия проникновению на объекты, особой важности со стороны, акваторий // Специальная техника. 2012. №2. С. 2-8.
2. Козлов С.А., Львов Д.Г. Обзор технических средств активного противодействия вторжениям на объекты различной категории // Безопасность, достоверность, информация. 2009. №3-4. С. 30-35.
3. Лисанов М.В. и др. Аварийность на морских нефтегазовых объектах // Oil and Gas Journal Russia.- 2010. № 5 (39). С. 48 - 53.

Войтенко Игорь Владимирович — канд. техн. наук, ген. директор, Белецкий Максим Евгеньевич — директор по стратегическому маркетингу подразделения «Системы и сервис для зданий» ЗАО «Хоневелл». Контактный телефон (495) 796-98-00.

Программный пакет Honeywell RMG Gas Metering Management повышает точность и надежность измерения расхода газа

Корпорация Honeywell выпустила новую версию ПО RMG Gas Metering Management, с помощью которого операторы газоизмерительных станций могут осуществлять местный или дистанционный контроль технологических операций, выполнять анализ данных и проводить дистанционное техническое обслуживание. Это решение снижает эксплуатационные затраты и повышает точность и надежность измерений.

Система RMG Gas Metering Management совместима с измерительными приборами RMG от Honeywell и приборами других изготовителей, что позволяет оператору точно определить техническое состояние всех приборов учета газа на станции с помощью одного программного пакета. Кроме того, возможность удаленного доступа к измерительным приборам упрощает планирование и организацию технического обслуживания, а также снижает затраты, сводя к минимуму количество посещений станции.

Цель разработки нового решения заключалась в том, чтобы предоставить нашим заказчикам свободу и гибкость в выборе необходимых измерительных приборов вне зависимости от производителя. Система RMG Gas Metering Management работает как с приборами RMG, так и с обо-

родованием других компаний, что позволяет заказчикам во всем мире создавать узкоспециализированные решения, обеспечивая при этом контроль через единую централизованную надежную систему.

Honeywell уже провела испытания своей системы совместно с перспективными заказчиками, в числе которых компания Schwaben Netz GmbH (Германия). Результаты бета-тестирования модуля Gas Metering Terminal показали, что этот модуль удобен для операторов, а также достаточно надежен и стабилен. Предполагается эффективность от применения нового решения и в отделе технического обслуживания для оперативной дистанционной диагностики.

В системе Gas Metering Management, а также в ее модулях Gas Metering Analysis и Gas Metering Terminal используется легко конфигурируемая платформа, позволяющая устанавливать эту систему без внесения каких-либо пользовательских изменений в программу. Динамические экраны системы отображают параметры контролируемой станции и предоставляют техническому персоналу и сотрудникам отдела учета газа данные о текущем расходе, давлении, температуре и аварийных сигналах в реальном времени.

Новый программный пакет Honeywell RMG MeterSuite снижает издержки на создание полнофункциональной системы коммерческого учета

Корпорация Honeywell в сотрудничестве с компанией Swinton Technology, ведущего независимого интегратора измерительных систем, разработала систему учета MeterSuite, интегрируемую с платформой промышленного управления Experion Process Knowledge System (PKS). Система MeterSuite обеспечивает полнофункциональный учет расхода жидкостей и газов, повышение рентабельности, увеличение срока службы и оптимизацию управления. Это единственная коммерческая система измерения, которую можно встроить в систему управления.

Система MeterSuite предлагает заказчикам возможность выполнять измерения любого типа с использованием

единой готовой и поддерживаемой платформы, исключая потребность в специализированном оборудовании и дополнительных проектных разработках.

Двухуровневая архитектура MeterSuite позволяет убрать целый уровень из традиционной трехуровневой модели измерительной системы благодаря подключению непосредственно к распределенной системе управления объекта. В результате уменьшается число требующих обслуживания последовательных линий связи и каналов OPC. Кроме того, в отличие от традиционных измерительных систем, MeterSuite использует единую базу данных, что позволяет дополнительно уменьшить объем технического обслуживания.

[Http://www.honeywell.com/ps](http://www.honeywell.com/ps)