



БЕЗОПАСНОСТЬ ПРОМЫШЛЕННАЯ И ИНФОРМАЦИОННАЯ

А. Маляревский

Жизнь современного человека — и на производстве, и в быту, и в городе, и в поездках — неразрывно связана с техникой. К сожалению, все технические системы — это и помощь, и опасность. Ведь стоит чуть-чуть ослабить внимание, выпустив их из-под контроля, как происходят аварии разного масштаба, вплоть до техногенных катастроф, поражающих целые регионы. Гибнут люди, оказывается безнадежно испорченной среда обитания, в общественном сознании на многие годы остается травма, связанная с чувством незащищенности.

Полностью предотвратить такие катастрофы невозможно. Но в большинстве отраслей десятилетиями выработались правила, неукоснительное соблюдение которых позволяет с минимальным риском эксплуатировать опасные технические системы: шахты, вредные производства, атомные электростанции... Несмотря на очевидную необходимость соблюдения таких правил, в этом вопросе нельзя положиться на сами предприятия. Необходим жесткий контроль со стороны государства. Понимание этого возникло не сегодня: еще Петр Первый в 1719 году учредил Берг-коллегию, отвечавшую за самое опасное в то время производство — горное дело.

➤ Шло время, постоянно расширялось число опасных производств. Одновременно расширялись и сферы деятельности надзорных служб. Сегодня одна из крупнейших среди таких служб в России — Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор).

Ростехнадзор был образован во исполнение указов Президента Российской Федерации от 9 марта 2004 года № 314 и от 20 мая 2004 года № 649. Служба является федеральным органом исполнительной власти, осуществляющим функции по принятию нормативных правовых актов, контролю и надзору в сфере охраны окружающей среды в части, касающейся:

- ограничения негативного техногенного воздействия;
- безопасного ведения работ, связанных с пользованием недрами и их охраной;
- промышленной безопасности;
- безопасности при использовании атомной энергии;
- безопасности электрических и тепловых установок и сетей;
- безопасности гидротехнических сооружений на объектах промышленности и энергетики;
- безопасности производства, хранения и применения взрывчатых материалов промышленно-

го назначения, — а также специальные функции в области государственной безопасности в указанной сфере.

Ростехнадзор является также:

- органом государственного регулирования безопасности при использовании атомной энергии;
- специально уполномоченным органом в области промышленной безопасности;
- органом государственного горного надзора;
- специально уполномоченным государственным органом в области экологической экспертизы в установленной сфере деятельности;
- органом государственного энергетического надзора;
- специально уполномоченным органом в области охраны атмосферного воздуха.

Главной целью Ростехнадзора является обеспечение защищенности работников поднадзорных объектов и населения, а также окружающей среды от угроз техногенного характера путем применения предусмотренных полномочиями службы мер, направленных на недопущение нарушений обязательных требований по безопасности в установленной сфере деятельности.

КАК РАБОТАЕТ РОСТЕХНАДЗОР

Масштабы деятельности Ростехнадзора впечатляют. Ведь это ведомство контролирует буквально каждый потенциально опасный производственный объект на всей территории страны — от обычного лифта в жилом доме до заводов-гигантов и атомных электростанций. При этом необходимо отслеживать точное выполнение регламентных работ на каждом, даже самом маленьком участке. И если что-то не так, сотрудник Ростехнадзора должен вынести соответствующее предписание (вплоть до немедленной остановки производства) и обязательно проконтролировать его исполнение. Это очень большая работа — ведь за год выносятся сотни тысяч таких предписаний. А поскольку их исполнение связано с убытками предприятия, необходима безупречная аргументация каждого такого решения, чтобы его можно было отстоять в суде. Это и огромная ответственность, и необходимость опираться на постоянно меняющуюся информационно-справочную базу.

Удивляет и эффективность работы Ростехнадзора, ведь штат службы не превышает 12,7 тыс. человек. И это в масштабах всей страны!

Организационная структура Ростехнадзора является двухзвенной: центральный аппарат и территориальные органы федерального подчинения. В состав центрального аппарата входят 15 управлений, а к территориальным органам Ростехнадзора относятся 78 территориальных и межрегиональных управлений по технологическому и экологическому надзору, 7 межрегиональных территориальных округов по надзору за ядерной и радиационной безопасностью, а также межрегиональный территориальный округ по информатизации и защите информации. В систему Ростехнадзора входят также 5 федеральных государственных унитарных предприятий и 12 федеральных государственных учреждений.

ИНФОРМАТИЗАЦИЯ НА СЛУЖБЕ РОСТЕХНАДЗОРА

Возрождение реального сектора экономики, расширенное использование нового оборудования и технологий на одних производствах и устаревающего, а порой, и ветхого оборудования — на других значительно увеличивают нагрузку на службы Ростехнадзора. И тут существенную помощь могут оказать информационные системы. Такой опыт уже есть.

В ходе масштабной реорганизации системы исполнительной власти страны, произошедшей в 2004 году, Ростехнадзор объединил несколько ранее существовавших надзорных служб: Госатомнадзор России, Госгортехнадзор России и службы Экологического надзора и Энергонадзора. К этому времени в Госгортехнадзоре России уже была создана и прошла опытную эксплуатацию государственная автоматизированная **информационно-управляющая система регулирования промышленной безопасности (АИС ПБ)**.

Интересна история создания этой системы. В течение ряда лет различные структурные подразделения Ростехнадзора России разрабатывали своими силами компьютерные программы, упрощавшие решение тех или иных частных задач. Но и тогда было понятно, что это временная мера. Для кардинального повышения эффективности работы нужно было создать единую информационную систему, которая объединила бы все структурные подразделения и в которой были бы проработаны все аспекты деятельности ведомства.

Работа по созданию АИС ПБ заняла около 4 лет. Исполнителем работ стала некоммерческая организация АНО ИАЦ ПБ, а поставщиком системообразующих технологий — компания ИВК. Система сформировала единое информационное пространство для коллективной работы, обмена данными между удаленными объектами в автоматическом режиме, автоматизированной аналитико-статистической обработки собранной информации. При этом за счет использования в АИС ПБ решений ИВК «ИВК Юпитер» и «ИВК Кольчуга» обеспечивается необходимый уровень безопасности государственных информационных ресурсов.

Уже на начальных этапах создания АИС ПБ ее заказчики и разработчики ясно осознали, что для обеспе-

чения требуемой «живучести» и адаптивности этой системы в условиях динамично изменяющегося законодательства и при объективном ограничении человеческих и материальных ресурсов необходимо использовать технологию, которая позволит модернизировать систему в ходе ее эксплуатации без участия обслуживающего персонала на местах, в территориальных органах.

Задача модернизации состава (структуры) всех экземпляров информационных баз данных на каждом объекте без потери информации для внедрения обновлений прикладных задач требует значительных усилий и времени.

С учетом указанных обстоятельств в АИС ПБ был разработан уникальный механизм телекоммуникационного обмена, позволяющий не только «выравнивать контент», но и дистанционно управлять структурой накапливаемых сведений, а также устанавливать новые версии созданных программных средств, включая прикладные задачи и служебные программы по технологическому и экологическому надзору.

Сегодня АИС ПБ используется во всех 78 территориальных органах по технологическому и экологическому надзору и поддерживает лицензирование, разрешительную деятельность, регистрацию опасных

Главной целью Ростехнадзора является обеспечение защищенности работников поднадзорных объектов и населения, а также окружающей среды от угроз техногенного характера путем применения предусмотренных полномочиями службы мер, направленных на недопущение нарушений обязательных требований по безопасности в установленной сфере деятельности.

объектов, сбор и консолидацию отчетности в сфере надзора за промышленностью и горным делом. Доступная должностным лицам Ростехнадзора часть программного обеспечения АИС ПБ представляет собой комплекс так называемых «прикладных задач» — специальных программных средств, обеспечивающих

автоматизацию отдельных функций сотрудников системы Ростехнадзора. Центральный аппарат и каждый из 78 территориальных органов по технологическому и экологическому надзору оснащены одинаковыми комплексами прикладных задач АИС ПБ. Пользователи каждого отдельно взятого органа Ростехнадзора работают с контентом информационной базы данных только этого территориального органа.

БЕЗОПАСНОСТЬ В АИС ПБ

Система АИС ПБ обеспечивает все информационные потоки, связанные с деятельностью Ростехнадзора в области горного и промышленного надзора, включая наполнение консолидированной базы данных и доступ к хранящейся в ней информации. Благодаря этому в области надзора за промышленностью и горным делом ушли в прошлое неполные и несвоевременные сводки, просроченные поручения, отсутствие целостной картины состояния контролируемых объектов на всей территории страны. Иными словами, и текущая деятельность, и принятие ответственных решений получили адекватную информационную поддержку.

Вместе с тем такая концентрация данных ставит на повестку дня вопрос их надежной защиты, должное противодействие информационным угрозам. Эти угрозы реально существуют, ведь в системе находится абсолютно достоверная и полная информация об опасных производственных объектах и состоянии технической базы конкретных предприятий. Несанкционирован-

ный доступ к этим сведениям стал бы неоценимой услугой и для террористов, и для враждебных спецслужб, и для коммерческих организаций. При этом важно защититься не только от хакера, атакующего информационную систему из Интернет, но и от «недоброжелателя», имеющего к ней вполне легитимный доступ. Как показывает опыт различных отраслей, именно эта опасность чаще других служит реальной причиной масштабных утечек информации.

Уже при создании АИС ПБ было решено строить систему так, чтобы уровень ее защищенности соответствовал действующей государственной нормативной базе, но мог быть в любой момент повышен. Создание такой защиты в территориально распределенных информационных системах, использующих открытые линии связи и стандартные вычислительные платформы, СУБД и компьютерное оборудование, — это, без преувеличения, уникальная инженерная задача, которую удалось решить.

При создании системы информационной безопасности организация сталкивается с двумя важными проблемами. Первая связана с концептуальным различием моделей безопасности, которые приняты на организационном и информационном уровнях безопасности мыслят категориями должностных обязанностей,

типов документов и допустимых действий с ними, грифов секретности и других понятий, выработанных еще в «докомпьютерную эру» и доказавших свою эффективность. Вместе с тем специалисты по информационной безопасности ИС оперируют совсем другими понятиями, например правами доступа к файлам, коммуникационным портам, принадлежностью пользователя к определенным доменам или группам. Принципиальное отличие этих двух подходов создает брешу в защите. Другой причиной, действующей уже на уровне вычислительных платформ, является различие в системах безопасности и качестве их реализации на разных вычислительных платформах. Это различие существует даже между версиями одной и той же вычислительной платформы и, тем более, углубляется в гетерогенных вычислительных системах.

Понимая это, разработчики АИС ПБ приняли дальновидное, не типичное для современных организаций решение — применение программного обеспечения (ПО) класса middleware как архитектурной основы системы. Это позволило, не снижая уровня требований к безопасности системы, решить все поставленные задачи, одновременно повысив многие ее эксплуатационные характеристики: надежность, масштабируемость, простота сопровождения, управление изменениями в конфигурации системы и др. Вместе с тем сократились сроки разработки системы и затраты на ее создание.

Для решения задач обмена данными и обеспечения информационной безопасности используются ПО класса middleware «ИВК Юпитер» и межсетевой экран «ИВК Кольчуга».

В качестве транспортной среды «ИВК Юпитер» обеспечивает гарантированную доставку информации по надежным каналам связи, в том числе по каналам свя-

зи малой производительности, и гарантированное исполнение регламентов ее логической обработки. Как средство построения информационной безопасности «ИВК Юпитер» полностью устраняет отмеченные выше основные проблемы, защищает информацию при хранении и передаче по линиям связи и гарантированно препятствует подмене компонент системного и прикладного ПО в результате вирусных атак, умышленных или неумышленных действий системных администраторов и пользователей.

Межсетевой экран «ИВК Кольчуга» позволяет структурным подразделениям «Ростехнадзора» безопасно подключаться к сети Интернет и использовать ее как защищенную транспортную магистраль.

ИС РОСТЕХНАДЗОРА — ВЗГЛЯД В БУДУЩЕЕ

Руководство Ростехнадзора решило, что многоотраслевой и комплексный характер его деятельности ставит в качестве первоочередной задачи развитие информатизации с целью создания

Применение в АИС ПБ программного обеспечения (ПО) класса middleware как архитектурной основы системы позволило, не снижая уровня требований к безопасности системы, решить все поставленные задачи, одновременно повысив многие ее эксплуатационные характеристики: надежность, масштабируемость, простота сопровождения, управление изменениями в конфигурации системы и др.

единого информационного пространства, обеспечения планирования и мониторинга показателей работы службы.

Постановлением Правительства Российской Федерации от 01.02.2005 года № 49 Ростехнадзор был определен заказчиком работ по созданию единой информаци-

онной системы, в рамках которой намечено автоматизировать ряд актуальных задач, включая:

- планирование основных показателей деятельности службы;
- администрирование платежей за негативное воздействие на окружающую среду;
- создание необходимых реестров и кадастров для обеспечения деятельности органов государственного экологического надзора.

Создание такой системы — это актуальная государственная задача. Сложность ее решения еще более возрастает в связи с тем, что информационные системы ведомств, которые объединил Ростехнадзор, создавались независимо друг от друга.

Анализ возможных вариантов решения этой проблемы с использованием унаследованных средств автоматизации ранее самостоятельных надзорных ведомств показал, что наиболее предпочтительным является создание единого информационного ресурса Ростехнадзора на базе автономной информационной системы, разработанной по заказу Госгортехнадзора России (АИС ПБ). Ведь АИС ПБ демонстрирует сбалансированный подход к созданию систем, которые должны пережить и многократную смену нормативной базы, и «волны» технического прогресса, сопровождающиеся сменой вычислительных платформ и телекоммуникационных технологий.

