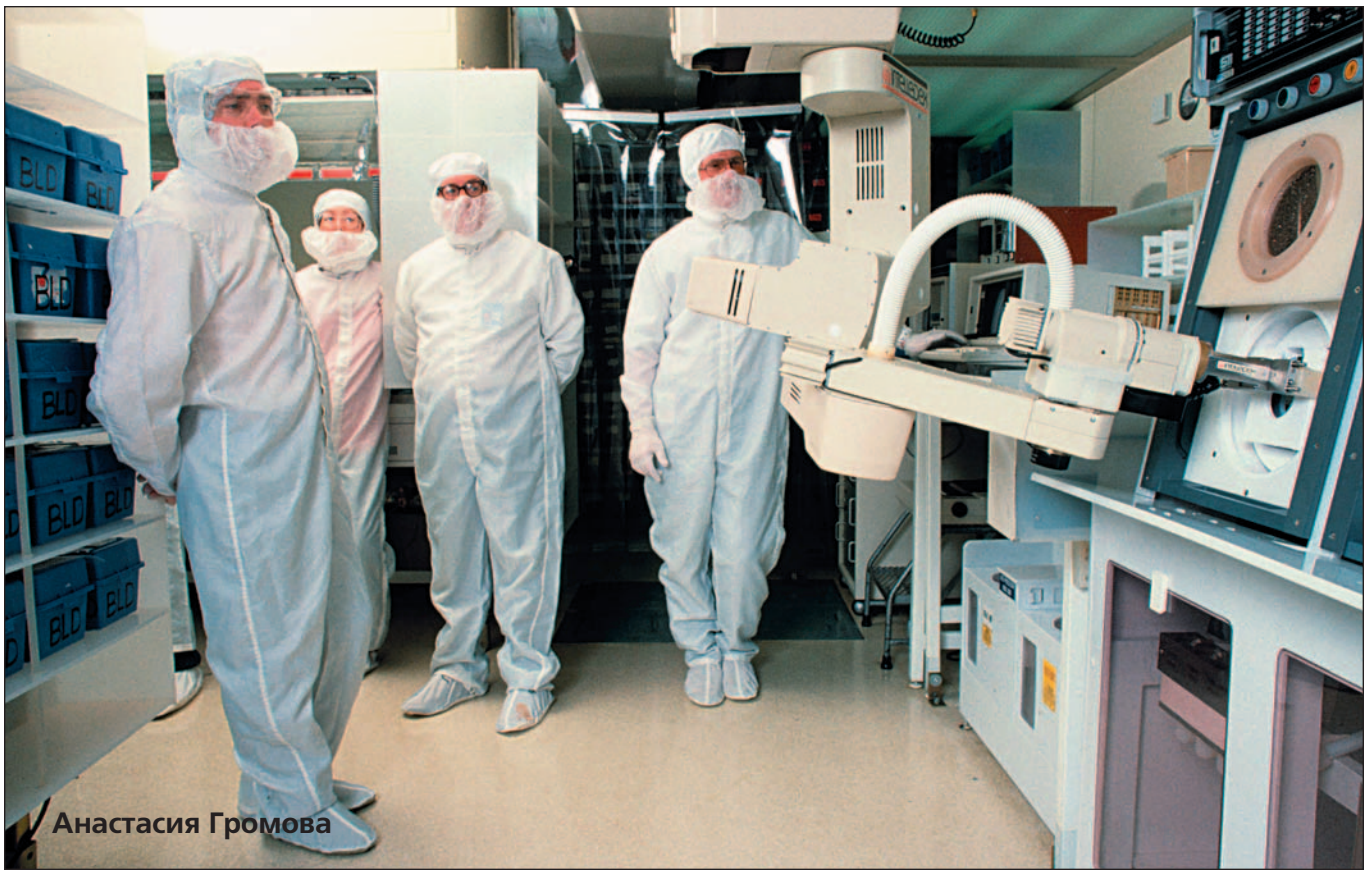
Химики США к угрозам готовы

Химические компании объединяются для противостояния современным угрозам



Анастасия Громова

В США Совет по информационным технологиям в химической промышленности объединил поставщиков и потребителей ИТ-услуг для эффективного решения проблем безопасности.

Опыт объединения

Вопросы безопасности для химических компаний играют первостепенную роль. Слабая компьютерная защищенность может повлечь за собой различные последствия: от потери прибыли до человеческих жертв. Пострадавшими могут быть и акционеры предприятия, и даже целый город.

Для предотвращения подобных катастроф и был создан американский Совет по информационным технологиям в химической промышленности (Chemical Information Technology Council).

Финансируется этот альянс за счет средств его участников. Все они активно работают также в рамках программы Chemstar, осуществляемой Американским химическим советом (American Chemistry Council). А 5 лет назад в поддержку инициатив Совета лидеры отрасли — Dow Chemical, DuPont, Rohm and Haas, Eastman Chemical, Nova Chemicals и Celanese — создали «Программу безопасности для химической промышленности» (Chemical Sector Cyber Security Program, CSCSP).

Данный альянс видит свою задачу в том, чтобы стать координирующим органом, который поможет отрасли ускорять внедрение средств обеспечения безопасности и обмениваться опытом их использования, а также реагировать на другие отраслевые потребности.

CSCSP призвана:

- способствовать распространению передового опыта в области компьютерной защиты,
- поддерживать усилия по повышению безопасности производственных и управляющих систем,
- стимулировать разработку более совершенных технологий,
- повышать интенсивность обмена информацией между химическими компаниями,
- согласовывать приоритеты отрасли с целями Министерства национальной безопасности.

Чтобы достичь поставленных целей, CSCSP сотрудничает с предприятиями, отраслевыми организациями и поставщиками ИТ-продуктов. Таким образом, химические компании имеют возможность непосредственно ставить задачи перед фирмами, работающими в сфере информационных технологий, и уже на этапе проектирования той или иной системы тестировать выпускаемые продукты и повышать их безопасность прежде, чем они будут выпущены в продажу.

Среди партнеров из числа ИТ-компаний есть те, кто создает производственные и управляющие системы, и те, кто предлагает оборудование, ПО и услуги. С альянсом сотрудничают такие крупные производители как IBM, SAP, Cisco, Microsoft и другие.

Химпром США

Химическая отрасль США — одна из крупнейших в мире и одна из важнейших для страны. Годовой объем производства химической промышленности Соединенных Штатов оценивается в сумму около 500 млрд долларов. При этом химическая индустрия является одним из 13 секторов промышленности, которые в 2002 году были выделены в качестве особо важной инфраструктуры в документе «Национальная стратегия внутренней безопасности». В связи с этим перед данной отраслью была поставлена задача разработки стратегии компьютерной защиты. ИТ-директора химических компаний уже сами понимали, что развитие технологий порождает такие угрозы безопасности, с которыми им не приходилось сталкиваться прежде.

Конечно, химическая отрасль сталкивается с такими же ИТ-угрозами, что и другие секторы промышленности, например с рисками для информационных бизнес-систем. Но для нее характерна и опасность другого рода, связанная с системами управления производством и наличием особо важной инфраструктуры. Среди примеров CSCSP приводит атаку в г. Квинсленде в Австралии на компьютерную систему очистки сточных вод, работавшую под управлением SCADA-системы. В результате миллионы галлонов нечистот заполнили близлежащие парки и реки. В США хакер вывел из строя ИТ-системы планирования одного из крупнейших грузовых портов мира в г. Хьюстоне, лишив суда помощи, необходимой для безопасного выхода в море.

Рост автоматизации производства и управления ведет к повышению производительности, но всегда увеличивает риск с точки зрения защищенности. Черил Флэннери, директор по информационной безопасности компании Air Products and Chemicals считает, что использование готовых решений на базе открытых стандартов влечет за собой все новые риски.

Еще одна опасность связана с тем, что химические компании часто являются друг для друга и поставщиками, и покупателями. Существует большое число совместных предприятий. Уровень развития технологий и систем защиты разный, не все компании и заводы используют передовой опыт в данной области. Тереза Джонс, директор Dow по информационной безопасности, считает, что такие компании тем самым подвергают риску всех партнеров.

«Стратегия кибербезопасности» химической отрасли

Организация CSCSP разработала «Стратегию кибербезопасности химической отрасли». Она представляет собой инструкцию для производителей систем защиты, поставщиков и партнеров. В стратегии есть описания, которые компании могут использовать для укрепления защиты систем управления бизнесом и производством.

В качестве важнейших вопросов CSCSP обозначила контроль доступа, безопасность главных компьютеров и сетей, а также оперативный мониторинг.

Что касается контроля доступа, то рабочие группы сосредоточили внимание на Microsoft Active Directory и интеграции этого каталога с производственными и управляющими системами и средствами аутентификации устройств, идентификации пользователей и контроля за обращениями к сети. Специалисты, занятые безопасностью главных компьютеров и сетей, изучают возможности беспроводных технологий, методы повышения компьютерной безопасности, возможности динамической защиты систем, сетей хранения. Специалисты, работающие в области оперативного мониторинга, отвечают за вопросы обнаружения сетевых вторжений и использования интеллектуальных агентов.

Партнером CSCSP является Национальная лаборатория Айдахо (Idaho National Laboratory, INL), одна из национальных лабораторий министерства энергетики, занимающаяся вопросами, затрагивающими национальную безопасность в таких областях, как беспроводная связь и коммуникации, управление производственными процессами, компьютерная безопасность и др.

И тактика

Сегодня перед ИТ-компаниями стоят две глобальные задачи: разработка для химической промышленности новых систем, отвечающих стандартам защищенности, и повышение безопасности уже действующих систем. Вторая, возможно, даже сложнее. Технологии, применяемые на заводах сегодня, разрабатывались в основном в расчете на надежность и эффективность, но не на безопасность. Ранее системы не были подключены к сетям, и к ним не было удаленного доступа, что предотвращало возможное проникновение злоумышленников. К тому же системы управления представляют собой мощные машины стоимостью в несколько миллионов долларов, менять которые каждые три месяца в соответствии с новыми угрозами, не представляется возможным, следовательно, решение должно быть масштабируемым.

CSCSP выступила с несколькими инициативами. Среди них — формирование Европейской группы по сетям и их развертыванию (European Networking and Implementation Team), которая должна обмениваться информацией и знаниями по компьютерной безопасности с зарубежными химическими компаниями. В рамках другой инициативы, направленной на стимулирование обмена опытом, группа по производству и управлению (Manufacturing and Control Team) пытается объединить специалистов по безопасности предприятий и представителей ИТ-бизнеса.

Техническая группа CSCSP продолжает разрабатывать и рассылать руководства по защите беспроводных сетей, вычислительной техники и служб каталогов, аутентификации устройств и пользователей.

Безусловно, все эти инициативы и сам факт объединения химических компаний в США для решения новых ИТ-задач и проблем безопасности являются принципиально новым шагом для индустрии в целом и способны стать адекватной реакцией на угрозы нового времени. ■

В статье использованы материалы Линн Хейбер (PC WEEK/RE)