И если в Венгрии эта богатая история ярко отразилась на архитектуре (памятники Римской империи соседствуют со строениями времен турецкого ига, романскими храмами в Яке, Лебеньсентмиклоше и Паннонхалме и с неприступными крепостями средневековья в Эгере, Шюмеге и Шиклоше), то у металлургов эта борьба за контроль над предприятием становится видна на системах управления.

Простой пример: ЧТПЗ недавно купил контрольный пакет акций ПНТЗ и уже практически завершил внедрение системы «Малахит», пришедшей на смену MS Axapta, которую, в свою очередь, тоже недавно по-стахановски внедрили (подробнее см. статью «Microsoft Business Solutions-Axapta для трубников» — журнал «Металлоснабжение и сбыт», №5'2003 г., стр. 88). Как бы консультанты не ругали металлургов за лоскутную автоматизацию, как бы не пытались реализовать проект методом большого взрыва, все равно останется вагон и маленькая тележка гетерогенных систем, разнородных приложений, охватывающий частями этот сложный процесс рождения металла.

Поэтому тема «Информационная безопасность», ради которой 30 CIO металлургических предприятий России и стран СНГ собрались в рамках круглого стола в Будапеште, является сейчас одной из самых актуальных в отрасли. Не секрет, что громадные размеры предприятий, множество гетерогенных информационных систем, территориальная распределенность, постоянно растущий объем обрабатываемой информации в совокупности со сменой собственников (и, как следствие, обновлением требований к ИТ-службам) и агрессивная конкурентная среда порождают массу возможностей для хищения коммерчески важных данных, кибер-атаки, уничтожения данных и даже временного прекращения производства. Все это приводит как к прямым (например, на Магнитке весь учет погрузки-разгрузки вагонов ведется в Oracle, и за каждые десять минут простоя вагонов по причине недоступности базы данных комбинат несет ощутимые финансовые потери), так и к косвенным затратам.

Риски, связанные с тем, что под управление ИТ переходит все больше производственных и бизнес-процессов, продолжают расти. Если раньше коммерческая информация складировалась в шкафах с папками, то теперь она хранится в виде файлов, и получить ее гораздо легче (и для этого подчас можно находиться даже в другом городе). ▶

Если недавно производство контролировалось операторами, то теперь повсеместно внедряется автоматика. Не использовать преимущества, которые дают владельцам предприятий информационные технологии невозможно. Внешняя конкурентная среда ставит участников рынка в безвыходное положение — нужно выпускать более качественный металл, быстрее обрабатывать заказы, иметь свежую и точную информацию о финансовых и производственных показателях для принятия правильных тактических и стратегических решений. Поэтому у руководителей остается один путь — идентификация рисков, связанных с использованием информационных технологий, их оценка и выработка методов борьбы с ними. Но российские управленцы в большинстве своем, к сожалению, не хотят вникать в эти сложные вопросы и надеются на «авось пронесет». Надо признать, что в большинстве случаев это недоработки ИТ-директоров и CIO, которые не могут донести до руководителей правильную оценку возможных угроз. Большинство защитных мер реализуются не превентивно, а постфактум, когда данные уже потеряны/серверная комната сгорела/доменная печь встала.

Круглый стол, организованный группой компаний Оптима совместно с Microsoft, Cisco Systems, Hewlett Packard, Intel, Chek Point и другими компаниями как раз и нужен был для того, чтобы главы ИТ-подразделений обменялись ценным опытом обеспечения информационной безопасности. Малую часть идей, высказываний и реплик участников этого мероприятия, мы и публикуем.

А. Фомин

Начальник управления
ИТ ОАО «Оскольский электрометаллургический комбинат»

В настоящее время вопросы, связанные с информационной безопасностью — не просто модная тема, а неотъемлемая часть бизнеса. Эта проблема становится острее день ото дня, и закрывать на нее глаза — значит, подвергать компанию неоправданным рискам.

В 2002 г. нам приходилось сталкиваться с автоматизированными нецеленаправленными атаками, наподобие тех, которые осуществляются посредством «червей», вирусов и другого вредоносного кода. Ущерб, нанесенный «червями» не был значителен для компании. Нам удалось в короткие сроки локализовать и предотвратить нависшую угрозу. Но это заставило нас иначе посмотреть на вопросы, связанные с предотвращением подобных инцидентов. Уверен, что сегодня куда опаснее несанкционированный доступ к информационным ресурсам компании извне; вредоносный контент в виде вирусов, спама и т. д.; проникновение изнутри корпоративной сети; низкая квалификация ИТ-персонала; человеческий фактор. Предотвращение подобных инцидентов невозможно без создания комплексной системы защиты информации, призванной если и не полностью блокировать потенциальные неприятности, то хотя бы существенно снизить их число и наносимый ущерб.

В рамках данной системы на ОАО «ОЭМК» была разработана политика информационной безопасности и принят комплекс мер, обеспечивающий защиту от проникновения злоумышленников извне к информационным ресурсам комбината; вредоносного внедрения нежелательного контента — вирусов, спама; дыр и брешей в системе безопасности операционных систем платформы Windows.

Что касается второго заседания в клубе CIO металлургии, то считаю, что живое общение с коллегами по вопросам ИБ чрезвычайно полезно. Их практический опыт технических и организационных решений позволяет по-новому взглянуть на собственные решения. Что-то подкорректировать, а что-то и переделать.

Г. Глезер

Начальник Управления информационных технологий
ОСП Трубной Металлургической Компании

Самым проблемным вопросом в области информационной безопасности на металлургических предприятиях я считаю отсутствие документов и правил, регламентирующих взаимоотношения служб информационных технологий и экономической безопасности. В данный момент все вопросы решаются «игрой мускулов»: кто сильнее, тот и продвигает свое решение той или иной задачи. И не всегда эти решения оказываются правильными, часть из них принимаются только для того, чтобы показать необходимость своей службы, а ведь надо избавляться от проблем, а не выяснять взаимоотношения. Поэтому, прежде чем заниматься вопросами безопасности, нужно четко разграничить права и обязанности этих служб, чтобы они не пересекались, а, наоборот, дополняли друг друга, оберегая бизнес компании от угроз. Круглый стол был лично для меня очень полезным. Существует немного форм, в рамках которых можно узнать не только официальные сведения о проектах или компаниях, но и неофициальные. Данное мероприятие было как раз одним из таких, когда можно услышать то, чего обычно никто не говорит. А ведь опыт в нашей работе, тем более опыт наших коллег, позволяет снизить риски и предотвратить ошибки в будущем.

Л. Перепелицына

CIO Объединенной Металлургической Компании

На практике приходилось сталкиваться в той или иной мере со всеми типами инцидентов: перебои с электропитанием, скачки напряжения, необходимость защиты внешнего периметра сети от вирусов и вторжений, нарушения внутренних правил доступа и аутентификации пользователей сетевых ресурсов, неустойчивость каналов связи и проч. Для металлургических предприятий, наверное, серьезными угрозами являются недостаточная квалификация и нехватка персонала, как пользователей, так и ИТ-специалистов, а также целый ряд возможных физических угроз для оборудования, связанных с их близостью к производственным процессам.

У нас достаточно большой опыт по защите внешнего периметра сети, обнаружению и предотвращению вторжений,

ведется большая работа по защите внутренних сетевых ресурсов. Разработаны инструкции реагирования на определенный ряд инцидентов, например, отключение электропитания, нарушение целостности сервиса и т.д.

Что касается вопроса содержания выделенного менеджера по ИБ — CISO (Chief Information Security Officer), то мне кажется, что промышленные предприятия уже имеют персонал, который отвечает за информационную безопасность, но эта функция еще очень далека от стандартизации и формализации, как это имеет место в западных компаниях. Наверное, необходимо какое-то время, чтобы сложилось понимание, с чем именно надо бороться и какие средства использовать.

Заседание оказалось полезным. В представленных докладах были затронуты разные направления обеспечения информационной безопасности, все это очень живо обсуждалось. Сложилось понимание того, над чем необходимо работать, какое направление активно развивать, чтобы не отстать от коллег.

В. Хайдаров

Директор по ИТ ОАО «Первоуральский новотрубный завод»

За годы работы в металлургической отрасли мне пришлось сталкиваться и с сетевыми атаками, и с нарушением процедур эксплуатации (человеческий фактор). Несколько раз мы противостояли вирусным атакам. Нередки и случаи нарушений процедур эксплуатации, а также выхода из строя серверного и коммуникационного оборудования.

Однако наиболее серьезными угрозами в области информационной безопасности я считаю пожар в серверной, террористическую атаку и взлом информационной системы.

Для предотвращения наиболее критичных угроз на ПНТЗ проведены следующие организационные мероприятия: установка многоуровневых межсетевых экранов; комплексная антивирусная защита; система мониторинга сетей; организация VPN каналов; разделение прав доступа; сегментация и резервирование маршрутов.

Кроме того, в 2006 г. планируется ввести в эксплуатацию резервную серверную. Общение в рамках заседания считаю полезным, ряд докладов и реплик оживил эту тему и дал толчок для дальнейшего развития нашей системы безопасности.

Б. Славин

Директор по информационным технологиям ЗАО «Группа ЧТПЗ»

Наиболее частые угрозы, на мой взгляд, связаны с банальной потерей информации в результате непрофессиональных действий пользователей, сбоев в работе при отсутствии или при неправильном применении систем архивации. В той или иной мере с этим сталкиваются все: от владельцев домашних компьютеров до администраторов крупных корпоративных сетей. Как это ни парадоксально, несанкционированное проникновение из глобальной сети или физический отъем серверного оборудования, столь часто описываемые в литературе, не являются первостепенными угрозами — существующие системы защиты вполне адекватны для решения этих задач. Наиболее же значительные угрозы в области ИБ — это утечка информации, вызванная нарушениями регламентов (намеренно или случайно) со стороны сотрудников компании.

Выделенный менеджер по ИБ необходим в связи с тем, что не все вопросы защиты информации решаются техническими средствами. Наиболее важно соблюдение регламентов работы с данными, контроль за которым не может осуществлять технический специалист. Менеджер по информационной безопасности — это сотрудник, который не только владеет технической основой защиты ИБ, но и знает бизнес компании, ее «уязвимые» точки, «стоимость» используемой информации и людей, работающих с ней.

Что же касается клуба, то общение между людьми всегда приносит пользу, а встреча с коллегами — тем более, поэтому положительный эффект от участия в заседании несомненен.

Е. Селиванов

Председатель клуба CIO металлургов, директор департамента промышленности Оптима Интеграция

Тема круглого стола была выбрана в конце прошлого заседания клуба И. Суковатиным, CIO НТМК при поддержке всех остальных участников. Предпосылка была такой, что те, кто уже создал у себя информационную или ERP-систему, с одной стороны, вплотную подошли к вопросам безопасности информации, с другой — менее всего были знакомы с этой темой. Поэтому в этот раз заседание оказалось частично просветительским. Главной его целью было донести до участников общую концепцию — где скрываются главные угрозы и как их решать. После небольшого опроса коллег, мы решили сделать второе заседание выездным, дабы отвлечься от работы и окунуться в другую культуру, другую страну, и вместе с ними и другую тему — не ту, которую они курируют в своих кабинетах. Это легче сделать за рубежом, и мы выбрали Венгрию, потому как это страна не самая известная, и в то же время есть на что посмотреть. И как «фон» для неформального общения она подошла очень хорошо. По предварительным отзывам, все участники остались очень довольны проведенной в рамках заседания работой. В данный момент в клубе CIO металлургии более 50 членов, и выбранный нами формат взаимодействия между ними — партнерский и доверительный — кажется нам весьма эффективным для обмена опытом и знаниями.

Темы, которые мы собираемся осветить на следующем заседании, связаны с организацией ИТ-подразделений и MES-системами. Эти вопросы членам клуба очень близки, и они смогут как поделиться своим опытом, так и узнать о том, как эти проблемы решили коллеги по цеху. ■

Материал подготовил Д. Дехканов