Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Информационная безопасность промышленных объектов

№ 5 (214)/2011

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:

Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Шедова Е.Л.
eshedova@jet.msk.su

Верстка:
Толоконникова Е.А.

Корректура:
Андрушко О.Ю.

Над номером работали:
Воронцов А.А.
Гуляев А.В.
Панченко Ю.В.
Шопин Д.В.

Издатель:
Компания
«Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
http://www.jetinfo.ru

От редакции

Мы живем в мире, одной из главных тенденций которого является забота о безопасности. Все чаще в прессе и на ТВ проскальзывают словосочетания «информационные войны», «информационная бомба», «борьба с фродом». И мы понимаем, что невещественное стало наиболее существенным, — зачастую виртуальные процессы начинают задавать ритм современной жизни. Поэтому JI периодически возвращается к этой все более актуальной теме. В новом номере наши эксперты освещают один из многих аспектов информационной безопасности — защиту автоматизированных систем управления технологическими процессами (АСУ ТП). Реализация систем информационной безопасности АСУ ТП предстает комплексной задачей, решение которой зависит от действий компании на разных функциональных уровнях: административном, процедурном, уровне программно-технических мер. На практике — это предотвращение промышленного шпионажа, мошенничества и хищения.

Приятного чтения!

С уважением, Ваш JI

СОДЕРЖАНИЕ

Компания «Инфосистемы Джет» построила СУИБ «Эльдорадо»

Компания «Инфосистемы Джет» построила систему управления информационной безопасностью (СУИБ) «Эльдорадо», которая прошла сертификационный аудит на соответствие требованиям международного стандарта ISO 27001. Проект позволил структурировать процессы обеспечения и управления информационной безопасностью, повысить прозрачность процессов управления безопасностью для заинтересованных сторон. Результаты проделанной работы одобрены независимым органом по сертификации BSI Management Systems, компания «Эльдорадо» получила сертификат соответствия требованиям стандарта.

«Мы осознаем важность повышения зрелости процессов управления безопасностью в нашей компании, поскольку всегда несем ответственность перед акционерами, партнерами, покупателями. Именно поэтому мы приняли решение построить систему управления информационной безопасностью. И не только построить, но и провести ее сертификацию. Наличие сертификата — одно из конкурентных преимуществ, которое укрепляет доверие к нам», — подчеркивает **Соня Пурдешова, вице-президент по операционной поддержке компании «Эльдорадо»**.

Для осуществления проекта в компании «Эльдорадо» была создана рабочая группа из представителей разных подразделений компании (в нее вошли специалисты Отдела внутреннего аудита, Департамента ИТ, Службы защиты бизнеса), которая определила критичные с точки зрения ИБ бизнес-процессы центрального офиса. Целью проекта стало построение и сертификация СУИБ с интеграцией требований ISO/IEC 27001 и Федерального закона № 152-ФЗ «О персональных данных».

В августе 2010 г. после победы в тендере к проекту приступила компания «Инфосистемы Джет». Всего со стороны заказчика были задействованы более 200 человек из 20 подразделений. В область действия СУИБ включены наиболее критичные бизнес-процессы, в число которых вошла программа лояльности компании «Эльдорадо».

На первом этапе проекта специалисты компании «Инфосистемы Джет» провели обследование текущего состояния ИБ на соответствие требованиям стандарта ISO 27001 и № 152-ФЗ, определили границы распространения бизнес-процессов, включенных в область действия СУИБ. По результатам проведенного аудита был подготовлен отчет с рекомендациями по модернизации существующих средств ИБ и достижению соответствия требованиям ISO 27001, также были выделены несколько ИСПДН и составлен план мероприятий по приведению их в соответствие с требованиями № 152-ФЗ.

В рамках второго этапа специалисты компании «Инфосистемы Джет» разработали обязательные с точки зрения сертификации процессы СУИБ, провели инвентаризацию и категорирование активов, анализ и оценку рисков, разработали и внедрили требуемые стандартом ISO 27001 политики и процедуры, обучили сотрудников «Эльдорадо» новым требованиям по ИБ и провели совместно первый цикл работы процессов СУИБ. Завершающим этапом стала сертификация СУИБ компанией BSI.

«Для нас важно не просто получение сертификата, а обеспечение реальной безопасности бизнес-процессов. Мы продолжаем сотрудничество с коллегами из компании "Инфосистемы Джет": в настоящее время ведется доработка и повышение зрелости необязательных с точки зрения сертификации процессов обеспечения ИБ, планирование внедрения подобран-

ных решений для минимизации рисков. В дальнейшем мы планируем существенное расширение области действия СУИБ», — комментирует **Менеджер по ИБ компании «Эльдорадо» Константин Коротнев**.

«Решение о построении и сертификации СУИБ является серьезным шагом и вместе с тем сулит ряд выгод, как внутренних, так и внешних. Внедрение СУИБ позволит "Эльдорадо" контролировать и оценивать процессы обеспечения ИБ, даст толчок к развитию ИБ в компании и расширению СУИБ на остальные бизнес-процессы "Эльдорадо". Наличие международного сертификата будет способствовать привлечению новых партнеров и инвестиций», — отмечает **Анна Костина, руководитель группы систем менеджмента ИБ компании «Инфосистемы Джет»**.

«Реализованная система менеджмента является неотъемлемой частью системы управления любой компании, — комментирует **Сергей Романовский, директор по сертификации и партнерским программам, Британский институт стандартов (BSI Management Systems)**. — Для такой крупной ритейловой сети, как компания "Эльдорадо", сертификация СУИБ на соответствие требованиям ISO/IEC 27001 — это показатель зрелости, гарантия качественного и безопасного управления информационными активами как в самой компании, так и в интересах ее клиентов и партнеров».

Проект для ОАО «МОЭСК»

Компания «Инфосистемы Джет» развернула комплекс технических средств для работы системы мониторинга сетей центрального узла связи ОАО «МОЭСК». Компания получила возможность осуществлять круглосуточный мониторинг состояния сетей и каналов связи. Это позволит оперативно реагировать на возникающие инциденты и существенно сократить время для их устранения.

В настоящее время ОАО «МОЭСК» реализует программу расширения комплексной системы обеспечения надежности и противоаварийного управления, в рамках которой потребовалось обеспечить круглосуточный мониторинг состояния корпоративной сети передачи данных (КСПД), транспортной сети передачи данных SDH/PDH, мониторинг каналов передачи данных системы АИИСКУЭ (автоматизированная информационно-измерительная система контроля и учета электроэнергии). Для решения этой задачи была привлечена компания «Инфосистемы Джет».

Специалисты интегратора спроектировали и внедрили комплекс из нескольких взаимосвязанных подсистем: кондиционирования, управления комплексом технических средств, коллективного отображения информации и др. В ходе проекта оборудованы рабочие места дежурной смены, установлены средства коллективного отображения информации и средства звукового оповещения.

Круглосуточный мониторинг сетей связи осуществляет смена из 2 диспетчеров. На экраны их персональных компьютеров выводится информация о состоянии каналов и оборудования сетей связи. Основные схемы, необходимые для работы дежурной смены, транслируются на видеостене, состоящей из 6 LCD-панелей. Подсистема управления обеспечивает возможности регулирования громкости оповещения и режимов отображения информации на видеостене.

«Создание системы круглосуточного мониторинга сетей связи имеет для нас, безусловно, высокий приоритет, — комментирует **Сергей Николаевич Воробьев, начальник центрального узла связи ОАО "МОЭСК"**. — При помощи сетей связи осуществляется доставка технологической информации с подстанций в Центр управления сетями. От того, насколько оперативно и непрерывно она поступает, зависит надежное функционирование электрических сетей Москвы и Подмосковья, а, значит, электроснабжение населения всего региона. Специалисты компании "Инфосистемы Джет" развернули решение, полностью отвечающее требованиям надежности».

«Передовой подход руководства и ИТ-службы ОАО "МОЭСК" к реализации программы повышения надежности и противоаварийного управления демонстрирует высокий уровень социальной ответственности и реальную заботу о населении, — комментирует **Алексей Догаев, руководитель Центра сетевых решений компании "Инфосистемы Джет"**. — В данном проекте мы использовали самые современные отказоустойчивые решения, что позволило обеспечить соответствие всем требованиям заказчика».

DLP-система «Дозор-Джет» – сервис «ВКонтакте»

Компания «Инфосистемы Джет» сообщает о расширении функциональности комплекса защиты от утечек информации «Дозор-Джет». В результате проведения оперативного обновления баз сигнатур система

может контролировать загрузки и передачу документов пользователями «ВКонтакте».

Новый сервис позволяет загружать и хранить документы и изображения в самых распространенных форматах (pdf, doc, ppt, png, gif, jpg, psd и др.) на своих страницах в сети. Кроме того, сегодня пользователи могут делиться документами, прикрепляя их к записям на «стене». Как предполагают создатели «ВКонтакте», эта опция может быть также востребована бизнесом.

«Этот функционал может стать еще одним каналом утечки информации из любой компании, — комментирует **Кирилл Викторов, заместитель директора по развитию бизнеса компании «Инфосистемы Джет»**. — Мы стремимся оперативно реагировать на потребности рынка и расширять возможности нашего комплекса, который на сегодняшний день занимает лидирующие позиции на национальном рынке DLP-решений*. А так как функции контроля безопасности передаваемых по сети документов остаются самыми востребованными на рынке и неизбежно охватывают социальные сети, мы активно развиваем это направление».

* По оценкам независимого информационно-аналитического агентства AntiMalware.ru.

Взлет в облака от EMC

Корпорация EMC анонсировала решение EMC Cloud Tiering Appliance, позволяющее администраторам систем хранения проще и эффективнее работать с файловыми неструктурированными данными. Cloud Tiering Appliance — простое и экономичное решение для реализации стратегии многоуровневого хранения, при которой корпоративная информация перемещается согласно своей ценности на тот или иной уровень с соответствующей стоимостью хранения. Кроме того, интеграция Cloud Tiering Appliance с унифицированными системами хранения EMC VNX распространяет простоту, эффективность и мощные возможности систем VNX на облака. Cloud Tiering Appliance позволяет первой и единственной унифицированной системе хранения EMC VNX автоматически перемещать данные на облачный уровень хранения в соответствии с заданными правилами, при этом предлагая все функции автоматизированного хранения в рамках СХД.

Виртуализация для следующего поколения

Avaya представила новые решения для ЦОД, упрощающие проектирование, развертывание и управление дата-центрами и сетевой инфраструктурой следующего поколения. Эти предложения расширяют охват и возможности Avaya Virtual Enterprise Network Architecture (VENA) в рамках общей корпоративной стратегии по виртуализации, упрощают управление сетевой инфраструктурой, внедрение облачных приложений и улучшают надежность доставки критически важных данных.

Avaya Virtual Services Platform (VSP) 7000

Avaya VSP 7000 — это стоечный коммутатор для высокопроизводительных ЦОД с поддержкой портов 10GbE высокой плотности, который упрощает управление центром обработки данных, поиск и устранение неполадок, также повышает его экономическую эффективность.

Avaya Virtual Provisioning Service (VPS)

Avaya VPS — это решение для управления виртуализированными системами, которое обеспечивает лучшую интеграцию между виртуализацией на уровне приложений и сетевой инфраструктуры, предоставляя сетевым администраторам инструменты, необходимые для управления, диагностики неполадок и обеспечения безопасности виртуальных машин в сети.

Экспертное мнение

Александр Гуляев, начальник Отдела сетевых проектов Центра сетевых решений компании «Инфосистемы Джет»: «Коммутатор Avaya VSP 7000 является вторым устройством** в новой линейке продуктов Avaya Virtual Services Platform, предназначенных, главным образом, для построения ЛВС центров обработки данных.

При все возрастающем интересе ИТ-отрасли к виртуализации и построению «облачных» вычислительных инфраструктур крупнейшие сетевые производители предлагают в настоящее время концепции и продукты для построения сети, подходящей под эти специфические нужды. Концепция компании Avaya — Virtual Enterprise Network Architecture (VENA).

** Первый продукт — коммутатор Avaya VSP 9000.

Возможности интеграции со средствами виртуализации вычислительных ресурсов, предоставляемые Avaya Virtual Provisioning Service, обеспечивают взаимосвязь сетевых настроек с вычислительной средой при развертывании или перемещении виртуальных машин, а технология Avaya's Virtualized Services, базирующаяся на стандарте Shortest Path Bridging (IEEE 802.1aq), существенно упрощает процедуры предоставления сетевых сервисов в крупных дата-центрах.

Новый продукт Avaya (VSP 7000) отличается от изделий конкурентов поддержкой функций маршрутизации, входящей в базовый комплект устройства. Поддержка стандартов DCB позволяет говорить о возможности применения VSP 7000 при построении конвергентных сетей.

С выходом этого продукта Avaya еще раз подтвердила, что является одним из лидеров рынка сетевых решений и продолжает выпускать востребованные рынком современные решения».

Быстрее, надежнее, экономичнее

Решение EMC Proven для Citrix XenDesktop от корпорации EMC нацелено на ускорение внедрения инфраструктуры виртуальных десктопов и реализацию ее преимуществ. Это надежное, гибкое и экономически эффективное решение, построенное на основе унифицированных систем хранения EMC VNX, обеспечивает предсказуемую, высокую производительность и доступность, поддерживая до 1000 виртуальных десктопов, и легко расширяется. В данном решении используется принцип компоновки из стандартных блоков, что позволяет масштабировать его до тысяч виртуальных десктопов.

Унифицированные системы хранения EMC VNX с усовершенствованной технологией флэш-памяти предоставляют заказчикам гибкость, возможности выбора и контроля при поддержке выделения ресурсов для виртуальных десктопов Citrix XenDesktop. Заказчики могут оптимизировать свою инфраструктуру и управлять ею с гарантией того, что системы хранения EMC будут функционировать и масштабироваться в соответствии с их конкретными требованиями. Технология EMC FAST Cache позволяет получить производительность в IOPS, необходимую для соответствия требуемым для виртуальных десктопов заказчика параметрам SLA, обеспечивает максимальную производительность, легко масштабируемую без свойственного крупным дисковым массивам увеличения энергопотребления, занимаемой площади и затрат на приобретение дополнительных ресурсов.

Новый продукт в линейке HDS

Компания Hitachi Data Systems вывела на российский рынок серверы стандартной архитектуры собственной разработки, готовые платформы для приложений и облачных вычислений. HDS решила представить в России новые модели своих модульных серверов Compute Blade (ранее BladeSymphony). В Compute Blade входят 2 линейки серверов — модели 320 (шасси 6U) для малого/среднего бизнеса и 2000 (шасси 10U) для средних и крупных предприятий. Шасси содержит до десяти 2-, 4- или 6-процессорных серверов.

В старших моделях компания использовала технологии серверов UNIX и мейнфреймов. В частности, 2 или 4 сервера на процессорах Intel Xeon 5600 или 7500 в шасси можно объединить с помощью шины QPI в один 64-ядерный многопроцессорный физический сервер с памятью емкостью до 1 Тбайта и производительностью, сопоставимой с мощными системами UNIX. Кроме того, в системе, поддерживающей большинство ОС, используется аппаратная виртуализация Hitachi Virtualization Manager — для этого задействована микросхема с гипервизором, позаимствованная из мейнфреймов. Она поддерживает создание до 16 виртуальных машин на сервер (в модели 320 — до 8 ВМ) со статическим или динамическим распределением ресурсов. Программная прослойка виртуализации отсутствует, и заказчик может сэкономить на лицензиях.

Подобно другим вендорам, HDS предлагает также конвергентные платформы для ЦОД с динамической балансировкой нагрузки. Это законченное ре-

Hitachi Compute Blade 320

Hitachi Compute Blade 2000

шение на основе Microsoft Hyper-V Cloud Fast Track, объединяющее серверы и СХД Hitachi. Еще одна платформа получила название Hitachi Unified Compute Platform (UCP). Она предназначена для крупных ЦОД и облаков. Это протестированное готовое решение на базе Microsoft Hyper-V Cloud Fast Track включает серверы Compute Blade 2000, системы хранения Hitachi AMS 2500 (110 Тбайт), коммутаторы Brocade и Alaxala Networks (FC и Ethernet/iSCSI). Такая система поддерживает до 200 или до 500 ВМ (причем поддерживается живая миграция ВМ между ЦОД) и может применяться для развертывания частных облаков. Для управления служит Microsoft System Center. Осенью компания планирует выпустить аналогичную платформу для ПО VMware.

Ленточные библиотеки в новом формате

Корпорация IBM анонсировала новые предложения для ленточного хранения, расширенного архивирования и дедупликации данных, разработанные с целью помочь клиентам в эффективном хранении больших объемов данных.

В частности, корпорацией анонсирована система ленточных библиотек, которая может обеспечить хранение свыше 2,7 экзабайт данных, что почти втрое превышает объем мобильных данных, сгенерированных в США в 2010 г. (экзабайт — это 10 в 18-й степени байт или 1024 петабайт). Создание системы IBM System Storage TS3500 Tape Library стало возможным благодаря разработанной IBM новой технологии — механического приспособления для подключения до 15 ленточных библиотек, позволяющего сформировать единый «библиотечный» комплекс высокой емкости с меньшими затратами. По данным IBM, система TS3500 предлагает более высокую (на 80%) емкость хранения по сравнению с сопоставимой ленточной библиотекой Oracle, что делает ее оптимальным выбором для крупнейших мировых архивов данных.

IBM также представила накопитель на магнитной ленте IBM

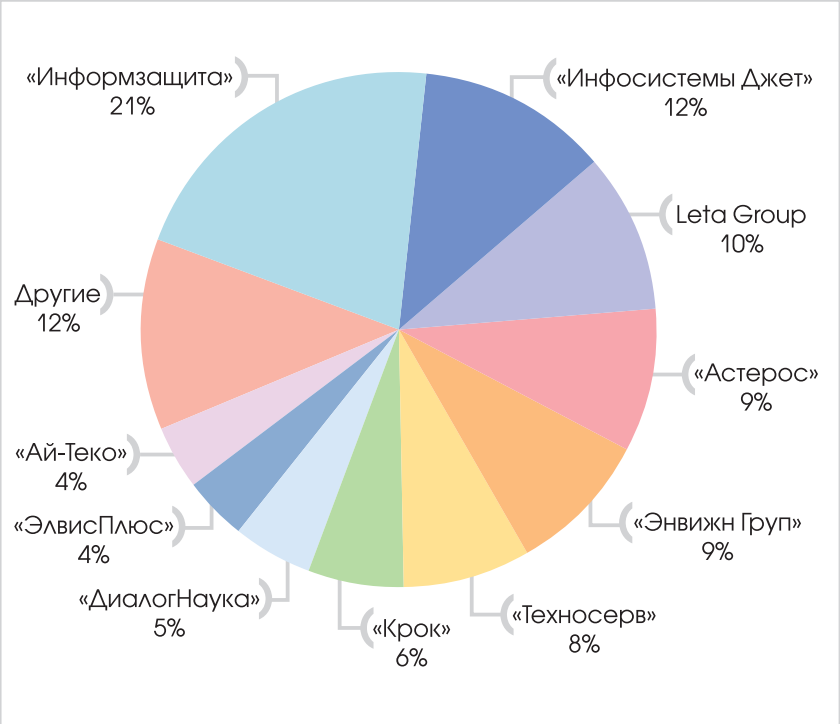
IBM System Storage TS3500 Tape Library

System Storage TS1140 Tape Drive, который способен хранить в 2 млн раз больше данных, чем первый ленточный накопитель IBM. Устройство TS1140 отличает меньшее количество и более высокая эффективность компонентов, разработанных при участии специалистов IBM Research, что позволяет обеспечивать почти 64% экономию потребляемой электроэнергии и более чем 80% прирост в производительности по сравнению с сопоставимым ленточным накопителем Oracle, утверждают в IBM.

Рейтинг системных интеграторов по ИБ в России в 2008–2011 гг.

Российский информационно-аналитический центр Anti-Malware.ru представил независимое исследование российского рынка ИБ в разрезе бизнеса системных интеграторов. Анализ охватывает 3-летний диапазон — с 2008 по 2010 г. В рейтинге представлены 10 крупнейших системных интеграторов, которые занимают лидирующие позиции в сегменте ИБ по показателю объема продаж продуктов и услуг: «Инфосистемы Джет», «Информзащита», Leta Group, «Ай-Теко», «Астерос», «ДиалогНаука», «Крок», «Техносерв», «ЭлвисПлюс», «Энвижн Груп».

Информация для анализа была получена информационно-аналитическим центром из различных источников, среди них: официальные данные интеграторов, данные из открытых источников, независимые экспертные мнения, а также оценки аналитиков Anti-Malware.ru.



Доли рынка интеграторов по направлению ИБ в 2010 г.

Исследование представляет расчеты суммарного объема рынка системной интеграции по направлению ИБ, объемы продаж и доли ключевых игроков на рынке по нескольким сегментам (поставка ПО, оборудования и услуги), также дается прогноз развития рынка на ближайший год.

В 2009 кризисном году у многих интеграторов наблюдалось падение доходов от направления ИБ. Наибольший спад отмечен у компании «ЭлвисПлюс», а также лидеров рынка — компаний «Информзащита» и «Инфосистемы Джет». В ряде случаев кризисное падение доходов связано не столько с падением объема работ, сколько с их удешевлением в силу уменьшения платежеспособности клиентов и увеличением конкуренции.

С другой стороны, целый ряд интеграторов довольно успешно пережили кризис и даже продемонстрировали хорошие темпы роста. Как правило, такая «аномалия» связана с участием интеграторов в крупных проектах государственных корпораций и ведомств, финансирование которых не было серьезно урезано в кризис. Это в полной мере касается компании «Техносерв» и группы «Астерос». Другим аспектом, кото-

Табл. 1. Изменение общих доходов системных интеграторов от продажи продуктов и услуг по направлению ИБ в 2008–2010 гг. (млн руб.)

Системный интегратор	2008 г.	2009 г.	2010 г.	Рост 2008–2009 гг., %	Рост 2008–2009 гг., %
«Информзащита»	1321	1208	2006	-9	66
«Инфосистемы Джет»	786	739	1146	-6	55
Leta Group	684	748	969	9	30
«Астерос»	492	588	894	20	52
«Энвижн Груп»	749	865	891	15	3
«Техносерв»	362	629	754	74	20
«Крок»	484	464	571	-4	23
«ДиалогНаука»	223	291	445	30	53
«ЭлвисПлюс»	387	315	350	-19	11
«Ай-Теко»	250	262	337	5	29
Другие	1445	1483	1186	3	-20
Всего	7185	7592	9549	6	26

рый позволил интеграторам показать рост во время кризиса (или уменьшить падение) были проекты, связанные с защитой персональных данных и приведением информационных систем в соответствие с ФЗ № 152 («О защите персональных данных») и отраслевыми стандартами обеспечения безопасности (PCI DSS, СТО БР ИББС и др.).

В 2010 г. все интеграторы из первого эшелона увеличили свои доходы от ИБ. Для многих из них темпы роста составили более 30%. Лидерами являются компании «Информзащита», «Инфосистемы Джет», «Астерос» и «ДиалогНаука», чьи доходы в сегменте ИБ увеличились на 50% и более. В абсолютных цифрах наибольший рост в 2010 г. показали «Информзащита», «Инфосистемы Джет» и «Астерос».

Рыночные доли в десятке лидеров можно назвать стабильными, несмотря на влияние экономического кризиса. Каких-либо существенных движений не наблюдается, за исключением уменьшения общей доли компаний, не вошедших в первый эшелон, что позволяет говорить о консолидации рынка (общей тенденции для всей индустрии ИТ в России).

Стоит отметить различия в стратегии лидеров ИБ-интеграции и, как следствие, в структуре клиентской базы. Группа компаний «Информзащита» в значительной степени ориентирована на государственные структуры. По оценке Anti-Malware.ru, их доля в портфеле заказов «Информзащиты» может превышать 70%. Этого нельзя сказать о компаниях «Инфосистемы Джет» и Leta Group, которые ориентированы в первую очередь на коммерческий сектор, и доля госзаказов в их портфеле составляет около 20 и 10% соответственно.

Если рассмотреть объем продаж лидирующей тройки системных интеграторов для негосударственных организаций, то у «Инфосистемы Джет» он составит ~917 млн руб., у «Информзащиты» — ~600 млн руб., у Leta Group — ~872 млн руб. Таким образом, тройка лидеров рынка ИБ для коммерческих организаций выглядит другим образом: «Инфосистемы Джет», Leta Group и «Информзащита».

В 2011 г. продолжится консолидация рынка ИБ-интеграции, которая была простимулирована финансовым кризисом 2009 г. Крупные игроки за счет накопленной экспертизы и подбору

Табл. 2. Доли рынка интеграторов по направлению ИБ и их изменение в 2008–2010 гг. (%)

Системный интегратор	2008 г.	2009 г.	2010 г.	Изм. доли рынка 2008–2009 гг.	Изм. доли рынка 2009–2010 гг.
«Информзащита»	18,4	15,9	21,0	-2,5	5,1
«Инфосистемы Джет»	10,9	9,7	12,0	-1,2	2,3
Leta Group	9,5	9,8	10,2	0,3	0,3
«Астерос»	6,8	7,7	9,4	0,9	1,6
«Энвижн Груп»	10,4	11,4	9,3	1,0	-2,1
«Техносерв»	5,0	8,3	7,9	3,2	-0,4
«Крок»	6,7	6,1	6,0	-0,6	-0,1
«ДиалогНаука»	3,1	3,8	4,7	0,7	0,8
«ЭлвисПлюс»	5,4	4,1	3,7	-1,2	-0,5
«Ай-Теко»	3,5	3,5	3,5	-0,03	0,1
Другие	20,1	19,5	12,4	-0,6	-7,1

более квалифицированного персонала будут успешно конкурировать с небольшими компаниями, выжимая их с рынка.

Основным фактором роста станут услуги по приведению систем защиты персональных данных в соответствие ФЗ № 152, который после ряда отсрочек должен вступить в полную силу 1 июля 2011 г. Сюда же можно отнести и проекты по выполнению требований отраслевого банковского стандарта СТО БР ИББС, а также международного стандарта PCI DSS.

По оценкам различных экспертов, с защитой персональных данных будет связано от 40 до 70% всех проектов интеграторов по направлению ИБ. В целом рост рынка ИБ-интеграции в 2011 г. может составить около 30 – 40%, т. е. в денежном выражении объем рынка может превысить 12 млрд рублей.

Подготовлено по материалам: http://www.anti-malware.ru

Системы Business Assurance как средство борьбы с фродом

Дмитрий Шопин,
руководитель направления «Fraud Management & Revenue Assurance» компании «Инфосистемы Джет»

Штирлицу нужно было мгновение, чтобы собраться с мыслями и перепроверить себя: не оставил ли он хоть каких-либо, самых, на первый взгляд, незначительных, компрометирующих данных.

Ю. Семенов, «Семнадцать мгновений весны»

Как известно, аббревиатура АСУ ТП расшифровывается как «Автоматизированная система управления технологическими процессами». Нужно подчеркнуть, что автоматизированная не означает автоматическая. Термин АСУ ТП по определению подразумевает участие человека в управлении технологическими процессами. Необходимо это как в целях сохранения человеческого контроля над процессом, так и в связи со сложностью или нецелесообразностью автоматизации отдельных операций.

Человеческий фактор

Но человеческий фактор в системе управления технологическими процессами — это не только необходимая составляющая, но и потенциальный источник проблем для предприятия. Данный высокоинтеллектуальный элемент технологической сети — человек — может не только принимать правильные решения в нужные моменты времени и выполнять операции, на которые пока не способны другие элементы АСУ ТП. Человек может также:

1) совершать мошеннические действия;
2) допускать ошибки;
3) неэффективно работать, нарушать регламенты и т. д.

Зачастую такие события наносят не меньший, а иногда и гораздо больший урон предприятию, нежели классические угрозы информационной безопасности, с которыми сталкиваются и которыми озабочены предприятия, использующие в своей деятельности АСУ ТП. Так, по оценкам аналитической компании PricewaterhouseCoopers, от 1 до 10% выручки теряют предприятия различных отраслей, использующие в своей деятельности АСУ ТП, из-за внутреннего фрода, хищений, нарушений при выполнении технологических процессов, ошибок в настройках измерительного оборудования и т. д. (см. рисунок).

Выявить факты таких нарушений и прежде всего — «фрода», как принято сейчас называть любое мошенничество, более или менее связанное с ИТ-технологиями, в технологи-

Industry	Estimated Leakage as % of Total Revenue
Airlines	2–3
Cable and Direct Broadcast Satellite	1–3
Financial Services	1–2
Healthcare	5–10
Hospitality	1–2
Telecom	2–5+
Utilities, energy	2–5
Web Services	5–10

Оценка потерь выручки в различных отраслях (по данным PwC)

ческих сетях непросто. До последнего времени поставщики такого рода систем если и предусматривали в своих решениях элементы информационной безопасности, то в основном традиционные для всех информационных систем функции — авторизация/аутентификация пользователей, закрытые протоколы обмена данными, физическая изоляция каналов данных и т. п. То есть меры, которые направлены на защиту от классических угроз ИБ — кибер-атак, вирусов, хищения данных, нарушения работоспособности систем и так далее. В то время как внутреннее мошенничество — это злонамеренные действия сотрудников, имеющих доступ к АСУ ТП на вполне законных основаниях как к инструменту для выполнения своих обязанностей. И операции, которые выполняют фродстеры, также не являются нештатными событиями с точки зрения АСУ ТП.

Приведем пример.

Типичный образец предприятия, использующего комплексную АСУ ТП в своей деятельности, — топливная компания, реализующая нефтепродукты через розничную сеть АЗК. Система управления технологическими процессами на АЗК включает различные элементы:

- топливно-раздаточные колонки с приборами учета (механическими или электронными), осуществляющие отпуск топлива;
- торговую систему, обеспечивающую выполнение расчетов при продаже нефтепродуктов и других товаров, а также управление контроллерами ТРК;
- систему бухгалтерского учета;
- датчики резервуаров (уровнемеры, плотномеры, термометры);
- прочие вспомогательные системы (например, системы процессинга топливных или скидочных карт).

Любая операция, осуществляемая на АЗК, — продажа топлива клиенту, прием топлива в резервуары — требует вовлечения в процесс нескольких элементов АСУ ТП, связующим звеном между этими элементами и является человек — оператор, кассир. Существует великое множество схем фрода, которые сотрудник АЗК может осуществить, формально не нарушая никаких требований ИБ — не взламывая пароли, не проникая в защищенные базы данных и т. п. Например, такая операция как технологический пролив предоставляет недобросовестным работникам возможность отпуска топлива «мимо кассы». Техпролив — это отбор фиксированного количества топлива из ТРК в откалиброванную мерную емкость для того, чтобы убедиться, что данная ТРК отмеряет топливо правильно (или неправильно). Помимо обязательных регулярных техпроливов, проводимых сотрудниками АЗК в соответствии с внутренними регламентами предприятия, любой покупатель также имеет право потребовать провести такую операцию при нем для того, чтобы убедиться в отсутствии недолива на данной АЗК. Естественно, что при выполнении техпролива отпуск топлива производится по нулевой стоимости (в торговой системе обычно предусмотрен специальный тип операции для этой цели), и слитое в мерник топливо должно возвращаться обратно в резервуар. Но может и не вернуться, а быть проданным клиенту без чека по стоимости ниже официальной.

Классические средства защиты АСУ ТП, как уже стало понятно, выявить такое мошенничество не помогут. Чтобы его обнаружить, необходим комплексный анализ данных о проводимых на АЗК операциях, сформированных различными элементами АСУ ТП. Например, можно проанализировать отклонения частоты проведе-

ния техпроливов на определенной АЗК от среднего значения по всей сети заправок. Или осуществить сверку реального объема топлива в резервуаре с расчетным, полученным путем суммирования всех поступлений и отпусков топлива на АЗК за период. И на многих предприятиях такие контрольные процедуры так или иначе проводятся, но обычно это эпизодические, выборочные, «ручные» сверки, инвентаризации и т. п. Обеспечить полноценное и, главное, своевременное выявление случаев хищений в таком режиме невозможно. Необходима автоматизация.

Выбор оружия

Так как для контроля мошенничества при осуществлении технологических процессов необходимо использовать данные разнородных систем и устройств, составляющих АСУ ТП предприятия, то очевидно, что такой контроль не может быть реализован средствами самой АСУ ТП. В качестве инструмента контроля должна использоваться внешняя система, способная собирать самые разнообразные данные из различных систем, обрабатывать их, преобразовывать в единый формат в режиме, максимально приближенном к реальному времени, анализировать эти данные на предмет наличия признаков фрода, ошибок персонала и т. д. Такими системами являются решения пока еще только зарождающегося класса — Business Assurance Systems (BAS).

Системы Business Assurance представляют собой программные комплексы, состоящие из 4 основных элементов:
1) ETL-модуль;
2) хранилище данных;
3) процессинговое ядро;
4) пользовательские интерфейсы.

В основе **ETL-составляющей (Extract, Transform, Load)** лежит набор интеграционных агентов — программных модулей, осуществляющих сбор и преобразование «сырых» данных, сформированных АСУ ТП предприятия. Часто сложность контроля фрода на предприятии усугубляется тем, что используются различные АСУ ТП от разных вендоров, с разной степенью автоматизированности, собственными проприетарными форматами данных и протоколами обмена. Поэтому ETL-модуль должен обеспечивать не только обработку стандартизованных файлов, таблиц баз данных и т. п., но и возможность быстрого создания новых интеграционных агентов, например, для обработки данных, сформированных уникальными «самописными» системами каждого заказчика.

Хранилище — это дисковый массив, на котором находится база данных, в которую ETL-модуль загружает собранные и преобразованные «сырые» данные. В качестве СУБД могут использоваться как собственные разработки поставщика системы Business Assurance, так и широко распространенное ПО сторонних поставщиков — Oracle, MSSQL и т. п. Конечно, предпочтительнее использовать ПО сторонних производителей, так как это снижает зависимость заказчика от вендора BAS в части поддержки и администрирования БД.

Процессинговый центр — это сердце, или, точнее, мозг Business Assurance System. В данном модуле реализуется логика всех контрольных процедур, формирование алармов в случае срабатывания правила. Эффективность системы как инструмента противодействия мошенничеству определяется в первую очередь именно функционалом процессингового модуля: система должна позволять реализовывать как можно больше различных типов контрольных процедур. Среди основных, наиболее часто используемых типов контрольных процедур можно выделить:
1) сверки агрегированных данных;
2) статистический анализ транзакций;
3) потранзакционные сверки (matching);
4) сверки баз данных;
5) hot-листы (черные и белые списки значений тех или иных параметров);
6) другие.

Кроме того, эффективная BAS также позволяет реализовывать ряд механизмов, обеспечивающих повышение надежности обнаружения фактов фрода. Например, автоматическое профилирование отдельных объектов анализа (клиентов, сотрудников, структурных подразделений, элементов технологической сети) предоставляет возможность автоматической подстройки порогов сраба-

тывания правил с учетом индивидуальных особенностей поведения каждого конкретного объекта. Функция положительной и отрицательной обратной связи позволяет аналитику, рассматривающему сформированные в BAS инциденты, «сообщать» системе о корректности определения факта фрода в каждом конкретном случае. В дальнейшем, обнаруживая аналогичные инциденты, система уже будет учитывать предыдущий опыт прежде, чем сформировать аларм.

И, наконец, пользовательские интерфейсы включают инструменты настройки и подключения новых потоков входных данных, создания и управления правилами контрольных процедур, кейс-менеджмент, отчетность и т. п. Привычным требованием уже стало наличие графического интерфейса пользователя, настраиваемость вида АРМ в зависимости от роли пользователя системы, возможность использования как «толстого», так и «тонкого клиента».

Таким образом, BAS — это новая ступень развития систем контроля технологических и бизнес-процессов, которая вобрала в себя лучшие черты таких классов решений, как Business Intelligence (BI), Business Activity Management (BAM), Fraud Management & Revenue Assurance Systems (FMRA). С последними системы Business Assurance роднят развитый функционал кейс-менеджмента и встроенные инструменты ETL для подключения потоков исходных данных из разнородных источников. От BI и BAM-систем были унаследованы гибкие возможности настройки правил анализа информации и отчетности.

Решение для различных отраслей

Одно из главных достоинств BAS — их универсальность. Такие системы (в отличие от специализированных антифрод-систем для банков или операторов связи) не являются «черными ящиками» с предустановленным набором контролей, ориентированным на одну конкретную отрасль (или даже одну конкретную область мошенничества). Системы Business Assurance позволяют предприятию любого профиля — компаниям ТЭК, промышленности, розничной торговли, страховым, банкам и т. д. — построить свой собственный набор контролей, исходя из специфики организации технологических и бизнес-процессов. Так, решение Business Assurance компании WeDo Technologies (официальным партнером которой на территории РФ и СНГ является компания «Инфосистемы Джет») было внедрено и успешно функционирует на предприятиях различных отраслей, например:

- операторы связи;
- компания по розничному сбыту газа;
- сеть автозаправок;
- энергосбытовая компания;
- почта;
- компания-оператор системы платных автодорог.

Таким образом, системы BA могут решать самый широкий круг задач — от обнаружения мошенничества до контроля уровня продаж или мониторинга процессов документооборота. Но в целом решения Business Assurance можно охарактеризовать как **универсальный инструмент автоматизации любых процедур контроля и мониторинга** на предприятиях самых разных отраслей. И чем выше уровень информатизации в компании, чем сложнее и разнороднее комплекс используемых информационных и технологических систем, тем выше потребность в решении, которое обеспечит контроль за любыми аспектами производственной и коммерческой деятельности компании.

Автоматизированные системы управления технологическими процессами. Вопросы безопасности

Алексей Воронцов,
архитектор инфраструктуры информационной безопасности компании «Инфосистемы Джет»

АСУ ТП – краткий экскурс в историю и проблематику

Проблемы, откладываемые на потом

Системы технологического управления (SCADA, Control Systems) и родственные им информационные системы (системы диспетчерского управления, противоаварийной автоматики и т. д.) прочно входят в нашу повседневную жизнь. Электричество, которое освещает нас, горючее, которым заправляются наши автомобили, системы управления дорожным трафиком и водоснабжением, «умными зданиями» и атомными электростанциями — все это примеры подобных систем. Они делают проще и понятнее процессы управления любыми сложными технологическими процессами — от передачи электроэнергии до обогащения урана. С каждым годом и каждым модернизированным производством их становится все больше и больше.

Проблематика защиты автоматизированных систем технологического управления обсуждается в специализированной прессе и в выступлениях ведущих экспертов по информационной безопасности (ИБ) достаточно давно. Однако заметного прогресса в защите систем этого класса за прошедшие 10 лет не произошло. Давайте разберемся, почему.

Наиболее распространенные угрозы безопасности в настоящий момент связаны с криминализацией киберпреступности, т. е. с получением денежной выгоды от реализации тех или иных атак на инфраструктуру. И с точки зрения потенциального внешнего нарушителя системы управления технологическими процессами малопривлекательны.

Причина этого довольно проста. Основная информация, циркулирующая в системах технологического управления, — это информация о технологических процессах (обьектах физического мира, их состоянии и динамике) и об управляющих воздействиях. Обладание этой информацией без физического доступа к обьекту управления не дает возможности совершить кражу, что резко ограничивает круг потенциальных нарушителей. Риски, связанные с мошенническими операциями в АСУ ТП, можно ограничить действиями внутреннего нарушителя — собственного персонала компании или компаний-партнеров. К примеру, для реализации схем с модификацией данных по расходу топлива на автозаправке надо иметь возможность слива и реализации этого топлива.

Среди монетизируемых внешних атак на ресурсы АСУ ТП наиболее распространенными остаются промышленный шпионаж (в тех случаях, когда данные технологического процесса представляют ценность для конкурентов) и в редких случаях — шантаж и заказные акции против конкурентов. Остальные инциденты являются немонетизируемыми: месть уволенных работников, нарушение функционирования вре-

доносным кодом, случайные взломы «подростками».

Из вышеописанного следует, что количество публично известных нарушений функционирования подобных систем крайне невелико. Кроме того, в случае серьезных нарушений функционирования процессов, контролируемых системой управления, борьба с последствиями не будет отличаться от борьбы с техногенной аварией. Системы технологического управления рассчитываются на быстрое восстановление после сбоев как в случае автоматизации, так и без нее. Да и компании, эксплуатующие системы автоматизации, все-таки уделяют внимание ИБ систем.

Однако низкая вероятность внешних атак на системы АСУ ТП не снижает актуальность угроз для систем управления. Согласно общепринятой практике актуальность угрозы пропорциональна как вероятности реализации угрозы, так и возможному ущербу от ее реализации. А если говорить о возможном ущербе от реализации угрозы, то здесь системы управления, особенно системы управления опасными производственными циклами или системы жизнеобеспечения целых городов и областей, будут вне конкуренции.

Возможный ущерб от реализации подобных атак включает, кроме финансовых потерь, репутационные риски и риски, связанные с потерей здоровья и жизни, а также риски возникновения экологических катастроф. Даже единичное нарушение функционирования систем технологического управления может привести к катастрофическим последствиям. Инциденты ИБ в системах технологического управления при их обнародовании вызывают большой общественный резонанс.

Особенности АСУ ТП как обьекта защиты

Проблемы ИБ, связанные с развитием и функционированием современных систем управления, представлены в табл. 1.

Эра после Stuxnet

Наиболее публичным инцидентом, показывающим уязвимость и возможность эксплуатации данной уязвимости сетей управления на практике, явился обнаруженный в июле 2010 г. вирусный код Stunxnet.

Табл. 1. Проблемы ИБ, связанные с развитием и функционированием современных систем управления

Большое количество «собственных» разработок программно-аппаратных решений при создании АСУ ТП	
Длительный срок эксплуатации систем	
Закрытость систем	• Разработка в расчете на выполнение в доверенной среде закрытых индустриальных сетей • Использование специализированных протоколов и средств связи, а также часто низкая скорость их работы • Отсутствие ревизий систем и кода на безопасность • Разработка без учета лучших практик разработки безопасного кода
Фиксированные конфигурации	• Отсутствие возможности своевременного обновления ПО и установки последних исправлений безопасности • Отсутствие возможности установки наложенных средств безопасности (например, антивирусного ПО) и их своевременного обновления • Использование паролей и настроек безопасности по умолчанию, включая настоятельные рекомендации производителя не менять данные значения
Производительность	• Системы технологического управления оперируют информацией в реальном времени, дополнительные проверки систем безопасности мешают процессу
Открытые стандарты	• Новое поколение систем технологического управления работает на открытых стандартах (прежде всего протоколы TCP/IP). При этом даже в случае разделения сетей (технологической, офисной, сети Интернет) связи сохраняются для технологических нужд (пересылка информации, удаленное управление)
Консервативный подход к проблемам безопасности (заключающийся, как правило, в периметровой защите и разделении сетей). Возможности управления доступом в рамках прикладных систем ограничены	
Информация (технологическая) не является основным объектом защиты систем, часто не является конфиденциальной	
Основной объект защиты – управляющее воздействие	

Данный вирус содержал целевой код, удовлетворяющий целому ряду специфических требований и реализующий полноценную атаку на системы АСУ ТП производства компании Siemens. В частности, для реализации потенциала нападения вирус требовал наличия частотных конверторов производства 2 компаний — «Vacon» (Финляндия) и «Fararo Paya» (Иран), — работающих на частотах от 807 до 1210 Гц. Наличие подобных требований позволило большинству экспертов, исследовавших данный код, сделать вывод о том, что вирус предназначался для точечной атаки вполне определенного производства или ряда производств.

Согласно анализу, проведенному специалистами компании Symantec, вредоносный код Stuxnet-а реализовывал атаку сразу на нескольких уровнях: на уровне операционных систем Windows, ПО управления АСУ ТП Siemens WinCC/PCS 7 и непосредственно контроллеров программируемой логики Siemens S7-300, обслуживающих конверторы частоты (которые, в свою очередь, управляли скоростью вращения электромоторов).

Атака вредоносного кода Stuxnet на уровне операционной системы не представляла из себя ничего особенного, за исключением эксплуатации беспрецедентно высокого количества уязвимостей нулевого дня — 4 уязвимости за раз. Как правило, вредоносный код, создаваемый киберпреступниками, не реализует больше 1—2 подобных уязвимостей за раз.

При заражении обычного компьютера вредоносный код вел себя как обычный вирус, занимаясь распространением своих копий и попытками установить связь с командным центром в случае наличия такой возможности. Однако при заражении компьютера с установленным ПО Siemens WinCC/PCS 7 вирус реализовывал следующий уровень атаки — перехват управления контроллерами программируемой логики Siemens путем внедрения в ПО управления (используя еще одну уязвимость нулевого дня — фиксированный пароль для работы ПО управления с СУБД). После чего посредством ПО управления вредоносный код реализовывал третий уровень атаки, «прошивая» в память контроллеров программируемой логики «боевую» часть своего кода.

Существует несколько вариаций вируса Stuxnet, отличающихся «боевым» наполнением. Но наибольший резонанс в сфере ИБ, дошедший до правительства ряда стран, вызвала одна из вариаций, проводившая время от времени модификацию частоты, генерируемой конверторами (и, соответственно, скорости вращения электродвигателей), сначала выше максимального предела оборотов, затем — ниже минимального, далее — устанавливая значение по умолчанию и скрывая при этом произведенные изменения от управляющего ПО. В результате выполнения данных команд происходило следующее: электродвигатели раскручивали находящуюся на них нагрузку до предельных оборотов и резко останавливались. При этом ПО управления и операторы, удаленно контролирующие работу аппаратуры, не фиксировали никаких изменений в функционировании производственного процесса.

Законодательные инициативы

Зарубежный опыт

В области защиты систем управления (Control Systems, SCADA) в настоящий момент существует целый ряд стандартов и рекомендаций. Они включают как отраслевые решения (к примеру, в США присутствует стандарт NERC для систем управления электрическими сетями, стандарт ChemITC для химической индустрии), так и рекомендации общего уровня (стандарты NIST, ISA и др.). Однако каких-либо обязательных требований к соответствию определенным критериям безопасности для коммерческих компаний не предьявляется.

Правовое поле Российской Федерации

В правовом поле Российской Федерации существует понятие ключевой системы информаци-

онной инфраструктуры (КСИИ), определяемое как информационная система, осуществляющая функции управления чувствительными для Российской Федерации процессами, нарушение ее функционирования приводит к значительным негативным последствиям. Предполагается, что система автоматизирует функционирование обьектов, включая социально значимые производства или технологические процессы, нарушение штатного режима функционирования которых приводит к чрезвычайной ситуации определенного масштаба. Среди подобных обьектов, кроме информационных систем государственных органов, присутствуют системы технологического управления в нефтегазовой отрасли, энергетике, на экологически опасных производствах, системы управления жизнеобеспечением городов и т. д. Федеральным органом исполнительной власти, уполномоченным в области обеспечения ИБ в КСИИ, Указами Президента РФ № 314, № 1085 был определен ФСТЭК России.

Табл. 2. Источники угроз для ключевых систем управления технологическими процессами и меры по их предотвращению

Угрозы
• Иностранные разведывательные и специальные службы (в случае недружественной политики иностранных государств) • Террористические организации и криминальные структуры • Отдельные посторонние лица или группы лиц с корыстными или иными интересами (хакеры, уволенные сотрудники и т. п.) • Представители иностранных организаций и конкурирующих структур, деятельность которых направлена против интересов госструктур РФ, крупных компаний, организаций и предприятий • Обслуживающий персонал ключевых систем, в обязанности которого не входят вопросы, связанные с функционированием ключевых систем
Меры
• Проведение работ по защите информации как при построении новых систем, так и при модернизации существующих • Привлечение лицензиатов ФСТЭК • Использование сертифицированных средств защиты, в том числе сертификация межсетевых экранов (класс защищенности в зависимости от уровня важности), использование иных средств защиты • Контроль отсутствия НДВ для всех применяемых средств защиты (включая встроенные в общесистемное и прикладное ПО) • Аттестация автоматизированной системы

Краткая справка по истории КСИИ в правовом поле Российской Федерации

2005 г.	Совет Безопасности РФ выпустил документ «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий», регламентирующий порядок отнесения к КСИИ.
2006 г.	Распоряжением Правительства РФ № 411 РС от 23.03.2006 г. утвержден (предварительный) перечень КСИИ .
2007 г.	ФСТЭК РФ выпустил ряд рекомендаций по обеспечению безопасности информации для КСИИ («Базовая модель угроз безопасности информации в КСИИ», «Методика определения актуальных угроз безопасности информации в КСИИ», «Общие требования по обеспечению безопасности информации в КСИИ», «Рекомендации по обеспечению безопасности информации КСИИ»), регламентирующий порядок защиты данных систем.
2009 г.	ФСТЭК РФ выпустил «Положение о реестре КСИИ» – единственный на настоящий момент документ по КСИИ, прошедший регистрацию в Минюсте РФ.

Совет Безопасности РФ не является законодательным органом и только выносит предложения для принятия решений Президентом РФ в области государственной безопасности.
Нормативного правового акта, устанавливающего обязательность выполнения требований по ОБИ в КСИИ, в настоящее время в РФ не существует.

Способы защиты систем АСУ ТП

Основные угрозы ИБ АСУ ТП

Организация обеспечения безопасности АСУ ТП — совокупность согласованных по цели, задачам, месту и времени мероприятий, направленных на ликвидацию (нейтрализацию) внутренних и внешних угроз безопасности информации в АСУ ТП и на минимизацию ущерба от возможной реализации таких угроз.

Введение термина «угроза безопасности информации» позволяет объединить в одно понятие все возможные негативные условия и факторы, влияющие прямым или опосредованным образом на безопасность информации, т. е. на ее целостность, доступность или конфиденциальность.

Среди угроз ИБ, свойственных АСУ ТП, можно выделить 3 класса: угрозы техногенного, антропогенного характера и несанкционированного доступа.

В зависимости от назначения, размещения и особенностей функционирования АСУ ТП различается состав конкретных угроз безопасности, следовательно, и содержание предъявляемых требований по ее обеспечению.

Угрозы техногенного характера — угрозы, обусловленные физическими воздействиями на компоненты АСУ ТП. Для защиты от данного класса угроз применяются меры и средства обеспечения безопасности от несанкционированного физического доступа, которые предотвращают проникновение нарушителей на охраняемую территорию и обеспечивают технический контроль доступа к ключевым компонентам АСУ ТП.

К угрозам антропогенного характера относятся угрозы преднамеренного и непреднамеренного действия людей, занятых обслуживанием АСУ ТП, в том числе ошибки персонала или ошибки в организации работ с компонентами АСУ ТП.

Угрозы несанкционированного доступа для АСУ ТП рассматриваются ввиду наличия взаимодействия ее компонент с ЛВС предприятия для передачи информации о состоянии технологической среды, а также формирования управляющих воздействий на технологические объекты. В связи с этим обязательными становятся меры по формированию выделенных технологических сетей передачи данных и использованию периметральных средств защиты (таких, как средства межсетевого экранирования, обнаружения вторжений криптографической защиты каналов связи).

Подход к реализации системы ИБ АСУ ТП

Реализация системы ИБ АСУ ТП представляет собой комплексную задачу, решение которой должно выполняться на следующих уровнях:

- административном;
- процедурном;
- уровне программно-технических мер.

Административный уровень

К административному уровню ИБ относятся действия общего характера, предпринимаемые руководством предприятия.

Главная цель мер административного уровня — формирование программы работ по обеспечению ИБ АСУ ТП с учетом общей концепции защиты АСУ ТП. Основой программы является набор документов, которые регламентируют высокоуровневый подход по обеспечению ИБ, а также описывают политику развития системы ИБ АСУ ТП.

Процедурный уровень

Процедурный уровень ИБ АСУ ТП ориентирован на человеческий фактор.

Главная цель — определение и выполнение требований по обеспечению безопасности компонентов АСУ ТП за счет формирования и принятия пакета организационной документации, направленной на создание и поддержание режима ИБ АСУ ТП.

Уровень программно-технических мер

Уровень программно-технических мер образует основной рубеж обеспечения ИБ АСУ ТП.

Рис. 1. Последствия реализации угроз ИБ АСУ ТП

Табл. 3. Меры по предотвращению ошибок сотрудников предприятия

Предотвращение ошибок персонала	Предотвращение преднамеренных («хулиганских») действий сотрудников
• формирование требований по защите информации в процессе разработки и внедрения систем АСУ ТП; • организация мониторинга действий персонала и состояния критичных компонентов АСУ ТП; • проведение обязательного повышения квалификации персонала, занятого обслуживанием АСУ ТП; • тщательный подбор и подготовка персонала для решения поставленных задач, включая личную ответственность за совершаемые действия.	• ограничение полномочий пользователей в использовании программной среды АСУ ТП рамками их должностных обязанностей; • контроль работы с переносными устройствами и устройствами ввода/вывода; • применение строгой аутентификации при доступе к программной среде АСУ ТП; • формирование строгой антивирусной политики и повсеместное применение средств антивирусной защиты; • проведение регулярных инструктажей об ответственности, возложенной на сотрудников, занятых в эксплуатации ключевых компонент АСУ ТП; • резервное копирование ключевых компонент АСУ ТП и средств, задействованных в обеспечении их безопасности; • автоматизированный мониторинг состояния защищенности ЛВС АСУ ТП.

На этом уровне реализуются следующие сервисы ИБ:

- управление доступом;
- обеспечение целостности;
- обеспечение безопасного межсетевого взаимодействия;
- антивирусная защита;
- анализ защищенности;
- обнаружение вторжений;
- управление системой ИБ (непрерывный мониторинг состояния, выявление инцидентов, реагирование).

Конкретные требования к перечисленным сервисам предъявляются на основании анализа обрабатываемой информации и оценки угроз безопасности АСУ ТП.

Управление доступом

Решение задачи разграничения доступа в АСУ ТП, как и в любых других информационных системах, выполняется как на сетевом, так и на прикладном уровне.

Управление доступом на сетевом уровне

Решение задачи управления доступом на уровне сетевого взаимодействия выполняется за счет создания демилитаризованных зон с применением средств межсетевого экранирования.

Подобные зоны представляют собой точку обмена информацией между различными ЛВС АСУ ТП с системами управления предприятием, обеспечивая баланс между доступностью и безопасностью информации.

Особенность построения таких зон при обеспечении ИБ АСУ ТП заключается в том, что корпоративная сеть рассматривается в качестве внешнего, недоверенного сегмента. Поэтому выделенная зона соответствующим образом обеспечивает как

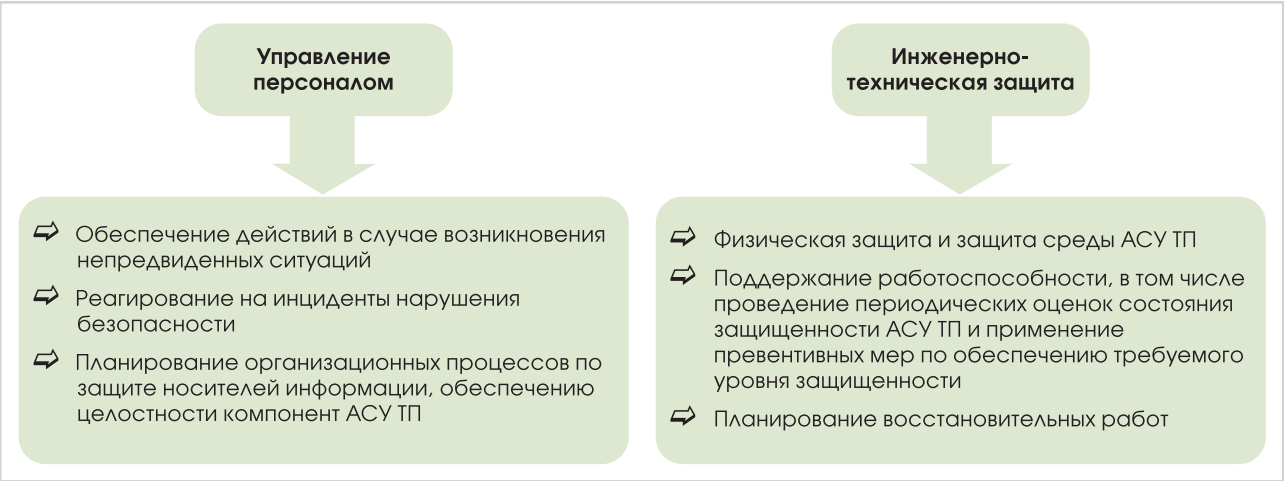


Рис. 2. Классы принимаемых на процедурном уровне мер

защиту информации, передаваемой из ЛВС АСУ ТП во внешние системы, так и блокировку внешних несанкционированных обращений к компонентам АСУ ТП.

Управление доступом на прикладном уровне

Программные средства блокирования несанкционированных действий, сигнализации и регистрации могут быть реализованы практически во всех подсистемах обеспечения безопасности АСУ ТП. Это специальные, не входящие в ядро какой-либо ОС программные и программно-аппаратные средства для защиты ОС, СУБД и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами и направлены на исключение или затруднение выполнения опасных для АСУ ТП действий пользователя или нарушителя.

Обеспечение целостности

Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций используются преимущественно на ОС и СУБД и основаны на расчете так называемых «контрольных сумм» — уведомлений о сбое в передаче пакета сообщения, в повторе не принятого пакета и т. д.

Обеспечение безопасного межсетевого взаимодействия

Использование Ethernet при создании сетей передачи данных, голоса и видео хорошо зарекомендовало себя в корпоративных сетях, где данная технология успешно применяется при объединении АРМ, серверов АСУ ТП и контроллеров. В настоящее время стало возможным использование Ethernet как единой среды пе-

редачи данных для самого нижнего уровня АСУ ТП, где размещаются контрольные датчики и исполнительные механизмы, подключаемые по протоколам Modbus/TCP, EtherNet/IP, PROFInet и др.

Для подключения устройств всех уровней АСУ ТП рекомендуется использование коммутаторов Ethernet, способных обеспечивать защиту от таких угроз, как:

- прослушивание трафика (с использованием атак переполнения таблицы MAC);
- подмена адресов участников информационного обмена (с использованием атак подделки сообщений протокола ARP, подделки IP-адресов, подделки MAC-адресов);
- несанкционированная передача трафика в другие виртуальные сегменты сети (с использованием атак прохождения VLAN);
- атака на сам коммутатор и сеть (с использованием особенностей протокола Spanning Tree, передачи анормального трафика и др.).

В некоторых случаях целесообразно использование технологии аутентификации устройств и/или пользователей при подключении к коммутируемой сети (например, по стандарту 802.1x).

Однако не следует забывать, что при осуществлении взаимодействия средств АСУ ТП через сети общего пользования (например, с ЛВС предприятия) обязательным является создание доверенного (защищенного) канала связи между взаимодействующими объектами с использованием выделенных каналов связи и криптографических средств.

Антивирусная защита

Хотя прямого подключения к сети Интернет не имеет практически ни одна АСУ ТП, в то же время использование различных технологий и протоколов в АСУ ТП создает благоприятную среду для сетевых вирусов, которые способны с большой скоростью распространяться в любых сетях передачи данных с помощью почтовых сообщений, файлов документов, исполняемых файлов, используя уязвимости в системном и прикладном программном обеспечении АСУ ТП.

Часто перед инициатором атаки не стоит каких-либо определенных целей, но даже в этом случае вторжения могут вывести компоненты АСУ ТП из строя, нарушить их связность, что приведет к лишению оператора возможности управлять ТП.

Поэтому так важно применение средств антивирусной защиты, которые обеспечивают:

- обнаружение и блокирование деструктивных вирусных воздействий на общесистемное и прикладное ПО, реализующее выполнение критически важных процессов АСУ ТП, а также на информацию, необходимую для выполнения управляемых технологических процессов;
- обнаружение и удаление неизвестных вирусов;

- обеспечение самоконтроля данного антивирусного средства при его загрузке.

Анализ защищенности
Средства анализа защищенности призваны осуществлять тестирование файловых систем, сетевых компонент и баз данных с целью сбора информации о функционировании элементов системы безопасности АСУ ТП.

Обнаружение вторжений
Одним из важнейших направлений совершенствования состояния защищенности АСУ ТП при межсетевом взаимодействии является применение систем обнаружения сетевых атак как на сетевом, так и на хостовом уровне.

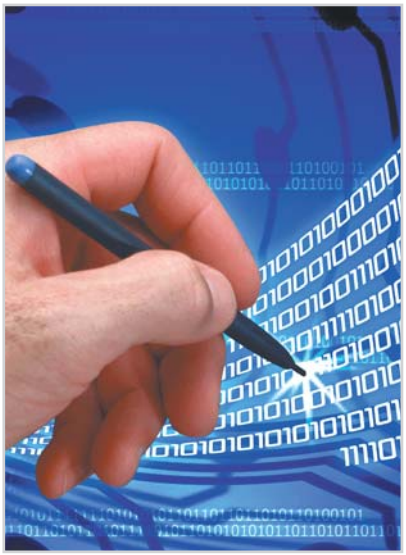
Средства обнаружения вторжений сетевого уровня
Зачастую сетевые системы обнаружения и предотвращения вторжения — единственный способ защиты для нижних уровней АСУ ТП, так как установка антивирусных программ на АРМ, контроллеры и серверы может быть затруднена или невозможна в принципе. Подобные системы могут функционировать как в режиме перехвата и блокирования нежелательных данных, так и в режиме прослушивания, сигнализируя о прохождении нежелательного трафика на консоль системы безопасности.

Средства обнаружения вторжений хостового уровня
Наиболее эффективным средством защиты операционных систем от распространения современных атак являются хостовые системы предотвращения вторжений — Host Intrusion Prevention System (HIPS), которые размещаются на всех операционных системах общего назначения, таких, как Microsoft Windows, Sun Solaris и Linux. Контролируя на системном уровне события, происходящие в операционной системе и приложениях, HIPS позволяет вовремя блокировать вредоносные воздействия самораспространяющихся червей или вирусов, ПО, имеющего несанкционированно установленные «закладки», предотвращать модификацию исполняемых файлов АСУ ТП и т. д.

Управление системой ИБ
Решение задачи управления системой ИБ АСУ ТП выполняется с использованием средств аудита и контроля защищенности, предназначенных для отслеживания состояния защищенности и оповещения администратора в случае возникновения угроз безопасности.

Принцип работы указанных средств строится на централизованном сборе данных журналирования (системные журналы и журналы аудита безопасности) и выполнении корреляции поступающих событий с целью выявления критичных для системы событий и оповещения о них администраторов безопасности.

Выделение перечня событий, подлежащих аудиту, а также настройка правил их корреляции выполняются исходя из существующих угроз.



Состав реализуемых мер по защите АСУ ТП
Состав реализуемых мер и набор используемых средств при защите АСУ ТП зависит от типа обрабатываемой в системе информации. С точки зрения информационного обеспечения АСУ ТП обеспечивает обработку следующих типов информации:

- программно-техническая (состав, структура и характеристики построения АСУ ТП, ее системы обеспечения ИБ, программы системного и прикладного характера, параметры настроек программно-аппаратных средств, в том числе средств защиты информации);
- управляющая (обеспечивает управление потенциально опасными объектами или процессами);
- контрольно-измерительная (отражает состояние потенциально опасных объектов или процессов, на ее основе принимаются решения по управлению такими объектами или процессами);
- информация с ограниченным доступом (в соответствии с действующими нормативными документами представляет собой тот или иной вид тайны).

С целью дифференцирования требований по обеспечению ИБ проводится разбиение АСУ ТП на следующие подсистемы :

- подсистемы, в которых обрабатывается информация ограниченного доступа (не подлежащая свободному распространению);
- подсистемы, в которых обрабатывается общедоступная информация;

- подсистемы, которые осуществляют управление критически важным объектом.

Возможное будущее – в центре информационной войны

Понятие «кибервойна»

В связи с проблемой защиты систем АСУ ТП на инфраструктурных обьектах и опасных производствах все чаще в СМИ и политических прениях упоминается новый термин — «кибервойна» (cyberwarfare).

В целом кибервойна определяется как один из видов информационной войны (включающий такие методы ведения военных действий, как намеренная дезинформация), подразумевающий нанесение урона противнику посредством направленного информационного воздействия на телекоммуникационную инфраструктуру и автоматизированные системы, в том числе находящиеся в частном пользовании. Среди вероятных целей при ведении кибервойны, в частности, называются сети управления электропитанием.

В настоящее время лишь несколько стран открыто заявляют о наличии специализированных армейских подразделений, предназначенных для проведения направленных атак на IT-инфраструктуру обьектов противника. При этом только США открыто предоставляет информацию об их организации, официально включая данные подразделения в структуру армейского командования. Согласно текущей схеме, данные подразделения включают:

- подразделение статегического командования USCYBERCOM;

- подразделение американской армии ARCYBER (Army Cyber Command) и подчиненные структуры;
- подразделения десантных войск Marrine Corps Cyberspace Command;
- подразделения флота Navy Cyber Command;
- подразделения ВВС 24AF.

При этом задачами армейских подразделений США являются:

- защита компьютерных сетей департамента безопасности;
- обеспечение потенциала ведения полномасштабных военных действий, включая как защиту, так и нападение в пределах информационного поля.

Возможные последствия для частных организаций

В реалиях наличия понятия «кибервойна» следует говорить о следующих практических аспектах, связанных с защитой систем управления стратегически важной инфраструктурой:

- возможное наличие угроз, связанных с нарушителем, обладающим высоким потенциалом нападения (финансовые и технические ресурсы, доступ к Ноу-хау поставщиков систем АСУ ТП и средств защиты информации).
- в случае затруднений внешнеполитической ситуации возможно резкое увеличение вероятности угроз, связанных с частными гражданами стран-участниц конфликта.

Пока наличие угроз со стороны армейских и разведывательных подразделений иных стран выглядит фантастикой. Однако угрозы ИБ имеют особенность только увеличиваться в количестве с течением времени. Системы АСУ ТП рассчитываются на длительный период эксплуатации, соответственно, должны рассчитываться и системы обеспечения ИБ. Обязательное условие при этом — возможность модификации и прицела на будущее, каким бы неприятным оно не оказалось.

Заключение

Автоматизированные и автоматические системы технологического управления прочно интегрированы в наш социум. Их функционирование может затрагивать не только интересы отдельных промышленных компаний — эксплуатантов подобных систем, но иногда — всех и каждого. Вероятность атаки на подобные системы ниже, чем на многие другие, но ответственность, связанная с их защитой, в некоторых случаях несоизмеримо выше. Это в полной мере относится к значимым и опасным областям промышленности и жизнеобеспечения городов. О проблематике защиты подобных систем управления не стоит забывать, перенося планы на очередной год.

Аутсорсинг Информационных Систем. Муки выбора

Юрий Панченко,
заместитель директора Сервисного центра по организации производства компании «Инфосистемы Джет»

В средствах массовой информации постоянно обсуждается тема аутсорсинга. Сегодня, пожалуй, каждый ИТ-руководитель задумывается над тем, а нужен ли аутсорсинг его компании. В то время как, по большому счету, практически каждая компания его уже использует, не всегда об этом подозревая. Например, аренда каналов связи. Или техническая поддержка. Или внедрение какого-либо проекта автоматизации.

Над аутсорсингом информационных систем или технической платформы ИТ некоторые из ИТ-руководителей не задумываются. И продолжают обслуживать свои системы большим штатом собственных инженеров.

Кроме того, время от времени практически любая компания сталкивается с проблемами информационных систем, обслуживающих их основную деятельность. Это могут быть и технические проблемы, и процессные, и финансовые, и человеческий фактор. И чем больше бизнес-процессов в компании автоматизировано, чем больше приобретено технических средств, тем больше бизнес компании попадает в зависимость от внутренней ИТ-службы. С одной стороны, это подразделение воспринимается как обслуживающее, и другие смотрят на «айтишников» (включая ИТ-директора), как на вспомогательную и не самую важную службу, «бесполезно тратящую деньги». С другой стороны, зависимость от службы ИТ настолько велика, что остановка работы основной прикладной системы способна практически полностью парализовать бизнес компании.

Конечно, в каждом конкретном случае решение находится. Беда в том, что время, за которое это решение будет принято, и вкладываемые в его реализацию финансовые средства спрогнозировать практически невозможно. А по всем странным законам жизни система «слетит» именно в момент «горячего сезона»: получения миллионного контракта или срочного письма из правительства, горящего выгодного тендера и т. п. Безусловно, «разбор полетов» будет, и инженер-стрелочник или даже CIO — «начальник вокзала» — будут строго наказаны или вообще уволены. Но ведь время не вернуть. И потерянной удачи тоже.

А выход есть! Это передача информационных систем на полный аутсорсинг. Сравните обязательства между конкретными сотрудниками и компанией, если они есть, и компанией и компанией. Какие надежнее? Бизнес компании и зарабатываемая годами репутация на рынке стоят очень дорого. А это значит, что аутсорсер внимательно «возьмет систему на об-

служивание», предварительно выявит и опишет большинство значимых рисков, предложив проактивные организационные и технические меры для снижения вероятности их наступления, обеспечит устранение зависимости от персоналий. Список достоинств можно продолжать. Однако потенциально потребителя аутсорсинга интересует «а что в пассиве?». Ответ на такого рода вопрос в общем-то банален. И сам потребитель может на него ответить, после того, как ответит на вопрос «А что важно/не важно для меня?». При этом выбор ответов ограничен — «Деньги? Сроки? Качество?». И выбрать можно только 2. Причем качество фактически уже выбрано, если вы, конечно, обратились к хорошему подрядчику.

Важны сроки и качество — будь готов платить больше. Важны стоимость и качество — будут делать не быстро, зато не дорого. Но главный выигрыш — в значительном снижении вероятности наступления значимых рисков при эксплуатации информационных систем. Внутренняя служба может оставить проблему «на потом», внешняя — никогда! И будет решать ее так, чтобы она впоследствии не повторилась.

Когда обсуждаешь с ИТ-директорами вопрос возможного аутсорсинга, в воздухе всегда витают 2 темы:

«Если я найму свой персонал, я смогу загрузить его дополнительными задачами. Вы же сделаете только то, что определено договором». Ответ прост: «Да, сможете, только скорее всего не стабильно, да и не всех. Не все задачи такого рода реально нужны бизнесу. А те задачи, которые нужны, проще и быстрее решить через аутсорсера, заплатив немного дополнительных денег. И главное — не нужно удерживать свой персонал, учить его, мотивировать, избавляться от «балласта» и т. п.».

Второй вопрос тоже типичен: *«Какой же я ИТ-директор, если у меня вместо 100 инженеров несколько менеджеров, управляющих договорами аутсорсинга?»* Тренд настоящего времени таков, что ИТ-директор начинает управлять не инженерным персоналом, а качеством и финансами. Фактически он становится вровень с финансовым директором или директором по качеству. Да, правильный выбор аутсорсера остается на совести ИТ-директора. Но теперь у него не 100 инженеров, а договор с ИТ-интегратором, в штате которого тысячи инженеров высокой квалификации и разных направлений. И эти ресурсы появятся практически сразу при необходимости, потому что компания-аутсорсер несет обязательства по качеству в виде конкретного соглашения об уровне обслуживания и финансовую ответственность в виде штрафных санкций по исполнению договора. Собственные ресурсы, если такая задача есть, можно ориентировать на более интересные бизнес-задачи.

Мы не затронули еще один немаловажный вопрос — стоимость. Мы рассчитываем ее на основании состава и сложности информационной системы заказчика, а также с учетом гарантии доступности для заказчика. Возможно, что стоимость покажется выше при прямом сравнении с зарплатой существующего персонала. Однако вам не стоит забывать и косвенные выплаты — налоги, премии, социальный пакет, затраты на рабочие места, работу руководителей, кадровой и хозяйственной служб, службы персонала и других подразделений, нагрузка на которые снизится.

Если у вас остались сомнения, спросите у наших специалистов. Мы поможем вам определиться с правильным выбором. Хотите посмотреть, как это работает? Приезжайте в наш Центр удаленного мониторинга, где вы сможете увидеть работу инженеров аутсорсинга.

Построение комплексного центра обработки данных для компании «Мосэнергосбыт»

О заказчике

ОАО «Мосэнергосбыт» — крупнейшая энергосбытовая компания страны, реализующая 6,9% вырабатываемой в России электрической энергии и поставляющая электрическую энергию более чем 180 тыс. предприятий и почти 6 млн бытовых потребителей г. Москвы и Московской области, которых обслуживают более 100 офисов продаж электрической энергии. ОАО «Мосэнергосбыт» действует на территории г. Москвы и Московской области. Общая площадь обслуживаемой территории — 47 тыс. кв. километров. 1 сентября 2006 г. ОАО «Мосэнергосбыт» получило статус «Гарантирующий поставщик» Московского региона. В конце 2006 г. акции компании прошли процедуру листинга и включены в котировальный список «Б» Московской межбанковской валютной биржи.

Задачи

В рамках экономической стратегии, разработанной компанией «Мосэнергосбыт», был запланирован запуск новых бизнес-приложений. Для реализации этих целей потребовалось и было приобретено дополнительное, более современное оборудование. Серверные помещения, в которых оборудование размещалось ранее, не отвечали заявленным стандартам эксплуатации. К тому же комнаты находились на удалении друг от друга, что затрудняло обслуживание систем. Возник вопрос о создании объединенного специализированного центра обработки данных. Рассмотрев возможные варианты, руководство компании «Мосэнергосбыт» приняло решение построить ЦОД уровня Tier II с применением «зеленых» решений, с соответствующей степенью надежности и масштабируемости.

В качестве исполнителя проекта была выбрана компания «Инфосистемы Джет», специалисты которой обладают практическим опытом и необходимыми компетенциями в данной области.

Решение

Над проектом трудилась целая команда специалистов самого разного профиля: инженеры, конструкторы, проектировщики, строители. При подго-

«Одним из основных требований к рабочей площади под проект была вместительность. Единственным подходящим по размеру оказалось складское помещение, расположенное на территории заказчика в центральном офисе, – рассказывает **Сергей Андронов, директор Департамента проектирования, внедрения и сопровождения компании "Инфосистемы Джет"**. – Естественно, никаких специальных условий на данной площади не было. Поэтому мы разработали комплексное решение по созданию нового ЦОДа "с нуля", начиная с планировки и ремонта помещения».

«Несмотря на то, что фрикулинг – это очень выгодная и практичная технология, пока ей пользуются лишь немногие, – рассказывает **Сергей Андронов**. – В отличие от других систем охлаждения – холодильных машин (чиллеров), вентиляторов-доводчиков (фанкойлов) – охлаждение достигается за счет низкой (от +5 °С) температуры наружного воздуха. Таким образом, устанавливая своим клиентам фрикулинг, мы решаем ряд очень важных проблем: снижение затрат на энергосбережение, снижение уровня шума, сокращение времени работы дополнительных холодильных компрессоров, если они есть».

товке помещения был проведен комплекс работ, связанный с усилением перекрытий. Возведенные конструкции позволили выделить ряд зон: гермозону, операторскую часть, помещения под ИБП, зону размещения кондиционеров, внешних блоков и так далее.

Некоторые виды работ велись в офисном здании компании, что накладывало ряд существенных ограничений. В числе обязательных условий заказчиком было названо соблюдение тишины и создание минимальных помех в работе сотрудников. Поэтому каждый этап выполнения проекта был четко спланирован и организован, а часть работ проводилась в ночное время и выходные дни.

Для реализации системы кондиционирования специалисты компании «Инфосистемы Джет» применили 2 высокоэффективных технологии — «фрикулинг» и зонированную воздухораздачу кондиционирования. В первом случае для охлаждения центра обработки данных используется температура окружающей среды, а во втором задействован механизм зонированного распределения воздуха — «холодные» и «теплые коридоры». Благодаря этому не происходит смешение воздуха, минимизируется тепловыделение, а значит, уменьшается нагрузка на кондиционеры, существенно снижаются расходы на систему кондиционирования. С учетом использования технологии фрикулинга энергопотребление становится еще эффективней.

В нашем климате такой принцип может работать до 9 месяцев в году — именно на этот период сохраняется прохладная погода. По оценкам специалистов компании «Инфосистемы Джет», отсутствие искусственной системы охлаждения существенно сокращает энергозатраты, что позволит владельцам современного ЦОДа в среднем за год экономить более 1 000 000 рублей.

Использованное в проекте оборудование разработано разными вендорами и имеет разные габариты, поэтому разместить его оптимальным образом было непросто. С целью оптимизации пространства все техническое оснащение было классифицировано по типам, что позволило установить стойки в заранее предустановленные площади — типоместа. Организация типомест заключается в создании под фальшполом специальной кабельной инфраструктуры, достаточной для размещения оборудования любого типа в рамках заявленного списка.

При построении ЦОДа был применен ряд методик для распределения нагрузки за счет использования специальных рам под тяжелыми объектами, например, под элементами питания. Также была спроектирована и реализована система вентиляции, которая использовалась в помещении для создания избыточного давления и предотвращения проникновения мелкодисперсной пыли.

Отдельного внимания заслуживает конфигурация системы кондиционирования, которая была построена на базе конструктивных элементов разных производителей. Выбирались лучшие компоненты в соотношении цена/качество, и, соответственно, они были заложены в решение. Такой подход позволил сэкономить на компонентах, которые не оказывают критического влияния на качество функционирования

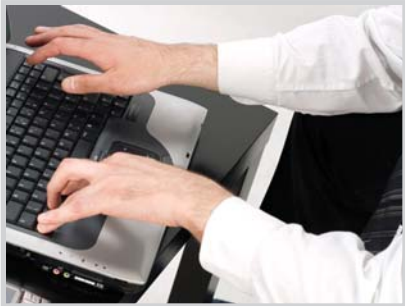
«В ближайшем будущем мы хотим полностью отказаться от серверных помещений в удаленных офисах и разместить все данные на центральном ЦОД, тем более что мощности позволяют, – делится планами **Василий Цветков, начальник управления сопровождения инфраструктуры ОАО "Мосэнергосбыт"**. – Для нас гораздо удобнее, выгоднее и безопаснее обслуживать оборудование, развернутое на одной площадке. К тому же совсем скоро мы будем внедрять биллинговую систему, которая прекрасно разместится на нашем новом ЦОДе».

системы, например, на кожухах, без потерь в надежности.

Средства кондиционирования, электропитания и другие инженерные системы ЦОД реализованы в проекте с учетом основных положений международных (TIA-942) и отечественных (ГОСТ 34, СНиП 512-78) стандартов. Обновленное помещение отвечает требованиям уровня Tier II общепринятой классификации, разработанной организацией Uptime Institute.

Результат

На сегодняшний день в Москве и России существует достаточно большое количество ЦОДов. Очень много центров обработки данных находятся на этапе строительства. Однако «зеленые» технологии



энергосбережения применены лишь в единичных случаях.

По итогам проекта компания «Мосэнергосбыт» получила усовершенствованную систему хранения и обработки данных уровня Tier II, созданную в соответствии с лучшими мировыми практиками. Все оборудование расположено на одной площадке, надежно защищенной от перегрева и негативного влияния внешней среды. Также благодаря внедрению современной системы охлаждения (фрикулинга) значительно снижены энергозатраты.

Благодаря оптимально просчитанной инженерной инфраструктуре новый ЦОД вмещает 22 высокозагруженные стойки и имеет возможность установки негабаритного оборудования класса Hi-end. При этом он расходует всего 60% от собственного резерва в текущей конфигурации и имеет широкие возможности для дальнейшего масштабирования. По расчетам специалистов компании «Инфосистемы Джет», планомерно наращивать комплекс, не изменяя его структуры, можно будет в течение последующих 5—7 лет. В случае, если будет происходить частичная замена серверного оборудования или его оптимизация, сроки увеличатся до 10 лет.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Главный редактор: Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01 факс (495) 411 76 02
e-mail: JetInfo@jet.msk.su *http://www.jetinfo.ru*

Подписной индекс по каталогу Роспечати **32555**