4. Хаммер М., Чампи Дж. Реинжиниринг корпорации: Манифест революции в бизнесе. Пер. с англ. – СПб.: Издательство С.-Петербургского университета, 1997. 332с.

Ю.Ю. Палунина, А.А. Волков, Н.Ф.Бахарева

АВТОМАТИЗАЦИЯ КОМПЛЕКСНОГО УПРАВЛЕНИЯ ТЕКУЩИМ СОСТОЯНИЕМ ЗАЩИЩЕННОСТИ ПРЕДПРИЯТИЯ

(Поволжский государственный университет телекоммуникаций и информатики)

Одной из наиболее актуальных задач в настоящее время является задача обеспечения безопасности функционирования предприятия в плане снижения рисков потери, искажения и разглашения информации, подлежащей защите. Развитие информационной безопасности следует за развитием информационных технологий и является его неотъемлемой составляющей.

Поскольку информационная безопасность не является статической характеристикой, необходимо решать задачу динамического управления безопасностью предприятия. Поддержание в актуальном состоянии данных о существующих информационных активах, поиск и исправление уязвимостей в системе защиты и проверка соответствия требованиям законодательства и международным стандартам в современных информационных системах является нетривиальной задачей. Постоянно изменяющиеся угрозы еще больше усложняют этот процесс.

Каждое предприятие решает проблему самостоятельно, путем принятия соответствующих организационно-технических и правовых мер, подчас требующих привлечения значительных временных и человеческих ресурсов.

Обязательные процедуры безопасности: инвентаризация имеющегося на предприятии аппаратного и программного обеспечения, контроль обновлений используемого программного обеспечения, поиск и устранение неисправностей оборудования, оценка текущего уровня защищенности, управление уязвимостями и контроль соответствия системы защиты требованиям законодательства, могут проводиться нерегулярно и с большими временными промежутками, а на некоторых предприятиях не проводятся вообще. Это приводит к тому, что информация о состоянии информационной системы предприятия теряет актуальность и ситуация выходит из-под контроля, что может значительно упростить задачу по преодолению барьеров систем защиты.

Для решения данной проблемы необходимо применение комплексного подхода и использование интеллектуальных средств автоматизации процесса управления безопасностью, которые позволят добиться следующих результатов:

– уменьшения затрачиваемого времени на проведение технического аудита предприятия;

– уменьшения вовлеченности специалистов по информационной безопасности в процесс технического аудита, что позволит им сосредоточить больше усилий не на сборе, а на анализе полученной информации о системе.

Такие средства автоматизации должны обладать свойством интеллектуальности. Это свойство крайне эффективно при устранении уязвимостей в информационной системе предприятия. Оно позволяет таким системам не только обнаруживать уязвимости, но и рекомендовать пути их устранения.

Подобные решения стали появляться на рынке информационной безопасности. Примером служит система MaxPatrol – комплексное автоматизированное программное решение, разработанное компанией Positive Technologies, которое позволяет контролировать уровень защищенности информационных ресурсов всего предприятия. Но, как и любое решение подобного масштаба, оно обладает рядом сложностей:

– высокая стоимость решения делает его недоступным для малых и средних предприятий;
– данное решение является программным, что вызывает некоторые психологические трудности у руководства предприятия при необходимости оплачивать столь дорогостоящее программное решение;
– отсутствие возможности самостоятельной установки и настройки данного решения, без привлечения специально обученных специалистов, что увеличивает стоимость реализации данного решения;
– отсутствие на многих предприятиях высококлассных специалистов по информационной безопасности, обладающих таким комплексом знаний по администрированию сетей, работе с базами данных, организационно-правовыми аспектами безопасности, которые требуются для работы с подобными системами.

Существует решение, в котором нет вышеуказанных недостатков, сканер безопасности XSpider, это упрощенный вариант тяжелой и полновесной системы MaxPatrol. XSpider характеризуется разумной ценой и стоимостью владения, но функционал достаточно ограничен и решает значительно меньше требуемых задач. На рынке информационной безопасности складывается ситуация, когда есть решения для крупного сектора заказчиков и решение с явно ограниченным функционалом, но доступное для малого и среднего сектора.

В связи с указанными особенностями имеющихся в настоящее время систем автоматизации процесса управления безопасностью, очевидна потребность в разработке интеллектуальных автоматизированных систем комплексного управления состоянием защищенности предприятия с оптимальным набором функций и доступных по цене, удовлетворяющих потребностям не только крупных, но также средних и малых предприятий.