ЛИТЕРАТУРА

1. М.Хаммер, Д. Чампи. Реинжиниринг корпорации. Манифест революции в бизнесе – М.: Манн, Иванов и Фербер, 2007 г. – 288 с.
2. Строилова Э.В. Проектный менеджмент и реинжиниринг // Фундаментальные исследования. – 2013. – № 4 (часть 5). – стр. 1206-1210; URL: www.rae.ru/fs/?section=content&op=show_article&article_id=10000602 (дата обращения: 22.03.2014).
3. Ермоленко А.Г. Реинжиниринг бизнес-процессов как радикальный метод корпоративного управления предприятиями // Вестник ТГУ. – 2013 – Выпуск 2. – стр. 167-173.
4. Мельцас Е. Бенчмаркинг и реинжиниринг бизнес-процессов // Финансовая жизнь. – 2012. – № 3. – стр. 44-46; URL: http://www.flife-online.ru/upload/iblock/7b9/7b9d48a3100525e4174911309ec138c4.pdf (дата обращения: 22.03.2014)

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УПРАВЛЕНИИ ОРГАНИЗАЦИЕЙ

А.В. Шадт, Л.И.Иванкина
(г. Томск, Томский политехнический университет)

PROBLEMS OF INFORMATION SAFETY IN ORGANIZATION MANAGEMENT

A.V. Shadt, L.I. Ivankina
(c.Tomsk, Tomsk Polytechnic University)

Demonstrates the nature and specificity of information security, defines the concept, issues of information security.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин «информационная безопасность» используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность – многогранная, многомерная область деятельности, в которой успех может принести только системный, комплексный подход. Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. Управление информационной безопасностью – это управление людьми, рисками, ресурсами, средствами защиты и т.п.

При анализе проблематики, связанной с информационной безопасностью в управлении, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий в управлении – области, развивающейся беспрецедентно высокими темпами. Здесь важны не

столько отдельные решения (законы, учебные курсы, программно-технические изделия), сколько механизмы генерации новых решений государственными и муниципальными органами, позволяющие жить в темпе технического прогресса.

Стратегические цели информационных технологий – обеспечить развитие бизнеса, его управляемость и качество, конкурентоспособность, снижение стоимости выполнения бизнес-процессов. Информационные технологии организации служат стратегическим целям бизнеса, используются для управления деятельностью структур и объектов, финансовыми, информационными, материальными потоками, рабочими местами и коллективами людей. Спрос на информацию и информационные услуги в сфере экономики и управления обеспечивает развитие, распространение и все более эффективное использование информационных технологий (ИТ). Создание современных технологий немыслимо без использования разнообразных технических средств и в первую очередь компьютеров.

Многочисленные публикации последних лет показывают, что злоупотребления информацией, циркулирующей в информационной системе (ИС) или передаваемой по каналам связи, совершенствовались, не менее интенсивно, чем меры защиты от них. В настоящее время для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мер (использование специальных технических и программных средств, организационных мероприятий, нормативно-правовых актов, морально- этических мер противодействия и т.д.). Комплексный характер защиты проистекает из комплексных действий злоумышленников, стремящихся любыми средствами добыть важную для них информацию.

Сегодня можно утверждать, что рождается новая современная технология – технология защиты информации в компьютерных информационных системах и в сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз ИС и ИТ.

Создание системы защиты информации в корпоративной сети ИС порождает целый комплекс проблем. В комплексе корпоративная система защиты информации должна решать следующие задачи:

1) обеспечение конфиденциальности информации;

2) защита от искажения;

3) сегментирование (разделение на части) и обеспечение индивидуальности политики безопасности для различных сегментов системы;

4) аутентификация пользователей – процесс достоверной идентификации отождествления пользователя, процесса или устройства, логических и физических объектов сети для различных уровней сетевого управления;

5) протоколирование событий, дистанционный аудит, защита регистрационных протоколов и др.

Построение системы информационной безопасности сети в организации основывается на семиуровневой модели декомпозиции системного управления OSI/ISO. Согласно стандартам Международной организации по стандартизации (ISO), разрабатывающей стандарты взаимодействия открытых систем (OSI), выделяют семь уровней сетевой архитектуры, которая обеспечивает передачу и обработку информации в сети. Такая

семиуровневая модель обеспечивает полный набор функций, реализуемый открытой по стандартам ISO архитектурой сети. Семь уровней сетевого управления включают: физический, канальный, сетевой, транспортный, сеансовый, представительский, прикладной уровни.

На физическом уровне, представляющем среду распространения данных (кабель, оптоволокно, радиоканал, каналообразующее оборудование), применяют обычно средства шифрования или сокрытия сигнала. Они малоприменимы в коммерческих открытых сетях, так как есть более надежное шифрование.

На канальном уровне, ответственном за организацию взаимодействия двух смежных узлов (двухточечные звенья), могут быть использованы средства шифрования и достоверной идентификации пользователя. Однако использование и тех и других средств на этом уровне может оказаться избыточным. Необязательно производить (пере-)шифрование на каждом двухточечном звене между двумя узлами.

Сетевой уровень решает задачи распространения и маршрутизации пакетов информации по сети в целом. Этот уровень критичен в отношении реализации средств криптозащиты. Понятие «пакета» существует на этом уровне.

На более высоких уровнях есть понятие «сообщения». Сообщение может содержать контекст или формироваться на прикладном уровне, защита которого затруднена с точки зрения управления сетью.

Сетевой уровень может быть базовым для реализации средств защиты этого и нижележащих уровней управления. К ним относятся: транспортный (управляет передачей информации), сеансовый (обеспечивает синхронизацию диалога), уровень представлений (определяет единый способ представления информации, понятный пользователям и компьютерам), прикладной (обеспечивает разные формы взаимодействия прикладных процессов).

Однако защита на сетевом уровне недостаточна, так как неизвестно, что за информация упакована в пакеты, не видно пользователей и процессов, порождающих эту информацию. Ряд задач защиты информации лежит выше сетевого уровня: шифрование и обеспечение достоверности опознавания (аутентификация) сообщений, а не пакетов, обработка протокола с обеспечением его защиты, контроль доступа и соблюдения полномочий, протоколирование событий.

Управление уровнями выше сетевого сложное и разнообразное и поэтому рассмотреть возможные стратегии защиты информации для них трудно. Решение может быть найдено на пути поиска единой технологической базы, обладающей максимальной общностью и распространенностью, для защиты информации и сетевой интеграции распределенных пользовательских приложений.

Недооценка проблем, связанных с безопасностью информации в управлении, организацией приводит к огромному ущербу. Рост компьютерной преступности вынуждает заботиться об информационной безопасности.

Эксплуатация в российской практике однотипных массовых программно-технических средств (например, IBM-совместимые персональные компьютеры, операционные системы Windows, Unix, MS DOS, Netware и т.д.) создает в определенной мере условия для злоумышленников.

Стратегия построения системы защиты информации должна опираться на комплексные решения, интеграцию информационных технологий и систем защиты, использование передовых методик и средств, универсальные технологии защиты информации промышленного типа.

Таким образом, управление информационной безопасностью является неотъемлемым элементом управления и позволяет коллективно использовать конфиденциальную информацию, обеспечивая при этом ее защиту, а так же защиту вычислительных ресурсов

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ УПРАВЛЕНИЯ

О.С. Швабауэр, Л.И.Иванкина
(г. Томск, Томский политехнический университет)

INFORMATION TECHNOLOGY IN MANAGEMENT

O.S. Shvabauer, L.I. Ivankina
(c.Tomsk, Tomsk Polytechnic University)

The urgency of the application of information technologies in the field of management in terms of becoming a transnational economic space. It is proved that without the use of information technology management of the enterprise sphere in the new socio - economic conditions ineffective.

Изменения, происходящие в России и в мире, требуют новых подходов к управлению предприятиями. Информационные технологии существенным образом преобразуют бизнес, снижают трансакционные издержки, вовлекают в оборот интеллектуальные продукты. Все это требует своего научного осмысления и соответствующего учета в управленческой практике.

Особенностью современных информационных технологий является то, что они выступают не только средством автоматизации уже существующих процессов на предприятии, но и становятся своеобразным носителем и катализатором распространения передового управленческого опыта и технологий менеджмента. Новые информационные системы воплощают в себе передовой опыт управленческих технологий. При этом они оптимизируют бизнес-процессы в соответствии с последними достижениями теории и практики менеджмента. В связи с использованием таких технологий информация становится важной составляющей производственного процесса и теснит в нем традиционные компоненты – природные ресурсы, труд и капитал.

Информационные технологии в настоящее время способствуют трансформации самого менеджмента. Основным их содержанием является не набор технических инноваций, а совокупность мирового управленческого опыта и решений, воплощенных в соответствующем инструментарии при помощи современных способов обработки и хранения информации. Информационные технологии создают мультипликативный механизм тиражирования и развития современного менеджмента.

Эффективная экономическая деятельность в настоящее время основывается на преобразовании информации, которое предполагает целенаправленный обмен