УДК 004.05

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КАК ФАКТОР УСПЕШНОГО УПРАВЛЕНИЯ КАЧЕСТВОМ

Должженкова А.В. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – к.э.н., доцент Варламова Д.В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Аннотация. В работе рассматриваются особенности системы менеджмента информационной безопасности. Проводится изучение необходимости её внедрения и исследование её влияния на управление качеством предприятия, а также преимуществ обеспечения защиты информации.

Введение. Система менеджмента информационной безопасности (СМИБ) становится всё более популярной в условиях развития цифровизации предприятий. Всё больше сертификатов получают предприятия по ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности», что можно объяснить воздействием наличия СМИБ на успех организации. Компании так или иначе пользуются в своей деятельности информационными системами, автоматизированными системами управления, или хотя бы компьютерным оборудованием и электронной почтой, которые являются носителями, хранителями и обработчиками информации. Информация – важнейший ресурс, который обеспечивает функционирование всех процессов, именно поэтому защита информации является одним из приоритетных направлений развития многих стратегически важных предприятий. Цель данной работы – рассмотреть основные преимущества СМИБ для управления качеством и сделать выводы о целесообразности её применения.

Основная часть. Информация сопровождает продукт, изделие или услугу на всех этапах жизненного цикла. В крупных компаниях с полной автоматизацией бизнес-процессов производство управляется системами MES (Система оперативного управления производством), SCADA (Диспетчерское управление и сбор данных), CNC (Числовое программное управление), MRP (Планирование потребности в материалах), ERP (Управление ресурсами предприятия). Контроль и испытания находятся под управлением системы SCADA. Упаковка и хранение осуществляются системами SCADA, ERP. Реализация происходит под управлением систем CRM (Управление отношениями с клиентами) и SCM (Система управления цепочками поставок). Монтаж и эксплуатация происходят с помощью систем IEMT (Интеллектуальное управление предприятием) и CRM, техническая помощь и обслуживание работают в тех же системах, в системе IEMT также осуществляется утилизация. Во всех этих системах есть информационные активы, которые постоянно находятся под влиянием внешних и внутренних пользователей компании.

СМИБ направлена на повышение технологической и исполнительской дисциплины, персональной ответственности за соблюдение коммерческой тайны, конфиденциальности, целостности и доступности информационных активов, упорядоченности и организованности всех процессов. Защищенность информационных активов непосредственно влияет на работоспособность предприятия и достигается путём реализации соответствующего комплекса мер, включая политики, процедуры, а также функции программного и аппаратного обеспечения.

Инциденты информационной безопасности (ИБ) – несанкционированный доступ, отказ в обслуживании, нарушение физических мер защиты, системные сбои и другие опасности – могут остановить, нарушить или замедлить работу процессов, что негативно отразится на управлении качеством. То есть обеспечение информационной безопасности влияет на степень удовлетворенности требованиям заинтересованных сторон и потребителей что в свою очередь определяет, насколько качественно будут произведены продукты и услуги.

Стандарт, принятый на предприятии в соответствии с ГОСТ Р ИСО/МЭК 27001-2006, преследует следующие цели: сохранение конфиденциальности важных информационных активов (ИА); обеспечение непрерывности доступа к ИА предприятия; защита целостности деловой и технологической информации; минимизация ущерба от реализации угроз информационной безопасности; повышение осведомленности пользователей в области рисков, связанных с информационными активами предприятия; улучшение деловой репутации и корпоративной культуры предприятия; определение степени ответственности и обязанностей работников по обеспечению ИБ на предприятии. Стандарт содержит принципы и понятия ГОСТ Р ИСО 9001-2015, что позволяет при надобности применить на предприятии интегрирование систем менеджмента. Оба стандарта основаны на процессном подходе, а процессы реализуются в соответствии с Циклом Деминга (PDCA). Главным отличием циклов является наличие в СМК прямой ориентированности на внешнего потребителя. Можно сказать, что управление ИБ напрямую влияет на функционирование СМК и как следствие на результаты деятельности СМК. Цикл PDCA СМИБ будет содержать следующие этапы:

- Plan (Планирование): Разработка СМИБ, в том числе разработка Политики ИБ, установка целей в области ИБ, разработка планов обеспечения безопасности, планы по реагированию на инциденты, установление ответственности и полномочий;
- Do (Осуществление): Внедрение и функционирование СМИБ, в том числе организационные мероприятия по обеспечению ИБ, управление документацией, управление рисками ИБ, организация связей с заинтересованными сторонами;
- Check (Проверка): Проведение мониторинга и анализа СМИБ, в том числе внутренние аудиты СМИБ, анализ функционирования со стороны высшего руководства;
- Act (Действие): Поддержка и улучшение СМИБ, в том числе постоянное улучшение, коррекция и корректирующие действия, предупреждающие действия.

СМИБ, обеспечивающая защиту информационных активов, сможет защитить коммерческую и производственную тайну; контролировать информацию и средства обработки информации, которые доступны контрагентам. Кроме того, в процессе функционирования СМИБ при оценке рисков будут контролироваться:

– информация, средства ее обработки и передачи, к которым контрагентам предоставляется доступ;
– ценность и важность информации, ее значимость для осуществления операций;
– последствия, возникающие при недоступности контрагентов к доступу к информации, когда это необходимо, и при заведении или получении контрагентами неточной или ложной информации;
– требования законодательства Российской Федерации и обязательства по заключенным договорам с предприятием;
– тип предоставляемых прав доступа контрагентам к информации и средствам обработки информации, например, физический доступ, логический доступ, возможность сетевого взаимодействия локальной сети Предприятия и локальной сети контрагентов, осуществляется ли доступ через подключение к локальной сети Предприятия или дистанционно;
– что доступ предоставляется на основании принципа необходимости, т.е. предоставляется только тот доступ, который необходим для ведения деятельности (т.е. ограничение доступа к данным, информационным системам и приложениям, протоколам, ограничение по времени);
– процедура по контролю за использованием прав доступа контрагентов и удаления права доступа после того, как необходимость в них отпадает;
– необходимые меры для защиты информации, которая не предназначена для доступа контрагентов.

Данные аспекты дадут компании преимущества в условиях конкурентной среды, так как уменьшая влияние рисков и опасностей, повышается качество работы предприятия и эффективность процессов, что приведет к снижению издержек и привлечению заинтересованных сторон, а также повысит имидж компании.

Выводы. Внедрение СМИБ обладает большим количеством преимуществ среди которых возможность улучшения бренда, выход на международный уровень, новые партнеры и контракты, прозрачность управления. СМИБ довольно неплохо согласована с другими системами менеджмента, что позволяет использовать интегрированные системы управления, применяя единый аудит и аналогичные инструменты для управления системами. Но важность СМИБ в век информационных технологий должна быть в полной мере осознана компаниями, и внедрение СМИБ как отдельной системы менеджмента позволит тщательнее защитить информационные активы. СМИБ предполагает контроль всех ИС и АСУ предприятия, поэтому любая автоматизация процессов СМИБ оправдана. Не смотря на затраты, которые потребуется для её внедрения и покупку дорогостоящего программного обеспечения, обеспечивающего защищенность, затраты на несоответствие в следствие инцидентов ИБ могут нанести компании урон во много раз больший. Поэтому влияние СМИБ, как средства повышения эффективности процессов, так и управления рисками и поддержки IT-инфраструктуры, отразится на качестве работы предприятия в положительном ключе.

Долженкова А.В. (автор) _____

Варламова Д.В. (научный руководитель) _____