

ТИПОВАЯ МОДЕЛЬ ПОЛИТИКИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ НА ОСНОВЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

Л.В. Астахова, Е.Д. Середкина

В статье обоснована концепция построения и расширения структуры Типовой модели Политики управления информационной безопасностью на основе международных стандартов и зарубежных подходов к их внедрению с учетом убеждения сотрудников в достижении целей.

Ключевые слова: информационная безопасность, управление, политика, убеждение, стандарт.

Построение системы менеджмента информационной безопасности (СМИБ) позволяет обеспечить конфиденциальность, целостность и доступность информации за счет применения процессов управления [1]. Основными документами, регламентирующим построение СМИБ на предприятии, являются международный стандарт ISO/IEC 27001:2013 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [1] и

русский стандарт, являющийся аналогом международного, ГОСТ ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [2].

Согласно стандартам ISO/IEC 27001:2005 и ГОСТ ИСО/МЭК 27001-2006 разработка любой СМИБ строится по методологии PCDA, известной как цикл Шухарта: Plan (Планирование) – Check (Испытание) – Do (Действие) – Act (Поддержка и совершенствование.). Методология PDCA представляет собой простейший алгоритм действий руководителя по управлению информационной безопасностью. В новой редакции стандарта ISO/IEC 27001:2013 нет требований к использованию подхода PCDA, поэтому может использоваться как подход PCDA, так и любой другой. Полагаем, однако, что этот подход, положенный в основу международных стандартов менеджмента качества, вполне жизнеспособен в сфере управления информационной безопасностью. Однако содержание каждой из четырех фаз требует уточнения.

Так, например, в книге «How to Achieve 27001 Certification. An Example of Applied Compliance Management» описаны практические советы по построению системы менеджмента информационной безопасности. В число этих советов зарубежные специалисты включают в фазу поддержки и совершенствования такие действия, как обсуждение результатов, убеждение в достижении целей [3]. Заметим: не принуждение, а убеждение.

Убеждение и принуждение касаются различных проявлений человеческой деятельности: убеждение связано с сознанием, принуждение – с поведением. Поэтому убеждение – объект исследования в психологии. В отличие от принуждения, которое укоренилось в управленческих технологиях, убеждение организовано в воспитательных практиках. [4, с. 12]. Из этого следует, что включение убеждения сотрудников в достижении целей информационной безопасности организации расширяет традиционные рамки управления информационной безопасностью, требует интеграции управления информационной безопасностью с воспитательной работой в этой организации. Очевидно, что если воздействовать на сознание сотрудника с помощью убеждения, то у него появляются внутренние моральные стимулы и потребность в правомерном поведении соблюдать правила информационной безопасности, а это – уже вопросы культуры информационной безопасности [4, с. 12], индивидуального и корпоративного культурного капитала информационной безопасности, доверия к сотрудникам организации как пользователям информационной системы.

Из сказанного следует, что Политика управления информационной безопасностью организации, кроме процессов управления, составляющих содержание всех четырех фаз, должна органично включать процессы планирования, организации, контроля и совершенствования деятельности по формированию убеждений сотрудников в достижении целей организации,

развитию их культуры и культурного капитала информационной безопасности. Разработанная нами Типовая Политика управления информационной безопасностью организации включает названные компоненты.

Библиографический список

1. ISO/IEC 27001:2013 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М., 2013.
2. Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М., 2006.
3. Arnason S. T., Willett K. D. How to Achieve 27001 Certification: An Example of Applied Compliance Management: Auerbach Publications, 2008. – 352 p.
4. Осинцев, Д.В. [Убеждение и принуждение в системе государственного управления: корректна ли классификация?](#) / Д.В. Осинцев // [Полицейское право](#). – 2008. – № 1 (11). – С. 9–12.
5. Astakhova, L.V. [The concept of the information-security culture / L.V. Astakhova // Scientific and Technical Information Processing](#). – 2014. – Т. 41. – № 1. – С. 22–28.