Начальные условия для внедрения системы управления информационными рисками

написано Александр Астахов | 11 июня, 2023

Внедрение СУИР осуществляется не на пустом месте. Помимо документов, продуктов и методологий, в организации должны существовать определенные предпосылки в виде осознания руководством необходимости в осуществлении систематического и планомерного контроля информационных рисков. Также быть созданы определенные начальные условия, которые включают в себя следующее:

- *Первоисточники*. Лицензионный сборник стандартов в области управления информационной безопасностью на русском языке KIT 20 RU включает в себя следующие стандарты: BS ISO/IEC 27001:2005 RU, BS ISO/IEC 27002:2005 RU, BS 7799-3:2006 RU и ISO/IEC 27005:2008 RU (см. Приложение № 12).
- *Политика безопасности.*В организации должна быть принятая политика информационной безопасности высокого уровня, определяющая базовые требования по управлению информационными рисками. Требования, предъявляемые к политике безопасности организации, определяются в разделе 4.2.1 b) стандарта ISO 27001 и в разделе 5.1.1 стандарта ISO 27002 (ISO 17799).
- *Политика аудита.*В организации должен быть проведен внешний и/или внутренний аудит информационной безопасности, а также документально оформлены политика и процедура внутреннего аудита. Без проведения комплексного аудита информационной безопасности невозможно провести оценку рисков.
- *Политика инвентаризации активов.*В организации должна быть принята политика инвентаризации информационных

активов, в соответствии с которой осуществляется идентификация активов и разрабатывается реестр активов.

- *Организационная структура.* В организации должна существовать организационная структура для управления информационной безопасностью, предполагающая наличие менеджера информационной безопасности, отдела информационной безопасности и управляющего комитета по информационной безопасности. Соответствующие функциональные роли, ответственность и полномочия должны быть закреплены в официально утвержденных положениях об отделе (комитете), а также в должностных инструкциях. Основные правила организации информационной безопасности приведены в разделе 2 стандарта ISO 27002.