

Управление конфигурацией является составной частью управления жизненным циклом продукции.

Существует ряд стандартов в области управления конфигурацией, разработанных различными организациями, например ISO и IEEE. Часть этих стандартов принята в Республике Беларусь. В каждом из этих стандартов существует свой, несколько отличный подход к управлению конфигурацией, сравнение этих подходов, требований и приведенной информации позволит наиболее полно и разносторонне организовать управление конфигурацией в рамках организации. Именно такое сравнение представлено в данном докладе.

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ В ОБЛАСТИ ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ

А.А. ЗАМУЛА, В.И. ЧЕРНЫШ, К.И. ИВАНОВ

С повышением уровня информатизации современных предприятий задача анализа и оценивания информационных рисков становится все более актуальной. Основной задачей данного направления является объективная идентификация и оценка наиболее значимых информационных ресурсов предприятия, а также адекватность используемых средств контроля за безопасностью информации.

В докладе рассматриваются международные стандарты в области оценивания рисков информационной безопасности (ИБ). В качестве основополагающего и наиболее «общего» среди международных стандартов можно выделить ISO/IEC 27001:2005 «Информационные технологии – Методы защиты – Системы менеджмента информационной безопасности – Требования». Этот стандарт дает компании инструмент, позволяющий управлять конфиденциальностью, целостностью, доступностью такого важного актива компании как информация. Данный стандарт определяет методологию подхода к обеспечению ИБ в организации и акцентирует внимание на наиболее критичных составляющих информационной системы.

Стандарт Великобритании BS 7799 посвящен управлению информационной безопасностью организации. Частью BS 7799 является стандарт BS 7799-3. Данный стандарт посвящен вопросам управления информационными рисками. Стандарт содержит разделы по оценке рисков, обработке рисков, обеспечению непрерывных действий по управлению рисками, а также приложения с примерами активов, угроз, уязвимостей, методов оценки рисков. BS 7799-3 допускает использование как количественных, так и качественных методов оценки рисков, но, к сожалению, в документе нет обоснования и рекомендаций по выбору математического и методического аппарата оценки рисков ИБ.

В докладе даются практические рекомендации о применении и гармонизации указанных стандартов в Украине и СНГ. Применение упомянутых нормативных актов предполагает, как правило, частичное изменение ИТ-инфраструктуры организации и, в том числе, перестройку системы информационной безопасности как части инфраструктуры, а также изменение подходов к ее построению.