УДК 535.317

АКТИВЫ И СРЕДСТВА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

Студент гр. 113111 Новицкий
Ст. преп. Рогальский Е.С.
Белорусский национальный технический университет

Автоматизация процессов обработки информации, содержащей сведения, доступ к которым должен быть ограничен, вынуждает владельцев информационных систем искать пути создания эффективной системы защиты информации. Особо остро стоит вопрос в обеспечении защищенности сведений коммерческого характера, утечка или потеря которых нанесет ущерб бизнесу ее владельца. Объектом хищения может стать практически любая, даже очень надежно защищенная информация. Существуют различные способы противодействия потери информации:

- ***Организационные*** – внедрение и развитие в организации системы менеджмента информационной безопасности
- ***Технические*** – применение специального аппаратного и программного обеспечения
- ***Аудит информационной безопасности*** – способ оценки эффективности принятых мер, в том числе классический и эвристический аудит (тесты на проникновение).

Комплексную реализацию информационной безопасности может обеспечить внедрение систем менеджмента информационной безопасности, требования к которой устанавливает международный стандарт, в частности **ISO/IEC 27001:2005 «Система менеджмента информационной безопасности. Требования».** Такой подход обеспечивает продвижение программных продуктов на международные рынки и рынки стран Таможенного союза. Положительные результаты даёт сочетание использования стандартных требований в сочетании с оригинальными техническими решениями, например использованием удалённого доступа и облачных технологий. Следует учитывать, что одним из самых уязвимых звеньев любой системы безопасности является человеческий фактор. Это означает, что подбор, обучение, оценка лояльности персонала должны быть составной частью системы безопасности и постоянно находиться в поле зрения руководителя.