ВОПРОСЫ ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Е.А. СВИРСКИЙ

Рассматривается применение организационно-административных мер и методов защиты в условиях функционирования информационной системы в учреждении, организации, на предприятии, связанных с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке. Организационные меры — это относительно недорогие методы и средства защиты, которые доступны для освоения всеми субъектами хозяйствования и, которые, в состоянии решить многие проблемы защиты информации в организации.

В системе организационного обеспечения информационной безопасности выделяются два направления — направление, связанное с реализацией мер организационно-правового характера и направление, связанное с реализацией мер организационно-технического характера. Организационное обеспечение базируется на нормативно-правовой базе управления системой защиты информации. Рассматривается возможный вариант создания нормативно-правовой базы управления системой защиты информации и организации доступа к ней специалистов.

Основные проблемы, связанные с обеспечением защиты информационных ресурсов, являются следствием недостаточной компетентности, как обслуживающего персонала информационных систем, так и пользователей в вопросах обеспечения информационной безопасности. Человеческий фактор является едва ли не определяющим в обеспечении защиты информации в информационных системах каждой организации. Рассматриваются вопросы организации мероприятий по повышению общей культуры пользования информационными ресурсами населением в целом и соблюдением принципов и правил информационной безопасности в частности.

О ВОЗМОЖНОСТЯХ ПРОТИВОДЕЙСТВИЯ СОВРЕМЕННЫМ ВЫЗОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.И. ИВАНЧЕНКО, Е.А. СВИРСКИЙ

Вызовы:

– быстрые темпы обновления знаний и, соответственно, изменений технологий и средств информатизации;

– деградация классического образования;

– усиливающаяся зависимость бизнеса, обороноспособности, общественной жизни и т.д. от информационных технологий усиливают кадровый «голод» и требуют выработки новых подходов к формированию кадрового обеспечения информационной безопасности.

Эти новые подходы необходимо сформулировать в расчете на предотвращение (недопущение, упреждение) событий безопасности. Это по нашему мнению возможно путем:

– воспитания культуры информационной безопасности в максимально широкой общественной среде»;

– создания профессиональных институтов высочайшей квалификации, способных выполнять роль ведущих (локомотивов) в решении не только текущих или уже известных проблем информационной безопасности, но и (а может быть и в большей степени) будущих.

В условиях упомянутых вызовов:

– повышение культуры информационной безопасности представляется возможным через «управляемое» самообразование на корпоративном уровне в рамках «Программ повышения осведомленности»;

– исследование проблем ИБ и поиск путей их решения, а также упреждение от воздействия быстро развивающегося деструктивного программного обеспечения на основе