режима информационной безопасности, четко содержать описание области действия, а также указывать на контактные лица и их обязанности [2].

Литература

1. *Скрипник Д.А.* Обеспечение безопасности персональных данных. М., 2011.

2. Политики безопасности компании при работе в Internet [Электронный ресурс]. — Режим доступа http://citforum.ru/security/internet/security_pol/. Дата доступа 30.03.2015.

ПОДХОД К ОРГАНИЗАЦИИ КОНТРОЛЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

А.В. Федорцов

Системы защиты информации различных информационных систем по своей архитектуре идентичны, и, как правило, представляют собой совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации [1]. Ключевым элементом в таких структурах являются исполнители, несанкционированные действия которых, в большинстве случаев способствуют, а иногда, приводят к выводу из равновесия четко выстроенной системы защиты информации. Как следствие, в лучшем случае — снижается уровень защищенности данных информационной системы в стандартных условиях эксплуатации, в худшем случае — возникают новые риски и угрозы для обрабатываемой информации, на действия которых названная система не способна своевременно и адекватно реагировать и противодействовать. С целью своевременной реакции системы защиты информации на новые угрозы должен осуществляется контроль, который целесообразно выполнять поэтапно: на 1-м этапе — документальный контроль; на 2-м этапе — инструментальный контроль. В ходе документального контроля подлежит изучению и анализу вся учетная информация об эксплуатации ОИ СВТ. Инструментальный контроль необходимо проводить с применением программно-технических средств по общепринятой методике для проверки и (либо) дополнения полученных данных при осуществлении документального контроля. Результаты двухэтапного контроля позволяют в полном объеме оценить эффективность проведенных мероприятий по защите информации. Реализация вышеуказанного подхода является простым и эффективным методом защиты информации.

Литература

1. Защита информации Основные термины и определения, СТБ ГОСТ Р 50922-2000: Введ. 22.05.2000. Минск: Государственное проектное и научно-исследовательское предприятие «Гипросвязь», 2000. 6 с.