С учетом достоинств и недостатков вышеприведенных подходов предлагается адаптивный подход к системе защиты информации. Обращая внимание на необходимость исполнения должностных обязанностей (в зависимости от занимаемой должности), а также учитывая навыки работы с ПК (низкий, средний, высокий, профессиональный) возможно ограничение доступа к информации — с разрешением только на чтение, модификацию, копирование либо удаление. Стоит обратить особое внимание при внезапном изменении поведения сотрудника и ограничить доступ к возможности модификации либо удаления информации в такой ситуации. Более подробно об этом будет рассмотрено в ходе выступления.

Литература

1. *Леонов А.П.* Безопасность автоматизированных банковских и офисных систем. Минск, 1996.

ПОЛИТИКИ БЕЗОПАСНОСТИ КАК СОСТАВНАЯ ЧАСТЬ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Р.В. Паршукова, А.М. Прудник

Производственные, технологические, коммерческие данные, которые используют предприятия, обладают высокой стоимостью, а их утрата или утечка может привести к серьезным финансовым потерям. Поэтому одной из целей для предприятий отрасли является создание надежной системы защиты информации.

Система защиты информации — это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия. Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления и задействованы при выполнении бизнес-процессов [1].

Процесс создания системы защиты информации можно разделить на три этапа:

– формирование политики предприятия в области информационной безопасности;

– выбор и внедрение технических и программных средств защиты;

– разработка и проведение ряда организационных мероприятий.

Фундаментом для создания системы защиты информации является документ, в котором формулируются принципы и основные положения политики предприятия в области информационной безопасности.

Политика информационной безопасности определяет стратегию и тактику построения корпоративной системы защиты информации. Политика безопасности компании является основой для разработки целого ряда документов безопасности: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и прочее другое [2].

Общий жизненный цикл политики информационной безопасности включает в себя ряд основных шагов:

– проведение предварительного исследования состояния информационной безопасности;

– разработку политики безопасности;

– внедрение разработанных политик безопасности.

Политика безопасности затрагивает практически каждого сотрудника компании. Опыт создания политик безопасности показывает, что внедрение политики безопасности часто приводит к возникновению напряженности во взаимоотношениях между сотрудниками компании. Если это возможно, о том, что разрабатывается новая политика информационной безопасности компании необходимо уведомить сотрудников заранее. До начала внедрения новой политики безопасности желательно предоставить сотрудникам текст политики на одну–две недели для ознакомления и внесения поправок и комментариев. Политика безопасности должна быть реалистичной и выполнимой, быть краткой и понятной, а также не приводить к существенному снижению общей производительности бизнес подразделений компании. Политика безопасности должна содержать основные цели и задачи организации

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.