ПРОБЛЕМНЫЕ ВОПРОСЫ КОНТРОЛЯ ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ПУТИ ИХ РЕШЕНИЯ

Государственное учреждение
«Научно-исследовательский институт Вооруженных Сил Республики Беларусь»
г. Минск, Республика Беларусь

Федорцов А. В.

Утин Л. Л. – к-т техн. наук, доцент

В государственных информационных системах обработка данных должна осуществляться после реализации установленных законодательством мер, с применением системы защиты информации [1]. Данная система представляет собой совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации [2]. Для повышения эффективности применения мер защиты информации на ОИ СВТ должен осуществляется контроль действий пользователей.

Имеется множество подходов к классификации контроля. Различают контроль по:

целям (соответствие требованиям законодательства, эффективность мероприятий по обеспечению безопасности информации);

используемым средствам (экспертный, комплексный, инструментальный);

периодичности (внезапный, непрерывный, периодический);

степени охвата (сплошной, выборочный);

динамике (динамический, статический);

принадлежности специалистов (внешний, внутренний);

степени осведомленности сотрудников (гласный, негласный);

характеру связи с объектом (дистанционный, встроенный).

Деятельность в области контроля основывается на следующих основных принципах:

законность действий контролирующих специалистов;

регулярность;

действенность;

независимость контролирующих специалистов от руководящего персонала;

гласность результатов;

расследование нарушений требований законодательства Республики Беларусь.

Результаты комплексного контроля, с соблюдением основных принципов, должны позволять оценивать полноту и качество проведенных мероприятий.

На практике, при осуществлении контроля эффективности мероприятий по защите информации возникает ряд проблем, основными из которых являются:

недостаточная оснащенность структурных подразделений по защите информации программно-техническими средствами;

привлечение к оценке эффективности мер защиты информации неквалифицированных должностных лиц (нештатных специалистов), не имеющих достаточных навыков и опыта;

отсутствие общепринятой методики контроля.

Обеспечение программно-техническими средствами и разработка методики являются первоочередными задачами на пути повышения эффективности контроля. В результате их решения персонал, ответственный за обеспечение защиты информации, получает инструмент для качественной оценки результативности проведенных мероприятий по заданным направлениям контроля, снижения ресурсоемкости (временных затрат, количества участвующих в контроле специалистов и т.д.) процесса оценки, повышения оперативности в представлении результатов (отчетов, анализов и т.д.) и своевременном реагировании на возникшие инциденты (угрозы для системы), принятии управленческих решений. Применение программно-технических средств позволяет снизить влияние «человеческого фактора» на полученные результаты и расширить границы контроля.

Вместе с тем, разработке программно-технических средств контроля предшествует этап исследований математического аппарата оценки эффективности мер защиты информации. В докладе предложен к обсуждению разработанный подход, реализация которого позволит частично устранить рассмотренные проблемные вопросы.

Список использованных источников:

1. Об информации, информатизации и защите информации, Закон Респ. Беларусь от 10.11.2008 № 455-З, текст по состоянию на 1.03.2015. – Минск – 21 с.
2. 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.