УДК 004.05

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Емельянова О.А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»),
Беляев Е.А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – доктор технических наук Лившиц И.И.
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Создание эффективной системы безопасности объектов критической информационной инфраструктуры (КИИ) – основная цель субъектов КИИ, как в рамках выполнения требований законодательства, так и с целью оптимального использования ресурсов. Большая часть объектов КИИ введены в эксплуатацию и активно функционируют. С целью определения актуального положения существующей СОИБ объектов КИИ, необходима независимая оценка состояния и принятия решения о необходимости модернизации, т.е. проведение аудита информационной безопасности субъекта КИИ.

Введение. Под требования Федерального закона № 187 от 26.07.2017 № 187-ФЗ «О безопасности КИИ Российской Федерации» попадают организации из 14 сфер. Соответственно, на момент выполнения требований нормативных правовых актов, часть из них активно используют систему информационной безопасности, существование без которой в современное время подвержено рискам с высоким влиянием на репутацию и ресурсы.
Основная часть. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» обязывает субъектов КИИ в рамках контроля состояния безопасности объектов осуществлять внутренний контроль организации работ по обеспечению их безопасности, и эффективности принимаемых организационных и технических мер, а также на предмет выполнения требований регулятора. Контроль должен проводится ежегодно. Проведение внешнего аудита состояния безопасности не является обязательным процессом и осуществляется по решению руководителя субъекта КИИ, и в таком случае внутренний контроль может не проводиться. Следуя ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности» и ГОСТ Р ИСО 19011-2012 «Руководящие указания по аудиту систем менеджмента», «аудит» есть систематический, независимый и зафиксированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев. Таким образом, законодательно предусмотрена обязательность проведения аудита значимых объектов КИИ в форме внутреннего, либо внешнего аудита после построения системы информационной безопасности, что влечет неэффективное распределение ресурсов субъекта КИИ в процессе создания или обновления функционирующей СОИБ.
Выводы. Первоочередное проведение аудита позволяет определить актуальное состояние информационной безопасности субъекта КИИ, соответствие требованиям нормативных правовых актов, организационно-распорядительных документов, и необходимость модернизации и оптимизации СОИБ объекта КИИ.

Емельянова О.А. (автор)
Лившиц И.И. (научный руководитель)