УДК 004.056

А.А. МАНЮГИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА СООТВЕТСТВИЯ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ СФЕРЫ ЭНЕРГЕТИКИ ПО ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Анализируются требования к оценке соответствия значимого объекта критической информационной инфраструктуры (КИИ) сферы энергетики по требованиям информационной безопасности информации. Одним из приоритетов являются исследования, направленные на функциональные требования безопасности и уровни доверия, установленными приказами ФСТЭК России. Предметом исследования является требования к защите информации объекта КИИ.

Введение

Одним из главных требований информационной безопасности объекта критической информационной инфраструктуры сферы энергетики по требованиям безопасности информации является оценка соответствия ЗО (значимый объект) КИИ требованиям информационной безопасности, что в свою очередь напрямую влияет на защищенность объекта информатизации. приоритетным направлением [1].

Цель и задачи

В связи вступлением в силу федерального закона от 26.07.2018 № 187-ФЗ «О безопасности информационной инфраструктуры Российской Федерации» появляются требования, которые необходимо соблюдать для обеспечения безопасности объекта КИИ. С принятием ФСТЭК России приказов №239 и №17 в части формирования требований по информационной безопасности к объектам КИИ, потребовалось реализовать требования по безопасности комплексной системы защиты информации (КСЗИ) на этапе проектирования и дальнейшего проведения оценки соответствия применяемых средств защиты информации. Для оценки соответствия, нужно написать программу и методику приемочных испытаний, по которой будет даваться оценка соответствия ЗО КИИ. Для средств защиты информации применяется ГОСТ 19.301-79, согласно которому, программа и методика испытаний оформляется в соответствие ГОСТ 19.105-78. Рассмотрим средства защиты информации,

которые предполагается использовать на ЗО КИИ.

Средства защиты информации, которые используются на объектах ЗО КИИ имеют определенные класс защиты. Перед владельцем ЗО КИИ стоит задача по использованию только сертифицированных средств защиты информации и только определенного класса, разрешенного к использованию на данном объекте [2].

Оценка соответствия может производиться в форме сертификации или испытаний. В случае, если на объекте уже внедрен КСЗИ, необходимо провести оценку соответствия самостоятельно на этапах внедрения организационных и технических мер по обеспечению безопасности информации.

Необходимость защиты информации ЗО КИИ обусловлена большими рисками утечки информации третьим лицам. По статистике, наибольшую опасность представляют собой внутренние нарушители. То есть, использование на рабочем месте недоверенных программных продуктов ведет к серьезным последствиям, которые в будущем могут привести к угрозе жизни людей и вред окружающей среды [3].

Заключение

Необходимо проводить оценку соответствия ЗО КИИ на этапе проектирования КСЗИ. При невозможности проведения этой своевременной процедуры, необходимо использовать только доверенное и сертифицированное программное и программно-аппаратное обеспечение соответствующего класса защиты информации. Методы проведения программы и методики испытаний могут быть полезны при подготовке частных заданий для проведения оценки отдельных систем ЗО КИИ

Список литературы

1. Приказ Минэнерго России от 26.12.2023 N 1215 «Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике» (Зарегистрировано в Минюсте России 16.05.2024 N 78165) URL: https://www.consultant.ru/law/hotdocs/84739.html?ysclid=m1b3zwb63q600659135 (дата обращения: 19.09.2024).

2. Голдобина А.С., Исаева Ю.А., Селифанов В.В. Основные аспекты соответствия DLP-систем, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, 2019.

3. Исаева Ю.А., Селифанов В.В. Оценка соответствия средств защиты информации в критических информационных инфраструктурах Российской Федерации, 2019.