

Аннотация статьи: «Исследование влияния компьютерных инцидентов на безопасное функционирование опасных производственных объектов»

28 июня 2026 года

Авторы: П.В. Ганченко, Д.В. Ибадулаев, В.П. Космачев
(ООО «Научно технический центр «Технологии и безопасности»)

Компьютерные инциденты и компьютерные атаки на предприятия топливно-энергетического комплекса (ТЭК) представляют серьёзную угрозу, так как могут привести к сбоям в работе критически важных объектов, утечке конфиденциальных данных, нарушению технологических процессов, остановке производства, репутационному ущербу, значительным финансовым потерям, в крайних случаях - к угрозе жизни, здоровью персонала и экологическим катастрофам.

Для предотвращения этих угроз и минимизации последствий их реализации на субъектов (владельцев) объектов критической инфраструктуры накладываются обязанности по соблюдению требований обеспечения информационной безопасности, требования по мониторингу за компьютерными инцидентами и информированию о них, реагированию и восстановлению функционирования объектов КИИ, взаимодействию с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов, а также требования по категорированию объектов.

Основную проблему категорирования объектов КИИ составляют данные по масштабам последствий аварий из декларации промышленной безопасности и/или паспорта безопасности, в частности, последствия аварий в этих документах не являются следствием реализации компьютерных инцидентов.

Для устранения этих проблем, организацией ООО «НТЦ «ТБ» и была разработана методология «Идентификации влияния компьютерных инцидентов на безопасное функционирование ОПО», целью которой, являлась разработка методики идентификации последствий компьютерного инцидента для ОПО и выработка технологии оценки последствий при его реализации.

В статье раскрывается содержание основных этапов предлагаемой методологии и приводится практический пример реализации данной технологии на практике. Предложенная в статье технология ИВКИ позволит более корректно осуществлять категорирование объектов критической информационной инфраструктуры, оценивать степень защищенности объектов КИИ от компьютерных инцидентов, разрабатывать меры защиты от последствий компьютерных инцидентов и оценивать их эффективность, выполнять обоснование структуры и состава средств защиты от компьютерных инцидентов и обеспечение безопасности объектов критической информационной инфраструктуры.