УДК 004.056

А.Н. ВАВИЧКИН, Д.А. ДЯТЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СФЕРЕ НАУКА

Анализируется опыт категорирования объектов критической информационной инфраструктуры в высшем учебном заведении, а именно особенности категорирования в сфере наука. Рассмотрена подготовительная работа по выявлению объектов, подлежащих категорированию, и этапы проведения категорирования. Предложен порядок действий по подготовке к категорированию, формированию перечня объектов, подлежащих категорированию, и процессу категорирования, а также документальное сопровождение всего процесса для объектов, функционирующих в сфере науки.

Введение

В соответствии с федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» к объектам критической информационной инфраструктуры (КИИ) относятся информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети субъектов КИИ, то есть организаций, функционирующих в нескольких сферах, в частности, в сфере наука [1]. Из этих объектов выделяют те, которые подлежат категорированию.

Категорирование является первым этапом в создании системы безопасности значимых объектов КИИ [2]. Выявление объектов КИИ, которые подлежат категорированию, а также дальнейшее проведение категорирования в каждой сфере деятельности имеют свои особенности. В исследовании представлена организация данного процесса для научной сферы деятельности, а также обозначены основные этапы работ.

Основные этапы категорирования

Для проведения категорирования в организации создается соответствующая комиссия. Для научных учреждений важно, чтобы в нее входили руководители всех подразделений, ведущих научные работы. Это во многом упростит задачу получения сведений от научных подразделений об объектах, которые могут относиться к КИИ.

Для получения информации об имеющихся объектах кроме сведений,

которые можно получить из управлений бухгалтерского учета, научных исследований, инновационного развития и других, целесообразно провести инвентаризацию имеющихся информационных объектов [3].

Для определения объектов КИИ и необходимости их категорирования используется ряд документов, которые утверждаются руководителями подразделений. Собирается как можно больше информации о каждом из объектов (его архитектура, состав программно-аппаратных и иных средств, пользователи и т.д.)

Эти этапы позволяют сформировать перечень объектов КИИ, подлежащих категорированию [4]. Важно учитывать то, что на момент рассмотрения не все научные объекты могут участвовать в каких-либо научных работах, а используются только в образовательном процессе.

Непосредственно этап категорирования заключается в присвоении объектам категории значимости. Для обоснования сведений о результатах категорирования готовится акт категорирования, который в свою очередь, подготавливается на основании рабочих материалов, заверенных ответственными работниками за эксплуатацию и безопасность объекта.

Заключение

Поэтапная организация процесса категорирования объектов КИИ, ведение документального сопровождения на каждом этапе, привлечение научных работников, участвующих в работе рассматриваемых объектов, принятие во внимание особенностей функционирования объектов в научной сфере деятельности и рабочие материалы, полученные в ходе категорирования, обеспечивают в дальнейшем формирование системы обеспечения информационной безопасности значимых объектов КИИ.

Список литературы

1. Бондаренко А.В., Мушовец К.В., Поршнев С.В., Рогова О.К. Структура действующих нормативных правовых актов в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации. Безопасность информационных технологий. 2023, Т. 30, № 3, с. 126–148. DOI: 10.26583/bit.2023.3.09.

2. Репьева В.Д., Ханмагомедов А.Х. Особенности и проблемы категорирования объектов критической информационной инфраструктуры. Вестник науки. 2023, № 1 (58), с. 193–196. URL: https://www.вестник-науки.рф/article/7156.

3. Салкуцан А.А., Гавдан Г.П., Полуянов А. А. Методика определения критических процессов на объектах информационной инфраструктуры. Безопасность информационных технологий. 2020, Т. 27, № 2, с. 18–34. DOI: 10.26583/bit.2020.2.02.

4. Бакулин М.А. Управление рисками нарушения информационной безопасности значимых объектов критической информационной инфраструктуры. Системная инженерия и информационные технологии. 2023, № 5 (14), с. 78–87. DOI: 10.54708/2658-5014-SIIT-2023-no5-p78.