ПРОКУРАТУРА
Забайкальского края
Петровск-Забайкальская
межрайонная прокуратура

ПАМЯТКА о требованиях к информационной безопасности объектов КИИ

г. Петровск-Забайкальский
2025 год

Что такое КИИ?

В соответствии с федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» КИИ представляет собой совокупность всех принадлежащих российским организациям, органам государственной власти, государственным учреждениям и индивидуальным предпринимателям объектов КИИ и обеспечивающих их взаимодействие сетей электросвязи

С точки зрения значимости, объекты КИИ подразделяются на два вида:

«значимый» и «не значимый», а значимые объекты делятся на три целевых уровня защищенности - «категории значимости» (в соответствии с ч. 3 ст. 7 Закона «О безопасности КИИ»): максимальный целевой уровень защищенности - первый, минимальный - третий.

От уровня защищенности значимого объекта КИИ, которому он должен соответствовать, зависит набор организационных и технических мер, обеспечивающих блокирование (нейтрализацию) угроз безопасности информации, последствиями которых может быть прекращение или нарушение его функционирования

Категорирование объектов КИИ

Под «категорированием» понимается установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения (процедура определяется Правилами категорирования объектов КИИ РФ, утв. Постановлением Правительства РФ от 8 февраля 2018 № 127).

Состав мер по защите объектов КИИ согласно Приказу ФСТЭК России № 239 от 25.12.2017

I. Идентификация и аутентификация
II. Управление доступом
III. Ограничение программной среды
IV. Защита машинных носителей информации
V. Аудит безопасности
VI. Антивирусная защита
VII. Предотвращение вторжений (компьютерных атак)
VIII. Обеспечение целостности
IX. Обеспечение доступности
X. Защита технических средств и систем
XI. Защита информационной (автоматизированной) системы и ее компонентов
XII. Планирование мероприятий по обеспечению безопасности
XIII. Управление конфигурацией
XIV. Управление обновлениями программного обеспечения
XV. Реагирование на инциденты информационной безопасности
XVI. Обеспечение действий в нештатных ситуациях
XVII. Информирование и обучение персонала

Обязанности субъектов КИИ

Общие обязанности субъектов КИИ:

• категорировать объекты КИИ которыми они владеют
• незамедлительно информировать о компьютерных инцидентах ФСБ
• оказывать содействие должностным лицам в деятельности, связанной с предупреждением, обнаружением и ликвидацией последствий инцидентов.
• обеспечивать выполнение порядка, технических условий установки и эксплуатации технических средств ГосСОПКА (в случае установки на объектах КИИ)

Владельцы значимых объектов КИИ:

• создать систему безопасности в соответствии с требованиями к созданию безопасности и обеспечению их функционирования
• соблюдать требования по обеспечению безопасности значимых объектов КИИ;
• обеспечивать беспрепятственный доступ должностным лица ФСТЭК к значимым объектам КИИ при осуществлении государственного контроля и выполнять предписания об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ;
• реагировать на компьютерные инциденты, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ