

## Методика категорирования объектов критической информационной инфраструктуры

Клишин Д.В.

Научный руководитель – доцент, к.т.н., Исаев А.С.

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»  
г. Санкт-Петербург

12 июля 2017 года Государственной Думой РФ был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Основными принципами обеспечения безопасности критической информационной инфраструктуры являются:

- 1) законность;
- 2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые, в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;
- 3) приоритет предотвращения компьютерных атак.

Первым этапом обеспечения безопасности критической информационной инфраструктуры является категорирование объектов. Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Правила категорирования представлены в постановлении Правительства Российской Федерации №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

После вступления Федерального закона в силу, организации, в которых осуществляется деятельность, связанная с показателями, представленными в постановлении правительства №127, вынуждены осуществить категорирование и по итогу присвоить категорию значимости.

Целью данной работы является создание методики по категорированию объектов критической информационной инфраструктуры, позволяющей упростить и ускорить классификацию по перечню показателей критериев значимости, представленных в постановлении Правительства №127.

Перед тем, как приступить к категорированию необходимо определить процессы, нарушение или остановка которых, приведет к негативным последствиям согласно постановлению Правительства №127.

В работе составлена методика, позволяющая с минимальными усилиями подготовить акт категорирования объектов КИИ, включающая в себя:

- Определение объектов критической информационной инфраструктуры организации;
- Определение процессов критической информационной инфраструктуры на объекте;

- Оценку следующих процессов: действий нарушителя, уязвимостей и потенциальных угроз, масштабы возможных последствий.

Автор:  
Клишин Д.В.

---

Научный руководитель:  
Исаев А.С.

---

Руководитель образовательной программы:  
Заколдаев Д.А.

---