Классификация политик мониторинга информационной инфраструктуры на предприятиях

Ревнивых Александр
Тюменский Государственный Нефтегазовый Университет (Тюмень), Россия
e-mail: alexchr@mail.ru

Аннотация

Надежный мониторинг информационной инфраструктуры (ИИ) особенно критичен в крупных организациях, где один человек чисто физически не способен уследить за всеми программно-аппаратными и организационными компонентами инфраструктуры (и, соответственно, нет ни единого человека, который бы конца представлял себе в каждый момент времени состояние ИИ полностью). Поэтому важно учитывать необходимость мониторинга при разработке и внедрении политики информационной безопасности (ИБ).

В последние годы на предприятиях стала популярной практика аутсорсинга ИИ (например, облачной, виртуализированной). Особенно это удобно небольшим организациям – это избавляет их от необходимости создавать собственную полноценную ИИ и, что немаловажно, в дальнейшем следить за ней. В клиентской организации, по сути, в том или ином виде остаются только кабельные соединения (или беспроводные сети) и автоматизированные рабочие места, что позволяет упростить выполнение политик ИБ в целом и отказаться от большей части мероприятий по поддержанию ИИ в работоспособном состоянии. Хотя и этот подход имеет свои особенности с точки зрения ИБ, так как важная для организации информация передается внешним исполнителям.

Качественная реализация мониторинга ИИ позволяет руководству организаций принимать своевременные и эффективные управленческие решения, в том числе, по основному направлению деятельности своих организаций.