Сопровождение и мониторинг механизмов безопасности

написано Александр Астахов | 10 июня, 2023

Большинство механизмов безопасности требуют сопровождения и администрирования на протяжении всего периода их существования. Внедренные механизмы контроля должны регулярно отслеживаться и анализироваться для того, чтобы гарантировать их корректное и эффективное функционирование, а также то, что изменения среды функционирования не снижают их эффективности. Существует тенденция к ухудшению, со временем, производительности любого сервиса или механизма. Мониторинг предназначен для выявления этих ухудшений и инициирования корректирующих действий.

Действия по мониторингу и сопровождению должны планироваться и выполняться на регулярной основе, согласно расписанию. Таким образом могут быть минимизированы накладные расходы и сохранена эффективность механизмов безопасности.

Действия по сопровождению и мониторингу механизмов безопасности:

- *проверка журналов и отчетов;*
- *модификация параметров механизмов контроля;*
- *анализ эффективности механизмов контроля;*
- *обновление механизмов контроля, политик и процедур;*
- *контроль соответствия требованиям.*

Основная цель – гарантировать корректное и эффективное функционирование.

Многие механизмы контроля производят выходные данные, которые должны проверяться на наличие событий, значимых с точки зрения безопасности, например, журналы, отчеты о сигналах тревоги, отчеты об управлении инцидентами, отчеты об уязвимостях и анализе приложений. Стандартные средства системного аудита могут предоставить для этого полезную информацию.