Н. Г. Милославская, Д. О. Ковалев
Московский инженерно-физический институт (государственный университет)

АРХИТЕКТУРА ОПЕРАЦИОННОГО ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматривается архитектура операционного центра информационной безопасности (ОЦИБ), которая является важной частью комплексной системы защиты. Архитектура определяет последовательность получения, обработки, анализа данных ИБ и выработки ответной реакции на инциденты ИБ.

ОЦИБ — это централизованный компонент, предназначенный для комплексного управления проблемами ИБ организации. Данный термин предлагается автором по аналогии с устоявшимся понятием сетевого операционного центра, решающего аналогичные задачи в области управления телекоммуникационной инфраструктурой. В зависимости от размеров организации ОЦИБ может представлять собой либо выделенный программный продукт, либо целый набор программных и аппаратных средств, основной задачей которого является управление ИБ организации [1].

Выделяют следующие пять основных технических операций, которые выполняет ОЦИБ: регистрация сообщений ИБ, сбор сообщений ИБ, хранение сообщений ИБ, анализ последовательностей сообщений ИБ и выработка ответной реакции. За выполнение каждой из этих операций в рамках ОЦИБ отвечает отдельный модуль или отдельный блок:

– Г-блоки: генераторы сообщений ИБ (от словосочетания «генерация сообщений»);

– Б-блоки: база данных сообщений ИБ (от словосочетания «база данных»);

– Р-блоки: вырабатывают ответную реакцию на событие и/или формируют отчет по событию (от словосочетания «реакция и отчетность»);

– А-блоки: отвечают за анализ сообщений ИБ (от словосочетания «Анализ сообщений»);

– С-блоки: отвечают за сбор и нормализацию сообщений ИБ (от слова «сбор и нормализация данных»).

– З-блоки: база данных знаний, отвечает за управление знаниями об инцидентах и поддержание базы данных сигнатур систем обнаружения вторжений и базы данных уязвимостей (от слова «знания»).

Каждый блок описывает функциональную группу модулей, выполняющих определенные действия. Например, Г-блок может представлять собой множество приложений, генерирующих сообщения безопасности посредством стандартного интерфейса Syslog (UDP/514). Г-блок может также быть представлен системами обнаружения и предотвращения вторжений, межсетевыми экранами, системами фильтрации почтовых сообщений или прочими средствами защиты информации [2].

СПИСОК ЛИТЕРАТУРЫ:

1. *Ковалев Д. О.* Идеология и реализация операционных центров информационной безопасности // Безопасность информационных технологий. 2008. № 4. С. 103.
2. *Renaud Bidou*. Security Operation Center Concepts & Implementation // IV2 Technologies. 2005.