УДК 004.056

Д.О. Ковалев, Н.Г. Милославская

Особенности построения современных систем управления информационной безопасностью

Операционный центр информационной безопасности (ОЦИБ) – это централизованная компонента, предназначенная для эффективного комплексного управления проблемами ИБ организации. ОЦИБ являются важной частью реализации стратегии обеспечения ИБ. Построение современных ОЦИБ требует проектирования, разработки и внедрения трех взаимосвязанных уровней: технического, организационного и поддержки принятия решений.

Первые программные реализации операционных центров информационной безопасности (ОЦИБ), ориентированные на широкий круг организаций, начали появляться в 2000–2002 гг. Примеры таких программ – *Netforensics nFX Open Security Platform* (*OSP*), *CA eTrust Security Information Management* (*SIM*), *Arcsight Enerprise Security Manager* (*ESM*) и т.д. Их целью являлось повышение уровня защищенности информационных и телекоммуникационных ресурсов, а также повышения уровня контроля над работой средств защиты информации (СЗИ). Принцип работы этих продуктов заключался в сборе, агрегации, корреляции и визуализации большого количества данных аудита ИБ, полученных от различных СЗИ: межсетевых экранов, маршрутизаторов, систем обнаружения вторжений, журналов регистрации событий операционных систем (ОС).

Процесс работы типового продукта происходил в четыре этапа:

- этап нормализации – собирались различные сообщения с объектов мониторинга и приводились к единому формату;
- этап агрегации – определялись и удалялись дублируемые сообщения и происходило распределение оставшихся сообщений по различным категориям.
- этап корреляции – происходил анализ агрегированных данных и выявление закономерностей, сигнализирующих о попытке проведения сетевой атаки;
- этап визуализации – происходило графическое представление данных безопасности, прошедших через все предыдущие этапы [1].

Перед продуктами ставились следующие задачи:

а) управление и мониторинг в режиме реального времени программно-технических средств обеспечения ИБ;

б) динамическая визуализация угроз ИБ на единой консоли управления с целью их дальнейшего анализа и анализа их последствий;

в) анализ данных журналов безопасности, сведений об уязвимостях, информации о ресурсах и сигналах тревоги;

г) немедленное принятие ответных мер при возникновении потенциальных угроз ИБ и быстрое разрешение проблемных ситуаций в сфере безопасности;

д) построение графических отчетов по событиям ИБ [2].

Со временем круг решаемых задач расширился, к ним добавились следующие:

а) оценка рисков для анализа общей защищенности телекоммуникационной сети и активов, находящихся в ней;

б) приоритезация обработки инцидентов ИБ;

в) документирование инцидентов ИБ и поддержание базы данных знаний по обработке инцидентов ИБ;

г) долговременное хранение данных аудита для обеспечения доказательств в случае проведения расследований и отслеживания состояния ИБ организации в течение времени.

После этого за классом продуктов, выполняющих вышеперечисленные задачи, закрепилось название *Security Operations Center* (*SOC*), в русской терминологии – операционный центр информационной безопасности (ОЦИБ).

Но современные ОЦИБ – это больше, чем просто набор программных компонент. Поскольку ОЦИБ является автоматизированной системой, то в его состав входят технические средства обеспечения ИБ, которые используют в своей работе некоторые методы поддержки принятия решений и персонал, который выполняет операции, направленные на обеспечение выполнения целей и задач ИБ [3].

Таким образом, в структуре ОЦИБ можно выделить 3 уровня (рис. 1):

1 – уровень организационной поддержки ОЦИБ;

2 – уровень методов поддержки принятия решения;

3 – уровень технического обеспечения ОЦИБ.

На уровне технического обеспечения ОЦИБ (иначе его можно назвать инфраструктурным уровнем) находятся программные и аппаратные средства построения ОЦИБ. К этому уровню относятся: источники данных аудита ИБ, различные СЗИ, серверы и специализированное ПО, которые используются для реализации ОЦИБ, активное сетевое оборудование и каналы связи. Основная задача данного уровня – реализовать функциональные возможности ОЦИБ.

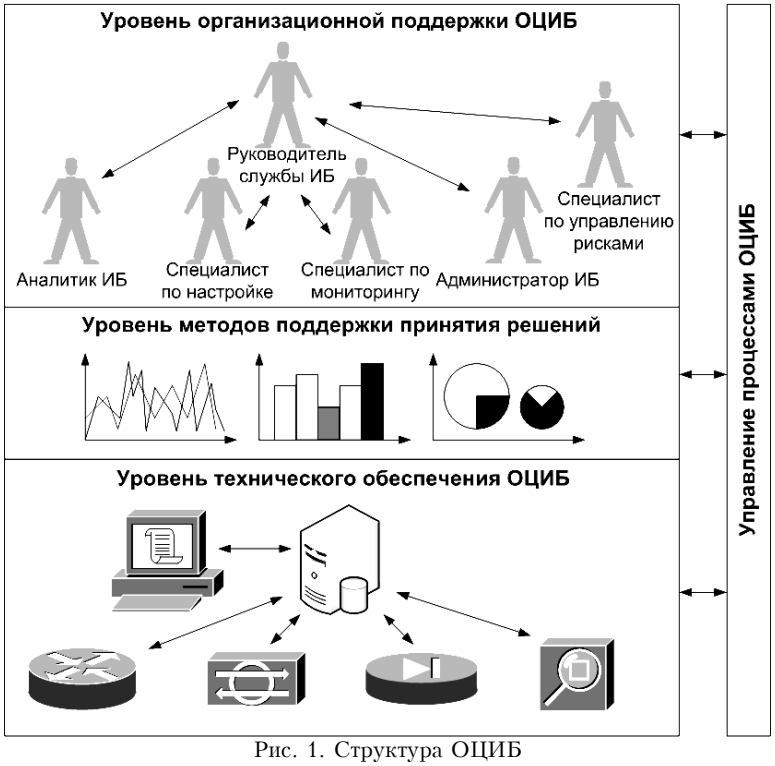

Рис. 1. Структура ОЦИБ

На уровне методов поддержки принятия решений происходят вся интеллектуальная обработка данных ИБ, анализ тенденций и выработка рекомендаций по необходимым управляющим воздействиям. На данном уровне работают математические и статистические методы и алгоритмы обработки информации. Уровень методов поддержки принятия решений базируется на уровне технического обеспечения ОЦИБ. Основная задача этого уровня — своевременно предоставить корректную информацию на уровень организационной поддержки ОЦИБ.

На уровне организационной поддержки ОЦИБ происходит работа команды специалистов по ИБ. Специалисты по ИБ во главе с руководителем службы ИБ осуществляют мероприятия по обеспечению ИБ организации. В своей работе они предоставляют исходные данные для уровня методов поддержки принятия решений и пользуются результатами его работы. Основная задача данного уровня — способствовать процессу обеспечения ИБ организации, используя средства других двух уровней.

Процессы реализации ОЦИБ на каждом из уровней требуют определенных управляющих воздействий.

Литература

1. Cisco Systems. Построение центра мониторинга и управления безопасностью Cisco. Архитектура, процессы и результаты. Cisco, 2006.

2. Kapur R., Rath S. Security Information Management, Netforensics, 2003.

3. Лукацкий А.В. Безопасность сети оператора // Информкурьер-связь. — № 2. — 2005.

Ковалев Дмитрий Олегович
Московский инженерно-физический институт (государственного университета), аспирант
Эл. почта: kovalevd@inbox.ru.

Милославская Наталья Георгиевна
Московский инженерно-физический институт (государственного университета)
К.т.н., доцент, зам. декана факультета «Информационная безопасность»
Эл. почта: milmur@mephi.edu.

N.G. Miloslavskaya, D.O. Kovalev

Construction Features of Modern Information Security Management Systems

Abstract — Information Security Operations Center (ISOC) is a centralized unit in an organization that deals with security issues. ISOC is a very important part of IS maintenance strategy implementation. It is the nucleus of the Intranet and Internet security operations, providing continuous protection, detection and response capabilities against threats, remotely exploitable vulnerabilities and real-time incidents on the network. Modern ISOC construction requires designing, development and implementation of three interconnected layers: technical, organizational and decision support.