УДК 004
ББК 32.81

МОНИТОРИНГ И АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Е.В. Багров

Разработана система мониторинга и аудита. Предложена схема размещения программного комплекса на компонентах сети. Разработаны архитектура и алгоритмы работы системы для мониторинга Solaris 10.

Ключевые слова: *мониторинг, аудит, информационная безопасность, агент сбора информации.*

На многих предприятиях используются информационно-вычислительные системы. Данные системы все прочнее входят в нашу жизнь, и их количественное и качественное использование со временем будет только возрастать.

В информационных системах хранится, обрабатывается, циркулирует различная информация, потеря или искажение которой может нанести существенный вред предприятию.

Правильное распределение ресурсов ИС и режима работы сотрудников является важным составляющим в работе организации. Находясь на рабочем месте, сотрудники зачастую вместо выполнения работы могут заниматься различными посторонними делами: посещением нерегламентированных интернет-страниц, социальных сетей, компьютерными играми и т. д.

Данная деятельность может нанести существенный ущерб работе организации, так как увеличивается расход интернет-трафика, простаивает работа, возрастает угроза информационной безопасности ИС.

Таким образом, возникает необходимость создания такой системы или программного комплекса, который смог бы решить вопрос безопасного функционирования информационной системы и обеспечить контроль деятельности пользователей, а также обеспечить возможность грамотного и эффективного распределения ресурсов ИС.

Исследовав наиболее распространенные операционные системы и выделив в них интересующие нас элементы и возможные уязвимости, мы разработали программный комплекс «Мониторинг и аудит информационной безопасности предприятия» (МАИБ).

На рисунке 1 представлена схема размещения комплекса «МАИБ» в ИС.

Алгоритм работы программного комплекса «МАИБ» (рис. 2):

На первом этапе осуществляется контроль за событиями в системе (анализируются системные журналы событий).

На втором этапе накапливаются статистические данные, на основе которых впоследствии создается так называемая «эталонная» картина событий. Впоследствии следующие состояния системы сравниваются с «эталонным» и при наличии отклонений происходит оповещение аудитора системы.

Комплекс состоит из нескольких функциональных модулей.

Модуль контроля – данный программный модуль устанавливается на пользовательские компьютеры и осуществляет сбор необходимых данных. В заданные периоды времени он высылает накопленные сведения на главный серверный модуль.

Серверный модуль – собирает воедино всю информацию, полученную от модулей контроля, и составляет единую картину событий, которая в свою очередь сравнивается с «эталонной» картиной на наличие подозрительного поведения. Если обнаруживаются различия, то этот сигнал поступает для дальнейшего рассмотрения администратору безопасности, или же вырабатывается программное решение для данной ситуации.

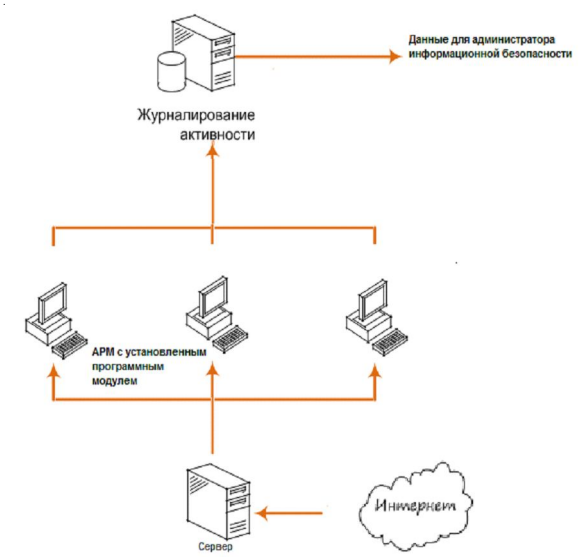

Рис. 1. Схема ИС с установленным комплексом «МАИБ»

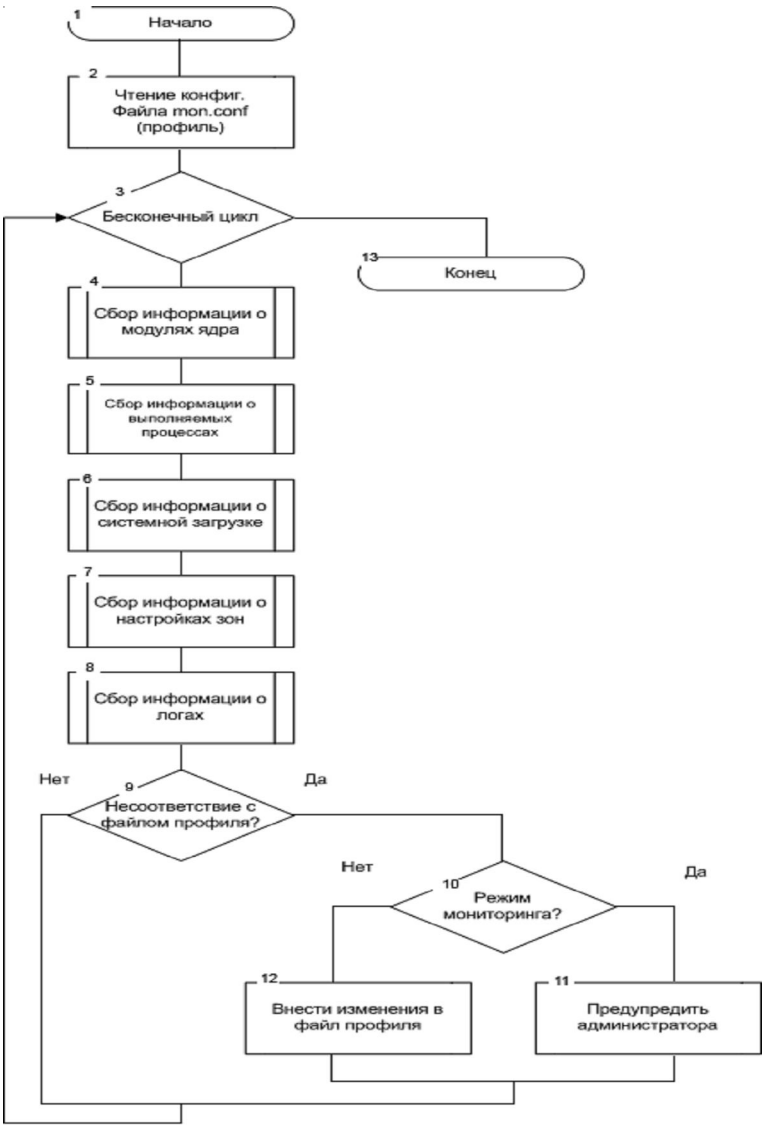

Рис. 2. Блок-схема программного комплекса по мониторингу безопасности Solaris 10

Установив такой программный комплекс в ИС, можно получить следующую информацию:

- Время прибытия/ухода сотрудника (считываем данные на контрольно-пропускном пункте предприятия).
- Время входа в компьютерную систему.
- Попытки доступа.
- Программы и приложения, запущенные пользователем, и время их функционирования.
- Списки посещаемых интернет-ресурсов.
- Установленные пользователем программы.
- Какие-либо изменения, вносимые пользователем в систему.
- Так же данный программный комплекс обеспечивает возможность обнаружения НСД и своевременного на них реагирования.

Областью применения программного комплекса является широкий спектр организаций и предприятий любого типа, где существует информационная система и необходимость осуществлять контроль деятельности пользователя и работы по обеспечению информационной безопасности. Данный комплекс является гибким и адаптивным и может быть сконфигурирован под различные системы. Использование комплекса «МАИБ» позволяет повысить уровень ИБ и дает возможность более эффективного использования ресурсов ИС.

MONITORING AND AUDIT OF INFORMATION SECURITY FOR THE COMPANIES

E.V. Bagrov

A system for monitoring and auditing is developed. The schema of software installation on the components of the network is proposed. The architecture and algorithms of the system for monitoring Solaris 10 are developed.

Key words: *monitoring, audit, information security, gathering information agent.*