МОДЕЛЬ АКТИВНОГО МОНИТОРИНГА ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ ВУЗА

А.А. Цветков

Россия, г. Шуя

В последние годы особый интерес вызывает вопрос построения корпоративной информационной среды вуза. Во многих высших учебных заведениях на сегодняшний день разработаны и приняты к внедрению концепции информатизации, при этом использование информационных технологий становится неотъемлемым элементом всех основных процессов вуза, включая процессы обучения и управления. Эффективное функционирование корпоративной информационной сети вуза видится актуальной задачей, требующей комплексного подхода к ее решению.

Во-первых, информационные сети, как правило, базируются на «клиент-серверной» архитектуре, которая связана со сложностью решения задач защиты данных в связи с разнородностью вычислительных компонентов – аппаратных платформ, операционных систем, систем управления базами данных и прикладного программного обеспечения. Во-вторых, ощущается проблема уязвимости операционных систем и программного обеспечения. Количество новых вредоносных программ достаточно быстро увеличивается, а программы-антивирусы на сегодняшний день не в силах полностью обезопасить пользователей, поскольку они могут противостоять лишь тем вирусам, которые им известны. В-третьих, из-за большого количества пользователей информационной сети и во избежание сбоев в системе, необходимо разграничивать права доступа и возможность изменения общих данных.

Таким образом, для поддержания корпоративной информационной сети в состоянии эффективного функционирования необходимо вести активный мониторинг не только состояния сети, но и действий клиентов сети в поисках проблем, вызванных перегруженными или отказавшими серверами, другими

устройствами или сетевыми соединениями, несанкционированными изменениями баз данных, параметров системы и пр.

В информационных сетях с архитектурой «клиент-сервер» необходимо вести активный мониторинг действий клиентов с целью контроля целостности баз данных, ведения статистического учета ошибок, установления популярных и неактуальных функций системы и др.

Необходимо вести аудиторские журналы приложений, в которых фиксируются ошибки и сообщения прикладной системы, а также информация о всех действиях пользователей. Кроме того, в аудиторском журнале необходимо фиксировать все подозрительные события за время работы системы (попытки проникновения в систему извне, подбора пароля, запуска приложений из закрытых каталогов и т.д.).

Активному мониторингу должны также подвергаться пользовательские права доступа к информационным ресурсам для выявления случаев попытки доступа к ресурсам клиентов с заведомо недостаточными на то правами, когда они вдруг приобретают сверхбольшие права. Все это позволит предотвратить несанкционированные действия пользователей, повысить корпоративную безопасность [1].

Выделяют большое количество методов и средств сетевого мониторинга, однако существуют общие элементы любого мониторинга сети. Начальный уровень любой проверки – тестирование физической доступности оборудования. Следующий этап – проверка работоспособности критичных служб и сервисов, запущенных в сети. Затем проводят проверки параметров, специфичных для сервисов и служб данного конкретного окружения [2]. И наконец, необходимо проводить проверку целостности баз данных. Кроме того, мониторингу подлежит определенный набор событий, таких, как системные события операционной системы, события на уровне системного реестра, события на уровне ядра операционной системы, события на уровне сеансов, события на уровне внешнего взаимодействия, события на уровне непосредственного обращения к логике приложений, события на уровне системы управления базами данных. Таким

образом, представляется следующая модель активного мониторинга клиентов информационной сети (рис. 1).

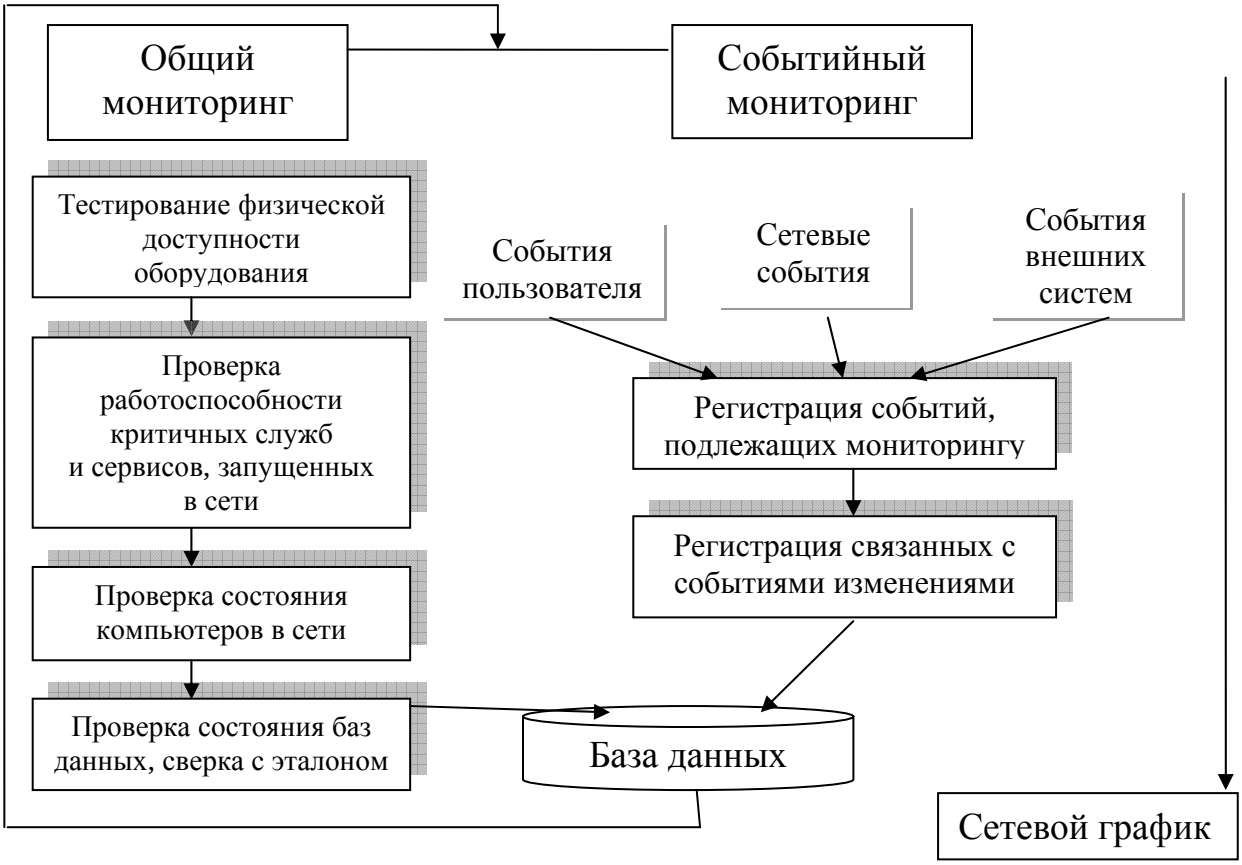

Рис. 1. Модель активного мониторинга клиентов информационной сети

Таким образом, на пути к достижению надежности работы корпоративных информационных сетей возникает множество сложностей, требующих комплексного подхода к их решению для снижения рисков информационной безопасности.

Литература

1. Защита информации в архитектурах клиент/сервер. URL: http://www.infocity.kiev.ua/hack/content/hack054.phtml

2. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети/ URL: http://www.securitylab.ru /analytics/301808.php?pagen=2&el_id=301808

3. Олифер Н.А., Олифер В.Г. Средства анализа и оптимизации локальных сетей. URL: http://citforum.ru/nets/optimize/index.shtml