# ИДЕНТИФИКАЦИЯ ПРОФИЛЯ ПОЛЬЗОВАТЕЛЯ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА ОСНОВЕ АКТИВНОГО МОНИТОРИНГА

**Цветков А.А.,**
Россия, г. Шуя

В связи со стремительным развитием инфраструктуры распределенных вычислительных сетей организаций все большую сложность и актуальность приобретает проблема обеспечения информационной безопасности [3; 4]. Увеличение количества пользователей сети зачастую приводит к риску возникновения как умышленной, так и неумышленной утечки информации. В организациях все чаще появляются так называемые *инсайдеры – сотрудники, наносящие вред фирме путем использования служебного положения для получения доступа к конфиденциальной информации, её считывания и передачи третьим лицам.* Для обеспечения устойчивости функционирования информационно-вычислительной сети необходимо аккумулировать информацию о состоянии сетевых ресурсов и несанкционированных действиях пользователей. Идентификация профиля пользователя может быть осуществлена на основе данных активного мониторинга состояния компонентов инфраструктуры сети [3; 4].

Под термином «профиль пользователя» будем понимать совокупность статистических данных о действиях и направленности действий конкретного пользователя в корпоративной сети, представленных в унифицированном формате и позволяющих сделать вывод о мере опасности данного пользователя для сохранения конфиденциальности информации. Для установления уровня опасности конкретного пользователя сети необходимо отслеживать его действия как внутри распределенной вычислительной сети, так и в глобальной сети Интернет. Другими словами, профиль пользователя должен складываться из информации о том, какие он, во-первых, использует внешние ресурсы (какие

сайты посещает, что скачивает), во-вторых, какие он использует внутренние ресурсы (базы данных, программы) и, в-третьих, какие действия он совершает (устанавливает программы, копирует файлы/папки и пр.).

Предполагается следующая схема классификации пользователей по уровню их опасности для сохранения конфиденциальности и целостности корпоративной информации: опасный – регулярно пытается нарушить уровни доступа; подозрительный – несколько раз нарушал уровни доступа; безвредный/безобидный – посещает неразрешенные сайты, но не наносит вреда; безопасный – соблюдает уровни доступа, не наносит вреда.

В таблице 1 приведена классификация пользователей с положительной или отрицательной содержательной оценкой их внутренних и внешних действий по отношению к корпоративной информационно-вычислительной сети организации.

*Таблица 1*

*Виды пользователей корпоративной сети*

| Название | Внутренние действия | | Внешние действия | |
|---|---|---|---|---|
| Безопасный | + | соблюдает уровни доступа | + | Посещает только разрешенные сайты |
| Безвредный | + | соблюдает уровни доступа | – | посещает неразрешенные сайты, но не наносит вреда |
| Подозрительный | – | несколько раз нарушал уровни доступа | + | Посещает разрешенные сайты, может посещать неразрешенные сайты, не наносящие вреда |
| Опасный | – | регулярно нарушает уровни доступа | – | может посещать неразрешенные сайты |

Таким образом, если на декартовой плоскости ось абсцисс обозначить как оценку положительности действий пользователей по отношению к внутренней среде информационно-вычислительной сети, а ось ординат – как оценку внешних действий пользователя, то в первую четверть попадают безопасные пользователи, производящие только положительные действия как внутри сети, так и за ее пределами (см. рис. 1). Опасные пользователи располагаются в третьей четверти, поскольку их действия оцениваются

отрицательно и внутри сети, и в глобальной сети Интернет, а подозрительные и безвредные пользователи занимают вторую и четвертую четверти, так как их действия определяются положительно только по отношению к одному из видов доступа.

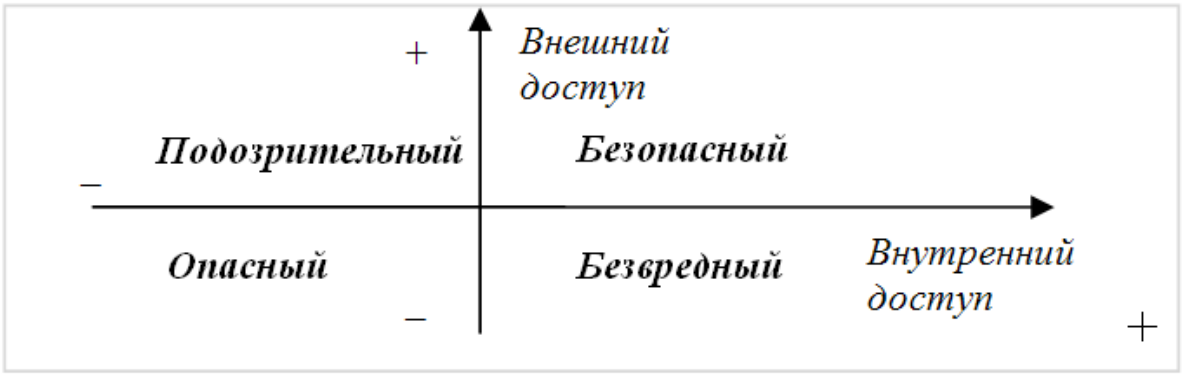


*Рис. 1. К оценке действий пользователей в сети*

Отметим также, что пользователи могут «мигрировать» из четверти в четверть, тем самым меняя свой вид. Так, например, безопасный пользователь, нарушив ограничения установленных прав доступа к некоторым ресурсам корпоративной сети, переходит в разряд подозрительных пользователей. Однако если такое нарушение было случайным и у данного пользователя больше не повторится в течение заданного промежутка времени, то он может быть возвращен в группу безопасных пользователей. Для инициализации процесса классификации необходимы определенные критерии отнесения пользователя к той или иной группе, для разработки которых должен быть определен набор критических ситуаций для проведения мониторинга действий пользователей в сети. Такими событиями, например, могут быть отказ в доступе, удаление файлов, посещение запрещенных сайтов и прочие.

Отнесение пользователя к какому-либо уровню может быть произведено, например, согласно таблице критериев, настраиваемой сетевым администратором (см. табл. 2).

*Таблица 2*

*Пример таблицы критериев разделения пользователей по видам*

| | Безопасный | Безвредный | Подозрительный | Опасный |
|---|---|---|---|---|
| Отказ в доступе | 0 | 0 | До 3 в месяц | Более 4 в месяц |
| Удаление файлов | до 2-х в день | до 2-х в день | до 5 в день | не ограничено |
| Посещение запрещенных сайтов | 0 | 1-2 раза в день | до 5 раз в день | не ограничено |

Итак, для идентификации профиля активного пользователя сети необходим следующий алгоритм. Пусть Т – промежуток времени просмотра данных мониторинга, установленный сетевым администратором. Через промежуток времени Т проводим следующие действия: просматриваем логи мониторинга с целью нахождения критических событий, в случае их наличия заносим сведения о выявленном неправомерном действии пользователя в базу данных. По окончании просмотра всех логов мониторинга необходимо обновить данные об отнесении пользователя к какому-либо уровню опасности согласно имеющейся таблице критериев (см. рис. 2).

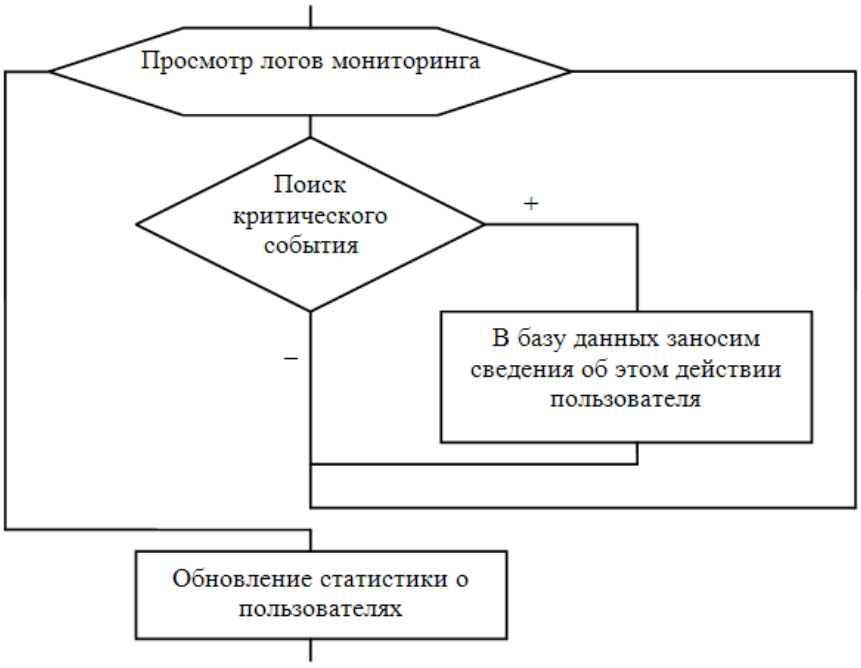


*Рис. 2. Фрагмент блок-схемы алгоритма идентификации профиля пользователя*

Оценка сходимости алгоритма может быть произведена на основе вычислительного эксперимента, построенного с помощью имитационной модели действий пользователя, в соответствии с рекомендациями работ [1; 2].

Предложенный алгоритм идентификации профиля пользователя основан на накоплении, систематизации и анализе результатов активного мониторинга компонентов сети, при этом должны быть установлены определенные критерии отнесения пользователя к одному из указанных видов по уровню его информационной опасности [4].

Внедрение системы активного мониторинга распределенной вычислительной сети организации должно способствовать повышению уровня её безопасности. Поскольку результаты мониторинга позволяют не только фиксировать возникающие информационные конфликты, проблемы и сбои, например, вызванные перегрузкой сервера, отказом в доступе к сегментам базы данных, но также в совокупности с учётными данными пользователей сети являются основанием для идентификации и обновления профиля активного пользователя сети. В свою очередь, анализ профилей пользователей системным администратором позволит своевременно определить потенциального инсайдера и предотвратить несанкционированные действия и возможную утечку информации.

В целом активный мониторинг инфраструктуры сети следует рассматривать как составной компонент системы интегрированной защиты информационных ресурсов организации [2]. На его основе могут быть построены гибкие автоматизированные механизмы контроля функционального состояния критических сегментов сети, выявления потенциальных инсайдеров, что позволит своевременно принять адекватные организационные меры и скорректировать параметры механизма разграничения прав доступа.

## Литература

1. *Надеждин Е.Н.* Научно-методические основы автоматизации процессов обеспечения информационной безопасности в сфере образования // Ученые записки ИИО РАО. 2012. Вып. 1. С. 56-74.

2. *Надеждин Е.Н., Смирнова Е.Е., Шершакова Т.Л.* Математические основы моделирования и анализа интегрированных систем защиты информации: учебное пособие. Тула: Изд-во ТулГУ, 2013. 206 с.

3. *Сердюк В.А.* Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. М.: Изд. дом Гос. ун-та – Высшей школы экономики, 2011. 572 с.

4. *Цветков А.А.* Сетевая модель активного мониторинга рабочих станций распределенной информационно-вычислительной сети // Информационная среда образования и науки. 2013. Вып. 15. URL: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2013/num_15_2013 (дата обращения: 05.11.2013).