УДК 004.056.5

магистр К.В. Назаренко
ГВУЗ «Национальный горный университет»

КАТЕГОРИЗАТОР ИНФОРМАЦИИ ДЛЯ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ДОСТУПОМ

Категоризатор является частью подсистемы управления доступом, поэтому на него могут возлагаться задачи автоматизации присвоения и контроля атрибутов доступа. Представлена схема и алгоритм работы категоризатора, который осуществляет распознавание меток безопасности, анализ соответствия с уровнем конфиденциальности содержимого, при необходимости – присвоение меток, а также принятие решения по каждому отдельному контейнеру информации.

Системы DLP, появившиеся на рынке ИБ не так давно, уже зарекомендовали себя как надежный комплекс средств защиты (КСЗ), позволяющий предотвратить утечку информации. Подобные системы целесообразно рассматривать как системы управления доступом, так как предотвращение утечек информации и сводит задачи системы к контролю циркуляции информации в информационной системе (ИС) предприятия.

Ядром любой системы DLP является категоризатор информации. Категоризация – процесс распределения различных данных по категориям на основе смысловой близости [1]. Категоризатор может не только отслеживать информацию с ограниченным доступом (ИсОД) по формальным признакам, но и управлять атрибутами доступа, что приведет к автоматизации процесса распределения полномочий согласно правилам разграничения доступа (ПРД) и к уменьшению нагрузки на инженера службы ИБ при достаточно большом объеме информации на предприятии. Согласно НД ТЗІ 1.1-002-99 метки (метки безопасности) являются атрибутами доступа [2].

Автоматизация процесса присвоения контейнерам информации атрибутов доступа является важной задачей для подсистемы управления доступом.

Украинские КСЗ, которые используют метки: SECRET NET, КСЗ «ЛОЗА», «Гриф–Мережа». Во всех решениях используется контейнерный метод распознавания информации. Недостаток состоит в обработке только тех контейнеров, на которых стоит метка, остальные не обрабатываются и не анализируются. Необходимо разрабатывать процедуру расстановки меток на

новые и входящие документы, а также систему противодействия переносу информации из помеченного контейнера в непомеченный посредством операций с буфером, копирования информации из временных файлов и т.д. Нет контроля над черновиками. Рабочая станция, на которой не стоит агент системы, не защищена от утечек. Слабость таких систем проявляется и в организации расстановки меток [3].

Категоризатор может выполнять задачи:

– контроль циркуляции и автоматического проставления атрибутов доступа;

– информирование службы ИБ в случае нарушений ПРД и т.п.;

– анализ непомеченных контейнеров информации методами контентной фильтрации на наличие ИсОД;

– анализ помеченных контейнеров информации на соответствие содержащейся конфиденциальной информации уровню атрибута доступа (соответствует, занижен, завышен).

Схема контроля атрибутов доступа категоризатором представлена на рисунке 1. Описание алгоритма работы категоризатора (рисунок 1):

1. На вход поступает контейнер информации.

2. Далее выявляются атрибуты доступа, которые проставлены на документы, содержащие ИсОД.

3. Если метка стоит, то:

а) Это значит, что информации присвоен определенный «гриф». Проводится анализ соответствия процесса передачи ПРД.

б) Если результат положительный, информация поступает на выход и далее передается по заданному маршруту.

в) Если выявляется нарушение ПРД, то передача останавливается и принимается решение о дальнейших действиях согласно заранее прописанных инструкций и настроек.

4. Если метка не стоит, информация передается на модуль категоризации.

5. Далее происходит категоризация информации.

6. Если ИсОД обнаружено не было, информация поступает на выход и далее передается по заданному маршруту.

7. Если была обнаружена ИсОД, на нее ставится метка, далее действия аналогичные описанным в пункте 3.

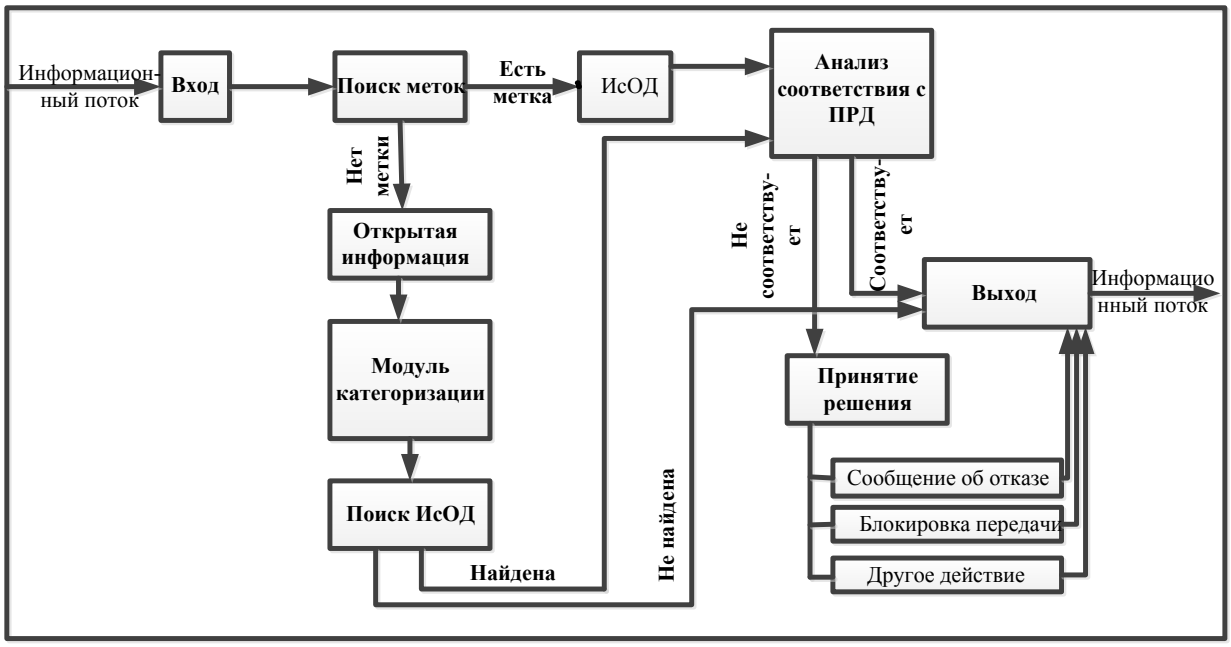

Рисунок 1. Схема контроля атрибутов доступа категоризатором информации

Применение категоризатора информации для подсистемы управления доступом – актуальное решение, так как с помощью категоризации возможно поточное отслеживание ИсОД. Контроль атрибутов доступа позволяет с помощью методов контентной фильтрации определить соответствие метки и контента. Использование категоризатора, который бы контролировал присвоение меток, их перемещение, а также мог бы информировать инженера ИБ при возникновении инцидентов, связанных либо с нарушением ПРД, либо с какой-либо другой спорной операцией с атрибутами доступа, повысит эффективность работы подсистемы управления доступом.

Перечень литературы:

1. Наталья Ефременко «Онтологии в DLP-системах третьего поколения», "Information Security/ Информационная безопасность" #4, 2009

2. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу»

3. Технологии предотвращения утечек конфиденциальной информации – (Электронный ресурс) / URL: http://www.tadviser.ru/index.php/Статья:DLP