Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет информатики и радиоэлектроники

УДК 537.86:004.056.5

Горботенко

Иван Игоревич

Методика централизованного управления учетными записями и прав доступа в локальной сети

АВТОРЕФЕРАТ

диссертации

на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель

Насонова Наталья Викторовна

к.т.н., доцент

Минск 2015

Введение

При создании единого информационного пространства современного предприятия одной из наиболее сложных проблем является управление правами доступа к приложениям и сервисам внутрикорпоративной сети. Для управления доступом к сервисам разных типов приходится использовать несколько разных систем управления и выполнять большое число операций, что создает большую нагрузку на администраторов. Управление учетными данными и правами доступа занимает первое место в первой пятерке приоритетов безопасности, в список которых входят межсетевое экранирование предотвращение вторжений, предотвращение утечки данных и антивирусное обеспечение. В сетях крупных организаций, с большим количеством сервисов и пользователей, многообразие технологий приводит к повышению сложности процесса управления доступом. Сервисы разных типов , использующие разные технологии управление доступом, требуют создания инфраструктуры управления репозитория правил разграничения доступа , системы управления доступом и тд. Для упрощения процесса управления доступом необходимо выполнить интеграцию систем управления доступом к сервисам, использующим различные технологии управления доступом.

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является разработка методики централизованного контроля учетных записей и прав доступа в локальной сети и средства ее реализации и тестирования.

Для достижения поставленной цели необходимо решить следующие **задачи**:

- провести анализ общих принципов управления доступом в сетях и системах и обосновать выбор технологии для централизованного контроля доступа;

- реализовать технологию списков контроля доступа (ACL) в различных сетевых операционных системах и на уровне приложений;

- на основе реализации технологии ACL разработать методику централизованного контроля учетных записей и прав доступа в локальной сети

- разработать средство централизованного контроля учетных записей и прав доступа в локальной сети;

- предложить практические рекомендации по внедрению разработанного средства в локальную сеть.

Объект исследования – учетные записи пользователей и права доступа в локальной сети.

Предмет исследования – механизмы управления учетными записями и правами доступа и технологии их реализации.

Положения, выносимые на защиту

1. Разработанная централизованная методика контроля учетных записей и прав доступа в сети на основе списков контроля доступа, позволяющая интегрировать управление доступом пользователей к информационным ресурсам на различных платформах (Windows, Unix, NFS) и в различных приложениях в единую систему для повышения уровня управляемости и защищенности информационных систем, повышения производительности труда системных администраторов.

Личный вклад соискателя

Основные результаты диссертации получены автором самостоятельно. В совместно опубликованных работах автору принадлежит анализ принципов управления доступом в сетях и системах и обоснование выбора технологии для реализации централизованного контроля доступа; разработка методики и

средства централизованного контроля учетных записей и прав доступа в локальной сети, рекомендации по внедрению разработанного средства в локальную сеть.

Апробация результатов диссертации

Теоретические и практические результаты диссертационных исследований докладывались и обсуждались на следующих научных конференциях и семинарах: XIX Международная науч.-тех. конф. «Современные средства связи», Минск, 14-15 октября 2014 г. и МНПК «Управление информационными ресурсами» 2014, Академия управления при президенте РБ, Минск.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 печатных работы в сборниках тезисов и докладов на международных научно-технической и научно-практической конференции.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трех глав, заключения, библиографического списка. Полный объем диссертационной работы составляет 75 страниц, из них 72 страницы основного текста, библиография из 27 наименований на 3 страницах, включая 2 публикации автора на 1 странице.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** обоснована актуальность темы диссертации, показана необходимость разработки методики централизованного контроля учетными записями и прав доступа в локальной сети, для создания централизованной системы управления офисной сети.

В **первой главе** описаны современные технологии управления доступом, стандарт ACL и математические модели политик безопасности

Концепция ACL формально не стала стандартом POSIX, а потому здесь будут рассмотрены различные аспекты реализации и использования ACL. В частности такие особенности, как реализация ACL в Linux, Solaris, Windows. Будут рассмотрены различия в способах хранения расширенных атрибутов в различных файловых системах (Ext2, Ext3, XFS, ReiserFS, NTFS и других).

Необходимость в стандартизации других смежных областей в безопасности в дополнение к ACL, привела к тому, что была сформирована специальная рабочая группа для определения расширений безопасности внутри POSIX 1003.1. Документы 1003.1e (System Application Programming

Interface/Программный интерфейс системных приложений) и 1003.2c (Shell and Utilities/Консоль и утилиты) были специфицированы этой рабочей группой. Рабочая группа фокусировала свое внимание на следующих расширениях POSIX.1: ACL, аудит, совместимость, мандатное управление доступом (MAC).

Оказалось, что стандартизация всех этих областей была непосильной задачей. В январе 1998 года спонсирование 1003.1e и 1003.2c прекратилось. Одна часть документов, которая была достаточно проработана, была выпущена рабочей группой, а другая часть была не готова к выпуску в качестве стандартов. Было решено, что драфт 17, последняя версия документов, выпущенных рабочей группой, должен быть выложен для общего доступа. В настоящее время эти документы могут быть найдены на сайте Винфрида Трампера (Winfried Trümper) [27].

Несколько производителей UNIX систем реализовали различные части расширений безопасности и в результате к версии операционной системы добавлялся ярлык “trusted” (доверенный), например Trusted Solaris, Trusted Irix, Trusted AIX.

В настоящее время поддержка ACL реализована на различных файловых системах практически на всех UNIX-подобных системах. Некоторые из этих реализаций совместимы с драфтом 17, в то время как остальные совместимы с более ранними версиями. К несчастью, это отразилось в некоторых коренных различиях среди различных реализаций.

Проект TrustedBSD (http://www.trustedbsd.org/), возглавляемый Робертом Ватсоном (Robert Watson) реализовал версии ACL, аудита, совместимости и MAC стандарта POSIX.1e для FreeBSD. Реализации ACL и MAC появились в FreeBSD-RELEASE в январе 2003 года. Реализация MAC до сих пор является экспериментальной.

Во **второй главе** показывается реализация ACL на всех самых популярных современных платформах.

Традиционная модель разграничений прав доступа в файловых системах согласно POSIX определяет 3 класса пользователей: владелец, группа-владелец и остальные. Определенные права доступа: чтение (read, r), запись (write, w) и выполнение (execute, x). В этой модели класс разрешений владельца определяет привилегии доступа для владельца файла, разрешения для группы-владельца – для группы пользователей, в которую входит владелец файла, разрешения для остальных – для всех остальных пользователей (которые не вошли в первые два пункта). Команда *ls –l* показывает разрешения для доступа для владельца,

группы и остальных в первой колонке своего вывода (например, запись “-rw-r-----” соответствует обычному файлу, который владелец может просматривать и редактировать, группа – только просматривать, а остальные пользователи не имеют никаких прав на доступ к этому файлу).

ACL состоит из набора записей (ACE). Каждый из трех классов пользователей представлен в виде ACE. Разрешения для дополнительных пользователей и групп содержатся в дополнительных ACE.

Таблица 3 показывает определенные типы записей и их текстовые представления. Каждая из этих записей состоит из типа, квалификатора, который определяет к какому пользователю или группе применяется запись, и набора разрешений (*тип:квалификатор:разрешения*). Квалификатор отсутствует для записей, которые в нем не нуждаются.

ACL, эквивалентный файловым битам доступа, называется минимальным ACL. Он состоит из трех записей. ACL с более чем тремя записями называется расширенным ACL. Расширенные ACL также содержат запись-маску и могут содержать любое (ограничивается конкретной реализацией ACL для конкретной файловой системы, где существует ограничение на максимальное число записей в одном ACL) количество записей для имеющихся пользователей и групп.

Таблица 4 – Типы записей ACL

Тип записи (ACE)	**Текстовое представление**
Владелец	user::rwx
Именованный пользователь	user:name:rwx
Группа владелец	group::rwx
Именованная группа	group:name:rwx
Маска	mask::rwx
Остальные	other::rwx

Записи именованных пользователей и групп относятся к классу групп, наряду с записью группы владельца. В отличие от модели разрешений POSIX.1, класс группы сейчас может содержать ACE с различными наборами разрешений, таким образом, класс разрешений группы сам по себе более не является достаточным для детального разграничения прав доступа для всех

ACE, которые он содержит. Более того, смысл класса разрешений группы переопределен: согласно новой семантике, они определяют верхнюю грань разрешений, которую каждая запись класса групп будет гарантировать.

Это свойство верхней грани гарантирует, что приложения POSIX.1, не знающие об ACL, не смогут нежданно и негаданно гарантировать дополнительные разрешения в случае поддержки ACL.

В минимальном ACL класс разрешений группы идентичен разрешениям группы-владельца. В расширенном ACL класс группы может содержать записи для дополнительных пользователей и групп. Это может создать проблему: некоторые из этих дополнительных записей могут содержать разрешения, которые не содержаться в записи группы-владельца, и, таким образом, запись разрешений для группы-владельца может отличаться от класса разрешений группы.

Эта проблема решается введением записи-маски. В минимальном ACL класс разрешений групп совпадает с записью разрешений для группы-владельца. В расширенном ACL класс разрешений групп совпадает с записью-маской разрешений, тогда как запись группы-владельца все еще определяет разрешения для группы-владельца. Рисунок 1 показывает эти два случая.

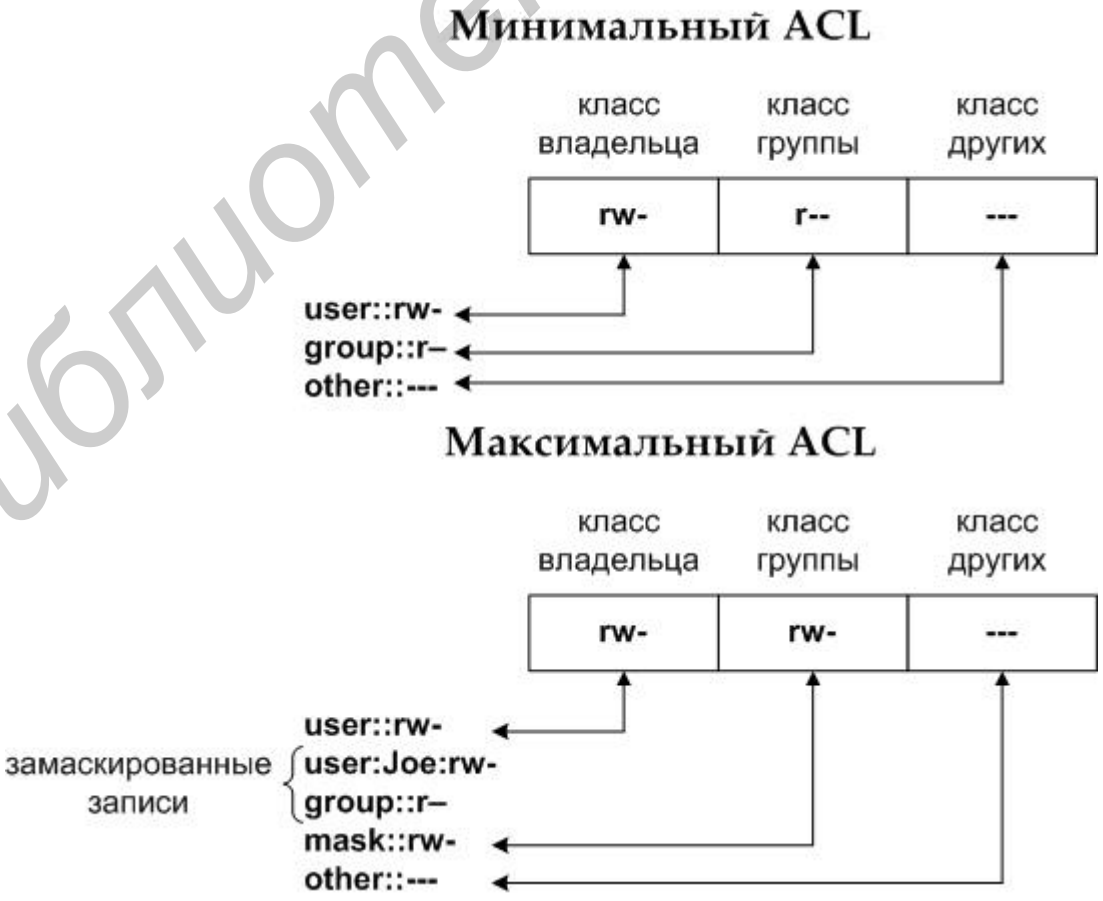

Рисунок 1. - Соответствие между ACE и файловыми битами прав доступа

Когда приложение изменяет класс разрешений для владельца, группы или остальных (например, команда *chmod(1)*), соответствующая ACE также изменяется. Подобным образом, когда приложение изменяет класс разрешений ACE, соответствующей одному из классов пользователей, изменяется разрешение для этого класса.

Класс разрешений группы определяет верхнюю грань разрешений, гарантированных записью класса групп. Случай минимального ACL тривиален. В случае расширенного ACL это реализовывается разрешениями записи-маски: эффективными будут разрешения в записях, относящихся к классу группы, который также присутствуют в записи-маске. Разрешения, которые отсутствуют в записи-маске не оказывают никакого эффекта. См. *таблицу 5*.

Таблица 5 - Маскировка разрешений

Тип ACE	**Текстовое представление**	**Разрешения**
Именованный пользователь	user:joe:r-x	r-x
Маска	mask::rw-	rw-
Эффективное разрешение	r-	

Записи владельца и остальных не принадлежат к классу групп. Их разрешения всегда эффективны и никогда не маскируются.

ACL по-умолчанию

До сих пор рассматривались ACL, определяющие текущие разрешения для доступа к объектам файловой системы. Этот тип называется ACL доступа (access ACL). Другой определенный тип называется ACL по-умолчанию (default ACL). Он определяет разграничения прав доступа к объектам файловой системы, которые наследуются у родительского каталога в процессе создания объекта. Только каталоги могут быть ассоциированными с ACL по-умолчанию. ACL по-умолчанию для объектов, отличных от каталогов, не имеют никакого смысла, поскольку никакие объекты файловой системы не могут быть созданы внутри объекта, отличного от каталога. ACL по-умолчанию напрямую не участвует в процессе проверки прав доступа.

Когда каталог создается внутри другого каталога, имеющего ACL по-умолчанию, новый каталог наследует ACL доступа и ACL по-умолчанию каталога-родителя. Объекты, не являющиеся каталогами, наследуют ACL по-умолчанию каталога-родителя в качестве своего ACL доступа.

Разрешения наследованного ACL доступа далее модифицируются параметром режима доступа, который имеется в каждом системном вызове создания объекта файловой системы. Этот параметр состоит из 9 битов разрешений, которые представляют собой классы разрешений для владельца, группы и остальных. Эффективным разрешением для каждого класса устанавливается пересечение разрешений, определенных для класса в ACL и в параметре режима доступа.

Если каталог-родитель не имеет ACL по-умолчанию, разрешения нового файла определятся согласно тому, как это рекомендовано в POSIX.1. Эффективными разрешениями устанавливаются разрешения, определенные параметром режима доступа за исключением тех, которые установлены текущем параметром umask (user mask, маска пользователя).

Umask не оказывает никакого эффекта в случае, если ACL по-умолчанию определен.

Алгоритм проверки прав доступа

Процесс запрашивает доступ к объекту файловой системы. Сначала выбирается ACE, которая в наибольшей степени совпадает с запросом процесса. ACE просматриваются в следующем порядке: владелец, именованный пользователь, группа (группа-владелец или именованная группа), остальные. Доступ определяется только одной единственной ACE. Далее проверяется, содержит ли соответствующая ACE достаточные разрешения на доступ.

Процесс может быть членом более чем одной группы, то есть ему могут соответствовать несколько ACE. Если какая-нибудь из этих ACE содержит необходимые разрешения, то она и выбирается. Если ни одна ACE не содержит достаточных разрешений, то в доступе будет отказано независимо от выбора ACE.

Алгоритм проверки прав доступа может быть описан в псевдокоде следующим образом:

1. **If**

UID процесса совпадает с UID владельца $\Rightarrow$ доступ будет определяться ACE владельца

else if

UID процесса совпадает с квалификатором в одной из ACE именованных пользователей ⇒ доступ будет определятся этой ACE

else if

один из GID процесса совпадает с GID группы-владельца и ACE группы владельца содержит необходимые разрешения ⇒ доступ будет определяться этой ACE

else if

один из GID процесса совпадает с квалификатором одной из ACE именованной группы и эта ACE содержит необходимые разрешения ⇒ доступ будет определяться этой ACE

else if

один из GID процесса совпадает GID группы-владельца или одной из именованных групп, но ни одна из этих ACE не содержит необходимых разрешений ⇒ в доступе будет отказано

else

доступ будет определяться ACE для остальных пользователей и групп.

2. If

соответствующая ACE (выбранная на предыдущем этапе) – это либо ACE владельца, либо ACE остальных и она содержит необходимые разрешения ⇒ доступ предоставляется

else if

соответствующая ACE – это ACE именованного пользователя, группы-владельца или именованной группы и она содержит необходимые разрешения и запись-маска также содержит необходимые разрешения (или запись-маска отсутствует) ⇒ доступ предоставляется

else

в доступе будет отказано

ACL в Linux

Статус ACL в Linux

Патчи, которые реализовывают ACL драфта 17 POSIX 1003.1e доступны для множества версий Linux уже несколько лет. Они были добавлены в версию 2.5.46 ядра Linux в ноябре 2002 года. Текущие дистрибутивы Linux до сих пор основаны на стабильной ветке ядер версии 2.4.x. Консорциум SuSE и United Linux интегрировал патчи ACL для ядер версии 2.4.x раньше остальных, и, таким образом, их текущие продукты предоставляют наиболее полную поддержку ACL в Linux на сегодняшний день.

Командные утилиты *getfacl(1)* и *setfacl(1)* в Linux не строго соответствуют драфту 17 стандарта POSIX 1003.2c. Это несоответствие выражается в основном в том, каким образом эти утилиты устанавливают ACL по-умолчанию.

Основные файловые системы, для которых реализована поддержка ACL в Linux, это Ext2, Ext3, IBM JFS, ReiserFS и SGI XFS.

Пример ACL доступа

Начнем с создания каталога и проверки разрешений на доступ к нему. Параметр umask определяет, какие разрешения будут замаскированы в процессе создания каталога. Если umask равен 027 (восьмеричное представление), то он будет запрещать доступ на запись для группы-владельца и полностью запрещать доступ для остальных пользователей.

$ umask 027
$ mkdir dir
$ ls -dl dir
drwxr-x--- ... agruen suse ... dir

Первый символ в выводе команды *ls* характеризует тип файла (d для каталога). Запись “rwxr-x---” характеризует разрешения на доступ к новому каталогу: чтение, запись и выполнение для владельца и чтение и выполнение для группы-владельца. Многоточие в данном примере соответствует тексту, которые не относится к данной теме, и поэтому он был убран с целью более легкого восприятия примеров.

Эти базовые разрешения имеют свой эквивалент в ACL. Просмотреть ACL можно при помощи команды *getfacl*.

$ getfacl dir
 # file: dir
 # owner: agruen
 # group: suse
user::rwx
group::r-x
other::---

Первые три строки вывода команды *getfacl* содержат имя файла, владельца и группу-владельца файла в виде комментариев. Каждая из следующих строк содержит ACE одного из трех классов пользователей: владельца, группы и остальных.

Следующий пример добавляет права на чтение, запись и выполнение для пользователя Joe к существующим разрешениям. Для этого

используется параметр *–m* (modify, изменить) команды *setfacl(1)*. Вывод итогового ACL будет опять осуществляться командой *getfacl(1)*. Опция *–omit-header* (пропуск заголовка) команды *getfacl(1)* не показывает первые три строки в выводе, которые содержат имя файла, владельца и группу-владельца файла и укорачивает вывод команды, как это показано ниже.

$ setfacl -m user:joe:rwx dir
$ getfacl --omit-header dir
user::rwx
user:joe:rwx
group::r-x
mask::rwx
other::---

В ACL были добавлены две дополнительные записи: одна для пользователя Joe, другая – запись-маска. Запись-маска автоматически создается, когда это необходимо. Ее разрешения являются объединением разрешений всех записей класса групп, и, таким образом, она не маскирует никакие разрешения.

Теперь запись-маска будет определять разрешения для класса групп. Вывод команды *ls* изменится и будет выглядеть так, как это показано ниже.

$ ls -dl dir
drwxrwx---+ ... agruen suse ... dir

Дополнительный символ “+” добавляется ко всем файлам, для которых определен расширенный ACL. На первый взгляд этот дополнительный символ кажется вовсе ненужным, но на самом деле POSIX.1 назначает этому символу необязательный флаг альтернативного метода доступа, который по-умолчанию устанавливается пустым, если не используются никаких альтернативных методов доступа. Таким образом, этот символ указывает на то, что если определен альтернативный метод доступа, то в процессе доступа к такому файлу будут использоваться именно он.

Разрешения класса групп содержат разрешение на запись. Традиционно такие биты файловых разрешений показывают возможность записи для группы-владельца. В случае, если определен ACL, эффективными разрешениями для группы-владельца будет пересечение разрешений группы владельца и записи-маски. Эффективные разрешения для группы-владельца в данном примере по прежнему “r-x”, т.е после создания дополнительных ACE командой *setfacl(1)* они не изменились.

Разрешения класса групп могут быть изменены при помощи команд *setfacl(1)* или *chmod(1)*. Если не определена запись-маска, *chmod(1)* изменит разрешения записи группы-владельца традиционно. В следующем примере командой *chmod(1)* запретим доступ на запись для класса групп и посмотрим, что изменилось.

```
$ chmod g-w dir
$ ls -dl dir
drwxr-x---+ ... agruen suse ... dir
$ getfacl --omit-header dir
user::rwx
user:joe:rwx            #effective:r-x
group::r-x
mask::r-x
other::---
```

Как показано выше, если ACE содержит разрешения, которые превышают разрешения записи-маски, команда *getfacl* добавляет комментарий к этой ACE, который показывает эффективный набор разрешений, гарантированный этой ACE. Если бы ACE группы-владельца содержала бы разрешения на запись, то к ней был бы добавлен такой же комментарий. Посмотрим теперь, что изменится, если вернуть разрешения на запись для класса групп.

```
$ chmod g+w dir
$ ls -dl dir
drwxrwx---+ ... agruen suse ... dir
$ getfacl --omit-header dir
user::rwx
user:joe:rwx
group::r-x
mask::rwx
other::---
```

После добавления разрешения на запись для класса групп, ACL вновь определяет те же разрешения на доступ, как и до запрещения записи для класса групп. Команда *chmod(1)* производит неразрушительный эффект на ACL. Это особенность является чрезвычайно важной для POSIX.1e ACL.

Операционная система Windows NT 4.0 поддерживает файловые системы FAT и NTFS. Первая поддерживается такими известными операционными системами, как MS-DOS, Windows 3.x, Windows 95/98 и OS/2, вторая — только семейством Windows NT. У FAT и NTFS различные характеристики производительности, разный спектр предоставляемых возможностей и т.д. Основное отличие файловой системы NTFS от других (FAT, VFAT, HPFS) состоит в том, что только она одна удовлетворяет стандарту безопасности C2, в частности, NTFS обеспечивает защиту файлов и каталогов при локальном доступе.

Защиту ресурсов с использованием FAT можно организовать с помощью прав доступа: чтение, запись, полный доступ.

Таким образом, наиболее удачным с точки зрения безопасности будет создание дисковых разделы NTFS вместо FAT. Если все же необходимо использовать раздел FAT, то его надо сделать отдельным разделом для приложений MS-DOS и не размещать в нем системные файлы Windows NT.

Поскольку файлы и каталоги в Windows NT являются объектами, контроль безопасности осуществляется на объектном уровне. Дескриптор безопасности любого объекта в разделе NTFS содержит два списка управления доступом (ACL) — дискреционный (DACL) и системный (SACL).

В операционной системе Windows NT управление доступом к файлам и каталогам NTFS возлагается не на администратора, а на владельца ресурса и контролируется системой безопасности с помощью маски доступа (access mask), содержащейся в ACE соответствующего ACL.

Маска доступа включает стандартные (Synchronize, Write_Owner, Write_Dac, Read_Control, Delete), специфические (Read(Write)_Data, Append_Data, Read(Write)_Attributes, Read(Write)_ExtendedAttributes, Execute) и родовые (Generic_Read(Write), Generic_Execute) права доступа. Все эти права входят в дискреционный список контроля доступа (DACL). Вдобавок маска доступа содержит бит, который соответствует праву Access_System_Security. Это право контролирует доступ к системному списку контроля доступа (SACL).

В списке DACL определяется, каким пользователям и группам разрешен или запрещен доступ к данному ресурсу. Именно этим списком может управлять владелец объекта.

Список SACL задает определенный владельцем тип доступа, что заставляет систему генерировать записи проверки в системном протоколе событий. Только системный администратор управляет этим списком.

На самом деле для администрирования используются не отдельные права доступа, а разрешения NTFS. Разрешения подразделяются на:

- индивидуальные — набор прав, позволяющий предоставлять пользователю доступ того или иного типа (*таблица 8.1*);
- стандартные — наборы индивидуальных разрешений для выполнения над файлами или каталогами действий определенного уровня (*таблица 8.2*);
- специальные — комбинация индивидуальных разрешений, не совпадающие ни с одним стандартным набором (*таблица 8.3*).

В **третьей** главе оказано внедрение разработанной методики вв офисную сеть предприятия

Рассмотрим типовую структуру локальной сети предприятия (Рисунок 2), включающую следующие элементы:

- пользователи, относящиеся к нескольким отделам, имеющие различные права доступа к информации компании;

- приложения, используемые пользователями, работают на разных операционных системах;

- информационные ресурсы предприятия с различной степенью конфиденциальности хранятся на локальных компьютерах пользователей и на файловом сервере, обмен информации с ним производится с помощью сетевой операционной системы

- АРМ администратора сети, обеспечивающего управление правами доступа в соответствии с политикой безопасности организации и имеющимся списком контроля доступа;

- в зависимости от отдела, в котором работает пользователь, он будет иметь разные права доступа к файлам и приложениям.

Учетные записи пользователей настраиваются администратором отдельно для каждой системы (почтовый сервер, файловый сервер, сервер баз данных и т.д.). Пользователь для работы с информационными ресурсами сети использует различные учетные записи (пусть даже и с одинаковыми логинами и паролями).

Кроме того, в соответствии с рекомендациями международных стандартов по информационной безопасности требуется обеспечить принцип минимально необходимого доступа, ограничивающего права доступа пользователей только к ресурсам, связанным с выполнением их должностных обязанностей.

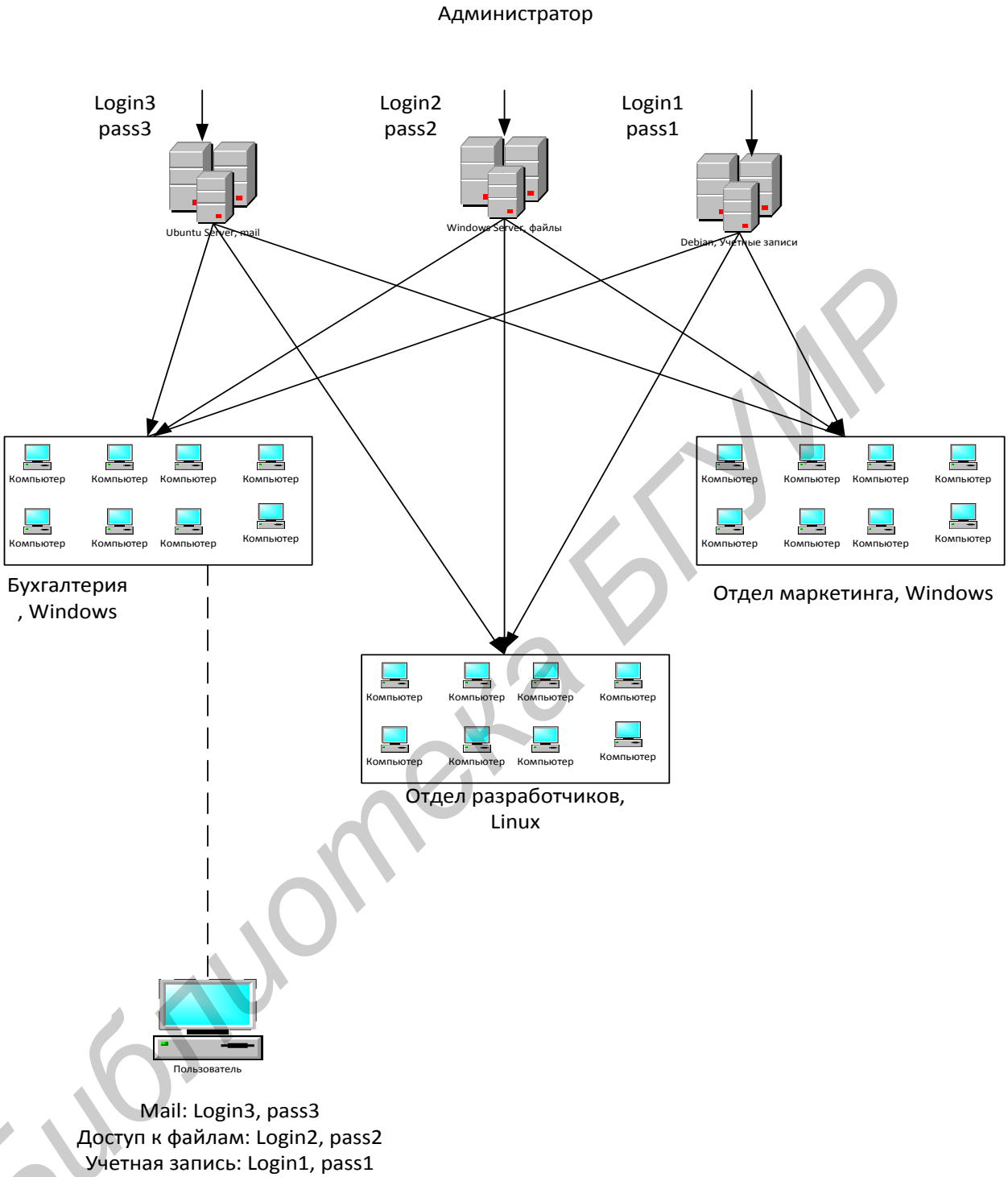

Рисунок 2. – Топология сети предприятия

1

2

3 3.2 Разработка практических рекомендаций по внедрению разработанного средства в локальную сеть

На рисунке 3 приведена схема работы предложенного средства контроля доступа.

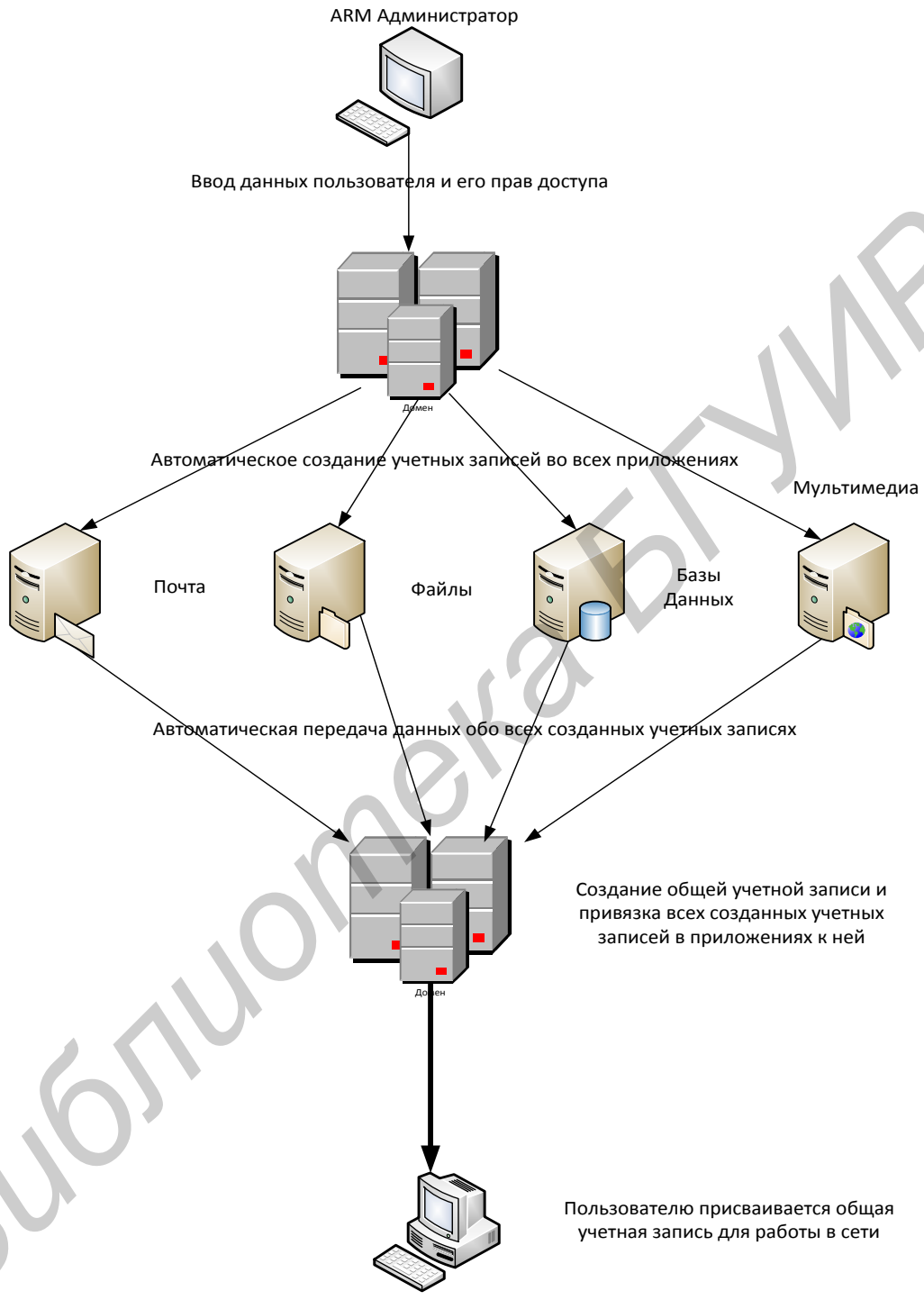

Рисунок 3. – Схема работы предложенного средства контроля доступа

Администратор вводит учетные данные пользователя (его ФИО, должность и т.д.), также вводит в какую группу безопасности он будет входить (группы безопасности распределены по списку контроля доступа). Далее следует создание пользовательских данных во всех сетевых приложениях и выдача прав доступа на всех файловых серверах предприятия (опять же в зависимости от

того к какой группе из списка контроля доступа он отнесен). Далее создается общая учетная запись, к которой прикрепляются все данные и права этого пользователя со всех приложений и серверов. В итоге пользователь получает свой логин и пароль на всех платформах предприятия и свои права доступа на файловых серверах в зависимости от того, к какой группе в списке контроля доступа он относиться. Создание аккаунтов во всех системах происходит одновременно и централизованно, и если это нужно получает один и тот же логин и пароль во всех системах. В итоге к одной общей учетной записи прикрепляются все остальные, и сеть предприятия будет понимать, что это один и тот же пользователь если он авторизуется в разных приложениях.

На рисунке 4 приведена схема внедрения разработанного централизованного средства контроля доступа в типовую локальную сеть предприятия.

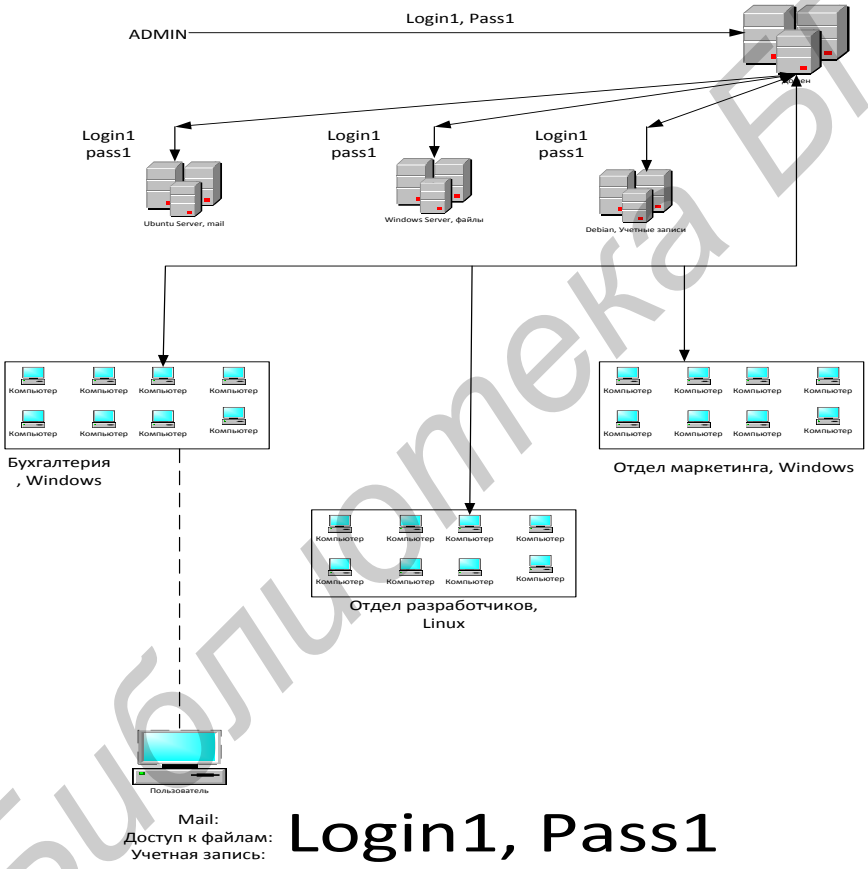

Рисунок 4. – Внедренная система централизованного контроля

В предлагаемой системе учетные записи пользователей и настройка прав доступа каждого пользователя производится в каждой системе, на доменном сервере находится список контроля доступа, в котором описаны группы, в зависимости от которых будут выданы права в ту или иную директорию к тому

или иному приложению. Изменение прав доступа пользователя производит администратор с единого центра на своем рабочем месте, указывает, к какой системе пользователь уже не имеет доступа. Если нужно удалить учетную запись, то удаляется все централизованно со всех серверов и приложений.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Актуальность исследования подтверждается широким применением списков управления доступа во всех основных операционных системах. Проблема управления доступа, а в конечном счете, и защиты информации, всегда остро стояла как перед рядовыми пользователями, так и перед государственными, военными организациями. Рассмотренные модели доступа в различных вариациях способны успешно решать заданные проблемы в зависимости от требований, которые к ним предъявляются. Анализ методов реализации дискреционной модели управления доступом на основе ACL показал, что эта модель наиболее проста в реализации, т.е. в наименьшие сроки система может приобрести достаточно стабильную и гибкую модель безопасности, кроме того, поддержка ACL реализована в большинстве основных операционных и файловых системах. В данный момент поддержка ACL на уровне приложений реализована не на 100%, но все большее количество программ начинает поддерживать ACL. В этой проведен анализ производительности ACL, при его реализации в различных файловых системах, который позволил обосновать применение стандарта ACL для централизации контроля доступа в крупных сетях. В случае, если в системе необходима реализация ACL,эта информация может быть полезна для выбора наиболее производительной файловой системы.

Интеграция поддержки EAs была важным шагом на пути упрощения развития различного рода приложений, включая расширения системы на уровне безопасности, таких как схема мандатного управления доступом, схема управления доступом на основе способностей, иерархическое управление хранением и многие решения на пользовательском уровне.

POSIX.1e ACL являются последовательным расширением модели разрешений POSIX.1. Они поддерживают более хорошо гарантированные и сложные сценарии разрешений, которые сложно или невозможно реализовать в традиционной модели.

Однако ни одна из этих областей так и не была формально стандартизована. Уже существует дикая смесь реализаций с коренными отличиями и несовместимостями. Чем больше становится доступных реализаций, тем менее возможной становится будущая стандартизация.

Результатом внедрения разработанной методики является унификация единого имени и пароля у каждого пользователя в системе предприятия, для доступа ко всем информационным ресурсам предприятия. Единая процедура управления правами имеет большие возможности по автоматизации процесса управления и поддержания данных в актуальном состоянии. Разработанная методика может применяться как в корпоративных сетях так и на одном локальном компьютере, стандарт ACL применим на разных платформах в том числе и сетевых

Рекомендации по практическому применению.

Практическая значимость предлагаемой методики заключается в повышении уровня управляемости и защищенности информационных систем предприятия, повышении производительности труда системных администраторов

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ СОИСКАТЕЛЯ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Волынчук Е.Г., Горботенко И.И., Смоляк Д.С., Насонова Н.В. Информационная безопасность корпоративной сети // Современные средства связи: материалы XIX Международной науч.-тех. конф., Минск, 14-15 октября 2014 г. / ВГКС; редкол.: А.О. Зеневич [и др.]. – Минск, 2014. - С. 188-189
2. Горботенко И.И., Насонова Н.В. Система централизованного управления учетными записями и правами доступа в локальной сети // Управление информационными ресурсами: Материалы МНПК, 2014 Академия управления при президенте РБ, 2014, Минск. С.48-49.