Биометрическая аутентификация в распределенных сетях масштаба предприятия

Авторские права

Информация, включенная в настоящий документ, отражает текущую точку зрения компании ООО «Биолинк Солюшенс» (далее — компания BioLink) по обсуждаемым вопросам на момент публикации. Компании BioLink приходится реагировать на постоянно меняющиеся требования рынка, поэтому изложенная информация не должна восприниматься как обязательство со стороны компании BioLink. Кроме того, компания BioLink не может гарантировать, что вся представленная информация сохранит точность после даты публикации.

Данный документ имеет чисто информативный характер.

КОМПАНИЯ BIOLINK НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ, НИ ЯВНО ВЫРАЖЕННЫХ, НИ ПОДРАЗУМЕВАЕМЫХ В СВЯЗИ С ДАННЫМ ДОКУМЕНТОМ.

Названия продуктов или предприятий, указанные в документе, являются или могут являться товарными знаками соответствующих владельцев.

Соблюдение всех надлежащих законов об авторском праве является прямой обязанностью конечного пользователя. Не ограничивая права, защищенные законом об авторском праве, никакая часть этого документа не может быть воспроизведена, скопирована, сохранена или передана полностью или частично, в любой форме и с использованием любых средств: электронных, механических, фотокопировальных и др. без предварительного письменного согласия со стороны компании BioLink.

Если не указано иное, все компании, организации, продукты, имена доменов, адреса электронной почты, логотипы, люди, места и события, описанные в настоящем документе, являются вымышленными. Любые возможные ассоциации с реальными компаниями, организациями, продуктами, именами доменов, адресами электронной почты, логотипами, людьми, местами или событиями не подразумеваются и являются случайным совпадением.

BioLink®, U-Match® являются зарегистрированными товарными знаками компании BioLink, и IDenium™, являются товарными знаками компании BioLink на территории Соединенных Штатов Америки и/или других стран.

Любые товарные знаки, упомянутые в данном руководстве, являются либо товарными знаками, либо зарегистрированными товарными знаками соответствующих владельцев. Компания BioLink признает все права компаний, имеющих зарегистрированные товарные знаки.

Содержание

Список иллюстраций

1. Введение

Управление правами доступа к информационным ресурсам предприятия должно соответствовать внутренним стандартам и политиками, установленными в организации.

Как правило, каждое предприятие обладает своим, уже сложившимся набором методов и принципов, определяющих политику информационной безопасности предприятия как внутри него (локальная сеть), так и снаружи (доступ через веб-интерфейс, удаленные соединения и т.д.). Такие политики основываются на огромном количестве паролей и других учетных данных, позволяющих идентифицировать пользователей, их предъявляющих. Ситуация осложняется использованием на предприятиях комбинированных способов идентификации: бесконтактных (смарт-) карт, цифровых сертификатов и т.д. В итоге, обычному пользователю, помимо необходимости иметь несколько различных учетных записей для доступа в разные операционные среды (у каждой из этих записей есть свое уникальное имя пользователя и пароль, часто сложный, состоящий из десятков цифр и букв) требуется держать при себе смарт-карту и/или другие идентификаторы.

Данная ситуация может с легкостью привести к серьезным проблемам в системе информационной безопасности предприятия, результатом которых будет повышение экономических рисков, снижение прибыли, потеря конфиденциальной информации, утрата коммерческой тайны и ноу-хау и т.д.

Данные проблемы чаще всего возникают из-за того, что пароль и имя пользователя могут быть забыты (случайно или нарочно), цифровой сертификат – украден или взломан и каким-либо образом модифицирован, смарт-карта – передана другим лицам (добровольно или по принуждению), вся информация на ней удалена и/или заменена фальшивыми данными. Все эти бесчестные методы преследуют одну цель – подделать личность законопослушного гражданина, незаконно проникнуть в охраняемые помещения, украсть информационные и/или коммерческие ресурсы и передать их заинтересованным третьим лицам (конкурентам, мошенникам и т.д.).

Именно поэтому управление паролями и аутентификацией пользователей информационных ресурсов становится в наше время одной из основных задач профессионалов IT индустрии.

1.1 Управление паролями

Управление паролями, как правило, требует привлечения существенных людских и финансовых ресурсов IT департамента. Исследования показали, что 1) управление паролями расценивается в 150-220$ на одного пользователя и 2) 40% обращений в службу поддержки вызвано проблемами, связанными с паролями (по информации Группы Gartner).

Кроме того, большинство пользователей с трудом запоминает сложные, постоянно меняющиеся пароли, столь необходимые для поддержания приемлемого уровня безопасности в корпоративной сети. Однако, существует возможность снизить затраты на управление паролями и вместе с тем создать еще один комплексный уровень

безопасности, заменив или дополнив традиционный доступ по паролю, не усложняя тем самым работу пользователя.

Каждому руководителю должно быть абсолютно понятно, на сколько важной является задача обеспечения целостности и конфиденциальности информационных ресурсов предприятия. Именно поэтому, когда говорят о безопасности и управлении, удобстве работы пользователя и оптимизации бизнес-процессов, современных технологиях и передовых разработках, имеют в виду биометрические инновации.

1.2 Биометрические инновации

В относительно недавнем прошлом, биометрические технологии были известны только узкому кругу специалистов.

В настоящее же время, в связи с повсеместным распространением программных и аппаратных решений на основе биометрии, почти каждый человек имеет хотя бы общее представление, о том, что такое биометрия, как она работает, каковы ее задачи и отличительные характеристики, и каким образом она может быть использована для решения его собственных бизнес-задач.

Тем не менее, прогресс не стоит на месте и постепенно на рынке появляются решения, основанные на мульти-биометрии - новейшей технологии, объединяющей передовые математические алгоритмы, и позволяющей идентифицировать человека, используя различные комбинации биометрических параметров. Мульти-биометрия позволяет объединить следующие технологии: распознавание по отпечаткам пальцев (в том числе по дактокартам), по лицу, сетчатке глаза, голосу, почерку и другим физиологическим и поведенческим параметрам, позволяя создавать полноценные программно-аппаратные решения как для небольших компаний, так и для крупных производственных предприятий. Мульти-биометрия представляет новую эпоху в создании и обслуживании биометрических систем, позволяя добиваться быстрой отдачи инвестиций и обеспечивая на предприятии максимальный уровень информационной безопасности, который когда-либо можно было бы достигнуть.

Компания BioLink уже предлагает поддержку десятипальцевого алгоритма в большинстве своих продуктов (включая IDenium). Мульти-биометрические решения также находятся на пути к своим потенциальным заказчикам (если вы хотите получить подробную информацию о мульти-биометрических решениях, посетите официальный сайт компании BioLink http://www.biolink.ru).

Скорость вычислений и обработки биометрических данных также значительно возросла, позволив внедрять биометрические решения в транснациональных корпорациях, имеющих офисы в разных странах по всеми миру и сложную распределенную инфраструктуру сети.

1.3 Распределенные сети

В настоящее время типичная структура сети предприятия уже не так проста и прозрачна, как было раньше. Географически распределенные сети, развернутые на предприятиях, имеющих офисы во многих странах мира, могут быть очень сложны и трудны для понимания.

К тому же в последнее время существенно возросли финансовые затраты предприятий на поддержание устойчивости и работоспособности таких сетей. С повсеместным развитием Интернета и сопутствующих технологий, проблема обеспечения безопасности сетей, их защиты от неавторизованного доступа и различных хакерских атак, вышла на первый план среди задач IT департаментов. В итоге все больше и больше ресурсов, как людских, так и финансовых, требуется для поддержания постоянно стабильной, корректно функционирующей, защищенной от взломов распределенной корпоративной сети.

Например, корпоративная сеть предприятия может включать следующие элементы, требующие авторизации:

- стандартная локальная сеть Windows, работающая под управлением службы каталогов Active Directory;
- удаленные веб-сервера, веб-консоли, и другие клиентские приложения, требующие аутентификацию пользователя;
- терминальные платформы (Citrix, терминалы Windows и т.д.)

Описанная выше сеть изображена на рисунке ниже, где эта сеть визуально распределена на 4 сегмента, каждый из которых определяет отдельную программно-аппаратную среду приложений, требующих аутентификации пользователя.

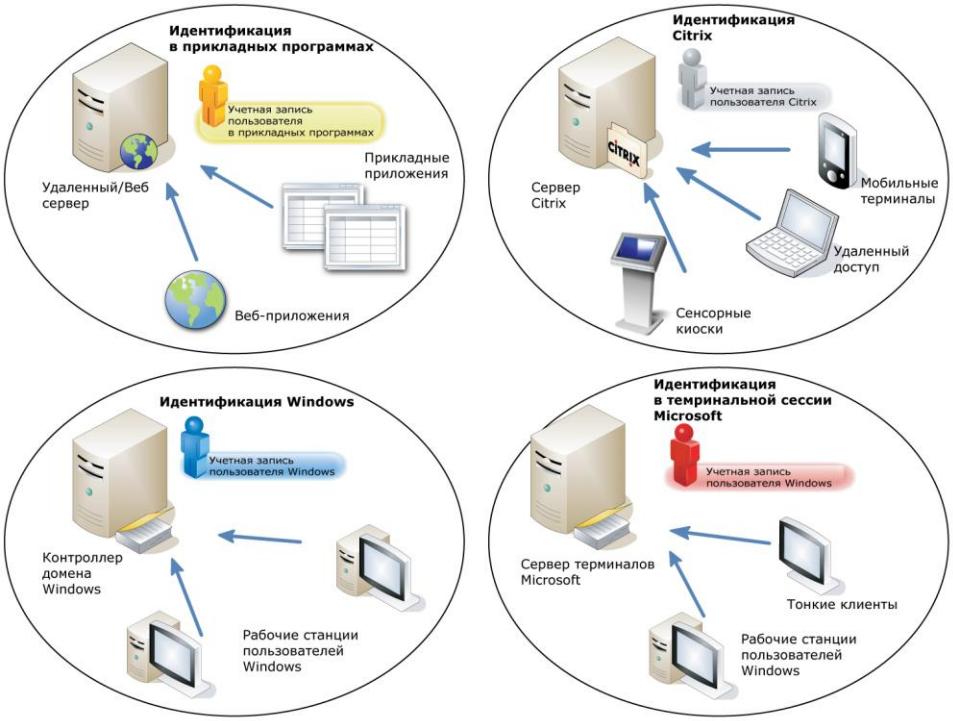


Рисунок 1. Распределенная сеть масштаба предприятия

Несмотря на теоретическую возможность аутентификации пользователя с помощью учетной записи Windows, скорее всего у пользователя такой сети будет множество учетных записей для каждого окружения/операционной системы. Результатом такой организации бизнес-процессов будет так называемая «парольная перегрузка», вызванная тем, что пользователю приходится помнить все свои учетные данные, включающие различные уникальные имена и пароли, используемые для доступа к тем или иным ресурсам.

Несмотря на все попытки сотрудников IT департамента, направленные на обеспечение и укрепление информационной безопасности на предприятии (использование сложных паролей, смарт-карт, PIN кодов и цифровых сертификатов совместно с паролями), сетевая инфраструктура все равно остается уязвимой из–за так называемого «человеческого фактора». В итоге, именно из-за того, что обычному пользователю приходится не только запоминать свои многочисленные учетные данные, но и иметь при себе другие средства идентификации, и происходит большинство ошибок, которые могут повлечь за собой крупные финансовые потери и подвергнуть риску конфиденциальную информацию предприятия.

Система BioLink IDenium призвана освободить пользователей от необходимости запоминать пароли, логины и/или иметь при себе другие средства идентификации. После установки и развертывания IDenium, пользователю нужно будет всего лишь приложить палец к сканеру отпечатков пальцев для того, чтобы получить доступ ко всем ресурсам сетевого окружения. IDenium позволит IT профессионалам сосредоточиться на других важных задачах, а не заниматься восстановлением паролей забывчивых пользователей.

Рисунок ниже показывает распределенную сеть (представленную на рис.1) после установки и развертывания BioLink IDenium.

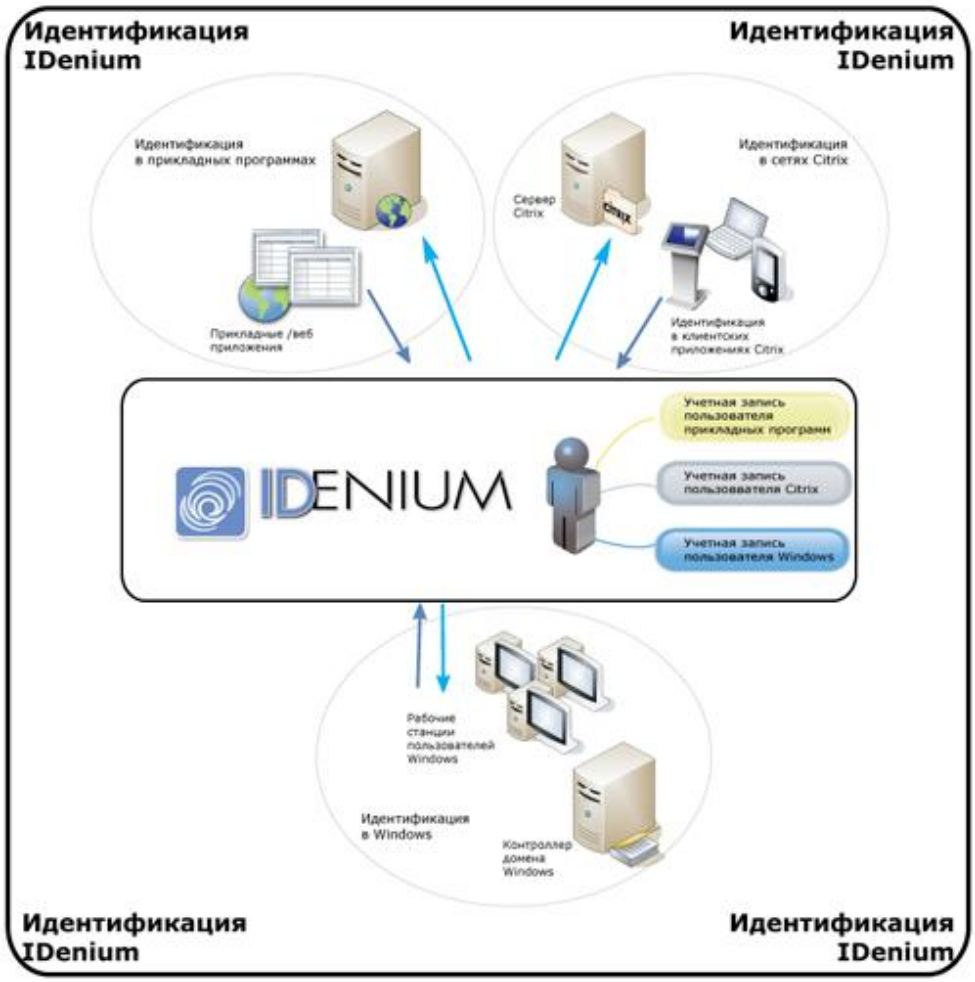


Рисунок 2. Аутентификация в IDenium

Схема, изображенная на рисунке 2, показывает, что теперь система IDenium принимает участие во всех процессах, требующих аутентификации пользователя, предоставляя информацию об учетных записях пользователей (и соответствующих учетных данных) всем заинтересованным системам, требующим авторизацию пользователя.

Пользователю больше не надо запоминать свои логины, PIN коды и пароли, иметь при себе смарт карты и т.д. Пользователю больше не надо задумываться о том, как и каким образом получить доступ к требуемым ресурсам. Теперь ему можно сосредоточиться на выполнении своих конкретных бизнес-задач.

Все вопросы доступа к информационным ресурсам теперь будут решаться системой BioLink IDenium.

2. BioLink IDenium

BioLink IDenium - это биометрическая система аутентификации пользователей, которая позволяет значительно эффективнее использовать стандартные средства защиты вашего операционного окружения, благодаря использованию одной из самых эффективных технологий распознавания - по отпечатку пальца. Применение IDenium позволит улучшить отказоустойчивый безопасный доступ к различным информационным ресурсам, усилить защиту конфиденциальной информации, упростить работу пользователей и оптимизировать соответствующие бизнес-процессы на предприятии.

2.1 Архитектура

Если предприятие использует несколько различных операционных окружений, сетевых конфигураций и защищенные паролем приложения (см. рис.1 в качестве примера), то сотрудники такой организации должны иметь несколько учетных записей и запоминать большое количество соответствующих паролей и логинов. Большинство таких учетных записей, зарегистрированных в разных окружениях, будут на самом деле принадлежать одному человеку. IDenium позволяет собрать воедино в одной базе данных всю информацию об учетных записях пользователя и «привязать» ее к одному пользователю, пользователю IDenium.

Принципом, лежащим в основе архитектуры IDenium, является централизованное хранение различных учетных записей пользователей в одной базе данных, легко доступной для всех приложений, требующих аутентификации пользователей. BioLink IDenium хранит учетные данные пользователей (пароли, логины и т.д.) и передает их приложениям, требующим эти данные, после предъявления пользователем биометрических идентификаторов.

Если предъявленные биометрические идентификаторы совпадают с теми, что хранятся в базе данных IDenium, то соответствующие учетные данные (логин и пароль) посылаются системой IDenium приложению, потребовавшему их. Далее приложение уже самостоятельно управляет полученными учетными данными. Только от конечного приложения и его правил доступа зависит, получит ли пользователь право выполнить требуемое ему действие (войти в операционную систему, получить право работать с защищенными ресурсами и т.д.). IDenium не влияет на политики безопасности, устанавливаемые конечными приложениями. Задача IDenium состоит в возврате корректных учетных данных пользователей в ответ на полученные биометрические идентификаторы.

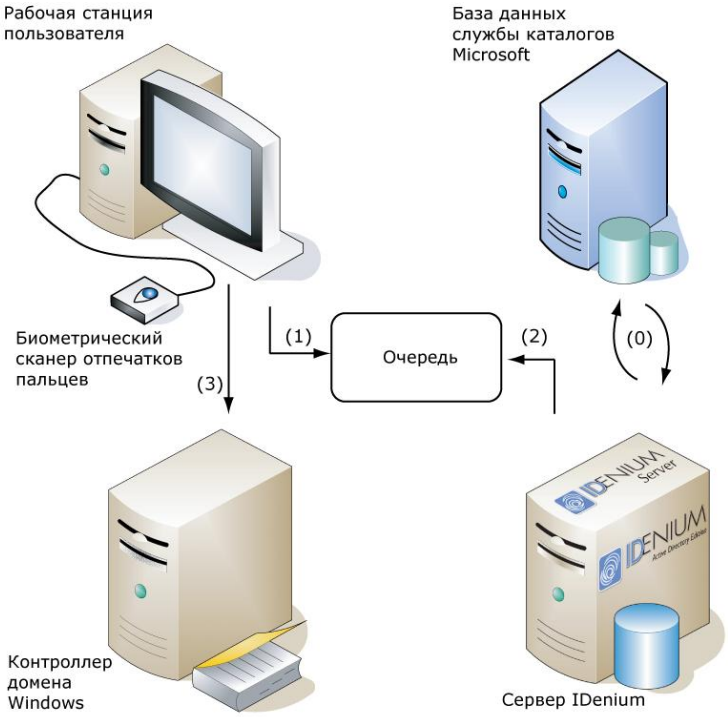


Рисунок 3. Принцип, лежащий в основе BioLink IDenium (в качестве примера использована сеть Microsoft Windows)

Рассмотрим подробнее схему, изображенную на рисунке 3. В первую очередь обратите внимание, что синхронизация биометрических идентификаторов осуществляется между службой каталогов Microsoft Active Directory и сервером IDenium - (0). Все операции сравнения выполняются сервером IDenium.

Предположим, что пользователю требуется предъявить свои учетные данные для доступа к какому-либо клиентскому приложению. Вместо того чтобы вводить имя пользователя и пароль, пользователь прикладывает свой палец к сканеру отпечатков пальцев. Полученные биометрические идентификаторы посылаются на сервер IDenium с использованием «Очереди сообщений». С технической точки зрения, клиентское приложение инициирует запрос на идентификацию (включающий биометрические идентификаторы) и помещает его в «Очередь» - (1). Сервер IDenium постоянно извлекает поступающие запросы на идентификацию, обрабатывает их и возвращает результаты сравнения - (2). При нахождении совпадения в возвращаемых результатах будут содержаться учетные данные пользователя. Как только результаты становятся доступными, приложение, инициировавшее запрос, извлекает эти результаты из «Очереди».

Клиентское приложение пересылает полученные результаты контроллеру домена для аутентификации - (3). В зависимости от результатов аутентификации на контроллере домена, приложение принимает решение, выполнять ли действие, запрашиваемое пользователем, или нет.

В качестве компонентов системы IDenium, компания BioLink предлагает следующие программные модули, подменяющие собой,

упоминаемое в предыдущем абзаце, понятие «клиентское приложение»:

- **BioLink IDenium Client** отвечает за доступ к компьютерам и ресурсам под управлением Microsoft Windows.
- **BioLink Citrix Logon** контролирует доступ к удаленным рабочим столам Citrix.
- **BioLink IDenium Terminal Services Components** контролирует доступ к темринальной сессии и удаленным рабочим столам Microsoft Windows.

Существует возможность «подключить» IDenium к любому пользовательскому приложению. Именно для этих целей служит пакет инструментов для разработчика **IDenium SDK** (если вы хотите получить подробную информацию об IDenium SDK и других продуктах, совместимых с IDenium, посетите официальный сайт компании BioLink, расположенный по адресу http://www.biolink.ru).

Вернемся к схеме, изображенной на рисунке 2 *Аутентификация IDenium* на стр. 4. Как видно из схемы, информация обо всех учетных записях пользователей (Windows, Citrix и других клиентских приложениях) хранятся непосредственно в базе данных Microsoft Active Directory. В результате, когда пользователь предъявляет свои биометрические идентификаторы, он/она не задумывается об именах (логинах), паролях и т.д. Пользователь просто прикладывает палец (пальцы) к сканеру отпечатков пальцев и сосредоточивается на выполнении своих собственных бизнес-задач.

Все это стало возможным благодаря использованию сервера IDenium.

2.2 IDenium Server

Сервер IDenium обрабатывает запросы, получаемые от клиентских систем, и создает ответные пакеты, содержащие учетные данные пользователя, инициировавшего запрос на идентификацию.

Отличительные характеристики сервера BioLink IDenium:

- *Удобство развертывания* – может быть развернут на любой рабочей станции под управлением операционной системы.
- *Удобство установки* - просто установите сервер IDenium на любой из компьютеров в вашей локальной сети.
- *Удобство масштабирования* – вы можете установить столько экземпляров сервера IDenium, сколько вам нужно для обеспечения максимальной производительности и отказоустойчивости.
- *Удобство администрирования* – после установки сервер IDenium НЕ требует какого-либо управления и/или вмешательства для продолжения нормальной эксплуатации. Наглядный мониторинг работы всех экземпляров серверов IDenium при помощи стандартного монитора ресурсов Microsoft Windows

Сервер IDenium был бы простым устройством для выполнения операций сравнения, если бы в него не были бы интегрированы новейшие биометрические алгоритмы компании BioLink.

2.3 Биометрические алгоритмы

Новейшие математические алгоритмы являются ядром системы BioLink IDenium.

Биометрическая часть системы реализует две основные функции:

- Считывание отпечатка пальца и его преобразование в цифровой шаблон. Цифровой шаблон хранится в базе данных Active Directory в качестве эталона. Сам отпечаток пальца по этому эталону восстановить невозможно.
- Распознавание пользователя. Для этого полученный в результате сканирования образ сравнивается с зарегистрированным ранее эталоном.

Чтобы использовать биометрическую идентификацию, отпечатки пальцев пользователей должны быть зарегистрированы в системе IDenium. Для каждого пользователя в IDenium может быть зарегистрировано до 10 отпечатков пальцев. Для каждого из них будет создан свой эталон, представляющий собой цифровой шаблон отпечатка, который впоследствии будет использоваться для идентификации пользователя. Тем самым обеспечивается непревзойденный уровень безопасности, так как невозможно восстановить реальное изображение отпечатка пальца из цифрового шаблона. Этот шаблон, вместе с другими данными системы IDenium, хранится базе данных Active Directory и используется в случае поступления запроса на аутентификацию от пользовательских приложений.

2.4 Масштабирование

Масштабируемость является отличительной особенностью системы IDenium в целом и сервера IDenium в частности.

Если у вас небольшая компания, и вы планируете поэтапное развертывание IDenium (например, на первом этапе вы развертываете систему только в IT департаменте), для вас будет выгодно купить один сервер IDenium и легко опробовать систему в работе.

Вы можете быть уверены в том, что когда вам потребуется расширить систему и установить IDenium во всей корпоративной сети, все что вам нужно будет сделать, это купить столько серверов IDenium, сколько необходимо для быстрой аутентификации ваших пользователей.

Также расширение IDenium, скорее всего, потребуется в случае, если у вас возрастет число используемых клиентских приложений, требующих аутентификации пользователей. В этом и других случаях (например, значительное увеличение числа рабочих станций в сети, расширение компании, открытие еще одного офиса) скорость обработки биометрических запросов может существенно снизиться. Решение данной проблемы простое: покупайте и развертывайте столько серверов IDenium, сколько вам необходимо для того, чтобы повысить пропускную способность сети и довести скорость обработки биометрических запросов до приемлемого уровня (т.е. такого уровня, когда обработка запросов происходит незаметно для конечного пользователя и не отнимает его/ее драгоценное рабочее время).

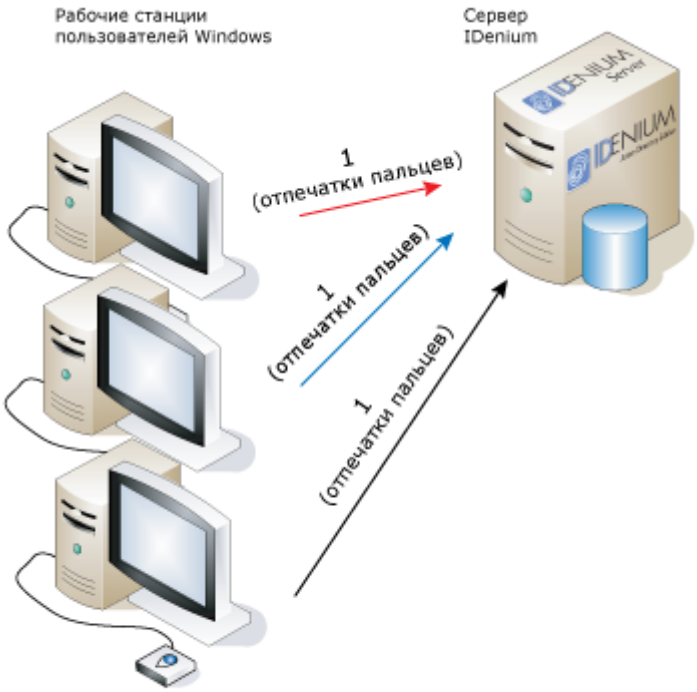


Рисунок 4. Сегмент сети с одним сервером IDenium

Вы можете установить столько серверов IDenium, сколько требуется. Каждый дополнительный сервер IDenium значительно увеличивает скорость получения и сравнения биометрических идентификаторов.

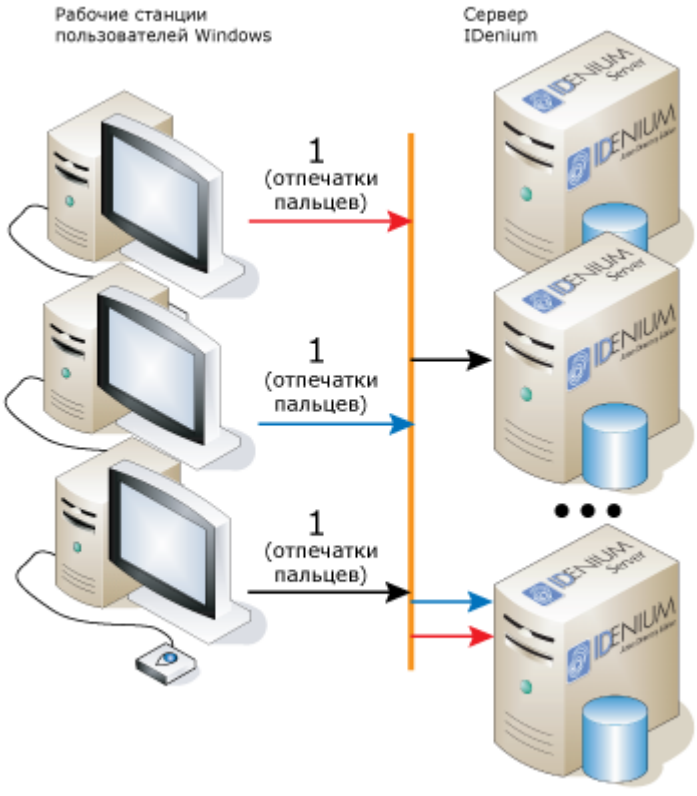


Рисунок 5. Сегмент сети с несколькими серверами IDenium

Как видно из рисунка выше все запросы, поступающие от рабочих станций пользователей, обрабатываются серверами IDenium в случайном порядке.

Репликация

Так как все учетные данные хранятся в Active Directory — не важно, сколько контроллеров домена в вашей сети, благодаря стандартным механизмам Active Directory, все данные системы IDenium (учетные записи, учетные данные, биометрические идентификаторы пользователей) автоматически реплицируются. Кроме того, BioLink IDenium поддерживает технологию сайтов в службе каталогов.

2.5 Отказоустойчивость

Система BioLink IDenium является полностью отказоустойчивой системой. Это достигается с помощью установки в вашей корпоративной сети нескольких серверов IDenium (подробнее см. раздел *Масштабирование* на стр. 9).

Несколько серверов IDenium

Для обеспечения отказоустойчивости вам необходимо иметь не менее двух серверов IDenium.

Распределение нагрузки между серверами IDenium выполняется автоматически

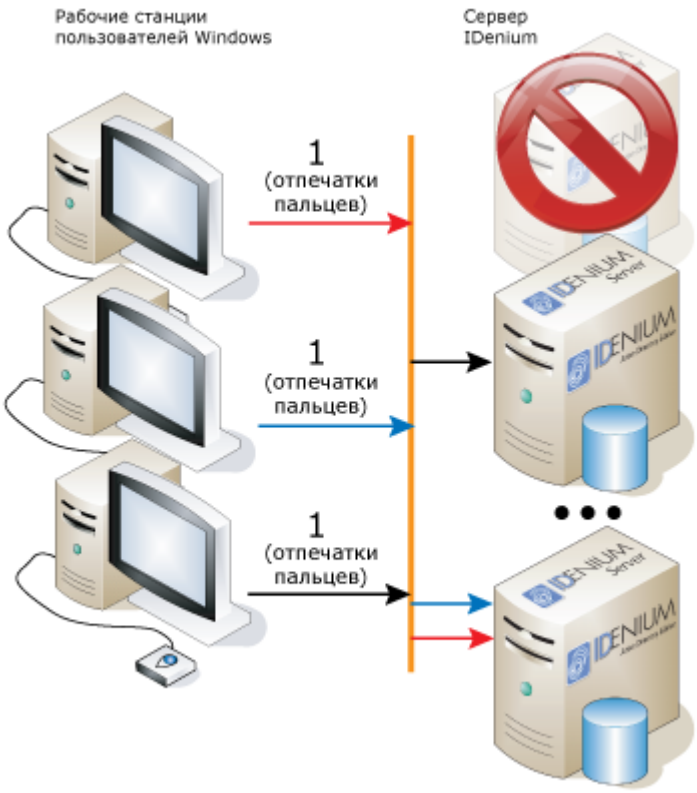


Рисунок 6. Отказоустойчивость IDenium

Кэши

Использование **кэшэй** является вторым способом обеспечения отказоустойчивости системы IDenium.

Кэши IDenium работают следующим образом: после того, как рабочая сессия текущего пользователя была успешно установлена, биометрические идентификаторы помещаются к кэш, расположенный на локальном жестком диске компьютера пользователя. В случае недоступности сервера IDenium, для доступа в операционную систему, используются идентификаторы, сохраненные в кэше.

Следует обратить внимание на то, что использование кэшей снижает общий уровень безопасности вашей системы. Поэтому включение кэшей следует производить только в том случае, если это действительно необходимо.

2.6 Шифрование и защита данных

Для защиты от перехвата и дешифрирования биометрических данных, совместно с протоколом SSL, IDenium использует права доступа Microsoft Active Directory. Это обеспечивает высокий уровень защиты и легко интегрируются с механизмами шифрования уже используемыми в корпоративной сети предприятия.

Все каналы передачи данных, по которым идет взаимодействие клиентских приложений с сервером IDenium, зашифрованы. Таким образом, обеспечивается то, что потоки, содержащие биометрическую информацию, не могут быть перехвачены, декодированы или каким-либо другим образом подвержены риску.

Вся информация, находящаяся в хранилище IDenium, также кодируется. К тому же отпечатки пальцев хранятся не в виде изображений, а в виде специальных закодированных цифровых шаблонов. Восстановить исходное изображение реального отпечатка пальца из этих шаблонов невозможно. Таким образом, дешифрование информации, находящейся в хранилище IDenium, становится достаточно сложной задачей.

3. Семейство продуктов IDenium

Система IDenium включает в себя различные программные компоненты, предназначенные для решения определенных задач, специфичных для отдельно взятого бизнес процесса. Все компоненты IDenium объединяет использование передовых математических алгоритмов, разработанных компанией BioLink.

4. IDenium для Active Directory

Почти везде, где в качестве операционной системы используется программное обеспечение Microsoft Windows, применяется служба каталогов Microsoft Active Directory для административного управления сетевыми объектами. Active Directory идеально подходит для сетей с географически распределенной инфраструктурой. Решение **IDenium** позволит поднять безопасность и защиту данных в таких сетях на новый, раньше не достижимый уровень.

В следующих разделах дается описание функциональных возможностей и отличительных особенностей развертывания и использования системы BioLink IDenium в сетях Microsoft Windows.

4.1 Архитектура IDenium для Active Directory

IDenium для Active Directory предназначен для повышения безопасности и эффективного использования стандартных средств защиты операционных систем семейства Windows

Применение BioLink IDenium для Active Directory, нацелено, прежде всего, на решение следующих задач:

- **Аутентификация пользователей в географически распределенных сетях масштаба предприятия** - благодаря тому, что процессом репликации данных между различными доменами управляет Active Directory;
- **Упрощение работы пользователя** - благодаря использованию стандартного дружелюбного Windows-интерфейса для управления учетными записями пользователей и биометрическими данными;
- **Повышение уровня отказоустойчивости системы** - благодаря тому, что процессом создания резервных копий биометрических данных, хранящихся на сервере IDenium, управляет Active Directory.

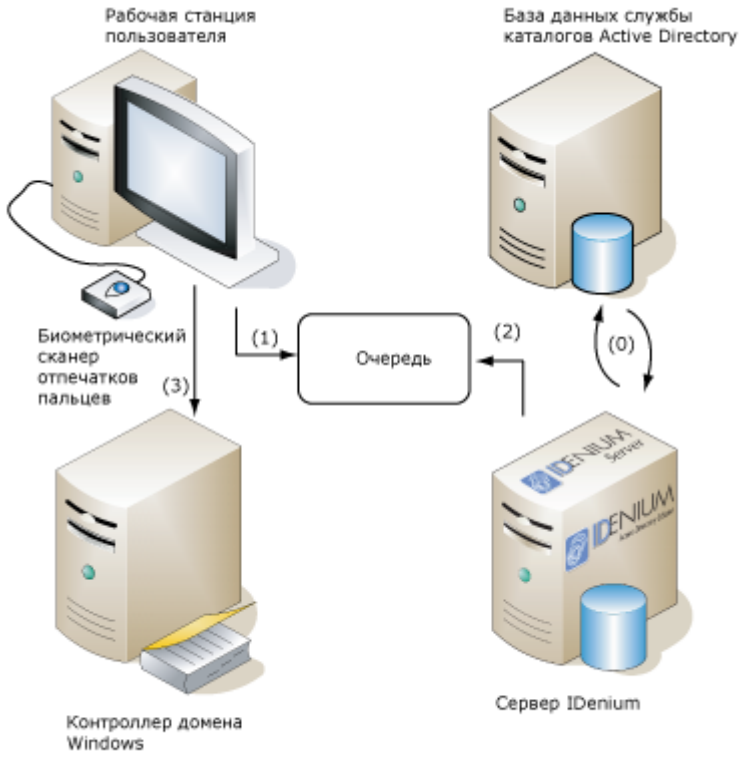


Рисунок 7. Механизмы работы IDenium для Active Directory

Рассмотрим схему, изображенную на рисунке выше. Стрелки № 0-3 обозначают те же действия, что были описаны в разделе *Архитектура IDenium* на стр.7. Единственное отличие заключается в том, **что в качестве Хранилища данных IDenium выступает Active Directory**. Также все очереди, созданные сервером (ами) IDenium также контролируются AD, избавляя администратора сети от необходимости устанавливать какие-либо дополнительные компоненты.

Механизм работы IDenium для Active Directory выглядит следующим образом:

1. Когда пользователь хочет получить доступ к ресурсам Windows-сети, он прикладывает свой палец к сканеру отпечатков пальцев.
2. Рабочая станция пользователя создает *запрос на идентификацию*, включающий зашифрованный цифровой шаблон отпечатка пальца, и размещает его в очереди AD.
3. IDenium server проверяет наличие новых запросов в очереди и в случае обнаружения последних извлекает их для обработки. Обработка включает в себя сравнение полученного цифрового шаблона отпечатка пальма с хранящимися в базе данных. В случае обнаружения совпадения, сервер IDenium возвращает учетные данные пользователя (имя пользователя (логин) и пароль).
4. Рабочая станция, инициировавшая запрос на идентификацию, получает учетные данные пользователя и, в свою очередь, отправляет их контроллеру домена для аутентификации.

5. В результате, в зависимости от соответствующих правил и/или (групповых) политик безопасности пользователь получает (или не получает) доступ к запрашиваемым ресурсам.

Далее архитектура IDenium для Active Directory рассматривается более подробно. В частности речь идет об усложненном варианте использования системы, когда сеть предприятия состоит их двух (и более) географически удаленных доменов (см. рисунок ниже).

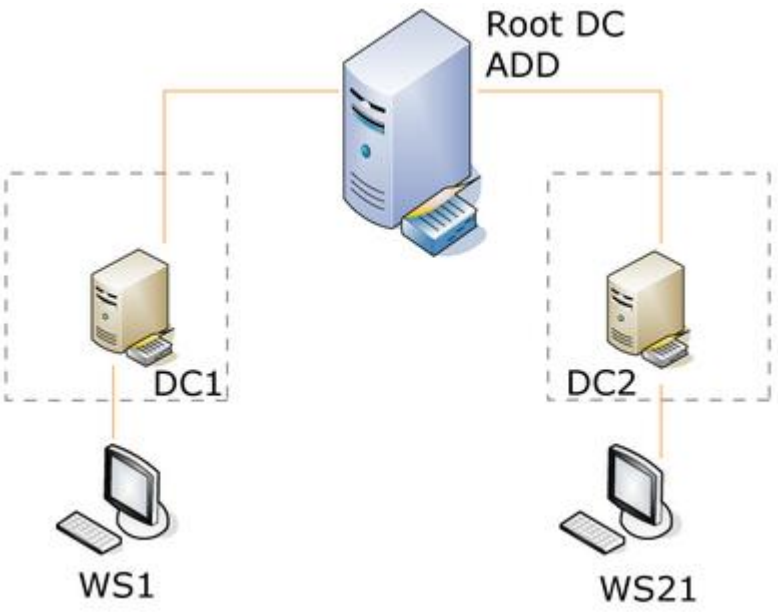


Рисунок 8. Географически распределенная корпоративная сеть с двумя доменами

IDenium эффективно интегрируется в такие сети, позволяя пользователю Домена 1 (обозначенного DC1 на рисунке выше), легко получить доступ к ресурсам Домена 2 (DC2) с помощью своего отпечатка пальца.

Схема ниже подробно иллюстрирует архитектуру IDenium для Active Directory в географически распределенной корпоративной сети (см. Рисунок 7. Механизмы работы IDenium для Active Directory и Рисунок 8. Географически распределенная корпоративная сеть с двумя доменами)

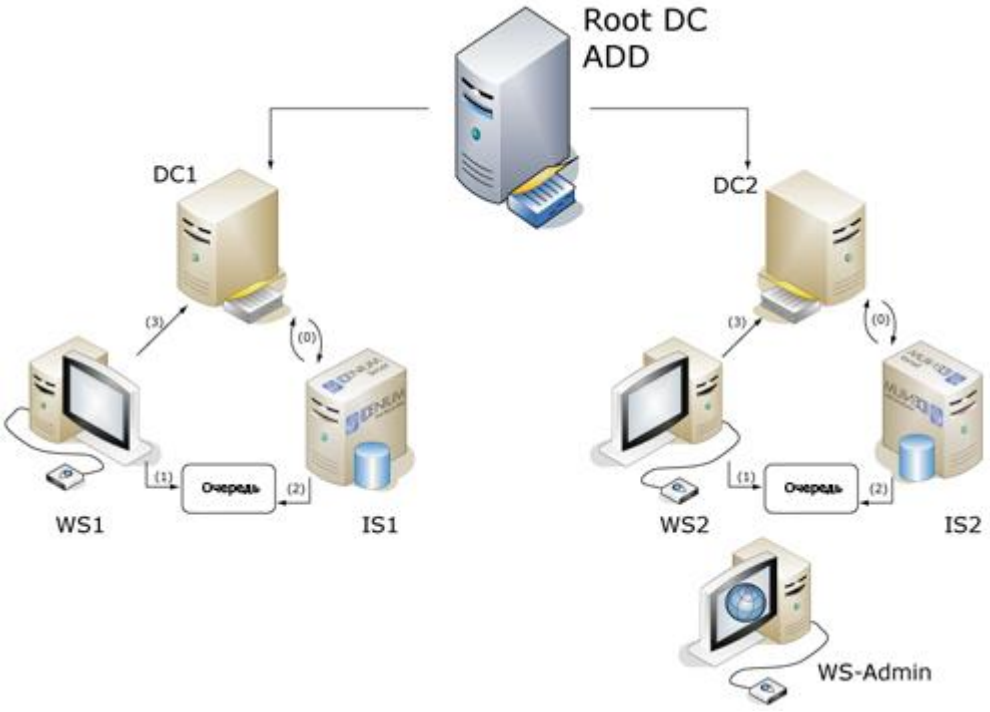


Рисунок 9. Архитектура IDenium для Active Directory

Расшифровка сокращений:

- WS1 – рабочая станция Домена 1.
- IS1 – сервер IDenium в Домене 1.
- DC1 – контроллер Домена 1.
- ROOT DC – корневой домен контроллер.
- ADD – Active Directory Database (база данных Active Directory).
- WS2 – рабочая станция Домена 2.
- IS2 – сервер IDenium Домена 2.
- DC2 – контроллер Домена 2.
- WS-Admin – рабочее место администратора локальной сети.

Пояснения к рисунку:

- Администратор локальной сети (WS-Admin) может управлять всеми учетными записями, расположенными на любом из IDenium серверов, входящих в текущую локальную сеть. С помощью Active Directory администратор может осуществлять управление всей распределенной структурой Active Directory, в том числе и учетными записями пользователей, разрешая или запрещая им использовать отпечатки пальца для доступа к ресурсам сети.

4.2 Компоненты IDenium для Active Directory

BioLink IDenium для Active Directory - это распределенная система, состоящая из компонентов устанавливаемых как на серверах, так и на клиентский рабочих станциях.

Клиентские приложения

В клиентскую часть IDenium для Active Directory входят следующие приложения:

- **BioLink IDenium Windows Logon** - отвечает за аутентификацию пользователя во время доступа к рабочему компьютеру.
- **BioLink Admin Pack** - предназначен для системных администраторов, позволяя им централизованно управлять биометрическими идентификаторами пользователей, конфигурировать клиентские рабочие станции, настраивать политики доступа и выполнять другие задачи администрирования IDenium.

Серверные приложения

Серверная часть IDenium включает в себя следующие программно-аппаратные модули:

- **Синхронизатор паролей** - обеспечивает синхронизацию учетных данных пользователей, хранящихся в каталогах Active Directory и на серверах BioLink IDenium).
- **Сервер BioLink IDenium** - является ядром системы биометрической аутентификации пользователей; в его функции входят обработка клиентских запросов, выполнение операций сравнения и передача готовых пакетов, содержащих учетные данные пользователей. Отличительными особенностями сервера являются наивысший уровень защиты конфиденциальных данных от несанкционированного доступа и быстрая обработка одновременно поступающих запросов.

4.3 Рекомендации по установке IDenium для Active Directory

Установить и развернуть IDenium для Active Directory не так сложно, как может показаться с первого взгляда. Конечно, перед тем как приступать к установке системы, вся сетевая инфраструктура должна быть спланирована, развернута и настроена соответствующим образом в зависимости от предъявляемых требований и ваших предпочтений. Рекомендуется также, по возможности, заранее настроить все групповые политики и права пользователей. И, наконец, до установки IDenium необходимо убедиться в том, что вся ваша сеть корректно функционирует и все работает именно так, как вы запланировали.

Только после этого можно устанавливать IDenium для Active Directory.

Развертывание IDenium для Active Directory в сети вашей компании необходимо проводить в следующей последовательности:

1. **Этап 1. Расширение схемы Active Directory**. На первом этапе выполняется добавление необходимых атрибутов и регистрация компонент IDenium в службе каталогов Active Directory.
2. **Этап 2. Установка компоненты Синхронизатор паролей**. На втором этапе на каждый контроллер домена в сети устанавливается компонент Синхронизатор паролей.

3. **Этап 3. Установка сервера BioLink IDenium**. На третьем этапе устанавливается сервер BioLink IDenium на любом компьютере под управлением операционной системы Microsoft Windows, входящем в локальную сеть.
4. **Этап 4. Установка программного обеспечения администратора Admin Pack**. На выделенном рабочем месте, подключенном к домену, разворачивается пакет программного обеспечения BioLink IDenium Admin Pack для работы администратора IDenium.
5. **Этап 5. Установка программного обеспечения BioLink IDenium Windows Logon на рабочих станциях пользователей.** Завершающий этап установки IDenium, в ходе которого выполняется установка клиентских компонент IDenium на рабочие места пользователей.

4.4 Системные требования IDenium для Active Directory

Системные требования можно разделить на четыре категории, а именно:

- **Требования к клиентским рабочим станциям** - все рабочие станции конечных пользователей должны удовлетворять этим требованиям. Кроме того, каждая клиентская рабочая станция должны быть оснащена биометрическим сканером отпечатков пальцев.
- **Требования к рабочей станции администратора** - роль рабочей станции администратора может играть либо компьютер администратора, либо отдельная рабочая станция, специально выделенная для решения задач по администрированию IDenium. Если у администратора будет право вводить в систему отпечатки пользователя, то необходим также сканер отпечатков пальцев.
- **Требования к серверу IDenium**
- **Требования к контроллеру домена** - настоятельно рекомендуется, чтобы все контролеры домена удовлетворяли этим требованиям.
- **Поддерживаемые биометрические устройства**.

Требования к клиентской рабочей станции

- Операционная система Microsoft Windows 2000 (с 4-ым пакетом обновлений) / XP (со 2-ым пакетом обновлений)/ 2003 (со 2-ым пакетом обновлений) / Vista / 7
- Персональный компьютер с процессором Pentium IV 1500 МГц или выше
- Объем памяти не менее 256 Мбайт (рекомендуется 512 Мбайт)
- 200 Мбайт свободного места на жестком диске (зависит от типа операционной системы)
- Дисковод для чтения CD-ROM (необходим для установки BioLink IDenium для Active Directory с компакт-диска)
- Сетевой адаптер

- USB-порт для подключения устройства сканирования отпечатков пальцев

Требования к рабочей станции администратора

- Операционная система Microsoft Windows Server 2000, 2003/ 2008 или Microsoft Windows 2000 (с 4-ым пакетом обновлений), XP (со 2-ым пакетом обновлений) с дополнительно установленной консолью для управления Active Directory
- Персональный компьютер с процессором Pentium IV 1500 МГц или выше
- Объем памяти не менее 512 Мб
- 200 Мб свободного места на жестком диске
- Дисковод для чтения CD-ROM (необходим для установки с компакт-диска BioLink)
- Сетевой адаптер
- USB-порт для подключения устройства сканирования отпечатков пальцев

Требования к контроллерам домена

Все контроллеры домена в сети, где будет развернута система IDenium для Active Directory должны удовлетворять следующим минимальным системным требованиям:

- Операционная система Microsoft Windows Server 2000 (с 4-ым пакетом обновлений), 2003 (со 2-ым пакетом обновлений); 2008 (со 2-ым пакетом обновлений)
- Персональный компьютер с процессором Pentium IV 3000 МГц или выше;
- Объем памяти не менее 512 Мб;
- 200 Мб свободного места на жестком диске.

Требования к серверам BioLink IDenium

Компьютеры, на которые планируется устанавливать сервера BioLink IDenium, должны удовлетворять следующим минимальным требованиям:

- Операционная система Microsoft Windows 2000 (с 4-ым пакетом обновлений), XP (со 2-ым пакетом обновлений), 2003, 2008 (со 2-ым пакетом обновлений), Vista;
- Персональный компьютер с процессором Pentium IV 3000 МГц или выше;
- Объем памяти не менее 1024 Мб;
- 200 Мб свободного места на жестком диске.

Поддерживаемые биометрические устройства

BioLink IDenium для Active Directory поддерживает следующие устройства:

- Мышь BioLink USB U-Match Mouse со встроенным сканером отпечатков пальцев

- Сканер отпечатков пальцев BioLink U-Match MatchBook 3.5
- Сканер отпечатков пальцев BioLink U-Match MatchBook. 5.0
- Сканер отпечатков BioLink U-Match BI USB
- Встроенный сканер UPEC

5. Обслуживание и работа с IDenium

Система IDenium дружелюбна к пользователю и не требует каких-либо специальных навыков или отдельного обучения. Все задачи по администрированию системы могут быть выполнены с помощью стандартных утилит базовой операционной системы. Например, управления IDenium для Active Directory происходит с помощью консоли Active Directory Пользователи и компьютеры.

5.1 Журналирование

Система IDenium позволяет администратору просматривать информацию обо всех действиях, совершенных системой, в виде наглядного журнала событий.

В журнал записываются следующие события, произошедшие в пределах системы:

- создание пользователя;
- регистрация биометрических идентификаторов;
- аутентификация пользователя и доступ к запрашиваемым ресурсам;
- синхронизация учетных записей пользователей и т.д.

Администратор может просматривать Журнал событий IDenium с помощью стандартной консоли **Управление компьютером**. Журнал позволяет проводить диагностику системы, обнаруживать, отслеживать и устранять ошибки, получать дополнительную (внутреннюю) информацию о событиях и операциях IDenium и выполнять другие операции по обслуживанию системы.

5.2 Монитор производительности IDenium

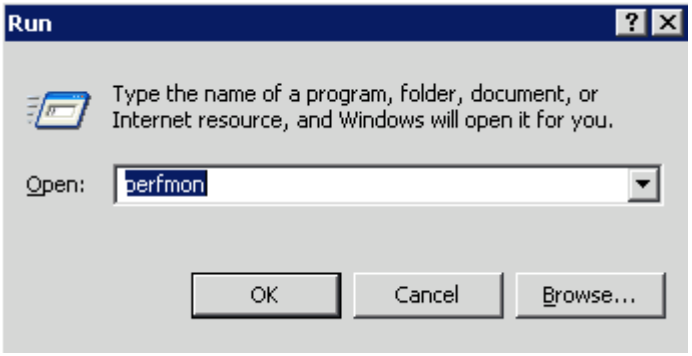
Для отслеживания нагрузки на сервер BioLink IDenium и его производительности, можно воспользоваться встроенным компонентом Windows **Монитор наджености и производительности.**

Для запуска моинтора производительности сервера BioLink IDenium, ыполните следующие действия:

I. Нажмите кнопку "Пуск"(Start)

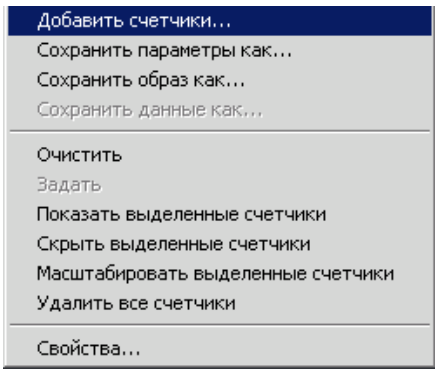
II. Выберите пункт "выполнить" (Run)

III. Введите `perfmon`



IV. У вас откроется окно Системный монитор или Монитора наджености и производительности Windows, взависимости от версии вашей ОС.

V. Кликните правой кнопкой мышке в пустой области монитора и выберети пункт **Добавить счетчики**кни



VI. В появившемся окне, вы можете ввести имя или IP адрес ПК, на котором установлен сервер BioLink IDenium, а так же необходимые счетчики.

5.3 Удаление

В том случае, если вы хотите вернуться к сетевой конфигурации, не предполагающей биометрической аутентификации, программное обеспечение IDenium может быть полностью удалено. В начале должны быть удалены клиентские компоненты IDenium с рабочих станций конечных пользователей. Затем удаляются серверные программные модули.

Однако, , так как процесс модификации схемы Microsoft Active Directory является необратимым, то удалить объекты IDenium из схемы AD невозможно. Единственным способом вернуться к предыдущей конфигурации схемы, это восстановить ее из резервной копии, однако, все изменения, сделанные после создания резервное копии, будут потеряны.

5.4 Устранение неисправностей и техническая поддержка

В случае возникновения каких-либо вопросов, обращайтесь в службу Технической поддержки компании BioLink (support@biolink.ru).