Руководство администратора BioLink IDenium для Active Directory

Содержание

1 Авторские права

Данное программное обеспечение (далее "Программа") является собственностью BioLink Solutions. Программа защищена законами и международными соглашениями об авторских правах, а также другими законами и договорами, регулирующими отношения авторского права. Запрещается производить декомпиляцию или восстановление исходного кода Программы.

Настоящий документ может быть изменен без уведомления в результате совершенствования или изменения Программы. Содержащаяся в документе информация является интеллектуальной собственностью BioLink Solutions и передается клиенту на конфиденциальной основе. BioLink Solutions не гарантирует отсутствие неточностей и опечаток в данном документе. При обнаружении неточностей в документации, сообщайте о них, пожалуйста, в службу технической поддержки.

Настоящий документ может содержать ссылки на веб-сайты, которые были действительны на момент публикации документа, но могут быть изменены или стать неактивными впоследствии. Настоящий документ может содержать ссылки на сайты в Интернет, принадлежащие и поддерживаемые сторонними организациями. BioLink Solutions не несет ответственности за содержимое сайтов сторонних организаций.

Любое воспроизведение, копирование, сохранение или передача данной публикации полностью или частично, в любой форме и с использованием любых средств: электронных, механических, фотокопировальных и др. без предварительного письменного согласия со стороны BioLink Solutions запрещено.

BioLink® является товарным знаком BioLink Solutions. U-Match® является зарегистрированным товарным знаком BioLink Solutions. Любые товарные знаки, упомянутые в данном руководстве, являются либо товарными знаками, либо зарегистрированными товарными знаками соответствующих владельцев. BioLink Solutions признает все права компаний, имеющих зарегистрированные товарные знаки.

Биолинк Солюшенс
125493, Россия, г. Москва,
ул. Авангардная, 3
Тел: +7 (495) 645-87-03 (-04,-05)
Техническая поддержка: +7 (495) 645-87-03 (-04,-05)

Контактная информация
службы технической поддержки:

support@biolinksolutions.com
Веб-сайт: http://support.biolinksolutions.com

2 Предисловие

Добро пожаловать в BioLink IDenium! **Система биометрической аутентификации пользователей BioLink IDenium** (далее IDenium) позволит эффективно использовать стандартные средства защиты операционных систем семейства Windows благодаря применению одной из самых эффективных технологий распознавания пользователей - по отпечатку пальца.

Данный документ предназначен для системных администраторов и содержит информацию о системе BioLink IDenium для Active Directory, включающей в себя программные компоненты, оптимизированные для работы в сетях Microsoft Windows.

Эта глава содержит рекомендации о том, как наилучшим образом воспользоваться данным *Руководством администратора IDenium* при выполнении ежедневных задач. В ней представлено краткое описание содержимого каждой главы с целью помочь читателю сориентироваться, которая из них может представлять для него наибольший интерес. Глава знакомит с терминами, сокращениями и системой условных обозначений, используемых в данном документе, и содержит ссылки на дополнительные источники знаний о продукции BioLink Solutions и контактную информацию для оперативной связи с представителями компании в случае необходимости.

2.1 О Руководстве администратора

В настоящем *Руководстве администратора* представлена информация о BioLink IDenium для Active Directory. Руководство включает в себя также обзор основных особенностей системы IDenium для Active Directory и подробные рекомендации по использованию IDenium для Active Directory при решении различных задач, с которыми сталкивается пользователь в своей работе.

Данное руководство включает в себя следующие главы:

- *Глава 1, Предисловие*. Настоящая глава рассказывает о том, как использовать данное **Руководство администратора IDenium** для знакомства с системой, а также содержит информацию о том, где можно получить дополнительную информацию о продукте.

- *Глава 2, Общие сведения*. В этой главе представлена обзорная информация по системе; ее компонентах и совместимых с нею программах. Из этой главы вы узнаете о назначении системы BioLink IDenium, системных требованиях и основных принципах работы данного продукта. Также эта глава содержит основные сведения об Active Directory, расшифровку сокращений, объяснение терминов и понятий.

- *Глава 3, Установка и начало работы*. В этой главе кратко рассказывается о способах развертывания системы, порядке установки и первого запуска системы.

- *Глава 4, Настройка серверных компонент IDenium*, содержит сведения, необходимые системному администратору для настройки серверных компонент IDenium. Также из этой главы вы узнаете о лицензировании IDenium.

- *Глава 5, Управление пользователями IDenium*, включает в себя как общую информацию, так и подробные инструкции по добавлению и удалению пользователей IDenium, по администрированию различных типов идентификаторов пользователей (пароль, отпечаток пальца и др.), а также выполнению других задач по управлению системой.

2.2 Комплект документации

Настоящее руководство является частью комплекта документации BioLink IDenium для Active Directory, состоящего из следующих документов:

- **Руководство пользователя.** Содержит подробные инструкции по работе пользователя с компонентом BioLink IDenium Windows Logon.
- **Руководство администратора** (настоящий документ). Детально описывает все аспекты функционирования системы BioLink IDenium для Active Directory, включая основные понятия Active Directory, концепцию работы системы IDenium для Active Directory и ее администрирование.
- **Руководство по установке**. Содержит инструкции по установке и развертыванию системы BioLink IDenium для Active Directory.

2.3 Используемые обозначения

Прежде чем приступить к работе с *Руководством*, рекомендуем ознакомиться с принятыми типографскими соглашениями по стилевому оформлению данного документа.

Вид форматирования	Тип информации
Заголовок процедуры	Пошаговые процедуры. Следуйте этим инструкциям для выполнения конкретной задачи.
Специальный полужирный	Элементы интерфейса, которые необходимо выбрать, например, пункты меню, кнопки команд или элементы списка.
Курсив	Важная информация, на которую необходимо обратить внимание или которая используется для обозначения переменных выражений, например, параметров.
ПРОПИСНЫЕ	Названия клавиш на клавиатуре, например, SHIFT, CTRL, ALT.
SHIFT+CTRL	Комбинация клавиш, при которой следует нажать и удерживать на клавиатуре сначала одну клавишу и затем нажать другую. Например: CTRL+P или ALT+F4.
`Моноширинный`	Текст исходного кода программы.

2.4 Термины и сокращения

Ниже представлен список специальных терминов и сокращений, используемых в данном документе.

- **Биометрия** [biometrics] - технология измерения и анализа физиологических и/или поведенческих особенностей человека, таких как отпечатки пальцев, характер произношения, генетический код, почерк, рисунок сетчатки глаза и др.
- **Идентификатор пользователя** [credential] - уникальная характеристика, используемая для идентификации пользователя. В различных системах идентификаторами могут являться имя пользователя, пароль или некая уникальная, присущая данному человеку характеристика, например, отпечаток пальца.
- **Отпечаток пальца** [fingerprint] - папиллярный узор пальца, используемый для распознавания его владельца. Отпечатки пальцев используются в качестве уникальных идентификаторов пользователя системы IDenium.
- **Эталон отпечатка пальца** [fingerprint template] – это цифровая модель отпечатка пальца пользователя, создаваемая с помощью средств BioLink IDenium. Эталон создается по специальной методике по результатам нескольких сканирований отпечатка пальца. Само изображение отпечатка при этом не сохраняется и не может быть восстановлено из эталона.
- **"Живой" палец** [live finger] - палец живого индивида. Биометрическая система получает его изображение посредством сканирования пальца конечного пользователя.
- **Муляж пальца** [false finger] - искусственный палец, обычно сделанный из резины или силикона, который используется для получения несанкционированного доступа к защищенным ресурсам. Устройства серии BioLink U-Match умеют отличать муляжи от "живого" пальца пользователя.
- **Сканер BioLink U-Match MatchBook** - сканер отпечатков пальцев разработки BioLink, выполненный в виде отдельного устройства, подключаемого к USB порту компьютера. Данное устройство использует шину USB 2.0, что обеспечивает быстрое и качественное сканирование отпечатков пальцев.
- **BioLink IDenium** - система аутентификации BioLink, обеспечивающая простой и в тоже время надежный, гарантирующий аутентификацию пользователя, доступ к защищенным ресурсам всего одним касанием пальца. Программное обеспечение IDenium включает в себя клиентское приложение BioLink IDenium Windows Logon и набор серверных компонент, включающих новый сервер BioLink IDenium.

- **Идентификация** [identification] – процедура распознавания пользователя путем сравнения предъявленного отпечатка с эталонами отпечатков пальцев, хранящимися в базе данных (так называемое сравнение "один ко многим").
- **Аутентификация** [authentication] (или "верификация") – это процедура подтверждения того, что пользователь является тем, кем он себя называет. Подтверждение основывается на результатах сравнения предъявленного пользователем отпечатка с эталоном, зарегистрированным ранее (сравнение "один к одному").
- **Пользователь IDenium** [IDenium user] – обычный пользователь домена, учетные данные которого расширены за счет добавления биометрических идентификаторов. Для такого пользователя доступ к различным операционным системам производится путем замены буквенно-цифрового пароля на использование цифровых моделей уникальных биометрических признаков, носителем которых является человек, пользователь IDenium. Такими признаками являются, например, отпечатки пальцев. Они уникальны и специфичны для каждого пользователя IDenium, что позволяет использовать их в качестве надежного средства распознавания и аутентификации пользователей IDenium для доступа к различным ресурсам операционных систем.
- **Active Directory** – это служба каталогов, разработанная корпорацией Microsoft и основанная на сервисах LDAP. Active Directory хранит сведения об объектах сети и упрощает поиск и использование этих сведений пользователям и администраторами. В Active Directory основой для логической, иерархической организации сведений каталога служит структурированное хранилище данных. Это хранилище данных, называемое также каталогом, содержит сведения об объектах Active Directory. В число этих объектов обычно входят общие ресурсы, такие как серверы, тома, принтеры, а также учетные записи сетевых пользователей и компьютеров.
- **АРМ** - автоматизированное рабочее место.

2.5 Контактная информация

Дополнительную информацию о компании BioLink Solutions можно найти в Интернете по адресу:

[для русской версии документации] http://www.biolink.ru

[для английской версии документации] http://www.biolinksolutions.com

За технической поддержкой обращайтесь:

http://support.biolinksolutions.com

3 Общие сведения

Стремительное развитие и распространение информационных технологий и персональных компьютеров чрезвычайно обострило проблему безопасности данных. Традиционно используемая защита по паролю уже не способна обеспечить должного уровня безопасности информационных ресурсов. Пароли, секретные коды, персональные идентификационные номера (PIN-коды) - все то, что пользователь должен знать - может быть легко забыто, скомпрометировано, использовано другими лицами или украдено. Поскольку "парольные" системы не обеспечивают надежной верификации пользователя, никогда нет возможности знать точно, кем был введен пароль: законным пользователем системы или злоумышленником. Кроме того, бесчисленное количество имен и паролей, которое приходится запоминать, создает пользователям дополнительные проблемы. Не удивительно, что многие из них предпочитают использовать один пароль для всех приложений, даже в ущерб безопасности.

Для того чтобы освободить пользователя от "парольной перегрузки" и избавить от неудобств и отсутствия надежной защиты, связанных с "парольными" системами, BioLink предлагает альтернативные решения, основанные на использовании не требующих ввода пароля биометрических программных и аппаратных средств защиты ПК и сетей. Биометрические устройства, разработанные компанией BioLink в сочетании со специализированным программным обеспечением производства BioLink, позволяют заменить ввод пароля удобной процедурой снятия отпечатка пальца и таким образом обеспечить более высокую защиту ресурсов на вашем компьютере и в сети лишь одним касанием пальца.

3.1 Назначение IDenium

BioLink IDenium - это биометрическая система аутентификации пользователей, которая позволяет значительно эффективнее использовать стандартные средства защиты вашего сетевого 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 пользователя и оптимизировать соответствующие бизнес-процессы на предприятии.

3.1.1 Назначение BioLink IDenium

Программный комплекс **BioLink IDenium** полностью интегрирован со службой каталогов Active Directory корпорации Microsoft и предназначен для замены традиционного способа аутентификации пользователя по паролю аутентификацией по биометрическим характеристикам, в частности по отпечатку пальца, с целью повышения общего уровня безопасности информационных систем.

Выполняемые программным комплексом BioLink IDenium функции включают в себя:

- замена громоздкой и уязвимой парольной системы надежной и удобной биометрической идентификацией (по отпечаткам пальцев);
- эффективное разграничение доступа к информационным ресурсам корпоративных сетей;
- централизованное управление правами и полномочиями пользователей и жизненным циклом их учетных записей;
- мониторинг, протоколирование и аудит процессов управления доступом к информационным ресурсам;
- однократная регистрация пользователей и их биометрических идентификаторов с последующим предоставлением зарегистрированным пользователям доступа к информационным ресурсам сети с любого из входящих в ее состав компьютеров;
- замена авторизации в прикладных приложениях и на веб-сайтах по имени пользователя и паролю на биометрическую идентификацию.

3.1.2 Преимущества IDenium для Active Directory

Основными **преимуществами IDenium для Active Directory** являются:

- повышение уровня информационной безопасности;

- сокращение трудозатрат пользователей, освобождаемых от необходимости помнить и вводить пароли;
- упрощение процедуры идентификации пользователей при соблюдении требований защиты информации;
- снижение (на 80-90%) нагрузки на администраторов благодаря уменьшению числа обращений пользователей, «забывших» или утративших пароли и материальные идентификаторы.

3.2 Общая информация об Active Directory

Ниже приводится справочная информация, касающаяся Microsoft Active Directory.

3.2.1 Что такое Active Directory?

Active Directory (AD) - это разработка корпорации Microsoft, реализующая службу каталогов LDAP (Lightweight Directory Access Protocol - упрощенный протокол доступа к сетевым каталогам) в среде Windows. Active Directory позволяет администраторам работать с корпоративными сетями, определять в них политики, правила доступа к сетевым ресурсам, устанавливать различное программное обеспечение и критические обновления на все компьютеры в сети. AD хранит данные и соответствующие настройки в централизованной, хорошо структурированной и доступной базе данных. AD может быть развернута как в небольших сетях (несколько сотен объектов), так и в крупных сетях масштаба предприятия, включающих несколько миллионов объектов.

3.2.2 Структура Active Directory

Active Directory предоставляет способ для разработки структуры каталога. При описании каталога Active Directory использует две структуры:

- **Физическая структура** Active Directory представляет собой файл, расположенный на жестком диске каждого контроллера домена, который содержит эту службу.
- **Логическая структура** Active Directory представляет собой контейнеры, содержащие объекты службы каталога.

3.2.2.1 Логическая структура

Логическая структура образуется за счет группирования ресурсов и позволяет искать ресурсы по именам, а не физическому расположению. База данных Active Directory содержит следующие структурные объекты:

- разделы;
- домены;
- деревья доменов;
- леса;
- сайты;
- организационные единицы.

Пространство имен. Как и любая служба каталогов, Active Directory в первую очередь является пространством имен. Пространство имен (namespace) - это любая ограниченная область, где возможно разрешение имени. Разрешение имени (name resolution) - это процесс сопоставления имени некоторому объекту или информации, которую оно представляет. Пространство имен Active Directory основано на схеме именования DNS, обеспечивающей взаимодействие с Интернетом.

Объект (object) - это отличительный набор именованных атрибутов, описывающих ресурс. Атрибутами (attribute) называются характеристики объектов в каталоге. Например, атрибуты пользователя включают его фамилию, имя, отдел, адрес электронной почты. Набор атрибутов объекта определяется классом (class) объекта. Классы объектов и их атрибуты определены в схеме Active Directory. Кроме того, выделяют контейнерные объекты (container objects), они могут содержать в себе другие объекты. Например, организационная единица и домен - контейнерные объекты.

Организационное подразделение (organizational unit) - контейнерный объект, предназначенный для группировки других объектов в логические административные группы в рамках домена. Организационные единицы могут содержать такие объекты, как учетные записи пользователей, группы, компьютеры, принтеры и т.п. Иерархия организационных единиц домена не зависит от других доменов - каждый домен может поддерживать свою собственную иерархию.

Домен (domain) - основная единица логической структуры в Active Directory. Домен Active Directory является прямым аналогом домена Windows NT и предназначен для логической группировки компьютеров. Обычно группировка осуществляется по подразделениям организации, что позволяет одновременно упростить обмен данными внутри подразделения и защитить данные от изменения сотрудниками из других подразделений. Все объекты существуют только в пределах домена. Каждый домен хранит сведения только о содержащихся в нем объектах. Теоретически каталог домена может содержать более 10 миллионов объектов, на практике проверена возможность хранения порядка 1 миллиона объектов.

Дерево (tree) - это группировка или иерархия одного или нескольких доменов Windows Server 2003 (Windows 2000). Типичное дерево Active Directory может содержать один домен.

Все домены в дереве представляют единый доступ к информации и ресурсам всего дерева. В дереве имеется только один каталог, но каждый домен предоставляет свою часть каталога, содержащую информацию о "своих" объектах. В пределах дерева пользователь, зарегистрировавшийся в одном домене, может обращаться к ресурсам других доменов (в пределах назначенных ему разрешений). Windows Server 2003 осуществляет репликацию информации между доменами, обеспечивая идентичность

данных, хранимых на всех контроллерах всех доменов дерева. Кроме того, в каждом домене создается свой собственный индекс, облегчающий поиск объектов в пределах домена.

Лес (forest) - объединение одного и более деревьев - позволяет группировать сети подразделений организации или нескольких организаций, которые не используют одинаковую схему именования, работают независимо друг от друга, но должны обмениваться данными.

Все деревья в лесу используют общую схему и общий глобальный каталог (ГК). Корневые домены деревьев леса связываются доверительными отношениями, что позволяет организовать доступ из одного дерева в другое.

Схема (schema) содержит формальное описание содержания и структуры хранилища Active Directory, включая все атрибуты, классы и свойства классов. Для каждого класса объектов схема определяет, какими атрибутами должен обладать экземпляр класса, какие дополнительные атрибуты он может иметь и какой класс объектов является предком текущего класса. Схема определяет структуру леса Active Directory, который может содержать несколько деревьев Active Directory, которые, в свою очередь, могут содержать несколько иерархически структурированных доменов Active Directory. В связи с этим в лесе Active Directory один из контроллеров объявляется мастером схемы (schema master) и отвечает за репликацию данных схемы на все контроллеры доменов.

Глобальный каталог (global catalog) - это центральное хранилище информации об объектах в дереве доменов и лесе Active Directory. Содержимое глобального каталога генерируется автоматически во время стандартного процесса репликации данных между контроллерами доменов. Глобальный каталог является как службой, так и физическим хранилищем части атрибутов всех объектов леса Active Directory. Процесс частичной репликации позволяет находить большинство сведений непосредственно в глобальном каталоге, без обращения к исходному домену. По умолчанию в глобальном каталоге хранятся атрибуты, наиболее часто используемые при поиске (например, имя пользователя, его учетной записи и т. п.), а также сведения, необходимые для обнаружения объекта (полный LDAP-путь к соответствующему объекту каталога). Хранение только основных атрибутов объектов в глобальном каталоге позволяет уменьшить его размер, поэтому один сервер глобального каталога может обслуживать много контроллеров домена Windows. Следовательно, глобальный каталог позволяет найти объект в любом месте сети, даже не реплицируя информацию между контроллерами домена.

Репликация (replication) - это процесс актуализации данных, хранящихся на контроллерах домена. В процессе репликации изменения, внесенные в атрибуты и состав объектов на одном контроллере домена, переносятся на другие. После

завершения репликации каждый контроллер домена хранит актуальные сведения об объектах.

Есть несколько видов репликации:

- Полная репликация данных. Используется между контроллерами одного домена. В полной репликации участвуют все атрибуты объектов домена.
- Частичная репликация данных. Используется между контроллерами домена и сервером глобального каталога. В частичной репликации участвуют только те атрибуты объектов, которые хранятся в глобальном каталоге.
- Межсайтовая репликация. Используется между контроллерами домена, расположенными в разных сайтах. Межсайтовая репликация осуществляется реже, чем полная. При межсайтовой репликации данные аккумулируются и передаются только итоговые изменения, что уменьшает трафик репликации.

3.2.2.2 Физическая структура

Физическая структура Active Drectory - это совокупность мер, направленных на управление репликацией между контроллерами доменов Active Directory. Обычно физическая структура Active Directory соответствует структуре IP-сетей организации.

Контроллер домена (domain controller) - это компьютер под управлением Windows Server 2003 или Windows 2000 Server, хранящий реплику раздела каталога (базу данных домена). Все контроллеры домена имеют полную базу данных домена. При внесении изменений в данные каталога они фиксируются в локальной БД на контроллере домена, после чего реплицируются на другие контроллеры. Изменение некоторых критичных атрибутов (допустим, пароля пользователя) реплицируются незамедлительно.

IP-сеть - это описание некоторой IP-сети, являющейся частью сайта Active Directory. Обычно IP-сети Active Directory соответствуют IP-сетям, используемым в локальной сети организации.

Сайт (site) - это совокупность одной или нескольких IP-сетей, объединенных высокоскоростными каналами связи. Сайт может содержать один или более доменов, либо домен может быть размещен в нескольких сайтах. Сайты предназначены для управления репликацией между сетями, соединенными каналами связи с низкой пропускной способностью. Между контроллерами доменов, расположенных в одном сайте, репликация осуществляется с небольшим интервалом времени (по умолчанию - 15 минут). Репликация между сайтами осуществляется по специальному графику, настраиваемому администратором, с гораздо большим временным интервалом. Кроме того, репликация между сайтами осуществляется однократно, понижая тем самым

объем передаваемых данных. Кроме того, сайты используются клиентскими компьютерами для определения ближайшего контроллера домена, который будет использован для авторизации пользователя.

3.3 Принципы работы IDenium для Active Directory

Система **IDenium для Active Directory** полностью интегрирована со службой каталогов Microsoft Active Directory, что позволило обеспечить централизованное хранение, защиту и передачу идентификационных данных пользователей средствами самой службы. Администрирование пользователями так же централизовано и осуществляется при помощи стандартной MMC (Microsoft Management Console) оснастки Active Directory Users and Computers (ADUC).

Принцип, который положен в основу механизма работы IDenium, состоит в том, что различные устройства, способные преобразовывать биометрические характеристики индивида в цифровую форму, подключены к рабочей станции пользователя и используются в качестве одного из главных источников информации о том, кто в действительности намеревается получить доступ к различным информационным ресурсам. Биометрическая информация, получаемая этими устройствами, передается на сервер BioLink IDenium для проверки соответствия полученных данных информации, хранящейся в учетных данных пользователей IDenium.

Сервер BioLink IDenium кэширует учетные данные пользователей сети из базы данных Active Directory. Синхронизация учетных данных пользователей между базой данных Active Directory и сервером (ами) BioLink IDenium осуществляется с помощью компонента **Синхронизатор паролей**. Если пароль или другие учетные данные пользователя домена были изменены, то именно благодаря компоненту Синхронизатор паролей сервер IDenium «узнает» об этих изменениях.

При поступлении запроса на идентификацию сервер IDenium сравнивает полученные биометрические идентификаторы с хранящимися в базе данных Active Directory и, в случае нахождения совпадения, возвращает системе, инициировавшей запрос, учетные данные (имя пользователя и пароль) соответствующего пользователя.

3.3.1 Подробная информация об архитектуре IDenium для Active Directory

Рисунок ниже иллюстрирует архитектуру IDenium для Active Directory с одним сервером BioLink IDenium. Далее по тексту цифры в скобках обозначают действия, проиллюстрированные на рисунке.

Когда пользователь на своем рабочем месте прикладывает палец к сканеру отпечатков пальцев, его рабочая станция создает запрос (содержащий закодированный отпечаток пальца) на идентификацию и отправляет его выбранному случайным образом серверу IDenium.

Сервер BioLink IDenium, получив запрос, обрабатывает его. Обработка заключается в том, что сервер по очереди сравнивает полученные биометрические данные с данными уже зарегистрированных в сети учетных записей пользователей.

Все учетные записи пользователей локальной сети попадают на сервер с помощью стандартных средств AD. Если совпадение найдено, сервер возвращает клиенту учетные данные соответствующей учетной записи.

Полученные рабочей станцией учетные данные пользователя аутентифицируются с помощью **стандартных средств операционной системы**. Именно операционная система определяет, достаточно ли у пользователя прав для выполнения запрошенных операций. IDenium лишь позволяет заменить ввод имени пользователя и пароля на биометрическую идентификацию.

3.3.2 Масштабирование IDenium для Active Directory

Система IDenium легко может быть масштабирована для увеличения/снижения производительности, заключающейся в быстроте обработки запросов на идентификацию. Увеличение производительности достигается за счет установки дополнительных серверов BioLink IDenium, благодаря чему происходит распараллеливание запросов на идентификацию.

3.3.3 Биометрическая составляющая IDenium для Active Directory

Биометрическая сторона работы системы включает две основные функции:

- Считывание отпечатка пальца и его преобразование в цифровую форму. Цифровой образ хранится в хранилище Active Directory вместе с учетной записью пользователя, которому он принадлежит. Сам отпечаток пальца по этому эталону восстановить невозможно.
- Распознавание пользователя. Для этого полученный в результате сканирования образ сравнивается с зарегистрированным эталоном.

В систему может быть введено до 10 отпечатков пальцев пользователя. Для каждого из них будет создан свой эталон, который впоследствии будет использоваться для идентификации пользователя.

3.4 Компоненты BioLink IDenium

Программный комплекс BioLink IDenium представляет собой распределенную систему, состоящую из компонентов, устанавливаемых как на серверной, так и на клиентской стороне.

Программное обеспечение BioLink IDenium состоит из следующих клиентских программных компонентов:

- **BioLink IDenium Client;**
- **BioLink Admin Pack.**

Серверные компоненты BioLink IDenium включают в себя:

- **Компоненты на контроллер домена** (компонент «Синхронизатор паролей», который должен быть установлен на каждом контроллере домена);
- **BioLink IDenium Server** (может быть установлен на любом компьютере сети; после установки этот компьютер начинает обрабатывать запросы на идентификацию).

Компоненты BioLink IDenium

Внимание! Программный комплекс BioLink IDenium предназначен для установки в сетях Microsoft и использует Active Directory. Службы каталогов других производителей не поддерживаются.

3.4.1 BioLink IDenium Client

Компонента **BioLink IDenium Client** позволяет пользователям применять биометрическую идентификацию для доступа к защищенным программам и ресурсам.

BioLink IDenium Client состоит из следующих двух модулей:

BioLink Windows Logon;

BioLink Password Vault.

3.4.2 BioLink IDenium Admin Pack

Компонент **BioLink Admin Pack** требуется для развертывания необходимых компонентов IDenium для Active Directory на рабочей станции (компьютере) администратора сети для обучения (переобучения) пользователя, настройки политик и выполнения других административных задач.

Данный компонент позволит при создании новых пользователей вводить в систему их отпечатки пальцев централизованно, используя только один компьютер локального администратора сети.

BioLink IDenium Admin Pack состоит из следующих компонентов:

- Программные библиотеки добавления дополнительной вкладки в диалоговом окне Свойства объекта Active Directory;
- Биометрические компоненты для обеспечения централизованного ввода в систему отпечатков пальцев пользователей;
- Драйвера поддерживаемых устройств.

3.4.3 Синхронизатор паролей

Серверный компонент **Синхронизатор паролей** обеспечивает синхронизацию учетных данных пользователей, хранящихся в каталогах Active Directory и на серверах BioLink IDenium. Этот компонент должен быть установлен на каждом из контроллеров домена в сети.

3.4.4 Сервер BioLink IDenium

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

Отличительные характеристики сервера BioLink IDenium:

- высоко надежная защита конфиденциальных данных от несанкционированного доступа;
- быстрая обработка одновременно поступающих запросов;
- простота развертывания и масштабирования.

Все биометрические данные хранятся в базе данных AD. Репликация биометрических

данных между всеми контроллерами домена также осуществляется с помощью стандартных механизмов AD.

3.4.4.1 Установка

Сервер BioLink IDenium может быть установлен на любом компьютере сети (включая и контроллер домена). Для повышения производительности разработчики IDenium рекомендуют устанавливать сервер на выделенном компьютере.

Подробнее об установке сервера см. в разделе *Установка сервера BioLink IDenium* . **Руководства по установке IDenium**

3.4.4.2 Масштабирование

Для увеличения производительности биометрической системы существует возможность простого масштабирования IDenium. Для этого достаточно установить еще один сервер сравнений IDenium. Сразу же после установки он начнет принимать запросы на идентификацию от клиентских рабочих станций.

3.4.4.3 Лицензирование

В системе BioLink IDenium для Active Directory лицензируется **количество пользователей**, которым будет разрешено использовать биометрические идентификаторы для входа в систему и доступа к защищенным ресурсам.

Подробнее о лицензировании IDenium см. раздел *Управление лицензией сервера BioLink IDenium*.

4 Установка и начало работы

Данная глава содержит рекомендации по установке и началу работы с IDenium для Active Directory.

Разработчики IDenium рекомендуют установить клиентское программное обеспечение IDenium для Active Directory на каждой рабочей станции для обеспечения надежной защиты сети в целом.

Внимание! Каждая из рабочих станций пользователей, на которых планируется установить программное обеспечение IDenium для Active Directory должна быть включена в домен.

На рабочем месте администратора системы должен быть установлен компонент **BioLink IDenium Admin Pack**.

Внимание! На каждом контроллере домена должен быть установлен компонент **Синхронизатор паролей**.

4.1 Порядок установки BioLink IDenium

Рекомендуется установить клиентское программное обеспечение BioLink IDenium на каждом автоматизированном рабочем месте (АРМ) пользователя для обеспечения надежной защиты сети в целом.

Внимание! Каждый АРМ пользователей, на которых планируется установить программное обеспечение BioLink IDenium должен быть включен в домен.

На АРМ администратора должен быть установлен компонент **BioLink IDenium Admin Pack**.

Внимание! На каждом контроллере домена должен быть установлен компонент **Синхронизатор паролей**.

Развертывание BioLink IDenium в локальной сети организации необходимо проводить в следующей последовательности:

Этап 1. Расширение схемы Active Directory. На данном этапе выполняется добавление необходимых атрибутов и регистрация компонент BioLink IDenium в службе каталогов Active Directory

Этап 2. Установка компонентов BioLink IDenium на контроллер домена. На данном этапе на каждый контроллер домена в сети устанавливается компонент «Синхронизатор паролей».

Этап 3. Установка компонента BioLink IDenium Server. На данном этапе

устанавливается и настраивается сервер BioLink IDenium.

Этап 4. Установка программного обеспечения администратора BioLink IDenium Admin Pack. На выделенном АРМ, подключенном к домену, разворачивается пакет программного обеспечения BioLink IDenium Admin Pack для работы администратора.

Этап 5. Установка программного обеспечения BioLink IDenium Client на АРМ пользователей. Завершающий этап установки BioLink IDenium, в ходе которого выполняется установка клиентских компонент BioLink IDenium на рабочие места пользователей.

4.2 Как прикладывать палец к окну сканера отпечатков пальцев

Отличительной особенностью программного комплекса BioLink IDenium является возможность применения биометрического сканера, позволяющего определять пользователей по отпечаткам пальцев. Для успешной работы с BioLink IDenium с самого начала необходимо ознакомиться с рядом нехитрых правил по использованию биометрического сканера. Несмотря на то, что BioLink IDenium поддерживает работу с большим количеством биометрических устройств по сканированию отпечатков пальцев, принцип сканирования одинаков для большинства сканеров и предельно прост:

1. Выберите палец, по отпечатку которого будут определяться ваши права доступа

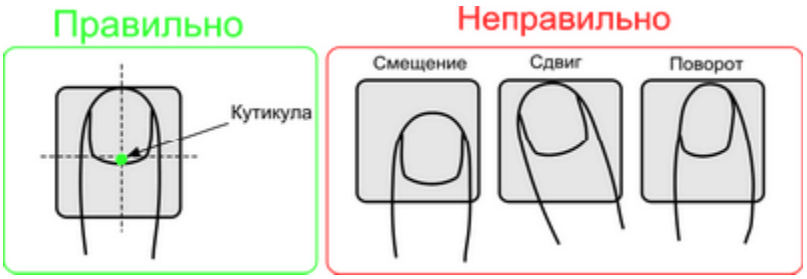
Вы можете использовать для верификации любой палец любой руки. Если к АРМ пользователя подключен сканер BioLink U-Match MatchBook, удобнее использовать указательный палец. Но следует помнить, что каждый из пальцев обладает своим уникальным отпечатком, не похожим на отпечатки других пальцев. Поэтому, если, например, в BioLink IDenium зарегистрирован отпечаток большого пальца правой руки, то и прикладывать к сканеру нужно именно этот палец.

2. Проверьте состояние пальца

Палец должен быть чистым, сухим и нормальной температуры.

3. Приложите палец к окну сканера

Оптимальное положение



Используйте всю поверхность окна сканера

Используйте всю максимально возможную площадь сканера, ориентируясь по изображению отпечатка на экране АРМ пользователя.

Размещайте кутикулу по центру окна сканера

Перекошенный, смещенный в какую-либо сторону палец не может быть корректно зарегистрирован и может стать причиной отказов в распознавании или существенного снижения скорости идентификации. Старайтесь прикладывать палец

таким образом, чтобы кутикула находилась в центре окна сканера.

Старайтесь прикладывать палец полностью и не разворачивать его относительно поверхности сканера

Не прикладывайте палец боком или частично. Это резко снижает качество отпечатка и рассматривается программой как ошибка.

Необходимо учитывать, что смещение или поворот пальца относительно поверхности сканера приводит к ошибкам распознавания отпечатка пальца.

Не прижимайте палец слишком сильно или слишком слабо

Если палец прижат слишком сильно, то оттиск будет иметь вид однородного темного пятна. Ослабьте силу нажатия.

Если палец прижат слишком слабо, то вместо четкой картины капиллярных линий будут видны отдельные точки и отрезки. Увеличьте силу нажатия.

Рекомендуется слегка поворачивать палец при вводе отпечатка пальца пользователя в систему. Например, сначала расположить палец так, чтобы ось пальца и ось симметрии сканера совпадали по центру, затем слегка повернуть палец влево, потом - слегка вправо

4.3 Вход пользователя в операционную систему

После установки BioLink IDenium Windows Logon на АРМ пользователя все информационные, программные и прочие ресурсы приобретают дополнительный уровень защиты благодаря использованию биометрической идентификации пользователей при входе в операционную систему.

Внимание! Если пользователь домена был зарегистрирован до установки BioLink IDenium, то для корректного функционирования BioLink IDenium необходимо чтобы этот пользователь, либо вошел в операционную систему, используя свое имя и пароль, либо произвел смену пароля (самостоятельно или с помощью администратора).

Это необходимо для получения пароля компонентом Синхронизатор паролей и отправки его на сервер BioLink IDenium. В дальнейшем в случае изменения пароля Синхронизатор паролей будет обеспечивать его синхронизацию с паролем и другими учетными данными, хранящимися на сервере BioLink IDenium

Способ первого после установки BioLink IDenium Windows Logon входа пользователя на АРМ пользователя может быть следующим:

- Если эталон отпечатка пальца пользователя был создан при создании учетной записи пользователя в Active Directory (пользователь присутствовал при регистрации своей учетной записи), то для того, чтобы зайти в систему в первый раз, пользователю достаточно приложить свой палец к окну сканера отпечатков пальцев. Более подробную информацию смотрите в разделе *Вход в операционную систему по отпечатку пальца*
- Если эталоны отпечатков пальцев пользователя отсутствуют, то администратор системы должен сообщить пользователю пароль для первого входа в систему. Это может быть обычный пароль пользователя для доступа в домен. О том, как войти на рабочую станцию с Windows Logon в этом случае, смотрите подробное описание в разделе *Вход в систему по паролю.*

Внимание! Рекомендуется настроить политики идентификации, до первого входа пользователей в систему. Политики идентификации позволяют более гибко и четко сконфигурировать правила доступа пользователей BioLink IDenium к защищенным ресурсам (подробнее см. раздел Настройка политик IDenium).

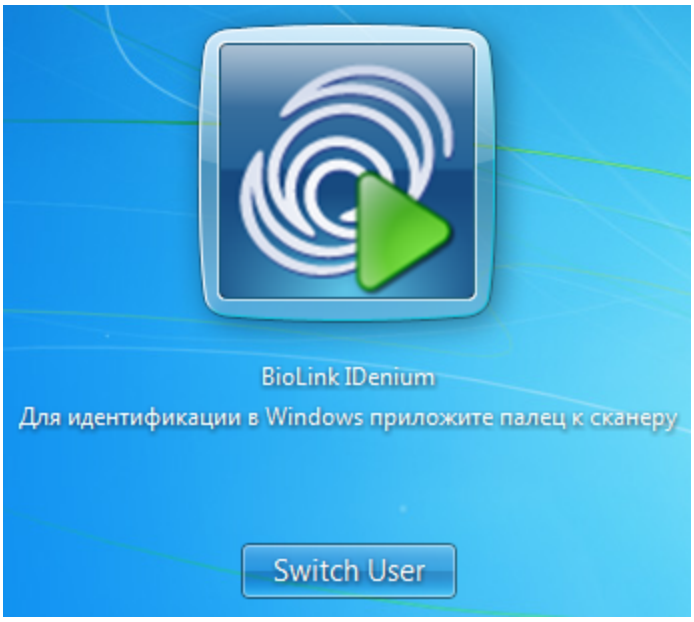
Процедура входа пользователя в операционные системы Windows XP и Windows Vista/7/8 немного отличаются. В настоящем документе вход в систему описан на

примере ОС Windows 7.

4.3.1 Вход в операционную систему по отпечатку пальца

Чтобы войти в систему по отпечатку пальца, выполните следующие действия:

1. Запустите АРМ пользователя;
2. После того как АРМ пользователя загрузится, на экране в зависимости от доменных политик появится сообщение о том, что для входа необходимо нажать Ctrl + Alt + Del, или непосредственно приглашение приложить палец к окну сканера отпечатков пальцев; в первом случае данное приглашение появится после нажатия Ctrl + Alt + Del;



3. Приложите палец к окну сканера, как вы это делали в процессе «обучения» программного комплекса BioLink IDenium распознаванию вас по отпечатку пальца;
4. После успешного распознавания вас по отпечатку вашего пальца запустится операционная система.

При необходимости пользователь может изменить, добавить или удалить эталоны отпечатков пальцев. Для этого необходимо воспользоваться пунктом **Панель управления BioLink Windows Logon**.

4.3.2 Вход в систему по паролю

Данная процедура не отличается от стандартной процедуры входа в операционные системы семейства Windows.

Замечание! Конкретные шаги пользователя при входе в операционную систему Windows по паролю зависят от настроек политик, определяемых администратором сети/домена.

После успешной авторизации пользователя запустится операционная система.

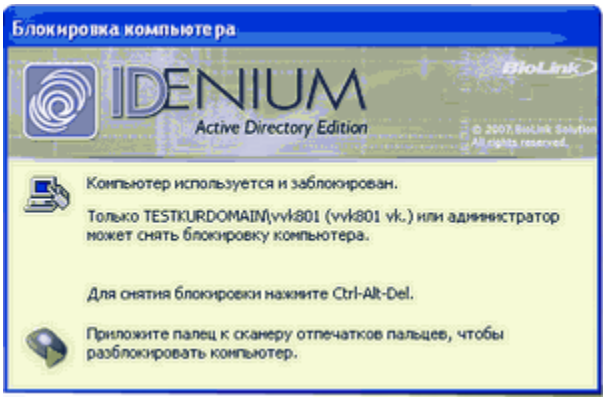
При необходимости пользователь может изменить свой пароль доступа к АРМ пользователя. Для этого необходимо нажать комбинацию клавиш CTRL+ALT+DEL, в окне «Безопасность Windows» нажать кнопку «Смена пароля» и далее следовать приглашениям программы. Детальную информацию о том, как изменить пароль персоны пользователя на сервере IDenium, смотрите в документе *Руководство пользователя Windows Logon*.

4.4 Разблокирование АРМ пользователя

Использование блокировки АРМ пользователя является одним из первостепенных условий надежной защиты ресурсов пользователя от несанкционированного доступа. BioLink IDenium позволяет использовать биометрическую идентификацию пользователя вместо парольной при разблокировании АРМ пользователя.

Для снятия блокировки используется описанная ниже процедура. Независимо от того, каким способом был заблокировал АРМ пользователя – вручную, нажатием клавиш CTRL+ALT+DEL, или с помощью защищенной паролем экранной заставки – на заблокированном компьютере в Windows XP отображается окно Блокировка компьютера, в более новых операционных системах - приглашение приложить палец к окну сканера отпечатков пальцев **.**

Окно «Блокировка компьютера» в Windows XP



Чтобы разблокировать АРМ пользователя, выполните следующие действия:

- Приложите палец к окну сканера отпечатков пальцев, следуя инструкциям в окне **Блокировка компьютера**;

-или-

- Осуществите вход по имени пользователя и паролю.

Более подробно о блокировке рабочих станций пользователя смотрите в документе *Руководство пользователя Windows Logon.*

5 Настройка серверных компонент IDenium

Настройка IDenium для Active Directory включает в себя выполнение следующих задач:

- Управление сервером BioLink IDenium:
- запуск службы BioLink IDenium Server;
- установка лицензии;
- просмотр журнала событий.

Настоящая глава содержит подробные рекомендации по выполнению вышеописанных задач.

5.1 Настройка компонента Синхронизатор паролей

Компонент **Синхронизатор паролей** должен быть установлен на каждом контроллере домена.

Компонент работает в фоновом режиме. Дальнейшая его настройка не требуется.

5.2 Управление сервером BioLink IDenium

Управление сервером IDenium включает в себя следующие задачи:

- управление запуском службы BioLink IDenium Server;
- управление лицензией сервера BioLink IDenium;
- просмотр журнала событий сервера BioLink IDenium.

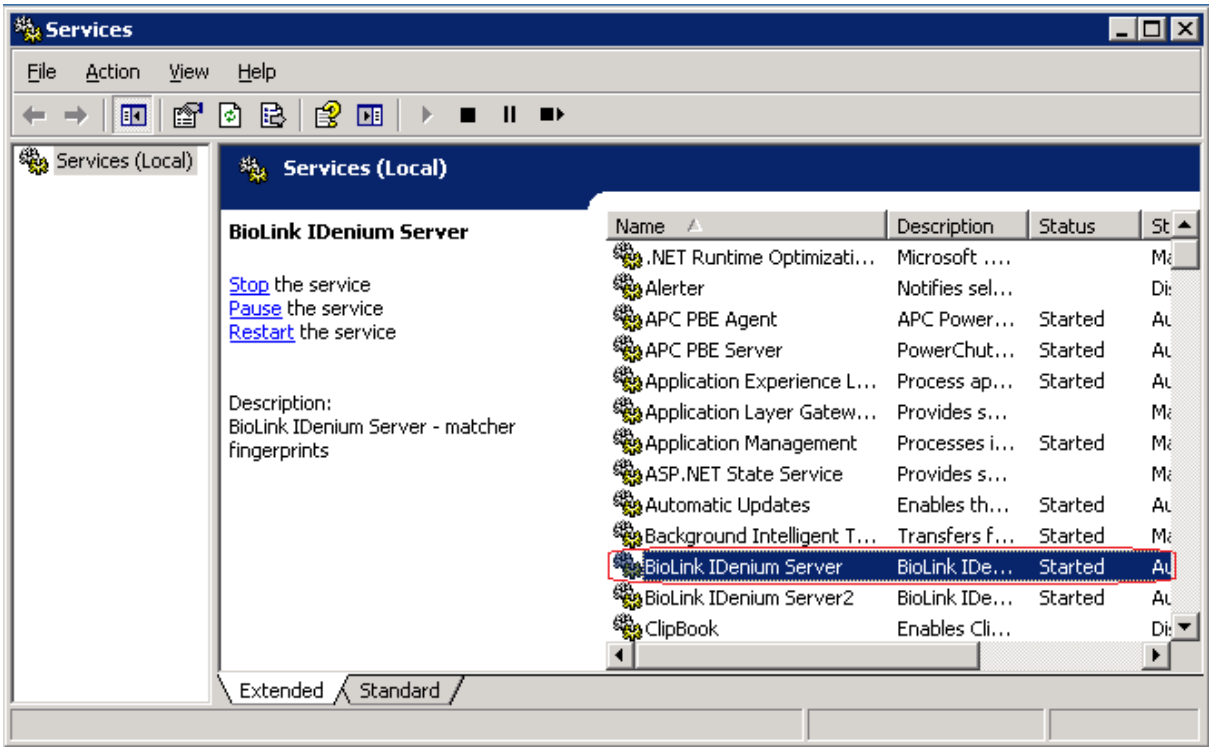
5.2.1 Запуск службы BioLink IDenium Server

Работа сервера BioLink IDenium обеспечивается службой BioLink IDenium Server. Эта служба должна запускаться под учетной записью пользователя, входящего в группу **Администраторы домена**. Данная учетная запись выбирается во время установки программного комплекса BioLink IDenium. Вы также можете выбрать другую учетную запись для запуска службы BioLink IDenium Server уже после установки программного комплекса BioLink IDenium.

Чтобы выбрать учетную запись для запуска службы BioLink IDenium Server, выполните следующие действия:

1. Нажмите кнопку **Пуск**, выберите команду **Панель управления**, щелкните категорию **Производительность и обслуживание**, щелкните значок **Администрирование**, затем в окне **Управление компьютером** дважды щелкните значок **Службы**;

Окно «Управление компьютером»



2. Щелкните правой кнопкой мыши службу **BioLink IDenium Server** и в контекстном меню выберите пункт **Свойства**;

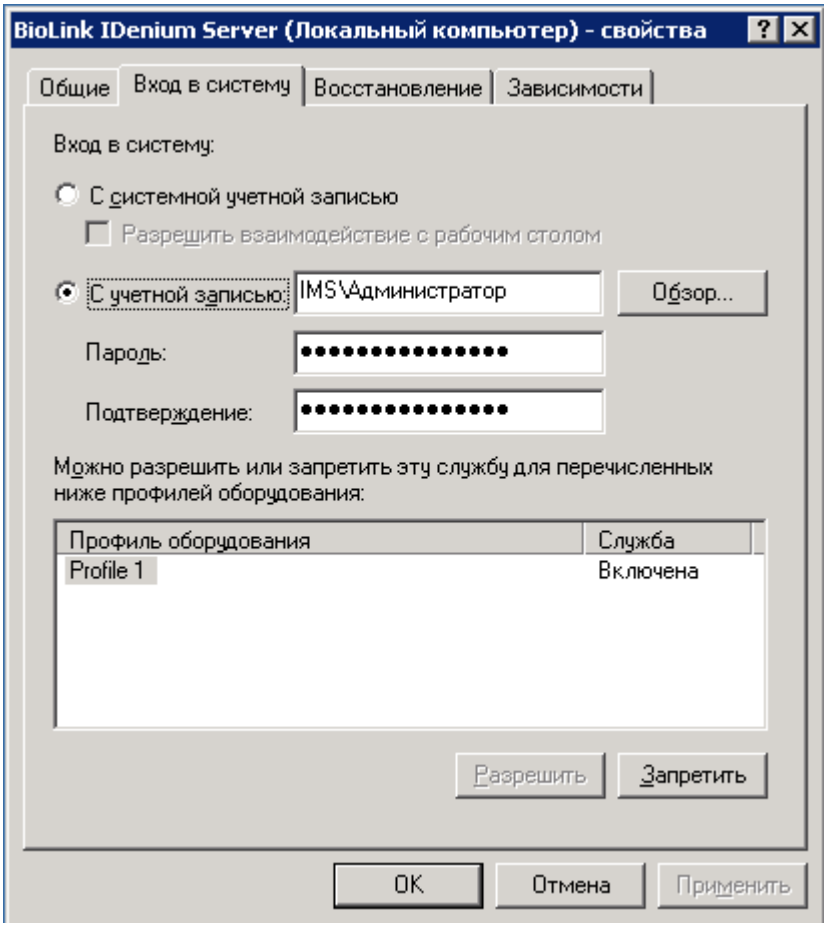
3. Откройте вкладку **Вход в систему**, установите переключатель в положение **С учетной записью**, нажмите кнопку **Обзор** и укажите учетную запись пользователя в диалоговом окне **Выбор пользователей**. Для продолжения нажмите кнопку **ОК**.

4. Введите пароль для выбранной учетной записи в полях **Пароль** и **Подтверждение** и нажмите кнопку **ОК**.

Примечание! В случае возникновения проблем, попробуйте указать имя пользователя в следующем виде: Имя_домена\имя_пользователя. Это особенно актуально, если используются АРМ пользователя под управлением операционной системы Windows 2000;

Примечание! Чтобы иметь возможность настраивать параметры выполнения службы BioLink IDenium Server, необходимо использовать учетную запись, входящую в группу **Администраторы**.

Вкладка «Вход в систему»

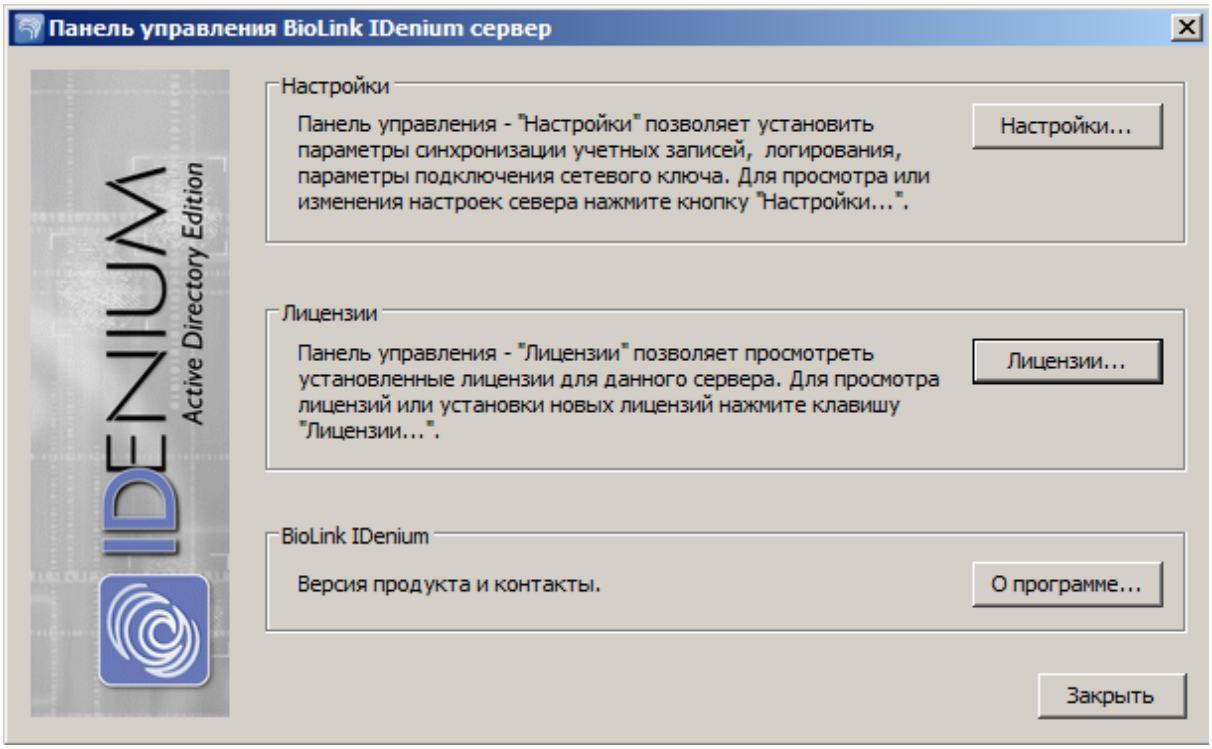


Автозапуск службы сервера при загрузке операционной системы будет возможен только под пользователем с правом входа в систему в качестве службы.

5.2.2 Панель управления сервером BioLink IDenium

Панель управления BioLink IDenium сервер предназначена для настройки сервера IDenium, а также для управления лицензиями IDenium

Окно «Панель управления BioLink IDenium сервер»



5.2.2.1 Управление лицензией сервера BioLink IDenium

В программном комплексе BioLink IDenium лицензируемым является количество пользователей BioLink IDenium. **Пользователь BioLink IDenium** – это обычный пользователь домена, но обладающий при этом набором уникальных биометрических идентификаторов (отпечатков пальцев). После установки BioLink IDenium все пользователи домена автоматически становятся пользователями BioLink IDenium, т.е. получают возможность использовать биометрию для входа в операционную систему и доступа к сетевым ресурсам. При этом биометрия будет доступна только для того количества пользователей, которое указано в лицензии на сервер BioLink IDenium.

Для того чтобы понять разницу между обычным пользователем домена и пользователем BioLink IDenium, рассмотрим следующий пример. В домене зарегистрировано 1020 пользователей. Лицензия сервера сравнений BioLink IDenium предусматривает количество пользователей BioLink IDenium равное 1000.

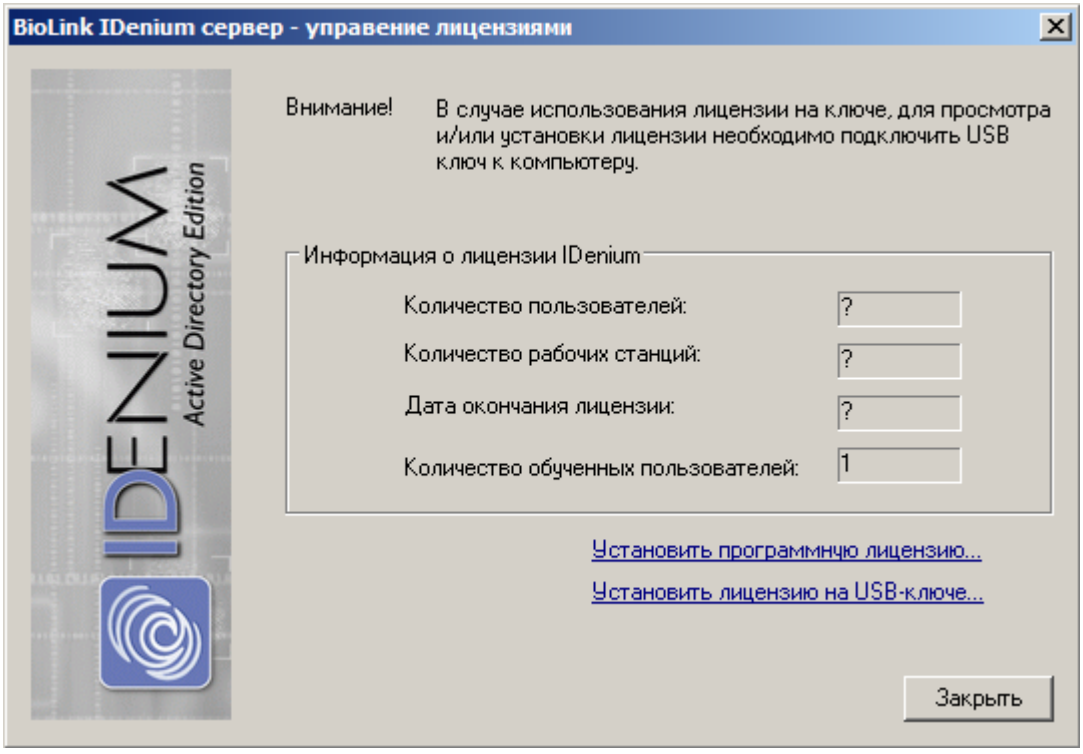
Таким образом, **только первые 1000 пользователей домена, для которых зарегистрированы биометрические идентификаторы**, смогут использовать биометрию. Остальные 20 будут вынуждены использовать стандартные методы аутентификации (по имени пользователя и паролю).

В комплект поставки сервера BioLink IDenium входит стартовая лицензия на 2 пользователя. Этого достаточно, чтобы провести небольшое тестирование программного комплекса BioLink IDenium. Если вам требуется лицензия на большее

количество пользователей, вам необходимо будет связаться с поставщиком BioLink IDenium и установить новую лицензию.

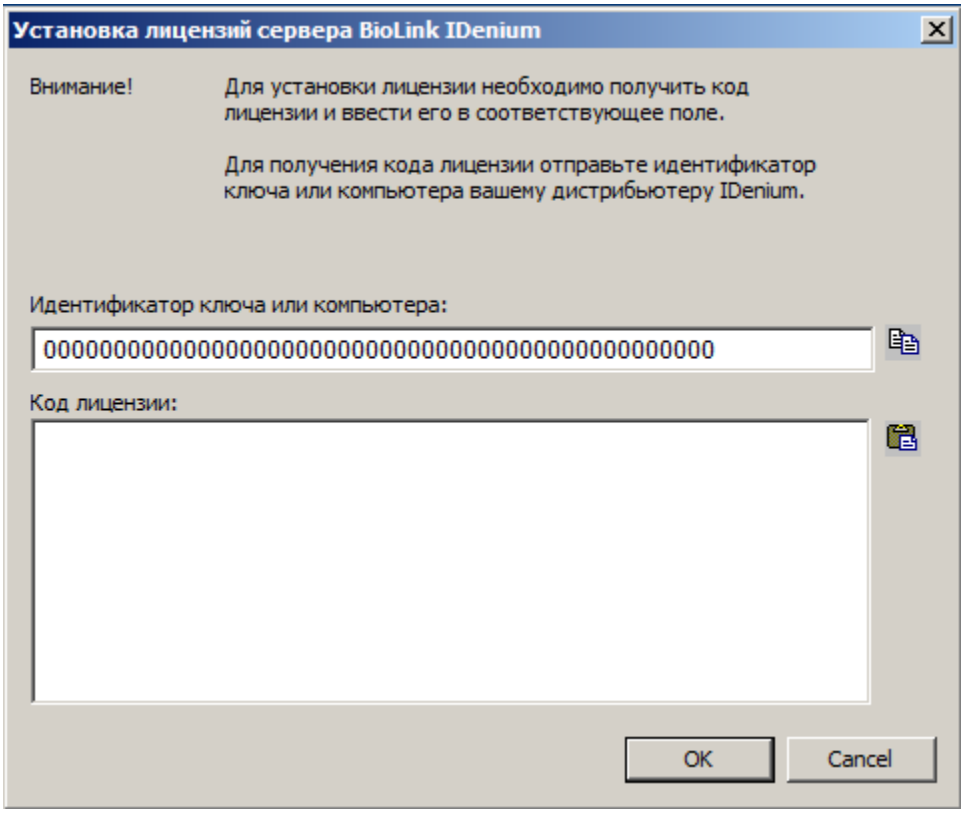
Чтобы установить новую лицензию, выполните следующие действия:

1. На АРМ пользователя с установленным сервером BioLink IDenium Server откройте окно **Панель управления BioLink IDenium сервер**, выбрав одноименный пункт в меню **Пуск**;
2. Нажмите кнопку "**Лицензии...**"



3. Выберите тип устанавливаемой лицензии (программная или на USB-ключе) щелчком по соответствующей ссылке;

Окно «Установка лицензий сервера BioLink IDenium»



4. Скопируйте **идентификатор ключа защиты** и отошлите его поставщику **BioLink IDenium**;
5. В ответ вам будет выслан код лицензии. Вставьте его в соответствующее поле и нажмите кнопку **OK**;
6. Обязательно перезапустите сервер BioLink IDenium после установки/обновления лицензии. Для перезапуска сервера перезапустите службу **BioLink IDenium Server**.

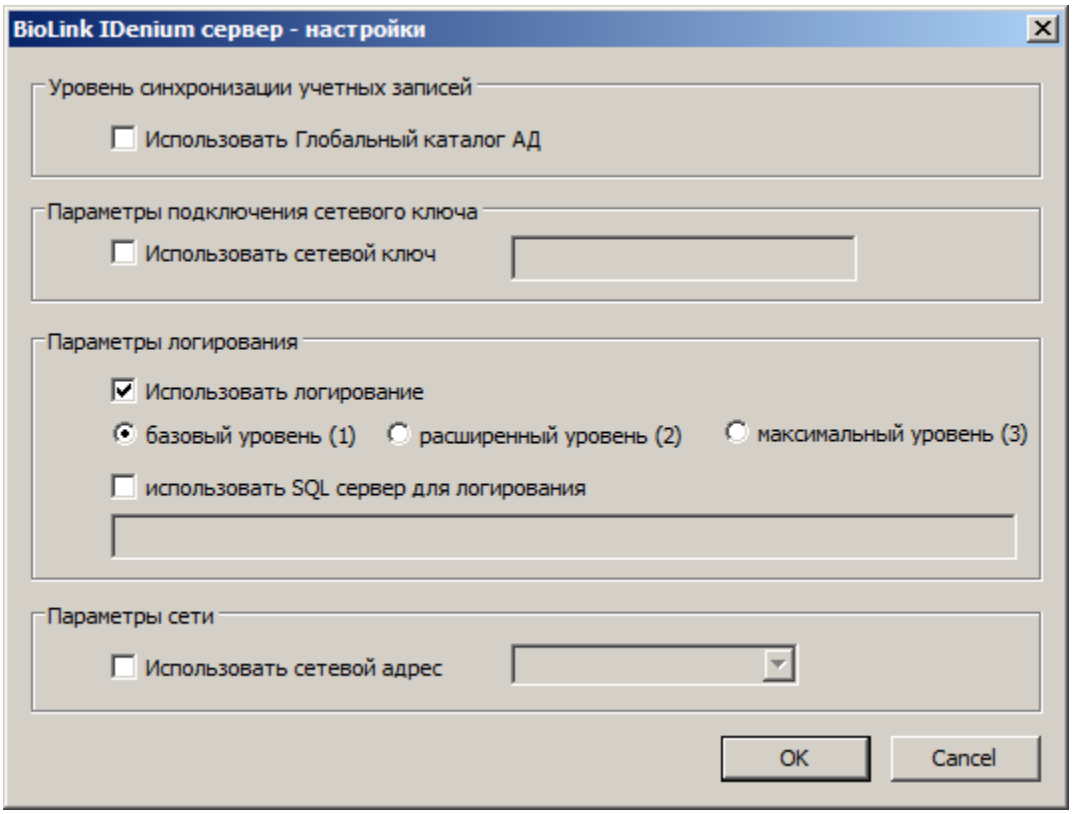
Примечание! При использовании сетевого ключа защиты необходимо в Панели управления BioLink IDenium сервер выбрать соответствующие пункт в меню "Настройки..." и указать, если необходимо ip адрес ПК на котором установлен сетевой ключ защиты.

5.2.2.2 Дополнительные настройки BioLink IDenium сервер

Для доступа в меню настроек сервера BioLink IDenium

1. На АРМ пользователя с установленным сервером BioLink IDenium Serveroткройте окно **Панель управления BioLink IDenium сервер**, выбрав одноименный пункт в меню **Пуск**;
2. Выберите пункт "**Настройки...**"

Окно «BioLink IDenium сервер - настройки»



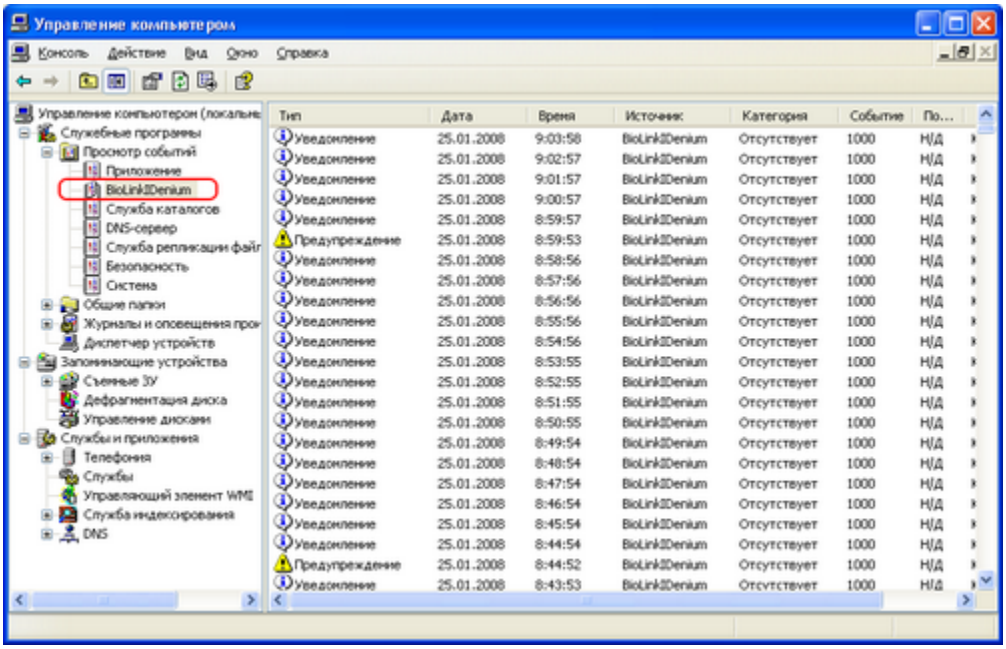
- "**Использовать глобальный каталог**" - указывается, использовать ли глобальный каталог для междоменной авторизации. По умолчанию не используется.
- "**Использовать сетевой ключ**" - указывает на использование сетевого ключа защиты Sentinel, без указания ip адреса на котором установлен сетевой ключ тип запроса для поиска ключа будет вида multicast.
- "**Использовать логирование**" - смотрите пункт Настройка уровня детализации информации
- "**Использовать SQL сервер для логирования**" - смотрите пункт Управление пользователями BioLink IDenium
- "**Использовать сетевой адрес**" - указывает IP-адрес для приема запросов (может использоваться при наличии у компьютера нескольких IP-адресов)

5.2.3 Просмотр журнала событий сервера BioLink IDenium

Все события сервера BioLink IDenium записываются в журнал, который находится в разделе **Просмотр событий** окна **Управление компьютером**.

В журнал сервера BioLink IDenium может записываться информация о следующих событиях:

- изменение учетных данных пользователя;
- запуск/останов службы BioLink IDenium Server;
- обработка запроса на сравнение с АРМ пользователей;
- информация о других событиях, содержащая различные отладочные и служебные данные.



Также журнал событий BioLink IDenium может содержать информацию о лицензии и различные данные для самостоятельного поиска неисправностей, сбоев, ошибок в работе и их устранения.

5.2.3.1 Настройка уровня детализации информации

Уровень детализации информации, выводимой в журнале событий сервера BioLink IDenium, может регулироваться пользователем через настройку параметров логирования в окне настроек сервера Biolink IDenium.

Существуют три уровня детализации:

1. Выводится информация о фактах успешной/неуспешной идентификации и запуске/

остановке службы.

2. Добавляется информация о приходящих запросах на идентификацию.
3. Добавляется информация обо всех возможных событиях, связанных с сервером BioLink IDenium.

5.2.3.2 Диагностика событий

Ниже представлены некоторые коды событий и их расшифровка.

Код события	Описание события	Дополнительная информация
1002	Запрос на идентификацию	Указывается, с какого АРМ пользователя пришел запрос на идентификацию (поле **From**).
1003	Учетная запись найдена	Имя учетной записи (поле **Account name**). Результат сравнения (поле **Score**). Указывается, с какого АРМ пользователя пришел запрос на идентификацию (поле **From**).
1004	Учетная запись не найдена	Указывается, с какого АРМ пользователя пришел запрос на идентификацию (поле **From**).

5.2.3.3 Запись событий IDenium в базу данных Microsoft SQL Server

Для поддержки записи событий в БД Microsoft SQL:

1. Необходимо включить поддержку протокола TCP/IP для вашего экземпляра Microsoft SQL Server.
2. Создать базу данных с именем BioLinkIDeniumLogs
3. Выполнить SQL запрос к БД BioLinkIDeniumLogs

```
USE [BioLinkIDeniumLogs]

GO

/****** Object: Table [dbo].[IDeniumLog] Script Date: 03/27/2010 11:06:52
******/
```

```
SET ANSI_NULLS ON

GO

SET QUOTED_IDENTIFIER ON

GO

SET ANSI_PADDING ON

GO

CREATE TABLE [dbo].[IDeniumLog](

[id] [int] IDENTITY(1,1) NOT NULL,

[idMsg] [int] NOT NULL,

[idType] [int] NOT NULL,

[dtDateTime] [datetime] NOT NULL,

[sIPAddress] [varchar](50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL,

[sMachineName] [varchar](50) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL,

[sMessage] [varchar](max) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL

ON [PRIMARY]

GO

SET ANSI_PADDING OFF
```

4. На ПК с установленным BioLink IDenium Client выставить уровень логирования (LogLevel) «3».
5. В системном реестре в ветви [HKLM]\Software\BioLink\Idenium создать ключ LogSQLConnect(String) и изменить его значение на Provider=SQLOLEDB.1;Persist Security Info=False;User ID=sa;Password=Qwerty123; Initial Catalog=BioLinkIDeniumLogs;Data Source=TEST-COMP-ROOT

Где, UserID и Password – имя пользователя и пароль на доступ к экземпляру SQL,

Source – имя компьютера в сети с установленным экземпляром Microsoft SQL Server в БД которого будет вестись запись событий IDenium.

Кроме того строку подключения

5.2.3.4 "Тонкая" настройка сервера BioLink IDenium

Для «тонкой» настройки сервера Biolink Idenium предусмотрены следующие параметры, которые управляются ключами реестра в ветвях:

[HKLM]\Software\BioLink\Idenium:

- **CodePage** (REG_DWORD) – локализация (0x409, 0x419)
- **UseGC** (REG_DWORD) – использовать ли глобальный каталог для междоменной авторизации (0-1, 0 – не использовать, 1 – использовать, по умолчанию 0)
- **LogLevel** (REG_DWORD) – уровень детализации журнала событий (1-3, 1 - выводится информация о фактах успешной/неуспешной идентификации и запуске/ остановке службы. 2 - добавляется информация о приходящих запросах на идентификацию. 3 - добавляется информация обо всех возможных событиях, связанных с сервером BioLink IDenium, по умолчанию 1)
- **QualityEnroll** (REG_DWORD) – минимальное качество при обучении отпечатка (0–100,по умолчанию 40)
- **QualityVerify** (REG_DWORD) – минимальное качество отпечатка для идентификации (0–100, по умолчанию 50)
- **LogSQLConnect** (REG_DWORD) – использовать ли SQL сервер для журналирования (0-1, 0 – не использовать, 1 – использовать, по умолчанию 0)
- **UseLogSQLConnect** (REG_SZ) – строка подключения к SQL серверу
- **ServerUseIP** (REG_DWORD) – использовать ли сетевой ключ (0-1, 0 – не использовать, 1 – использовать, по умолчанию 0)
- **ServerIp** (REG_SZ) – адрес сервера ключей

[HKLM]\Software\BioLink\XMatcher:

- **CodePage** (REG_DWORD) – локализация (0x409, 0x419)
- **LogLevel** (REG_DWORD) – уровень детализации журнала событий (1-3, 1 - выводится информация о фактах успешной/неуспешной идентификации и запуске/ остановке службы. 2 - добавляется информация о приходящих запросах на идентификацию. 3 - добавляется информация обо всех возможных событиях, связанных с сервером BioLink XMatcher, по умолчанию 1)
- **ScoreLevel** (DWORD) – порог распознавания отпечатков. Диапазон значений теоретически может быть от 0 до 2000, однако значения совпадения сравнения выше 1200 практически недостижимы, результатом чего может являться полная невозможность входа пользователей. Значения ниже 500 в свою очередь могут

приводить к ложным распознаваниям. Оптимальные значения, как правило, находятся в диапазоне 650-750, однако если при этих значениях ложных распознаваний не происходит, то можно порекомендовать при наличии такой возможности опытным путем выявить и настроить максимальное значение, при котором распознавание будет безошибочным.

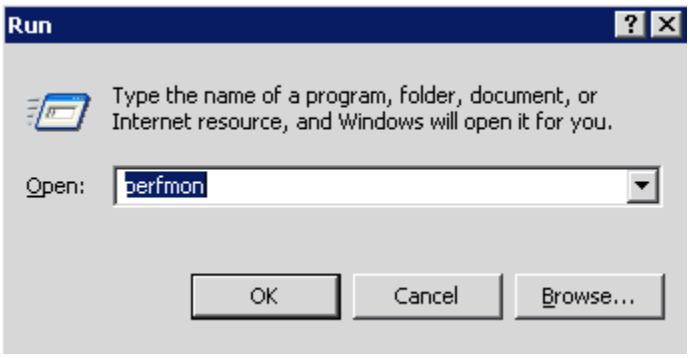
Внимание! Неправильное изменение параметров системного реестра с помощью редактора реестра или любым иным способом может привести к серьезным неполадкам. Для их устранения может потребоваться переустановка операционной системы. Разработчик не гарантирует, что эти неполадки можно будет устранить. Ответственность за изменение реестра несет пользователь.

5.2.4 Монитор производительности сервера BioLink IDenium

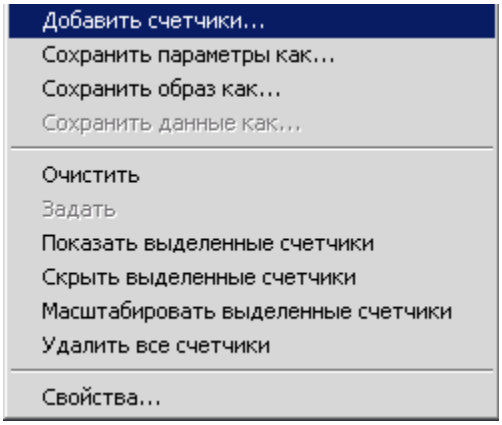
Для отслеживания нагрузки на сервер BioLink IDenium и его производительности, можно воспользоваться встроенным компонентом Windows **Монитор надежности и производительности.**

Для запуска монитора производительности сервера BioLink IDenium, выполните следующие действия:

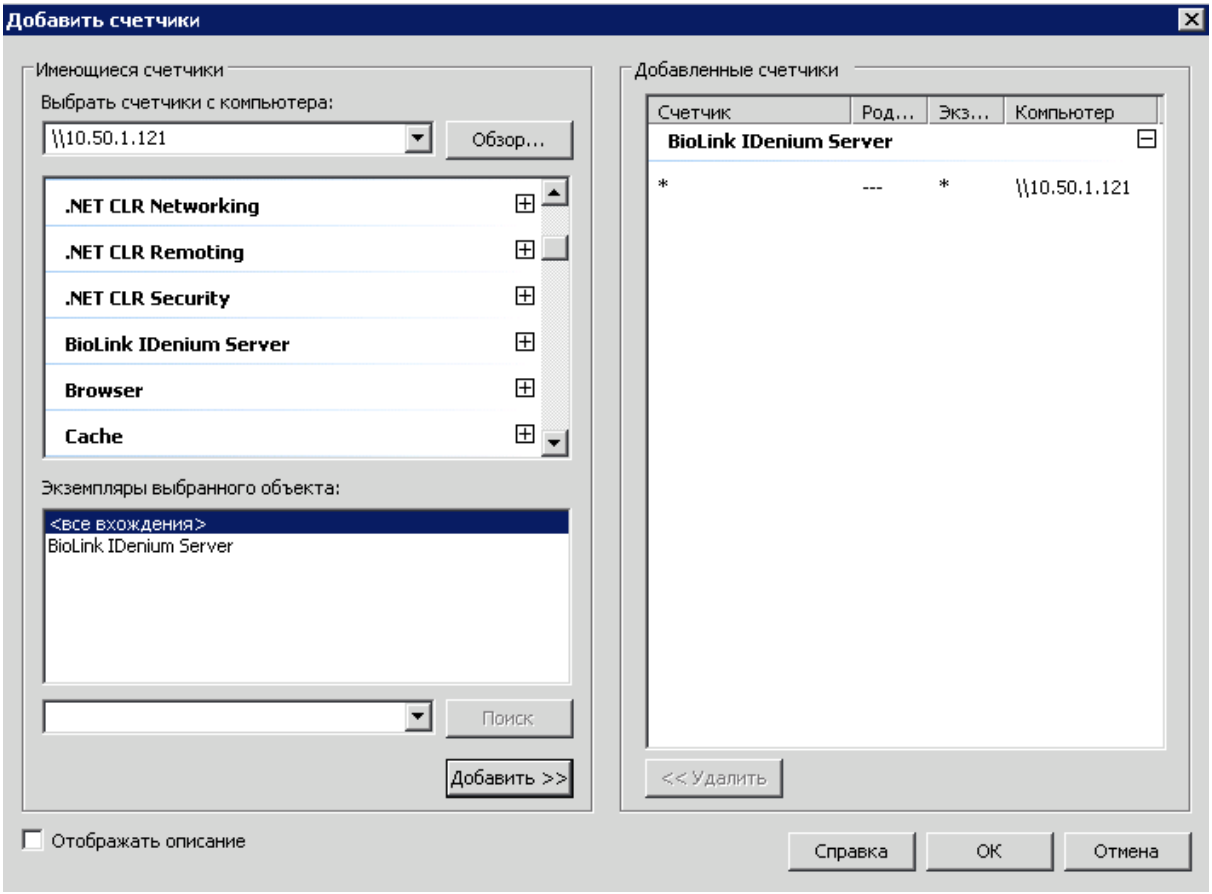
1. Нажмите кнопку "Пуск"(Start)
2. Выберите пункт "выполнить" (Run)
3. Введите `perfmon`



4. У вас откроется окно "Системный монитор" или "Монитор надежности и производительности Windows", в зависимости от версии вашей ОС.
5. Кликните правой кнопкой мышке в пустой области монитора и выберите пункт **Добавить счетчики**



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



6 Управление пользователями BioLink IDenium

Одной из основных задач администратора программного комплекса BioLink IDenium является управление пользователями BioLink IDenium. В настоящей главе описываются ключевые понятия и содержатся подробные инструкции, относящиеся к управлению пользователями BioLink IDenium.

6.1 Введение в управление пользователями BioLink IDenium

После развертывания BioLink IDenium все пользователи локальной сети становятся **пользователями BioLink IDenium**. Управление пользователями BioLink IDenium осуществляется с помощью стандартных средств администрирования пользователей Windows Active Directory, расширенных за счет компонента BioLink IDenium Admin Pack.

После установки BioLink IDenium пользователь может применять один из следующих способов регистрации в домене, прикладных системах, обращению к сетевым ресурсам и т.п.:

- по отпечатку пальца;
- по имени и паролю учетной записи пользователя (далее - идентификаторы пользователя);
- с использованием цифрового сертификата (записанного на смарт-карту).

Как уже отмечалось выше, одним из главных преимуществ BioLink IDenium является возможность снизить нагрузку на пользователя, связанную с необходимостью запоминать пароли к различным системам и ресурсам. BioLink IDenium добавляет к стандартным учетным данным пользователя уникальные биометрические идентификаторы, однозначно идентифицирующие этого пользователя, и предоставляет механизм, с помощью которого пользователь домена получает возможность использовать свои биометрические характеристики для доступа к ресурсам сети.

Таким образом, управление учетными данными пользователей BioLink IDenium включает в себя следующие задачи:

- создание биометрических идентификаторов пользователей

выполняется администратором локальной сети средствами BioLink IDenium Admin Pack или пользователем самостоятельно после регистрации в домене по имени и паролю пользователя средствами BioLink IDenium Windows Logon (см. Руководство пользователя Windows Logon)

- *изменение учетных данных пользователя*

выполняется либо администратором системы (см. Ввод отпечатков пальцев пользователя в IDenium), либо пользователем самостоятельно средствами BioLink IDenium Windows Logon (см. *Руководство пользователя Windows Logon*)

- *сброс учетных данных пользователя*
  - если пользователь забыл свой пароль, то сброс текущего пароля и замена его на служебный выполняется администратором системы средствами администрирования Active Directory;
  - в случае возникновения проблем с биометрическими идентификаторами пользователя (программный комплекс BioLink IDenium отказывается распознавать пользователя по его отпечатку пальца), то в этом случае необходимо заново ввести в систему отпечаток нераспознаваемого пальца пользователя, либо ввести в BioLink IDenium отпечатки других пальцев пользователя (BioLink IDenium поддерживает ввод до 10 эталонов различных отпечатков пальцев одновременно).
- *ввод ПИН кода карты пользователя*

выполняется администратором локальной сети средствами BioLink IDenium Admin Pack; позволяет пользователю предъявлять свои биометрические идентификаторы вместо ввода ПИН кода карты.

- управление сценариями BioLink IDenium Password Vault пользователя

выполняется администратором локальной сети средствами BioLink IDenium Admin Pack; позволяет администратору изменить и/или удалить сценарии BioLink IDenium Password Vault, записанные пользователем.

6.2 Создание нового пользователя BioLink IDenium

Регистрация нового пользователя BioLink IDenium аналогична созданию новой учетной записи пользователя в локальной сети.

Для создания нового пользователя можно использовать либо оснастку **Active Directory - Пользователи и компьютеры**, либо командную строку (подробнее об этом см. в документации Windows®). Ниже описывается способ создания нового пользователя с помощью оснастки **Active Directory - Пользователи и компьютеры**.

Чтобы зарегистрировать нового пользователя BioLink IDenium, выполните следующие действия:

1. Запустите оснастку администрирования доменов **Active Directory – Пользователи и компьютеры** из комплекта утилит **Active Directory**.
2. Выберите домен, в который должен быть добавлен новый пользователь.
3. В меню **Действия** выберите пункт **Новый пользователь**.
4. Следуя приглашениям мастера по созданию нового пользователя, введите требуемую информацию.
5. На последнем шаге нажмите кнопку **Готово** для завершения создания учетной записи пользователя.

Примечание. В любой момент можно прервать процесс создания нового пользователя нажатием кнопки **Отмена** либо клавиши **ESC**.

Если пользователь присутствует при создании своей учетной записи, то далее следует ввести отпечатки пальцев этого пользователя в программный комплекс BioLink IDenium.

6.3 Работа с учетными данными пользователя BioLink IDenium

Под учетными данными пользователя BioLink IDenium подразумеваются:

- Имя пользователя и пароль;
- Цифровые сертификаты, записываемые на смарт-карту;
- Уникальные биометрические идентификаторы (в текущей версии – отпечатки пальцев).

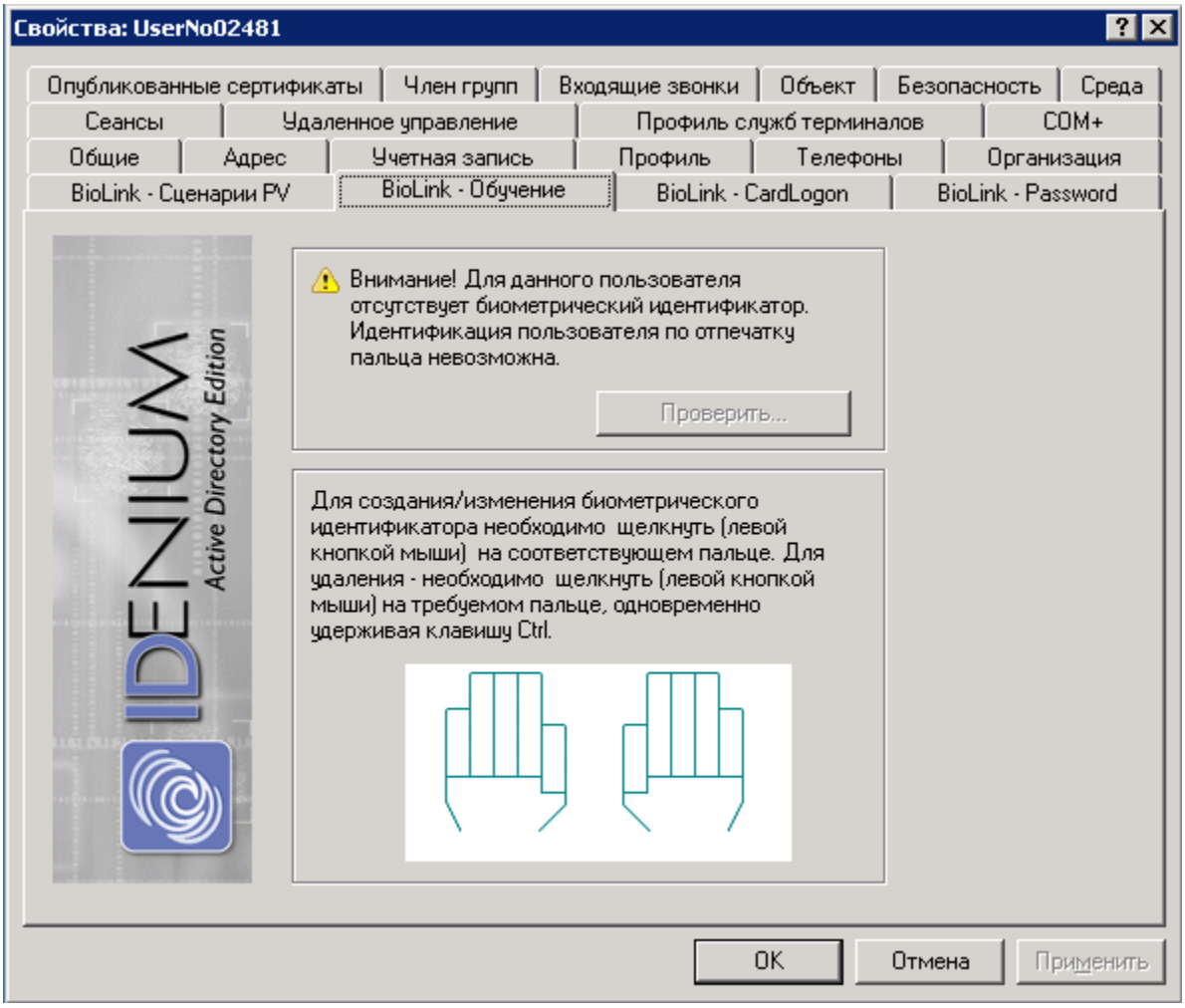
Разделы ниже рассказывают о том, как управлять учетными данными пользователя.

6.3.1 Ввод отпечатков пальцев пользователя в BioLink IDenium

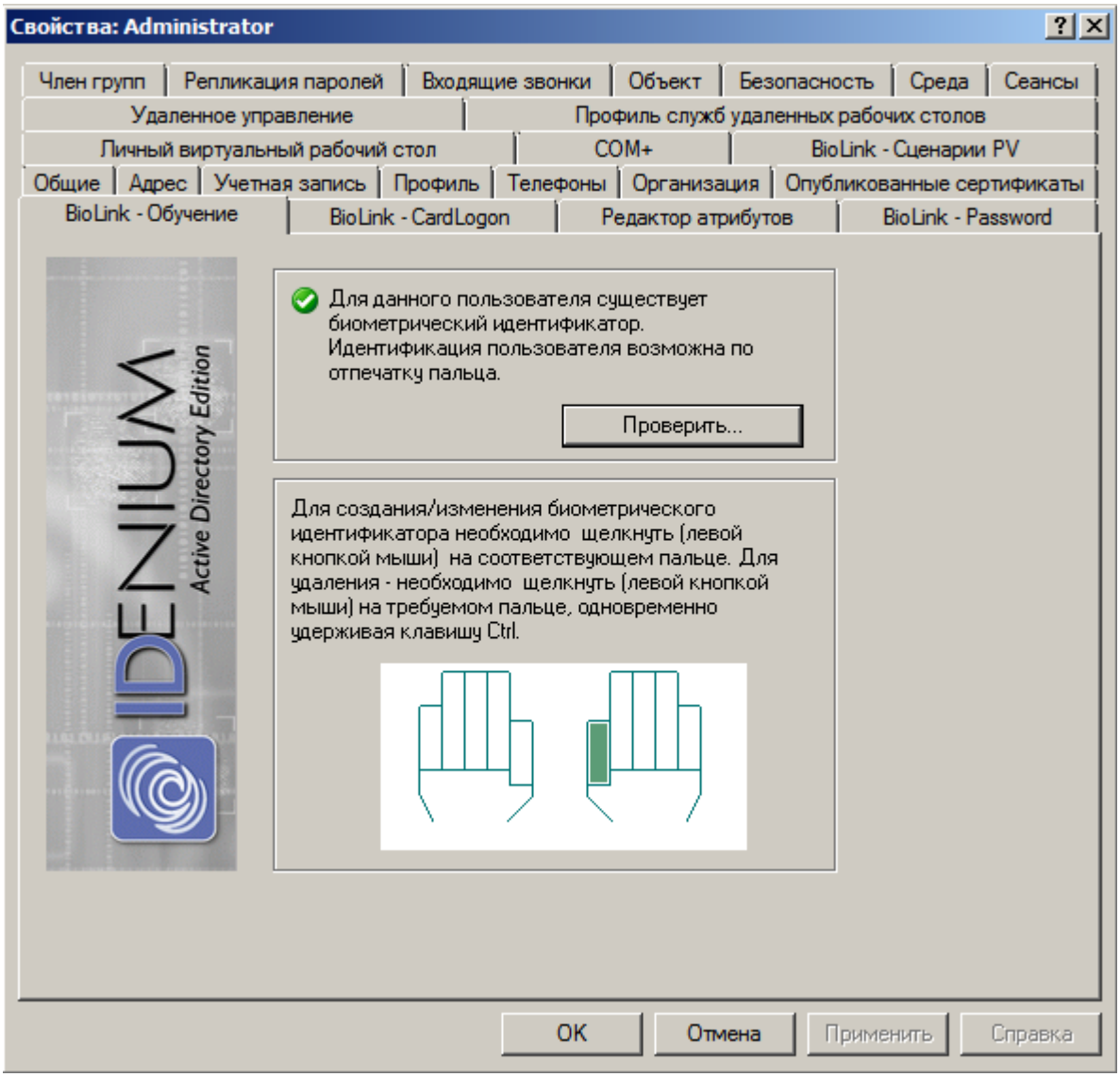
Администратор локальной сети может ввести отпечатки пальцев пользователя в любое время (либо сразу же после создания учетной записи пользователя (при условии, что пользователь присутствует при создании своей учетной записи), либо позже). Следует помнить, что пользователь может самостоятельно ввести отпечатки пальцев со своего АРМ.

Чтобы ввести отпечатки пальцев пользователя в BioLink IDenium с помощью BioLink Admin Pack, выполните следующие действия:

1. Запустите оснастку администрирования доменов «Компьютеры и пользователи» из комплекта утилит Active Directory.
2. Выберите домен, в котором зарегистрирован пользователь; затем выберите папку **Users.**
3. Выберите пользователя, для которого требуется создать эталоны отпечатков пальцев.
4. Выполните одно из следующих действий:
   - Выберите пункт **Свойства** в меню **Действия**.
   - Нажмите кнопку **Свойства**  .
   - Нажмите ENTER.
5. В окне свойств домена перейдите на вкладку **BioLink - Обучение**.



6. Чтобы ввести в BioLink IDenium отпечаток пальца, щелкните левой кнопкой мыши по выбранному пальцу. Откроется окно **Обучение**. Обратите внимание, вы можете ввести в BioLink IDenium отпечатки всех 10-ти пальцев пользователя;



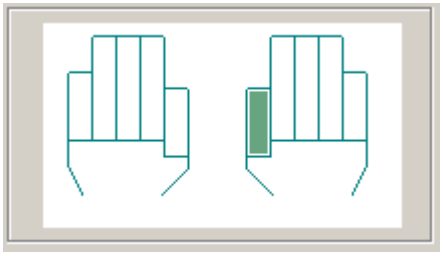
7. Следуя приглашениям программы в окне **Обучение**, приложите палец к окну биометрического сканера (например, это может быть BioLink U-Match MatchBook в.3.5). В процессе обучения необходимо несколько раз приложить палец к окну сканера, следуя приглашениям программы. После успешного создания эталона отпечатка пальца окно закроется автоматически.

Для отмены процесса обучения надо нажать кнопку **Отмена** до завершения сканирования.

Примечание. Обратите внимание, что для корректного обучения необходимо каждый раз немного изменять положение пальца при сканировании. Каждый раз при сканировании палец нужно приподнимать и вновь прикладывать с небольшим смещением и поворотом.

Если в окне обучения приглашение убрать палец с экрана сканера отображается даже тогда, когда палец не приложен к сканеру, почистите окно сканера с помощью специальных средств.

8. На вкладке **BioLink - Обучение** палец, для которого существует эталон отпечатка пальца, будет отмечен зеленым цветом. Чтобы удалить эталон отпечаток пальца, необходимо щелкнуть левой кнопкой мыши, удерживая клавишу CTRL на клавиатуре.



Примечание! Обратите внимание, что все изменения, сделанные при редактировании свойств пользователя, вступят в силу только после нажатии кнопки **ОК** или **Применить**. Если вы случайно удалили не тот эталон отпечатка пальца, можно нажать кнопку **Отмена**, и сделанные изменения не будут сохранены.

Администратор может запретить создаваемому пользователю использовать пароль для аутентификации. В таком случае вход в систему для такого пользователя будет возможен только с помощью отпечатков пальцев (подробнее об этом см. раздел см. Настройка политик IDenium).

6.3.2 Изменение пароля и цифровых шаблонов отпечатков пальцев пользователя

Пароль и биометрические идентификаторы пользователя (в текущей версии - отпечатки пальцев) могут изменить как сам пользователь, которому принадлежат эти идентификаторы, так и администратор.

Пользователь может изменить свой пароль с помощью стандартных средств Windows и ввести заново отпечатки пальцев с помощью панели управления BioLink IDenium Windows Logon.

Администратор локальной сети может создавать и изменять цифровые шаблоны отпечатков пальцев любого пользователя, зарегистрированного в корпоративной сети. Это может быть полезным в следующих случаях:

- Отпечаток пальца был поврежден, и пользователь забыл свой пароль доступа.

Доступ в операционную систему не может быть выполнен;

- Отпечатки пальцев не были введены в BioLink IDenium во время создания пользователя. Пользователь не может или не хочет ввести отпечатки пальцев самостоятельно, несмотря на то, что настоятельно рекомендуется ввести отпечатки пальцев в BioLink IDenium;
- Пользователь сам попросил администратора изменить цифровые шаблоны его отпечатков пальцев.

Все операции администратора по изменению биометрических идентификаторов пользователей производятся через интерфейс администрирования Active Directory (подробнее об этом см. Ввод отпечатков пальцев пользователя в IDenium).

6.3.3 Проверка биометрических идентификаторов пользователей

Процедура проверки биометрических идентификаторов пользователей может использоваться в следующих случаях:

- Пользователь не помнит, вводил ли он отпечаток выбранного пальца в систему или нет;
- Администратор и/или пользователь хотят удостовериться, что эталон выбранного отпечатка пальца создан корректно (например, в случае, если пользователь не может войти в систему, используя этот отпечаток пальца, хотя он точно знает, что эталон отпечатка пальца был создан ранее).

Чтобы проверить эталон отпечатка пальца пользователя, выполните следующие действия:

1. Запустите оснастку администрирования доменов **Active Directory – Пользователи и компьютеры** из комплекта утилит Active Directory.
2. Выберите домен, в котором зарегистрирован пользователь, выберите папку **Users**
3. Выберите пользователя, чей эталон отпечатка пальца должен быть проверен.
4. Выполните одно из следующих действий:
   - Выберите пункт **Свойства** в меню **Действия**.
   - Нажмите кнопку **Свойства**  .
   - Нажмите ENTER.
5. В окне свойств пользователя перейдите на вкладку **BioLink - Обучение**.
6. Нажмите кнопку **Проверить идентификаторы**. Откроется окно «Проверка

идентификаторов».

7. Следуя приглашениям программы, приложите палец к окну биометрического сканера. Если предоставленные биометрические идентификаторы соответствуют сохраненным в BioLink IDenium, то на экране появится сообщение «Пользователь успешно идентифицирован». Если отсканированный отпечаток пальца не совпадает с хранящимся в BioLink IDenium, будет выведено сообщение об ошибке.

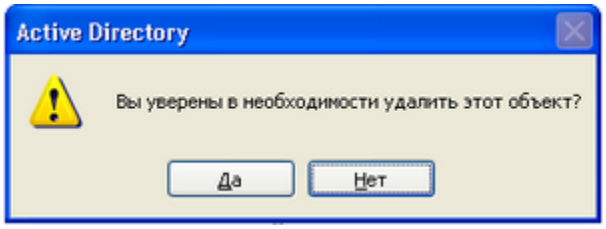
6.4 Удаление учетной записи пользователя BioLink IDenium

Удаление учетной записи пользователя BioLink IDenium выполняется автоматически при удалении учетной записи пользователя из каталога Active Directory.

Чтобы удалить учетную запись пользователя, выполните следующие действия:

1. Запустите оснастку администрирования доменов **Active Directory – Пользователи и компьютеры** из комплекта утилит Active Directory.
2. Выберите домен, а в нем папку **Users**.
3. Выделите пользователя и выполните одно из следующих действий:
   - В меню **Действия** выберите команду **Удалить**.
   - Нажмите кнопку **Удалить**.
   - Щелкните правой кнопкой мыши по выбранной учетной записи и выберите команду **Удалить** в контекстном меню.

Появится окно с запросом подтвердить удаление записи о пользователе. Нажмите **Да** для удаления записи о пользователе.



6.5 Настройка политик BioLink IDenium

Для каждого из пользователей и/или групп пользователей BioLink IDenium можно настроить собственные политики, которые будут действовать для всех приложений и сервисов BioLink IDenium.

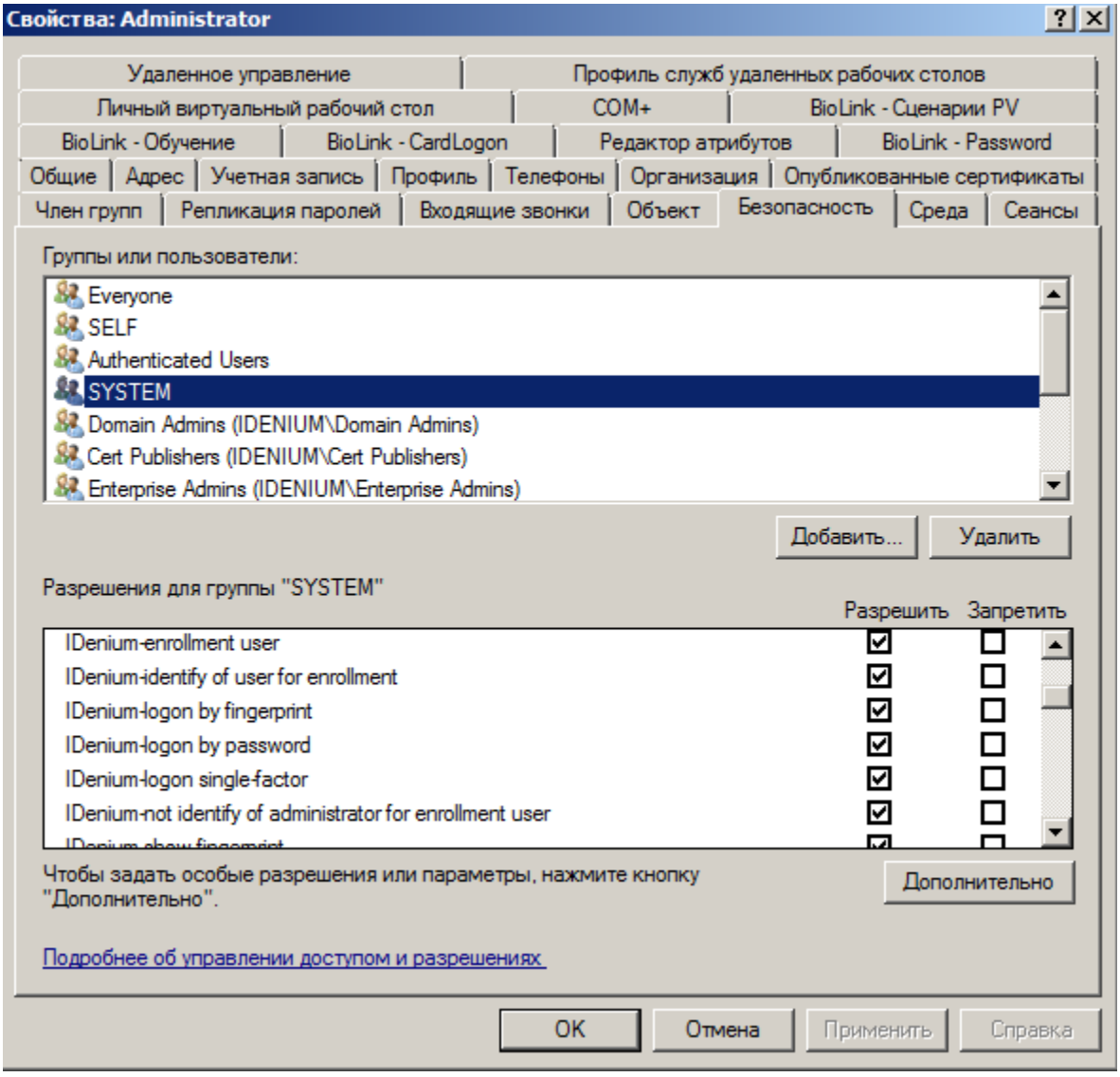
Политики BioLink IDenium представляют собой правила, определяющие, каким образом будет осуществляться доступ к защищенным ресурсам пользователями BioLink IDenium и настройки, позволяющие выбрать режимы работы BioLink IDenium для каждого конкретного пользователя.

Политики BioLink IDenium могут быть заданы для групп пользователей и для каждого конкретного пользователя. Работа с политиками IDenium осуществляется аналогично настройке разрешений для объектов Active Directory (подробнее об управлении доступом для объектов Active Directory см. раздел Советы и рекомендации по назначению разрешений для объектов Active Directory справочной системы Windows Server 2003 (информация в интернете).

Политики BioLink IDenium необходимо настраивать как разрешения для встроенной системной группы **SYSTEM** на вкладке **Безопасность** в свойствах объектов Active Directory.

Чтобы настроить политики BioLink IDenium для конкретного пользователя, выполните следующие действия:

1. Запустите оснастку администрирования доменов **Active Directory – Пользователи и компьютеры** из комплекта утилит Active Directory.
2. Выберите домен, в котором зарегистрирован пользователь; затем выберите папку **Users**
3. Выберите пользователя, чьи политики идентификации будут изменены.
4. Выполните одно из следующих действий:
   - Выберите пункт **Свойства** в меню **Действия**.
   - Нажмите кнопку **Свойства**  .
   - Нажмите ENTER.
5. В окне свойств пользователя перейдите на вкладку **Безопасность**. Если вкладка не видна, убедитесь, что вы включили отображение **Дополнительных функций** в оснастке «Active Directory Пользователи и компьютеры» (меню **Вид** - **Дополнительные функции**).



Далее выберите группу SYSTEM.

Замечание! Настраивать политики IDenium для выбранного объекта Active Directory необходимо ТОЛЬКО КАК разрешения для группы SYSTEM. Для остальных групп изменения в политиках действовать не будут.

6. В списке **Разрешения для SYSTEM** настройте политики BioLink IDenium.

Таблица ниже объясняет назначение всех политик BioLink IDenium.

Название политики	Если разрешено	Если запрещено
IDenium - вход по отпечатку	Для данного пользователя вход в операционную	Для данного пользователя вход в операционную

	систему по отпечатку пальца разрешен.	систему по отпечатку пальца запрещен.
IDenium - вход по паролю	Для данного пользователя вход в операционную систему по паролю разрешен.	Для данного пользователя вход в операционную систему по паролю запрещен.
IDenium - использовать однофакторный вход	Данный пользователь может входить в операционную систему, используя либо отпечаток пальца, либо пароль (при условии, что у него имеются соответствующие разрешения (см. две предыдущих политики)).	Для входа в операционную систему данный пользователь **должен** использовать и отпечаток пальца и пароль (многофакторная идентификация). Обратите внимание, что пользователь не сможет войти в операционную систему, если хотя бы одна из следующих политик запрещена: IDenium - вход по отпечатку; IDenium - вход по паролю.
IDenium - ввод отпечатков пользователем	Данный пользователь может использовать BioLink IDenium Windows Logon для самостоятельного ввода / изменения биометрических идентификаторов (отпечатков пальцев) в BioLink IDenium.	Данный пользователь **не может** самостоятельно ввести в BioLink IDenium свои биометрические идентификаторы (отпечатки пальцев).
IDenium – идентифицировать пользователя при вводе отпечатков	Перед тем, как изменить свои биометрические идентификаторы (отпечатки пальцев), данный пользователь должен идентифицировать себя,	Идентификация пользователя перед изменением биометрических идентификаторов (отпечатков пальцев) не требуется.

	предъявив уже введенные биометрические идентификаторы.	
IDenium - кэшировать креденшилы	Идентификаторы пользователя будут сохраняться на АРМ пользователя. Если по каким-либо причинам сервер BioLink IDenium становится недоступен, информация, хранимая в кэше локального АРМ пользователя, используется для предоставления доступа к защищенным ресурсам. Включение кэширования может привести к снижению уровня безопасности.	Идентификаторы пользователя **не будут** сохраняться на АРМ пользователя. Если по каким-либо причинам сервер BioLink IDenium становится недоступен, пользователь не сможет получить доступ к защищенным ресурсам.
IDenium - показывать отпечаток	Изображение отпечатка пальца пользователя будет показываться при выполнении операций обучения и проверки идентификаторов.	Вместо изображения отпечатка пальца при выполнении операций обучения и проверки идентификаторов будет отображаться абстрактная картинка.
IDenium – не идентифицировать администратором при вводе отпечатков	При введении или изменении отпечатков пользователя подтверждение администратора не требуется.	При введении или изменении отпечатков пользователя требуется подтверждение администратора с помощью отпечатка пальца.

6.6 Настройка использования смарт-карт

Программный комплекс BioLink IDenium поддерживает вход в операционную систему с помощью смарт-карты.

Программный комплекс BioLink IDenium позволяет заменить ввод ПИН-кода карты на биометрическую идентификацию. При этом стандартные Windows-процедуры по настройке центра сертификации и выдачи карт не меняются. Для того чтобы пользователь мог входить в операционную систему с помощью смарт-карты и использовать биометрическую идентификацию, достаточно в свойствах пользователя указать ПИН-код карты, которая выдана этому пользователю.

Подробнее о работе со смарт-картами в операционной системе Windows см.:

- Инструкции по использованию смарт-карт (http://technet2.microsoft.com/windowsserver/ru/library/17a1f58e-b176-4389-ab45-6aa3a314b5ef1049.mspx?mfr=true).
- Внедрение использования смарт-карт для входа в Windows (http://technet2.microsoft.com/windowsserver/ru/library/b989f4fd-febd-42e1-a130-9e0f338007341049.mspx).

Чтобы позволить пользователю использовать биометрические идентификаторы вместо ввода PIN-кода карты, выполните следующие действия:

1. Возьмите специальным образом отформатированную карту, на которую может быть записан цифровой сертификат. Вместе с картой вы получите и уникальный PIN-код для этой карты.
2. Выдайте пользователю **цифровой сертификат** и **запишите его на карту** (используйте стандартные средства Windows).
3. С помощью вкладки **BioLink–CardLogon**, введите PIN-код карты в соответствующие поля.

Теперь пользователь после вставки карты в считыватель карт должен будет предъявить свои биометрические идентификаторы вместо PIN-кода.

Разработчики BioLink IDenium настоятельно рекомендуют использовать устройство BioLink U-Match 5 (сканер отпечатков пальцев с интегрированным считывателем карт) для входа в систему с помощью смарт-карт.

6.7 Управление сценариями BioLink IDenium Password Vault

Модуль BioLink IDenium Password Vault позволяет записывать последовательность действий пользователя в окнах приложений в виде сценариев и впоследствии проигрывать эти сценарии в зависимости от соответствующей политики по предъявлению биометрических идентификаторов или без каких-либо запросов.

Как правило, данная функциональность особенно полезна в случае, когда приложение требует авторизации пользователя для выполнения каких-либо действий. Таким образом, пользователь может записать для каждого такого диалогового окна свой сценарий Password Vault. После записи сценария, пользователю больше не нужно будет вводить имя пользователя и пароль.

6.7.1 Предназначение модуля BioLink IDenium Password Vault

Модуль BioLink IDenium Password Vault в первую очередь предназначен для упрощения доступа к различным приложениям, требующим аутентификации пользователя.

С помощью BioLink IDenium Password Vault можно выполнять следующие действия:

- Записывать сценарии для последующего выполнения;
- Выполнять сценарии;
- Изменять параметры сценариев;
- Удалять сценарии.

Администратор BioLink IDenium может запретить пользователям самостоятельно изменять параметры созданных ими сценариев. Таким образом, администратор BioLink IDenium может требовать предъявление биометрических идентификаторов при авторизации в каких-либо приложениях.

Сценарии BioLink IDenium Password Vault хранятся в базе данных службы каталогов Active Directory.

6.7.2 Возможности администратора при управлении сценариями BioLink IDenium Password Vault

Администратор BioLink IDenium может управлять сценариями Password Vault каждого пользователя BioLink IDenium.

Данное управление включает в себя следующие задачи:

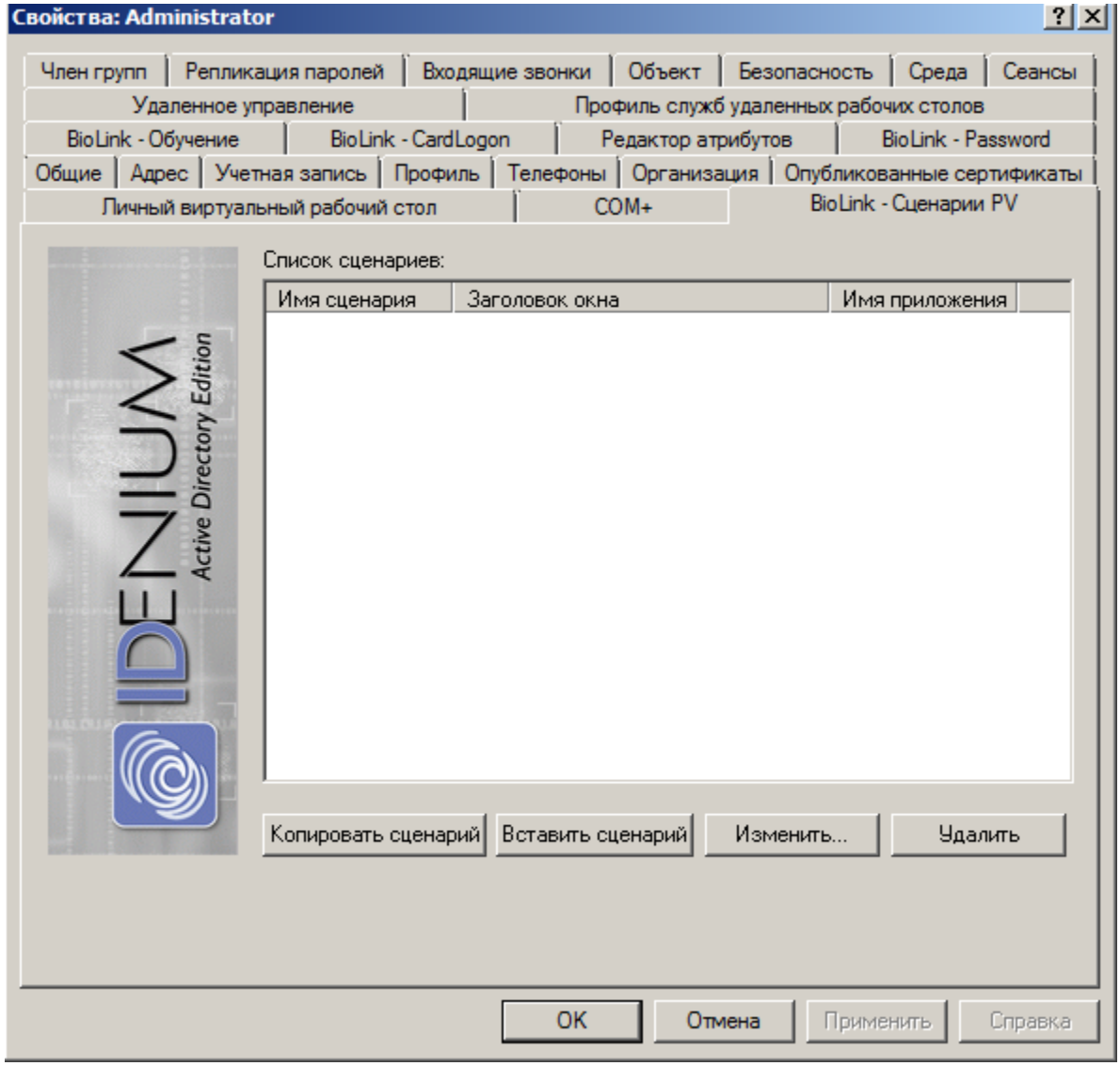
- Изменение сценариев Password Vault пользователя;

- Удаление сценариев Password Vault пользователя;
- Запрет самостоятельного изменения сценариев Password Vault пользователем.

Чтобы управлять сценариями Password Vault пользователя BioLink IDenium, выполните следующие действия:

1. Запустите оснастку администрирования доменов **Active Directory – Пользователи и компьютеры** из комплекта утилит Active Directory;
2. Выберите домен, в котором зарегистрирован пользователь. Затем выберите папку **Users**;
3. Выберите пользователя, чьи политики идентификации будут изменены;
4. Выполните одно из следующих действий:
   - Выберите пункт **Свойства** в меню **Действия**;
   - Нажмите кнопку **Свойства**  ;
   - Нажмите клавишу **ENTER**;
5. Перейдите на вкладку **BioLink – Сценарии PV**;
6. Выберите сценарий Password Vault и нажмите одну из следующих кнопок:
   - **Копировать сценарий** - для создания копии выбранного сценария;
   - **Вставить сценарий** - для добавления копии выбранного сценария;
   - **Изменить...** - для редактирования выбранного сценария;
   - **Удалить** - для удаления выбранного сценария.

Вкладка «BioLink - Сценарии PV»



Чтобы запретить пользователю BioLink IDenium самостоятельно вносить изменения в какой-либо сценарий Password Vault, выполните следующие действия:

1. Выберите **сценарий Password Vault**, самостоятельное изменение которого необходимо запретить;
2. Нажмите кнопку **Изменить**;
3. В диалоговом окне **Редактирование сценария** установите флажок **Запретить пользователю изменять этот сценарий**.

6.7.3 Структура ядра Password Vault

В ядро Password Vault встроены три объекта:

- **oInput,**
- **oSystem,**
- **oWin.**

Каждый из них имеет соответствующий набор методов:

- oInput.AbsoluteScreenCoordinates – позволяет указывать использование абсолютных координат или виртуальных,
- oInput.PlayInput ("string") – задает проигрывание последовательности нажатий клавиш клавиатуры или кнопок мыши,
- oSystem.FindTopWindow (class, name) – задает поиск окна с заданным именем класса или имени окна. Результат поиска – новый объект типа oWin,
- oSystem.Sleep (msec) – указывается задержка в миллисекундах,
- oWin.SetForegroundWindow – задается установка окна в состояние фокуса,
- oWin.SetWindowSize (x, y, cx, cy) – указывается позиция и размер окна,
- oWin.FindChildWindowWithID (class, id, title) – задается поиск дочернего окна с заданными параметрами (достаточно указать одно из них). Результат – новый объект типа oWin.

Поддерживаемые переменные:

##DOMAIN## - передача имени домена

##USER## - передача доменного имени авторизованного пользователя

##PASSWORD## - передача доменного пароля авторизованного пользователя

6.7.4 Публичные сценарии и параметры

Начиная с версии BioLink IDenium 4.2, добавлена возможность записи публичных сценариев и их параметризации.

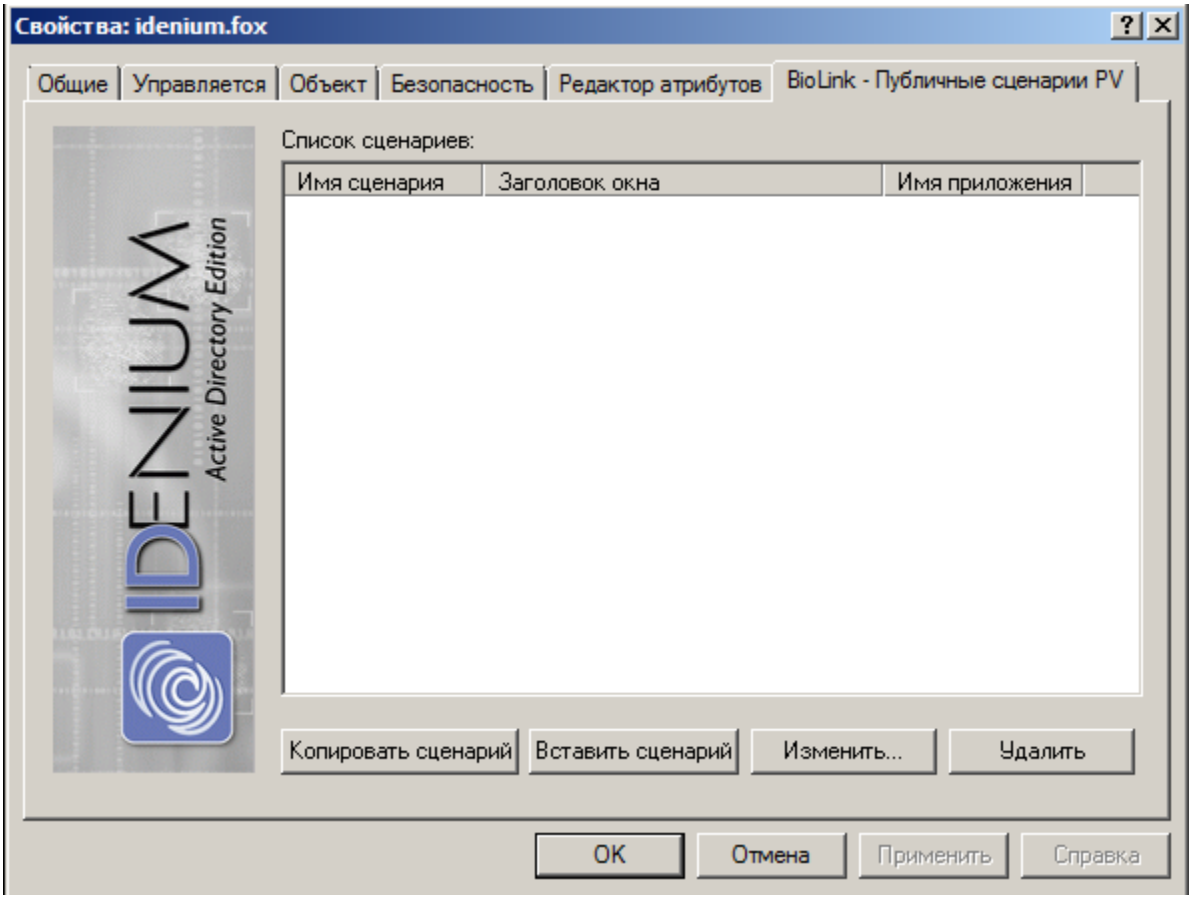
Внимание!!! Не рекомендуется использовать публичные сценарии совместно с обычными для одного приложения и/или пользователя (группы).

6.7.4.1 Запись публичного сценария

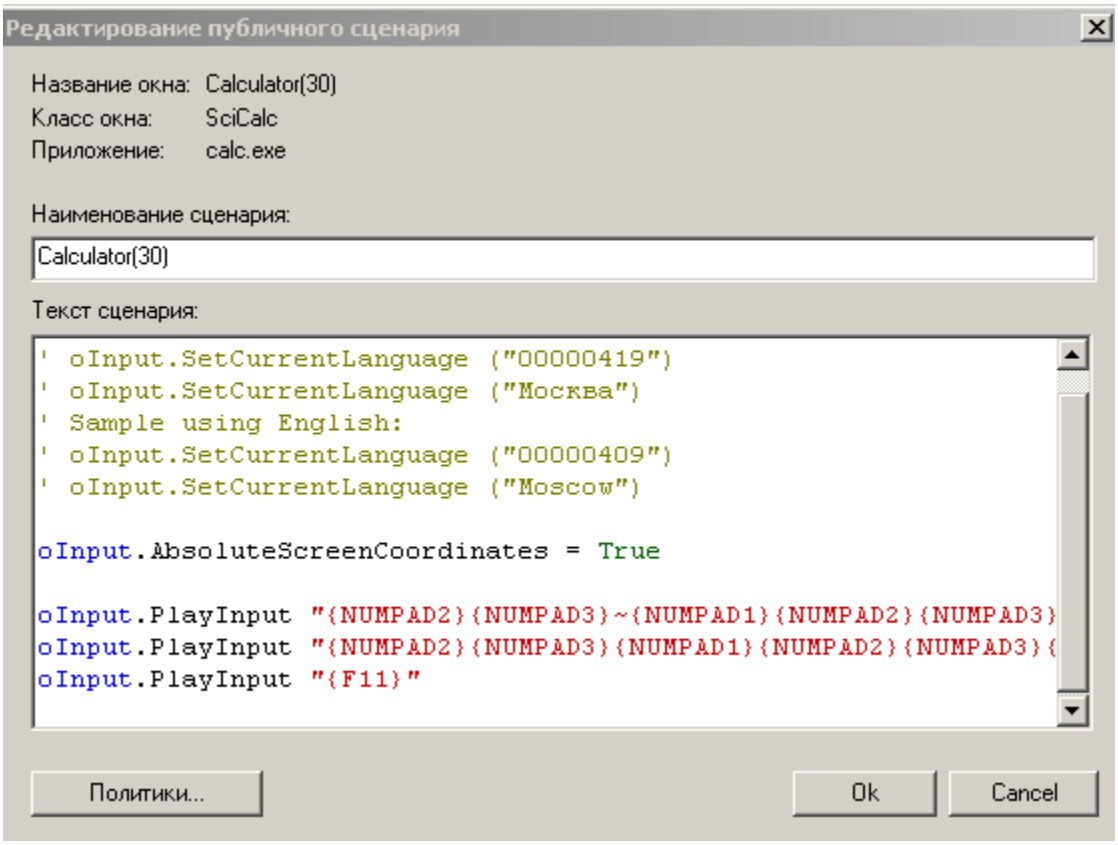
Для записи публичного сценария, необходимо выполнить следующие

действия:

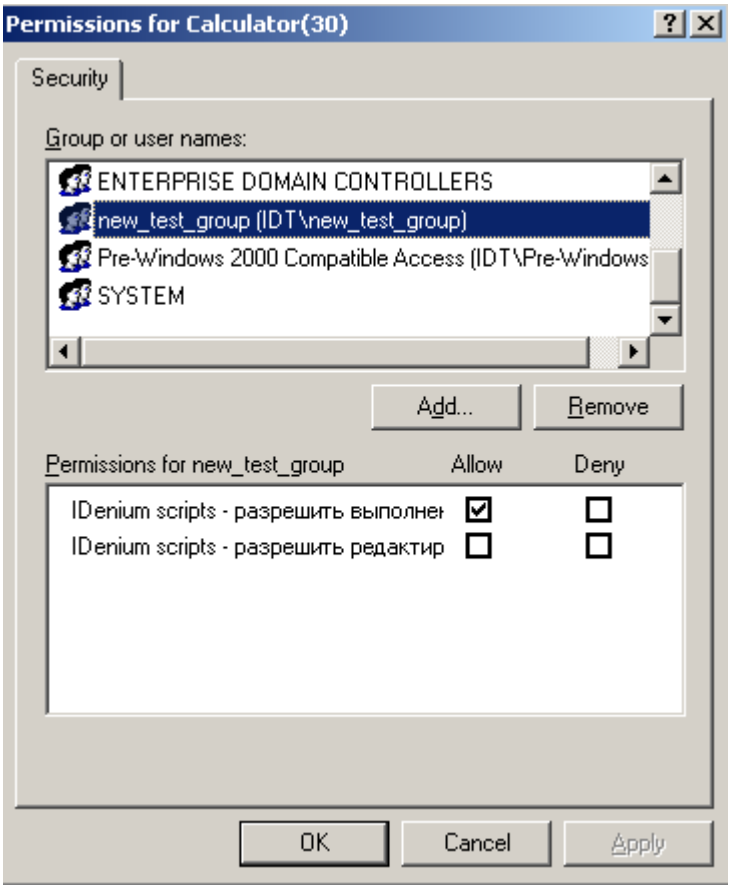
1. Запишите сценарий на приложение так, как указано в "Руководстве пользователя BioLink IDenium" или скопируйте уже записанный сценарий.
2. Далее в оснастке ADUC (Active Directory Users and Computers) выберите свойства вашего домена.
3. Перейдите на вкладку "BioLink - Публичные сценарии PV" и нажмите вставить сценарий.



4. Нажмите изменить и отредактируйте сценарий добавив, по необходимости параметры (подробнее параметры сценариев описаны в Параметры в публичных сценариях BioLink Password Vault)



5. Для назначения сценария группам пользователя нажмите кнопку "Политики".



IDenium scripts - разрешить выполнение, назначает выполнение сценария пользователю или группе пользователей.

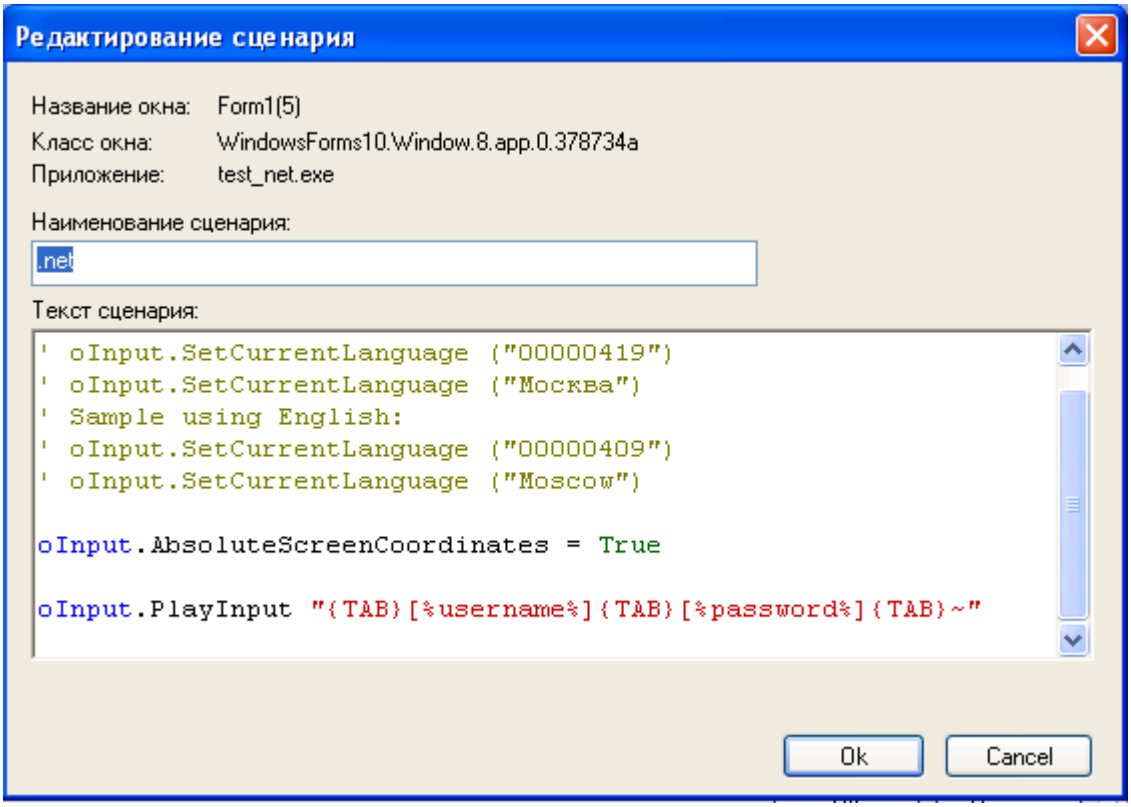
IDenium scripts - разрешить редактирование, разрешает редактирование тела сценария пользователю или группе пользователей.

6.7.4.2 Параметры в публичных сценариях BioLink Password Vault

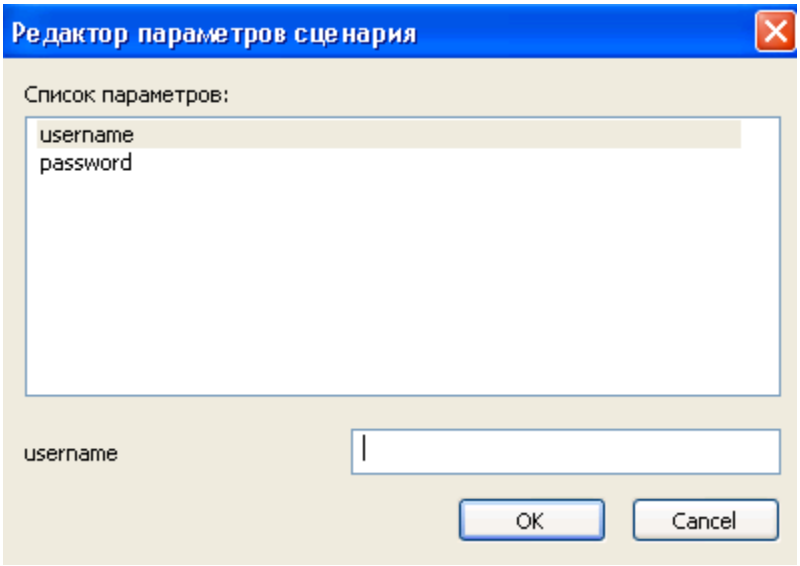
Параметры в публичных сценариях BioLink Password Vault

Параметры реализуют следующую схему воспроизведения сценариев Password Vault:

1. Параметры задаются тегами [% %]. Например, на скриншоте ниже приведен пример, когда заданы два параметра username и password, которые будет заполнить пользователю при прохождении первой успешной идентификации.



2. Со стороны пользователя заполнение параметров выглядит как указано на скриншоте ниже.



Также существует возможность отключить просмотр значения параметра в окне редактора параметров сценария. Для этого имя параметра в скрипте обрамляется тегами [%@ %].