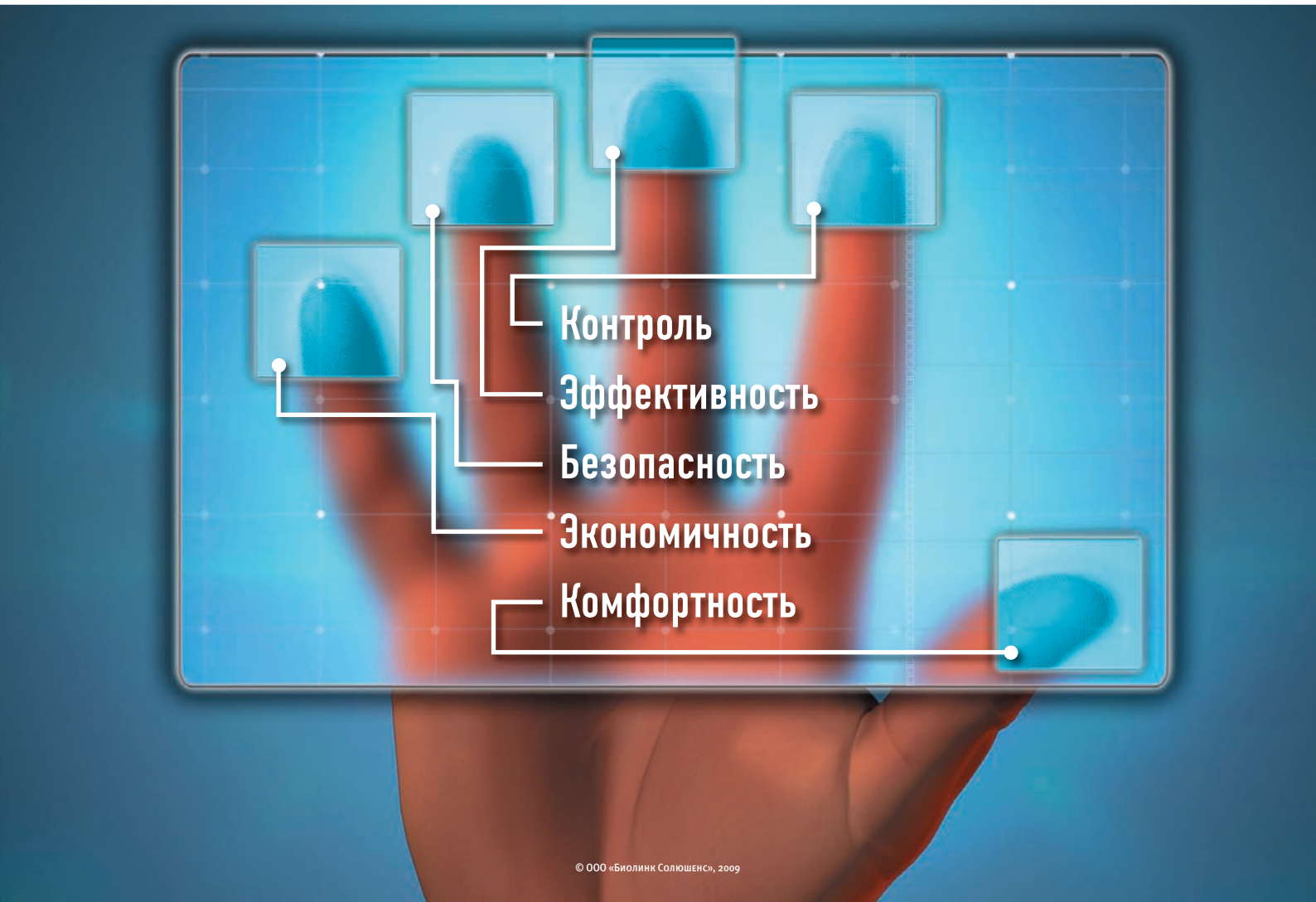
BioLink

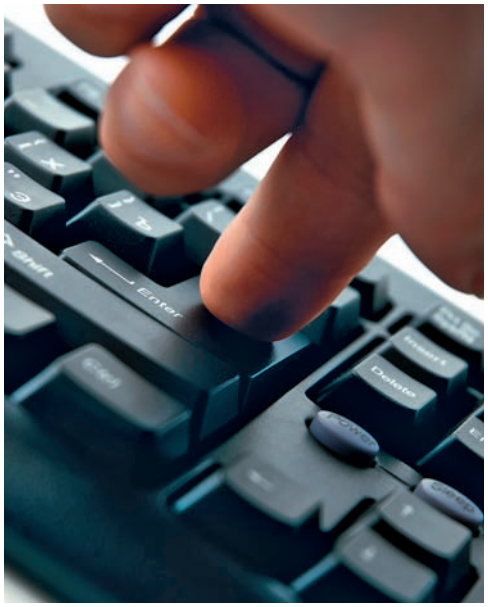
Передовые Биометрические Решения

IDENIUM

Сервис биометрической идентификации пользователей в корпоративных сетях и приложениях



Человеческий фактор — бороться или использовать?



Что служит главным звеном информационной безопасности — антивирусы, резервирование и шифрование данных, системы обнаружения атак? В информационной системе любой компании, независимо от ее размера и сферы деятельности, всегда имеется и чрезвычайно важны механизмы идентификации пользователей и управления их доступом к корпоративным ресурсам.

Наиболее распространенный из таких механизмов — «связка» логин+пароль. Считается, что пароли бесплатны, просты в применении и при надлежащем контроле обеспечивают нужную защиту. Но неужели Вы готовы доверять расхожим мнениям?

- 150 долларов на одного пользователя ежегодно — таковы затраты каждой компании на администрирование паролей. От 30 до 40 процентов от общего числа обращений в службу поддержки составляют запросы тех, кто забыл пароли и/или заблокировал вводом неправильных паролей свои рабочие станции (Gartner Group);
- не менее 9 неповторяющихся символов в каждом пароле, не менее 4 разных паролей для различных задач (доступ в сеть, к почтовому и файловому серверам, бухгалтерской, финансовой, CRM и ERP системам и т.д.), регулярная смена всех паролей — таковы минимальные требования безопасности парольной системы;
- 25% пользователей хранят пароли в виде обычного текста на компьютере, 22% применяют с этой целью портативные и мобильные устройства, каждый шестой пользователь записывает пароли на бумаге (RSA). 80 процентов от всех атак приходится на взлом или подбор паролей (Computer Emergency Response Team).

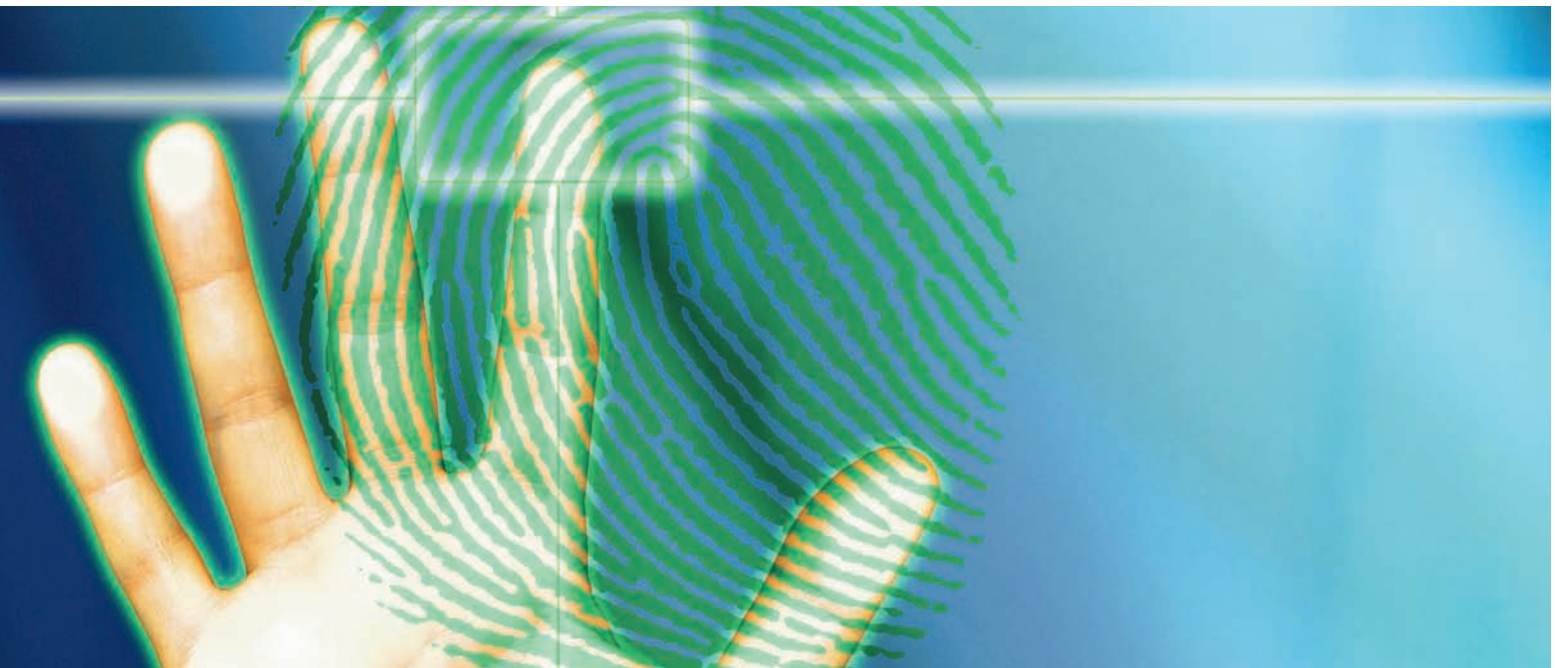
- **5 млрд евро — ущерб, нанесенный банку Societe Generale его менеджером Жеромом Кервьелем, использовавшим в своих махинациях пароли коллег.**
- **90 млн евро — сумма, которую пытался украсть у банка HSBC Джагмит Чанна с помощью похищенных паролей.**
- **6 евро — стоимость подарочного сертификата, на который готовы были обменять сведения о корпоративных паролях участники опроса moneysupermarket.com.**

Более высокий уровень защиты предоставляют аппаратные идентификаторы — карты, токены, брелоки. Однако их применение весьма затратно, но главное — их можно так же похитить или украсть, как и пароли.

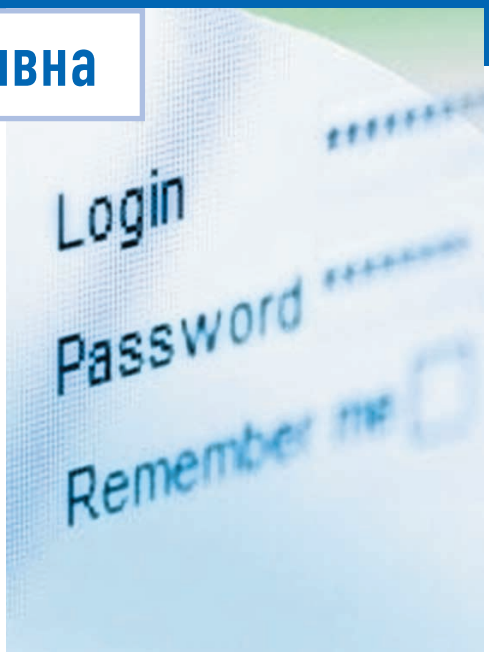
Так нужно ли «бороться» с пользователями, заставляя их помнить и вводить длинные, сложные и разные пароли? Или, быть может, израсходовать значительные суммы на аппаратные идентификаторы, всё равно не решив главных задач?

Ответ прост. Каждый человек обладает уникальными биометрическими параметрами. С одной стороны, их нельзя забыть, похитить или «одолжить на время». С другой — легко и просто применять для идентификации и управления доступом к информационным ресурсам. Биометрические технологии могут эксплуатироваться вместе с паролями и/или аппаратными идентификаторами, компенсируя их недостатки и усиливая систему безопасности в целом.

В России эффективные решения для защиты информации на основе технологий биометрической идентификации разработаны и в индустриальных масштабах производятся компанией BioLink. BioLink и его партнеры во всех федеральных округах выполняют полный комплекс необходимых услуг — от внедрения до сопровождения и технической поддержки — и поставляют весь спектр аппаратных и программных решений — от сканеров отпечатков пальцев до систем учета рабочего времени, контроля физического доступа, обслуживания клиентов и посетителей, интеграции биометрии в другие информационные системы.



Биометрия — защита, которая эффективна



В отличие от других решений по идентификации, внедрение биометрии не усложняет работу пользователей и не требует от них дополнительных действий и временных затрат на соблюдение регламентов по защите информации. Эти регламенты исполняются максимально быстро и легко, что, однако, не сказывается на уровне безопасности. И действительно — что может быть проще и скорей, чем коснуться сканера отпечатков пальцев или взглянуть на сканер радужной оболочки глаза!

По оценкам International Biometric Group и Acuity Market Intelligence, на мировом биометрическом рынке лидируют, занимая до двух третей от его общего объема, технологии идентификации по отпечаткам пальцев. Эти технологии эффективно синтезируют точность и надежность распознавания, удобство и скорость идентификации и приемлемую стоимость сканеров, которые поставляются и в виде отдельных устройств, и в качестве встраиваемых (в ноутбуки, смартфоны и т.п. устройства) модулей.

Чем же обусловлена популярность идентификации по отпечаткам пальцев в системах защиты информации?

Безопасность: устраняем слабое звено

- отпечаток пальца неотъемлем от пользователя. Биометрия естественным образом (в буквальном смысле этих слов) снимает проблемы хищения, утери, передачи, взлома или подделки паролей и материальных идентификаторов;
- отпечаток пальца характеризует конкретного человека и возлагает на него персональную ответственность за соблюдение регламентов безопасности. Их нарушения легко выявляются и не могут быть оправданы неустранимыми изъянами паролей и материальных идентификаторов;
- изображение отпечатка преобразуется в последовательность двоичных символов, из которой невозможно ни воссоздать реальное изображение, ни «сконструировать» поддельное.

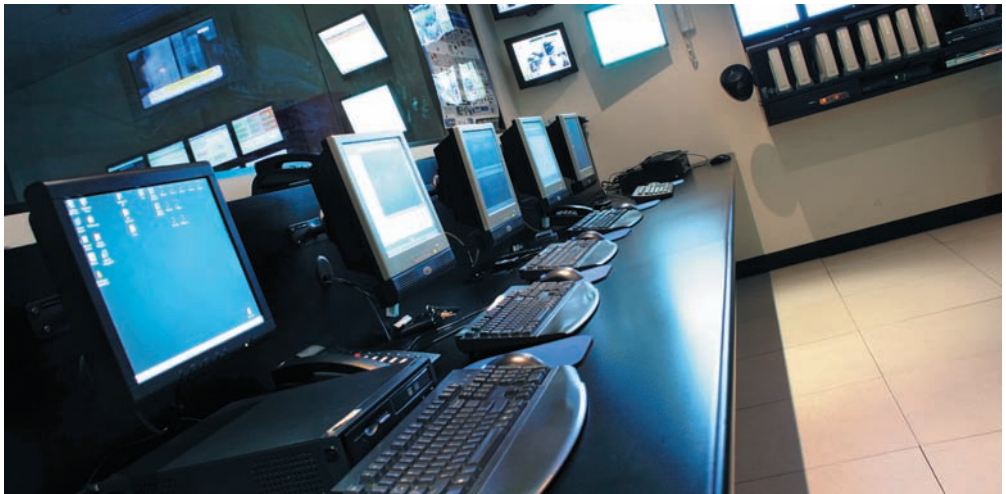
Экономичность: снижаем расходы на защиту

- минимизируются затраты рабочего времени при авторизации. Скорость сканирования отпечатка пальца не превышает 0,5 секунды;
- идентификаторы не теряются и не выходят из строя. Можно зарегистрировать несколько отпечатков пальцев, и, если пользователь, к примеру, порезался, он может пройти идентификацию по «резервному» отпечатку;
- сокращается нагрузка на администраторов и службу безопасности. Они избавляются от решения проблем пользователей, забывших или неверно набравших пароли.

Комфортность: повышаем лояльность персонала

- пользователи освобождаются от необходимости вводить пароли или носить с собой материальные идентификаторы, возмещая стоимость утраченных или испорченных карт, токенов и жетонов;
- у обычного человека 10 пальцев рук — в отличие от всего лишь одной головы, двух глаз или двух рук.

Алгоритмы биометрической идентификации, разработанные компанией BioLink , постоянно входят в число победителей открытых конкурсов, на регулярной основе проводимых Институтом стандартов и технологий (National Institute of Standards and Technology — NIST).



Успешные внедрения

Народный банк, Казахстан

- сканеры отпечатков пальцев и прикладное программное обеспечение биометрической идентификации на 9 000 рабочих мест;
- основной и резервный серверы биометрической идентификации;
- интеграция биометрической идентификации в специализированные банковские приложения;
- планы применения биометрических технологий в банкоматах.

Западно-Сибирский коммерческий банк, Россия

- биометрическая идентификация пользователей корпоративной сети;
- биометрическая система функционирует в головном офисе и 30 филиалах;
- идентификация сотрудников банка при доступе в корпоративную сеть, к финансовым системам, защищенным Интернет-ресурсам.

Завод «Тяжмаш», Сызрань, Россия

- биометрическая идентификация инженеров, конструкторов, техников;
- интеграция биометрии в специализированные программные продукты, применяемые при проведении опытно-конструкторских работ и в инжиниринге;
- планы распространения биометрии на филиалы предприятия и использования биометрических систем учета рабочего времени и контроля доступа.

Министерство массовых коммуникаций и связи, Россия

- оснащение аппаратными и программными средствами биометрической идентификации рабочих мест сотрудников центрального аппарата Министерства и находящихся в его ведении федеральных агентств и служб;
- программный сервер централизованной биометрической идентификации;
- проект реализован в два этапа с последовательным увеличением численности пользователей биометрической системы.

BioLink IDenium — сервис биометрической идентификации

IDENIUM

Администрирование с помощью стандартной оснастки управления пользователями Microsoft AD	✓
Автоматическая генерация и смена паролей пользователей домена	✓
Количество регистрируемых отпечатков пальцев	10
Централизованная или удаленная регистрация биометрических данных пользователей	✓
Возможность автономной работы (при временном отсутствии соединения с сервером идентификации)	✓
Полностью автоматическое развертывание клиентского ПО	✓

Сервис BioLink IDenium комплексно решает все задачи информационной безопасности, связанные с идентификацией пользователей и управлением их доступом к корпоративным ресурсам. Главные функции сервиса:

- замена (или дополнение) логинов, паролей, карт, брелоков, токенов надежной и эффективной биометрической идентификацией;
- централизованное управление правами и полномочиями пользователей и жизненным циклом их учетных записей;
- протоколирование событий доступа, мониторинг и аудит.

Полная интеграция с Microsoft Active Directory

- удобный интерфейс управления биометрическими идентификаторами и настройками системы;
- управление правами пользователя и параметрами клиентских рабочих станций через политики администрирования;
- репликация и синхронизация данных в масштабе организации.

Многофакторная идентификация

- возможно как применение исключительно биометрических технологий, так и их совместное использование с паролями и смарт-картами (в различных комбинациях) — например, для защиты доступа к особо ценным ресурсам.

Биометрия в терминальных приложениях

- биометрическая идентификация в удаленных приложениях через терминальные сессии Microsoft RDS и Citrix;
- биометрическая идентификация при входе в Microsoft Remote Desktop Services.

Поддержка Windows 7 и Windows 2008 Server R2

- полная поддержка новейших операционных систем Microsoft;
- соответствующую деятельность BioLink ведет в качестве сертифицированного партнера Microsoft.

Надежность и масштабируемость

- развертывание в организации любого масштаба;
- поддержка сложной многодоменной архитектуры (дерево, лес доменов);
- произвольное количество серверов идентификации в домене для отказоустойчивости и масштабирования нагрузки;
- включение/выключение дополнительных серверов в конфигурацию в «горячем» режиме.

Удобство администрирования

- не нужно выдавать пароли доступа в сеть и приложения и создавать новые пароли забывчивым пользователям;
- единый с Windows интерфейс управления биометрическими данными, настройками и политиками;
- поддержка автоматического развертывания программного обеспечения рабочих станций.

Password Vault — единый биометрический вход во все приложения

- отпадает необходимость вести списки паролей для всех Ваших приложений;
- единственное, что требуется от пользователя для входа во все корпоративные приложения — предъявить ранее зарегистрированный отпечаток пальца;
- обеспечены централизованное управление и настройка, импорт списков паролей.

BioLink
Передовые Биометрические Решения

ООО "Биолинк Солюшенс"
Россия, 125493, Москва, ул. Авангардная, д. 3
Тел./Факс: +7 (495) 645-8703, 645-8704

E-mail: biolink@biolink.ru
www.biolink.ru