Литература

1. Голицына, О.Л. Базы данных: учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - Изд. 2-е, испр. и доп. - М. : ФОРУМ : ИНФРА-М, 2007. - 399 с.

2. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=F01700314 – Дата доступа: 22.03.2024.

УДК 004.056.5

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ. ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ В ЗАЩИТЕ ИНФОРМАЦИИ

Савко Д.Д.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В современном мире при постоянно возрастающей популярности и необходимости использования информационных технологий острее становится проблема сохранения приватности данных, особенно, в сети Интернет. Поэтому защита пользовательской информации, начиная с аккаунтов в социальных сетях и заканчивая сохраненными в облаке деловыми документами, сегодня имеет большое значение в любой сфере деятельности человека.

Пожалуй, стоит начать с таких понятий, как идентификация и аутентификация, поскольку они являются самыми первыми и обязательными процедурами защиты данных.

Идентификация – это такая процедура, при которой пользователь (субъект) передает системе свой идентификатор, который индивидуализирует, однозначно определяет субъекта в информационном пространстве. В качестве примера идентификации можно привести ситуацию, когда система запрашивает у пользователя логин; если такой логин есть в базе данных системы, то субъект определяется как существующий в системе.

После того, как пользователь идентифицирован, система делает ему запрос на ввод пароля – это этап аутентификации. Эта процедура проверяет подлинность введенной информации, сравнивая ее с занесенной в базу данных ранее (еще на этапе регистрации). Важно отметить, что вводимая субъектом информация разнится в зависимости от способа аутентификации, но

об этом чуть позже. В результате сравнения паролей система соглашается или не соглашается с тем, что пользователь – настоящий владелец приложения, аккаунта или другой системы.

Также стоит сказать о популярной сегодня двухфакторной аутентификации. Наиболее известным примером можно считать аутентификацию в системе Mail.Ru, которая «требует подлинности двух факторов». Первый – это введение постоянного пароля, второй – одноразового пароля или кода проверки, который генерируется через физическое устройство или специальное приложение.

Таким образом, идентификация и аутентификация неразрывно связаны, так как проверку нельзя будет начать, пока система не сможет понять, подлинность какого субъекта необходимо проверить.

Поскольку уровень киберпреступности в информационно продвинутом обществе растет с каждым годом, использование биометрических данных в устройствах и программах защиты информации становится закономерным.

Существуют различные виды аутентификации в зависимости от уникальных для каждого пользователя биометрических показателей (образцов). Специалисты выделяют два метода, на которых основывается современная аутентификация: статический и динамический. С помощью первого метода распознаются врожденные физические параметры человеческого тела: отпечатки пальцев, геометрия лица, термограмма и др. Второй метод используется для анализа индивидуальных особенностей поведения, голоса субъекта аутентификации.

Несмотря на то, что долгое время основными на рынке биометрической защиты данных оставались статические методы аутентификации, в последнее время активно совершенствуются именно динамические методы защиты. Рассмотрим наиболее известные разновидности статического метода аутентификации:

Дактилоскопия, или распознавание отпечатков пальцев. Преимущества данного метода заключаются в легкости его использования и надежности уникальности данных, кроме того, дактилоскопический сканер относительно недорог. Минусами дактилоскопии можно назвать сбои при недостаточном контакте пальца со сканером, а также риски использования качественного муляжа или «мертвого» пальца.

Аутентификация по радужной оболочке/сетчатке глаза. Данный метод защиты значительно дороже, нежели дактилоскопия, однако надежность его применения гораздо выше. Своеобразность рисунка кровеносных сосудов глазного дна, а также уникальность радужной оболочки глаза обуславливают максимальную степень защиты данных. Более того, устройства такой аутентификации имеют дополнительную функцию определения жизнеспособности глаза, что практически исключает вероятность использования

муляжа. Данный вид защиты данных получил широкое применение в банковской сфере, а также в аэропортах для аутентификации работников при переходе в зону ограниченного доступа.

Аутентификация по геометрии рук/лица. С помощью этого метода проводятся измерения кистей рук или лица сразу комбинированно сразу по нескольким параметрам. Но серьезным недостатком аутентификации по геометрии рук является то, что при наличии заболеваний и повреждений костей проведение ее становится просто невозможным. Однако загрязненность, температура и влажность руки не станут препятствием при проверке; кроме того, процесс аутентификации занимает мало времени, всего несколько секунд. Что касается аутентификации по геометрии лица, вероятность ложной проверки двухмерного распознавания лица колеблется от 0,1 до 1%. Более совершенным сегодня становится трехмерное распознавание лица, однако оценки надежности нового метода еще не представлены специалистами.

Динамические методы биометрической аутентификации:

Распознавание голоса. В этом случае распознавание производится по большому количеству параметров: тональность, модуляция, произношение, интонация, особенности дыхания – анализируются все голосовые характеристики.

Распознавание клавиатурного почерка. Сейчас данный метод аутентификации является одним из наиболее перспективных, поскольку, практически, каждый человек является пользователем ПК или мобильного устройства. Данный метод рассматривает такие особенности клавиатурного почерка каждого пользователя, как скорость ввода символов, частота ошибок, сила нажатия на клавиши, использования комбинаций клавиш и другие.

Верификация биометрической подписи. Востребованность электронных подписей, опять же, связана с информационно-техническим прогрессом. Важно разграничить понятие электронной цифровой подписи (ЭЦП), которая официально регистрируется, и биометрической подписью. Первая (ЭЦП) накладывается как печать, созданная по шаблону (как копия). Верификация второй, биометрической подписи – это процедура, при которой анализируются динамические характеристики написания – угол наклона светового пера, нажатие и резкость выведения подписи и т.п.

При всем удобстве использования динамических методов защиты недостатки у них все же есть, и главный из них – это зависимость от психофизического состояния человека. Таким образом, современные технические возможности обуславливают разнообразие методов защиты информации, в особенности – биометрических методов. При этом преимущества и недостатки можно найти у каждого метода.

Литература

1. Аутентификация и авторизация [Электронный ресурс]. – Режим доступа: https://vladislaveremeev.gitbook.io/qa_bible/seti-i-okolonikh/autentifikaciya-i-avtorizaciya-authentication-and-authorization. – Дата доступа: 18.03.2024.

2. Современные методы биометрической идентификации [Электронный ресурс]. – Режим доступа: https://www.azone-it.ru/sovremennye-metody-biometricheskoy-identifikacii. – Дата доступа: 18.03.2024.

УДК 004.6

БАЗЫ ДАННЫХ: ОБЛАСТИ ПРИМЕНЕНИЯ

Савко Д.Д., Капустина Д.С.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Современные информационные технологии играют одну из наиболее важных ролей в жизни общества, поскольку данные (информация) – основа и фактор эффективности любой сферы деятельности.

Любая информация требует компьютерной обработки и целесообразного структурирования. Именно качественная структура данных позволяет пользователю оптимизировать его работу, т.е. быстро и безопасно получать доступ к данным, упорядочивать огромные объемы запрашиваемой информации и др. Такую структуру может обеспечить база данных (БД) – своеобразный контейнер с информацией, хранимой в соответствии с нуждами пользователей в электронном виде.

Классифицировать базы данных следует исходя из способов обработки и хранения данных:

– БД с иерархической моделью может быть представлена в виде древовидной модели, включающей объекты различных уровней и подуровней;

– БД с сетевой моделью состоит из объектов, связанных между собой иерархическими связями, но при этом эти объекты могут ссылаться на объекты других уровней;

– реляционная БД структурирует информацию в виде таблиц, где строки представляют собой отдельные элементы данных, а столбцы хранят данные определенного типа. [1]

Закономерно, что в зависимости от приведенной классификации, базы данных обладают разными характеристиками. Плюсами иерархической БД являются простота структуры, эффективная навигация и поиск данных, легкость создания, в то время как ограниченная гибкость модели, трудности в