Е. Ю. Гурина, А. А. Модестов

МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ДЛЯ ДИСТАНЦИОННЫХ СИСТЕМ ОБРАЗОВАНИЯ

Виды дистанционного образования

Прежде чем строить физическую систему защиты, нужно определиться с самим объектом защиты, а именно выяснить, какие системы дистанционного образования (ДО) существуют, какая у каждой из них архитектура, и только после этого можно будет определить, что нужно защищать. Для этого прежде всего необходимо рассмотреть понятие дистанционного образования.

Согласно Концепции создания и развития единой системы дистанционного образования в России, принятой 31 мая 1995 г. Минобразования РФ, под дистанционным образованием понимается «комплекс образовательных услуг, предоставляемых широким слоям населения в стране и за рубежом (страны СНГ, Азия, Африка) с помощью специализированной информационно-образовательной среды на любом расстоянии от образовательного учреждения. Информационно-образовательная среда дистанционного образования представляет собой системно организованную совокупность средств передачи данных, информационных ресурсов, протоколов взаимодействия, аппаратно-программного и организационно-методического обеспечения, ориентированную на удовлетворение образовательных потребностей пользователей» [1].

В сравнении с традиционными системами образования ДО позволяет для каждого пользователя ресурсов системы построить собственную «траекторию» обучения, которая была бы удобна как пользователю, так и тем, кто предоставляет ДО. Согласно работе [2], системы ДО отличаются от традиционных систем гибкостью, адаптируемостью, модульностью, экономичностью, большей ориентацией на пользователя и большей опорой на внешние и внутренние коммуникативные и информационные технологии.

Существуют следующие виды ДО:

1. *Рассылка* файлов учебных материалов по электронной почте пользователям;

2. *Удаленный доступ* к учебным материалам как через Интернет, так и по локальной сети ДО. При этом пользователю предоставляется возможность скачивать материалы или использовать специальную обучающую программу;

3. *Чат-занятия* осуществляются с помощью чат-технологий. Во время занятия все участники имеют одновременный доступ к чату;

4. *Веб-форумы* — совместная работа пользователей по выделенной задаче при помощи записей и сообщений, оставляемых на сайте с установленной на нем программой.

Отличие (3) от (4) в том, что во втором случае возможен более длительный (многодневный) период работы над задачей без одновременного взаимодействия участников.

5. *Телеконференции* проводятся на основе списков рассылки участников по электронной почте, где в письме указываются логины и пароли входа в систему телеконференции, задается точное время начала телеконференции и имя ведущего.

Все системы ДО по методу доступа можно разделить на 3 категории: в режиме реального времени, по запросу, смешанные (первое и второе одновременно). В иностранной литературе существует похожая классификация: синхронное обучение, асинхронное обучение, смешанное. Из-за множества различных способов дистанционного обучения синхронное и асинхронное обучения размыты.

Вышеперечисленные системы ДО используют следующие информационные ресурсы: электронные библиотеки, аудио- и видеоматериалы, базы данных (БД).

Обзор архитектур информационных систем, реализующих дистанционное обучение

На рис. 1 представлена упрощенная схема структуры ДО.

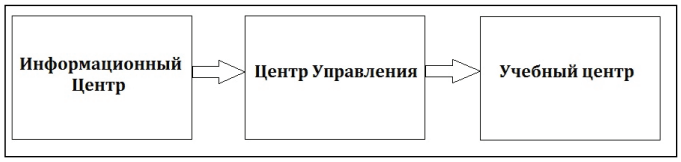

Рис. 1. Упрощенная схема архитектуры системы ДО

Элементами архитектуры Информационного Центра являются базы данных учебных материалов (электронные библиотеки, видео- и аудиоматериалы и др.), процессы разработки новых учебных материалов, сотрудники (преподаватели), разрабатывающие учебные материалы и курсы, и др.

Элементами архитектуры Центра Управления являются сервер, управляющий сетью и каналами связи, веб-сервер, база данных участников системы ДО, процессы поддержки обучения в режиме реального времени и др.

Элементами архитектуры Учебного центра являются персональные места пользователей (например, находящийся у него дома), учебные места, находящиеся в компаниях / центрах образования, и др.

В определенных системах все три центра могут быть обьединены в один центр или быть разнесенными в пространстве, и связь между ними осуществляется через выделенную сеть (рис. 2). Каналы связи могут быть как защищеными (например, вся сеть находится на одной выделенной территории с ограниченным доступом), так и незащищенными (связь идет через Интернет, где легко перехватить пересылку данных).

Рис. 2. Соединение между блоками через выделенную сеть

В любом случае, **хранение учебных материалов, занятия, запись видео- и аудиоматериалов, их разработка и т. д. производятся** либо в одном, либо в нескольких связанных/несвязанных помещениях.

Угрозы в системах ДО

Существует множество угроз, связанных с информационной безопасностью (ИБ), но хотелось бы отметить специфические угрозы, относящиеся к ДО:

1) изменение/удаление/подмена материала по обучению посторонними лицами;

2) изменение/удаление оценок за выполненные задания посторонними лицами или участниками системы ДО;

3) изменение/удаление выполненных заданий посторонними лицами или участниками системы ДО;

4) копирование конфиденциальной информации системы ДО посторонними лицами;

5) выполнение тестов/заданий или других работ лицами, не являющимися пользователями системы ДО (пользователь просит кого-то сделать за него задание);

6) изменение содержания/доступа к проверочным тестам/заданиям;

7) получение несанкционированной помощи во время экзамена;

8) перехват идентификационных данных преподавателей/пользователей при входе в систему ДО.

Самое слабое звено ситемы безопасности — человек. Поэтому одной из главных проблем ДО является уверенность в том, что пользователь (студент) не нарушает правил пользования системой ДО, что он действительно тратит выделенное время на изучение материала по курсу, выполняет сам все задания. Это регулируется различными методами идентификации/аутентификации [3].

Традиционные методы аутентификации в системах ДО и их недостатки

Виды аутентификации пользователей системы ДО показаны на рис. 3.

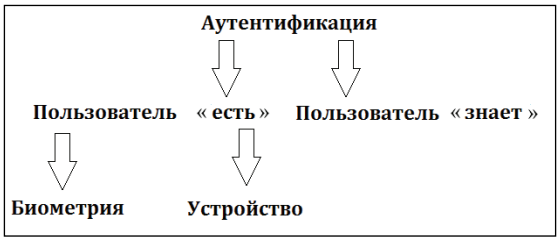

Рис. 3. Виды аутентификации пользователей системы ДО

Вид аутентификации «Пользователь "знает"» зависит от сохранности идентификационных данных. Аутентификация с помощью пары «логин — пароль» является наиболее распространенным методом. Но логин и пароль могут быть переданы кому-то еще. Это же относится и к аутентификации по почте или по методу «вопрос — ответ» (в иностранной литературе используется термин Q/A based authentication).

Аутентификация по устройству может производиться с помощью специальных карточек (например, IC cards). Карточку сложно подделать, пользователю будет неудобно ее кому-то передавать, так как существующие карточки используются во многих целях (кредитные карты, пропуска студентов и др.). Но для реализации этого метода пользователю нужно приобретать считывающее устройство, что увеличивает финансовые затраты и ликвидирует главное преимущество ДО: везде и в любое время.

Аутентификация по биометрическим показателям в данный момент является наиболее продуктивной. Этот метод значительно уменьшает вероятность подмены одного пользователя другим. Однако такие средства требуют высоких затрат.

Во многих иностранных системах вводится понятие «Инфраструктура аутентификации и авторизации» (AAI — Authentication and Authorization Infrastructure). AAI использует интегрированный подход, поскольку каждая сторона контролирует действия, производимые ею: учебные центры регистрируют и аутентифицируют своих членов, а информационные центры определяют свои правила доступа. Сама схема AAI может быть различной для каждой из организаций/стран, но идея одна. Понятие AAI похоже на понятие «управляющий центр», но все же в иностранной и российской литературе можно найти различия между ними.

Методы защиты ДО с помощью биометрических характеристик

К сожалению, в России методы защиты с помощью биометрических характеристик в ДО не распространены, хотя за рубежом они широко применяются для ДО. Проверка биометрических характеристик производится по следующим направлениям [4]:

Верификация — нужна для проверки подлинности индивида (является ли человек тем, за кого он себя выдает). Данные об индивиде хранятся следующими способами: централизованное хранение верификационных данных (когда биометрические данные хранятся в базе данных и сравниваются с живым оригиналом) и распределенное хранение верификационных данных (когда биометрические данные человека хранятся на носителе, который находится у человека, и сравниваются с данными в базе данных). При верификации есть два рода ошибок — принятие своего за чужого или чужого за своего пользователя.

Идентификация — применяется, когда биометрические данные пользователя неизвестны. Для этого метода необходима уже существующая база биометрических характеристик для всех пользователей, иначе метод не может быть применен. Когда пользователь проходит идентификацию, по считанным с него биометрическим характеристикам делается шаблон, который сравнивается со всеми шаблонами базы данных на единичное (или множественное) совпадение.

Ограничение доступа — (в отличие от двух первых методов) составляется список биометрических параметров (так называемые чек-листы), при совпадении с которыми пользователю отказывается в доступе. Это может быть полный шаблон биометрической характеристики или ее часть.

Перечислим целесообразные для применения в отечественных системах ДО методы биометрической аутентификации, а также их достоинства и недостатки.

1) Контактные биометрические технологии

а) Отпечаток пальца.

Плюсы:

- простота в использовании;
- большое количество данных для создания чек-листов;
- метод доказал свою эффективность во многих крупномасштабных системах в течение многих лет использования;
- отпечатки пальцев уникальны для каждого пальца каждого человека, и расположение линий остается неизменным на протяжении всей жизни.

Минусы:

- общественное предубеждение, связанное с уголовными последствиями, а также конфиденциальность в этом плане;
- получение изображения высокого качества «от ногтя до ногтя» требует подготовки и мастерства, но в настоящее время технология плоских считывателей имеет большую надежность;
- возраст и вид деятельности могут привнести трудности в считывание полного и точного изображения отпечатка.

б) Отпечаток ладони — отличие от отпечатка пальца в том, что отпечаток ладони больше. Для этого нужна более сложная и более дорогостоящая аппаратура, поэтому он в системах ДО не эффективен.

в) Динамика работы с клавиатурой — метод проверяет динамику работы пользователя на клавиатуре. К сожалению, он все еще находится на стадии разработки.

г) Динамическая проверка подписи — метод включает большое количество параметров и предполагает использование стилуса и поверхности, на которой человек пишет.

Это один из наименее точных методов, так как подпись очень легко подделать.

2) Бесконтактные биометрические технологии

а) Распознавание лица — метод связан с распознаванием геометрических характеристик лица.

Плюсы:

- не требуется физический контакт;
- легкодоступные считыватели (камеры);

- большое количество данных для создания чек-листов;
- легко сравнить результаты по разным людям.

Минусы:

- часть лица может быть сокрыта волосами, очками и др.;
- лица меняются со временем;
- метод чувствителен к изменению освещения, выражения лица и позы;
- склонность пользователей предоставлять видеоизображения плохого качества, но ожидать точных результатов.

б) Термография лица — аутентификация по термографии лица предполагает, что у пользователя есть своя инфракрасная камера, чтобы снять выделение тепла, создаваемое сосудистой системой лица.

Рисунок выделяемого тепла не меняется со временем и уникален для каждого человека, причем этот метод более точен по сравнению с распознаванием геометрических характеристик лица.

в) Распознавание голоса — метод использует вокальные характеристики человека для его распознавания по определенной фразе.

Плюсы:

- положительное отношение со стороны пользователей;
- не требует физического контакта;
- широко употребляемые считыватели (телефоны, микрофоны).

Минусы:

- влияние шумов;
- характеристики являются недостаточно характерными для идентификации при больших базах данных.

г) Сканирование сетчатки глаза — измеряется расположение кровеносных сосудов в задней части глаза. Эта технология стала менее популярна из-за того, что многие пользователи считают ее слишком навязчивой.

д) Сканирование радужной оболочки глаза.

У этого метода очень много плюсов, например:

- не требуется физический контакт;
- защищенность от повреждения глаза;
- считается наиболее надежным из-за неизменности радужной оболочки;
- считается наиболее точным из-за большой степени случайности рисунка радужной оболочки;
- изменение размера зрачка подтверждает наличие живого пользователя;
- чрезвычайное быстродействие метода.

Но в то же время для осуществления этого метода необходимы затраты на считыватели пользователей.

Некоторые минусы:

- сложности в снятии рисунка у некоторых людей;
- возможность исказить рисунок ресницами, линзами, веками и др.;
- не может быть проверен/сравнен человеком;
- маленькая цель для считывания с большого расстояния.

3) Новые биометрические методы

К перспективным методам защиты относятся:

а) Методы, основанные на распознавании расположения ногтей и их контуров, идентификации солености тела, геометрических характеристик уха.

b) Множественная биометрия, при которой идентификация/аутентификация ведется по нескольким биометрических характеристикам сразу.

c) Метод биометрического шифрования (находится на стадии разработки);

d) Аутентификация и контроль пользователей по телефонным звонкам, при котором во время сдачи экзамена или выполнения задания пользователю в любой момент может позвонить оператор, который поговорит с пользователем некоторое время для подтверждения его личности, после чего пользователь может вернуться к тому, что он делал ранее. С одной стороны, это очень эффективный метод, но с другой — пользователям это может показаться актом недоверия, и постоянные звонки могут надоесть. Здесь есть риск потерять клиентов [5].

e) Метод идентификации по почерку вместе с проверкой пароля. Пользователь рисует свои пароли в некоторой программе, используя только мышь, стилус или тачпад. Плюсы метода в том, что он не требует никакого дополнительного аппаратного или программного обеспечения и может быть использован на любом компьютере в любом месте и в любое время. Биометрические характеристики, проверяемые системой, не могут быть переданы или скопированы кем-либо другим. Это совокупность методов биометрической аутентификации («Пользователь “есть”») и аутентификации по паролю («Пользователь “знает”») [6].

f) Метод аутентификации по входу в систему через LAN/Internet и одновременно через свой мобильный телефон [7].

g) Методы считывания изображения расположения вен, аутентификации по ДНК, биометрии мозговых волн, определения запаха тела, распознавания походки находятся на стадии разработки.

Выводы

При выборе метода аутентификации для ДО необходимо учитывать, с одной стороны, удобство его использования пользователем, а с другой — затраты на считыватели биометрических признаков. Многие существующие методы являются очень продуктивными, но будут слишком затратными для использования в системах ДО.

Уровень затрат на приобретение средств защиты ДО определяет выбираемый метод защиты, который в свою очередь обусловлен ценностью самой информационной базы ДО и стоимостью ее ИТ-инфраструктуры, затраты на восстановление которой нужно учитывать при нарушении защиты ДО.

В статье рассмотрены методы аутентификации, применимые для ДО, со своими достоинствами и недостатками, а также перспективные методы. Нельзя выделить из них универсальный метод защиты для абсолютно всех систем ДО. При выборе метода защиты следует принимать во внимание тот факт, что невозможно достичь 100-процентной безопасности, но снизить риски всегда можно. Каждый метод защиты ДО определяет, насколько эти риски могут быть снижены.

При выборе метода защиты нужно учитывать также, что некоторые методы могут вызывать недоверие и даже раздражение у пользователей. Поэтому следует выбирать более простые, но надежные методы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Овсянников В. И., Густырь А. В.* Введение в дистанционное образование. Учебное пособие для системы повышения квалификации и профессиональной переподготовки специалистов. М.: РИЦ “Альфа” МГОПУ им. М.А. Шолохова, 2001.

2. *Бикмухаметов И. Х.* Дистанционное обучение. Учебное пособие. Уфа: Уфимская государственная академия экономики и сервиса, 2006.

3. Presentation by Dr. Mohd Faiz Hilmi. E-Learning: An Information Security Perspective. School of Distance Education, University Sains Malaysia, 2011.

4. Biometrics and Authentication in Elearning wiki. URL: http://biometrics.pbworks.com (дата обращения: 12.12.2012).
5. Voice Biometrics Group. Authenticating the Identity of Distance Learning Students. Voice Biometrics Group (VBG) Vocal-ID™ Service Assures Identity. URL: www.voicebiogroup.com (дата обращения: 29.11.2012).
6. *Levey S., Ed. D.* Associate Vice Chancellor, Jeff Maynard B.Sc., CEO and Founder. Identity Proofing for Online Student ID Verification: Report of Pilot with Houston Community College, January 17, 2011.
7. *Takamizawa H., Kaijiri K.* Reliable Authentication Method by Using Cellular Phones in WBT. Faculty of Engineering, Shinshu University. Japan, 2006.

В. И. Королев, В. Ю. Статьев

СОЗДАНИЕ ДОВЕРЕННОЙ ВИРТУАЛЬНОЙ СРЕДЫ

Опыт создания автоматизированных систем показывает, что информатизация охватывает различные процессы и проблемно-тематические области деятельности организаций, все чаще порождает новые вызовы, связанные с нерешенными проблемами.

Современный этап информатизации требует создания автоматизированных систем в защищенном исполнении (АСЗИ), включающих в свой состав информационно-вычислительные комплексы различного уровня функциональной и архитектурной сложности, которые связаны между собой единой информационной моделью и единой телекоммуникационной средой.

Разработчики создаваемых АСЗИ сталкиваются с рядом серьезных проблем, которые не позволяют обеспечить требуемую ритмичность проектирования систем и уровень качества информатизации, что приводит к удорожанию конечного продукта проектирования.

Основными из таких проблем являются:

1. Концептуальные идеи обеспечения информационной безопасности ИТ-систем, нормативная база, регламентирующая вопросы создания АСЗИ, и процесс ее развития отстают от динамики модернизации и совершенствования современного аппаратного, программного и информационного обеспечения автоматизированных систем, от появления новых образцов изделий ИКТ и применения новых подходов к архитектурному построению ИТ-систем.

2. Существующее доверенное общесистемное программное обеспечение (операционные системы, системы управления базами данных, системы управления ресурсами и т. д.), как правило, не соответствует требованиям по созданию АСЗИ необходимого класса защищенности, предъявляемым в соответствии с актуальной в момент создания системы нормативной базой.

3. Для реализации целевых функций информатизации отсутствует доверенное прикладное программное обеспечение с требуемыми тактико-техническими характеристиками применения.

4. Допустимые к использованию технологии и средства защиты информации, степень развития которых напрямую связана с уровнем развития доверенных аппаратных и программных платформ, как правило, отстают по своим функциональным и техническим возможностям, которые требуются в создаваемых АСЗИ.

Имеет место ряд объективных факторов, которые влияют на решение указанных проблем. Значимыми факторами являются большие затраты временных, финансовых и людских ресурсов на выявление недекларированных возможностей в программных продуктах и аппаратных средствах, определение скрытых каналов мониторинга и управления информационными процессами. Это, прежде всего, относится к изделиям производителя, не имеющего доверенного статуса.