Кашкин Евгений Владимирович
канд. техн. наук, доцент
Васильев Дмитрий Олегович
магистрант
Бубнова Ольга Олеговна
магистрант
ФГБОУ ВО «Московский технологический университет»
г. Москва

СОВРЕМЕННЫЕ МЕТОДЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Аннотация: *авторы статьи отмечают, что важнейшим фактором работы с информацией является обеспечение законного доступа. При определении методов реализации политики безопасности важным фактором является степень уникальности ключа доступа. Таким образом, использование биометрических данных при реализации системы безопасности информационной системы в максимальной степени позволяют гарантировать законность использования пользователем информации.*

Ключевые слова: *информационная безопасность, информация, информационные технологии, информационные ресурсы, биометрические данные.*

Процедуры идентификации и аутентификации применяются в любой информационной системе, так как при доступе к системе необходимо определить полномочия пользователя. Во многих системах идентификация и аутентификация пользователя считается наиболее востребованной задачей, по сравнению с обеспечением конфиденциальности ценных данных. Практически все сетевые многопользовательские приложения, а также банкоматы, терминалы требуют не только процедуры идентификации, но и аутентификации. Необходимо ещё раз подчеркнуть, что аутентификацией является процесс верификации принадлежности идентификатора субъекту. При успешном прохождении процедуры аутен-

тификации, выполняющейся на основании секретного аутентификатора, которым располагает как субъект, так и сервис, к которому происходит доступ, идентификатор субъекта используется системой, чтобы предоставить данному пользователю определенный уровень прав доступа и полномочий к системе. Важно подчеркнуть, что в системе находится не сам аутентификатор, а некая информация о нём, и в соответствии с данной информацией система принимает решение о сходстве пользователя с определенным идентификатором.

Субъект имеет возможность предъявить системе различные сущности. Например, сущность «на основе знания чего-либо» предполагает, что пользователь введёт пароль, PIN-код или криптографический ключ. Сущность «на основе обладания чем-либо» подразумевает, что пользователь применит имеющуюся у него магнитную карту, смарт-карту, электронный ключ или другое устройство. Будущее методов идентификации в большей мере относится к сущности «на основе каких-либо неотъемлемых характеристик», то есть того, что является частью самого пользователя. Здесь используются алгоритмы, которые базируются на биометрических характеристиках субъекта, таких, как сетчатка и радужная оболочка глаза, голос пользователя, отпечаток пальца, распознавание лица пользователя, геометрия ладони пользователя и множество других [1–3].

В алгоритмическом представлении аутентификация изображается как передача пакетов данных между субъектом и системой, которые в промежутках времени обрабатываются обеими сторонами, в результате удостоверяющимися в подлинности друг друга. После идентификации и аутентификации выполняется процедура предоставления субъекту определенных прав доступа – авторизация, которая уже работает с легальными пользователями, прошедшими аутентификацию. Авторизация устанавливает доступные пользователю ресурсы и сферу разрешенных ему действий. В случае передачи информации по линии связи должна выполняться процедура взаимной аутентификации, которая основывается на взаимном подтверждении подлинности субъектов. Обычно она выполняется в

начале сеанса связи, целью является обеспечение установления соединения с законным субъектом и уверенности в том, что данные дойдут до места назначения [4].

Таким образом использование биометрических данных пользователя позволяет в максимальной степени решить проблему несанкционированного доступа к системе и обеспечить возможность безопасной работы с данными.

Список литературы

1. Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности / П.Ю. Филяк, В.М. Шварев // Информация и безопасность. – 2015. – Т. 18. – №4. – С. 580–583.

2. Информационный стресс – фактор, снижающий качество систем управления безопасностью / С.А. Рыбин, Б.В. Чувыкин // Труды международного симпозиума Надежность и качество. – 2008. – Т. 2. – С. 172–175.

3. Математическая модель для обработки данных с тепловых датчиков для управления системой задвижек тепловых контуров зданий специального назначения / Е.В. Кашкин, Т.Ю. Морозова // Естественные и технические науки. – 2013. – №6 (68). – С. 289–292.

4. Разработка методов и средств планирования и управления производственными процессами и их результатами / М.А. Назаренко, Е.В. Кашкин, И.А. Маркова, В.И. Селиванов, И.В. Макарова // Международный журнал экспериментального образования. – 2016. – №11–1. – С. 114–115.