УДК 004.75

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Фролова М.Е., студентка 4 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *Идентификация, аутентификация, автоматизированная система, пользователь, пароль, зашита информации, безопасность.*

В данной статье рассмотрены понятия и значимость основных механизмов защиты информации - идентификации и аутентификации. Также рассмотрены современные средства идентификации и аутентификации.

На сегодняшний день существует огромное количество разнообразных методов и средств защиты информации в автоматизированных системах, вследствие чего, возникает многообразие способов и средств возможных несанкционированных операций. Так, идентификация и аутентификация считаются основой информационно-технологических средств безопасности, так как другие сервисы непосредственно ориентированы на работу с поименованными объектами и субъектами автоматизированной системы.

Идентификация-это процесс определения системы, как правило, с помощью предварительно определенного идентификатора или другой уникальной информации – каждый субъект или объект системы должен быть однозначно идентифицируем. В процессе идентификации обнаруживаются права доступа, характеристики пользователя, свойства и на основании его имени, логина или какой-либо иной информации о нем.

Аутентификацией называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Для того чтобы доказать свою подлинность, необходим аутентификатор, это нечто, что может предъявить только субъект с определенным идентификатором, и никто другой [3].

Согласно взгляду Галатенко В.А. , методы аутентификации можно классифицировать по используемым при проверке средствам. В этом случае разделим указанные методы на четыре группы:

-основанные на знании лицом пароля.

-использующие технологию токенов (карточек) или основанные на использовании уникального объекта: смарт-карты, touch-memory и др.

-основанные на измерении биометрических характеристик человека – физиологических или поведенческих атрибутах живого организма.

- основанные на определенных данных, ассоциированных с пользователем, к примеру, с его координатами его пребывания [2, стр.11].

Наиболее распространенными, простыми и привычными считаются методы аутентификации, базирующиеся на паролях – секретных идентификаторах субъектов. Когда субъект вводит свой пароль, подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. Пароли должны совпасть, и в этом случае, подсистема аутентификации дает право на доступ к ресурсам информационной системы. Обеспечить приемлемый уровень информационной безопасности, можно только при правильном использовании паролей.

Рассмотрим следующие методы парольной защиты, основанные на одноразовых паролях:

Башлы П.Н. отмечает, что на сегодняшний день приобрели распространение комбинированные методы идентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающее достоверность субъекта. Плюсом данных методов, можно считать то, что обрабатывание аутентификационной информации осуществляется устройством чтения, информация в память компьютера не передается. А это означает, то, что вероятность электронного перехвата по каналам связи исключена [1,стр. 105].

В последнее время, стали использовать методы, основанные на применении средств биометрии. Биометрическая аутентификация- это аутентификация пользователя по его уникальным биометрическим характеристикам. Примерами внедрения отмеченных методов служат уникальные особенности пользователя: формы ушей, черты лица, подчерку, геометрия кисти руки, отпечатки ладони, и даже ДНК.

Новейшим направлением аутентификации является подтверждение подлинности удаленного пользователя по его местонахождению. Данный защитный механизм базируется на использовании системы космической навигации, типа GPS (Global Positioning System),что позволяет ее использовать в случаях, когда авторизованный удаленный пользователь должен находиться в необходимом месте.

Таким образом, современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. К сожалению,

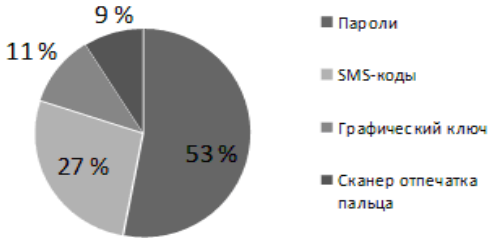

Рисунок 1 - Распространенные методы аутентификации за 2017 год

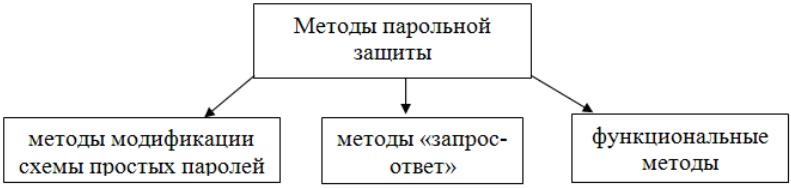

Рисунок 2 - Методы парольной защиты

пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформированы. Необходимо находить компромиссное решение между надежностью, доступностью по цене и удобством применения и администрирования средств идентификации и аутентификации.

Библиографический список

1. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / П.Н. Башлы. — М.: Евразийский открытый институт, 2013.— 311с.
2. Галатенко, В.А. Основы информационной безопасности. Идентификация и аутентификация: учебное пособие / В.А. Галатенко.- М.: Интернет- Университет Информационных Технологий, 2014г. —278с.

IDENTIFICATION AND AUTHENTICATION

Frolova M. E.

Key words: *automated system, user, password, protection, information, security.*

This article examines the concept and importance of basic mechanisms of information security - identification and authentication. Also considered modern means of identification and authentication.