Информатика, вычислительная техника и управление

УДК 004.056.53
DOI: 10.30987/1999-8775-2020-8-47-52

Н.М. Кузнецова, Т.В. Карлова, А.Ю. Бекмешов

АНАЛИЗ И ПРИМЕНЕНИЕ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ЗАЩИТЫ РЕСУРСОВ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Оптимизировано применение методов биометрической аутентификации в автоматизированных системах защиты ресурсов промышленного предприятия. Были использованы методы классификации, сравнения и информационного анализа современных технологий аутентификации. Научной новизной является представленная структура модуля аутентификации системы защиты.

Ключевые слова: автоматизация, защита информации, компьютерные атаки, биометрическая аутентификация, идентификация.

N.M. Kuznetsova, T.V. Karlova, A.Yu. Bekmeshov

ANALYSIS AND APPLICATION OF BIOMETRIC AUTHENTICATION METHODS IN AUTOMATED SYSTEM OF INDUSTRIAL ENTERPRISE RESOURCE PROTECTION

The work purpose consists in the efficiency increase of automated system operation for industrial enterprise resource protection at the expense of the optimization of authentication method application, in particular, biometric one.

To achieve the purpose it is necessary to solve the problem of efficient joint use of modern authentication methods, particularly, a static and dynamic biometric authentication.

But biometric methods are most expensive from the point of view of their realization. In this connection, within the limits of the paper there is carried out the analysis of modern methods of biological authentication from the point of view of a special order of introduction and joint use.

In the paper there is shown a classification of static and dynamic methods for biometric authentication, an example of method combination in the authentication module is presented, there are considered and analyzed the latest methods, in particular, those based on DNA investigations, thermograms of a face and hands (static), gestures (dynamic).

The work novelty consists in the presented diagram of authentication module operation.

As a conclusion it should be noted that modern authentication systems offer the application of a complex approach: use both biometric methods and other ones for authentication in modules, in particular, based on secret knowledge and material carrier possession. The approach mentioned will allow minimizing the errors of the first and the second kinds, increasing a general level of safety.

Key words: automation, information protection, cyber threats, biometrical authentication, identification.

Введение

Современные промышленные предприятия обладают несколькими видами стратегически важных ресурсов: информационными, интеллектуальными, программно-аппаратными, а также инфраструктурными, при этом необходимо обеспечение высокого уровня защиты. Для решения данной задачи наиболее рациональным является использование автоматизированной системы защиты, включающей модуль аутентификации, в которую входит несколько видов биометрической аутентификации.

Методы аутентификации применяются в системах разграничения доступа к единицам ресурса промышленного предприятия [1-5]. Помимо биометрической, также используются методы аутентификации, основанные на владении секретом (пароль, пин-код, последовательность сим-

волов языка «эмодзи» и т.д.) или материальным носителем (смарт-картой, брелоком и т.д.) [6, 7].

В зависимости от степени важности защищаемых ресурсов, а также от цены реализации, применяют однофакторную, двухфакторную и трехфакторную аутентификацию. Трехфакторная аутентификация содержит все возможные типы методов (на основе владения секретом, владения материальным носителем, биометрических характеристик).

Биометрическая аутентификация как часть автоматизированной системы защиты

В статье рассматривается применение биометрической аутентификации в рамках комплексного подхода защиты стратегически важных ресурсов предприятия – как модуль управления физическим доступом (МУФД) соответствующей автоматизированной системы защиты ресурсов промышленного предприятия (АСЗРПП).

На рис. 1 представлена структурная схема МУФД как части АСЗРПП.

Согласно рис. 1, МУФД содержит все виды аутентификации. Однако применение того или иного метода (а также их совокупности) зависит от точки доступа к запрашиваемым ресурсам («проходная», «вход в помещение N», «вход в серверную M» и т.д.).

Комплексное взаимодействие методов аутентификации в МУФД как части АСЗРПП заключается в системном принятии управленческого решения о допуске сотрудника к ресурсам на основе единого «банка данных о сотрудниках» (содержащего данные по индивидуальному допуску). Уровень иерархии допуска позволяет определять технологии аутентификации в зависимости от ценности ресурса и от точки доступа.

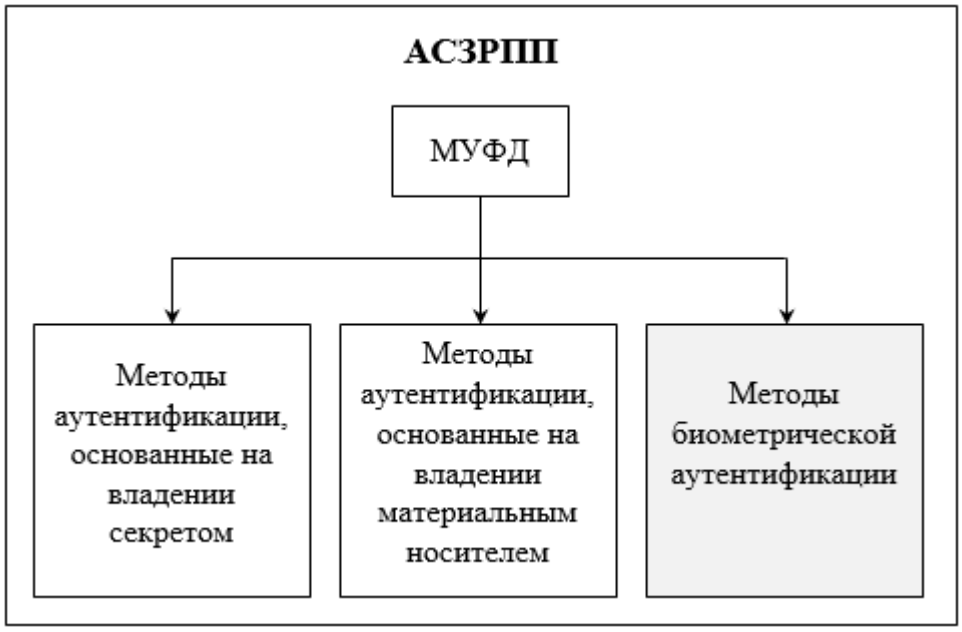

Рис. 1. Структурная схема МУФД

Классификация современных методов биометрической аутентификации

Современные методы биометрической аутентификации составляют два класса:

- статические методы аутентификации;
- динамические методы аутентификации [7, 8].

Основным достоинством статических методов аутентификации является их высокая точность. Преимущество динамических методов – наличие дополнительной возможности оценки психического состояния сотрудника предприятия (особенно важно при допуске операторов к управля-

ющим элементам автоматизированных систем реального времени, от которых зависит жизнь и здоровье людей, к ресурсам объектов критической информационной инфраструктуры – далее КИИ – и т.д.) [8, 9].

На рис. 2 представлена классификация методов статической биометрической аутентификации.

К методам статической аутентификации относятся методы распознавания относительно постоянных физических характеристик сотрудника предприятия.

Наиболее часто применяемыми являются дактилоскопические методы в силу того, что:

- на данный момент «набрана» достаточно широкая база данных отпечатков пальцев;
- методы хорошо проработаны;
- сравнительно невысокая цена реализации [7, 8].

Наиболее точными считаются методы, основанные на анализе характеристик глаз (сетчатки, радужки).

Самыми новыми, дорогими и сложными в реализации являются методы, основанные на анализе ДНК [8]. Основными препятствиями для внедрения данных методов является:

- сравнительно большое время для принятия решения;
- сравнительная небезопасность метода ввиду высокого уровня контактности.

Метод «Термограмма» основан на анализе капиллярного рисунка руки или лица. Как правило, данный метод применяется в совокупности с другими методами, так как относится к менее точным.

Наиболее доступными по стоимости являются методы анализа форм лица и рук.

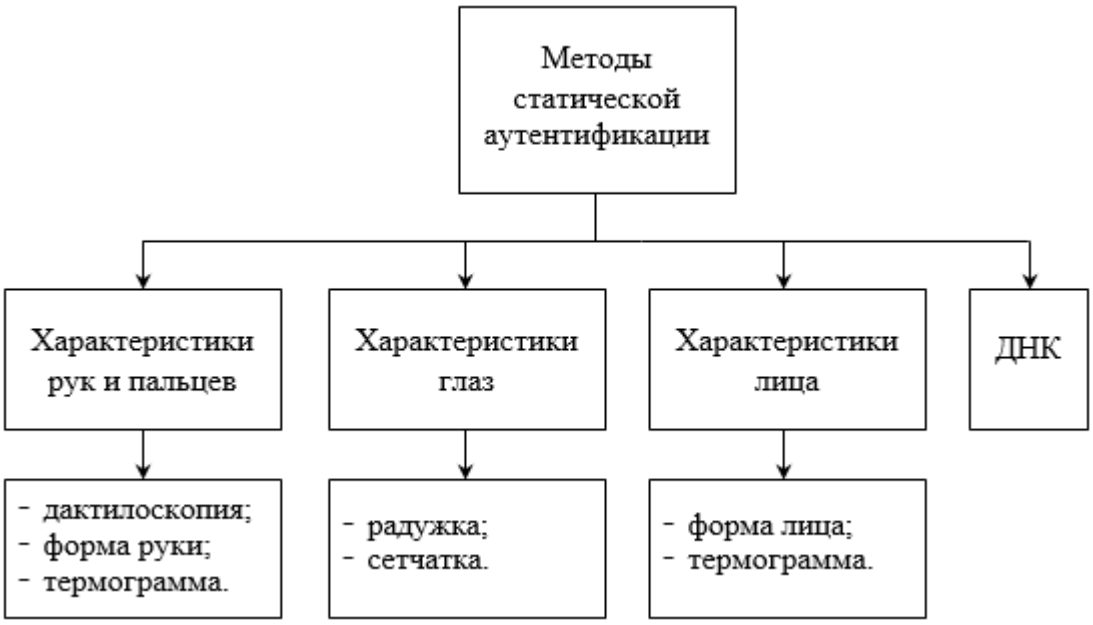

Рис. 2. Классификация методов статической биометрической аутентификации

На рис. 3 представлена классификация методов динамической биометрической аутентификации.

Методы динамической биометрической аутентификации основаны на исследованиях поведенческих характеристик сотрудника предприятия [8].

Данные методы являются менее точными по сравнению со статическими методами, однако позволяют принимать решения о допуске сотрудников, исходя из анализа их психического состояния.

Методы физиогномики являются относительно новыми, однако именно они набирают популярность в силу высокой точности определения настроения человека, а соответственно и его эмоционального состояния.

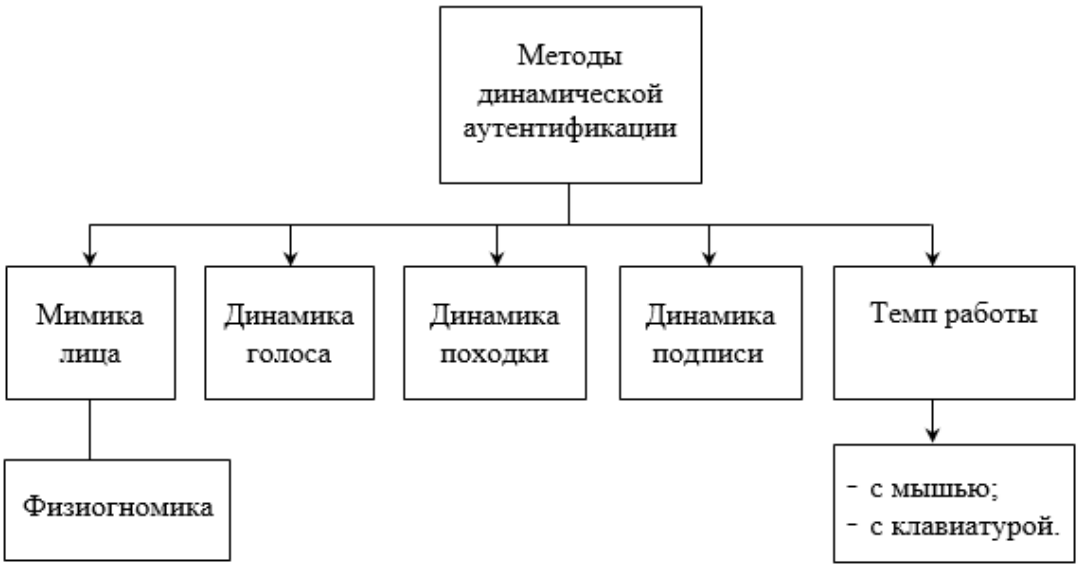

Рис. 3. Классификация методов динамической биометрической аутентификации

АСЗРПП применима при защите стратегически важных ресурсов промышленного предприятия, относящегося к объектам КИИ. При этом необходимо применение комплексного подхода при построении АСЗРПП [10, 11]. МУФД является одной из важнейших частей системы, поэтому должен содержать самые новые и точные методы аутентификации.

Наиболее рациональным является применение в МУФД многофакторной аутентификации, обязательно включающей как статические, так и динамические методы биометрической аутентификации.

Пример реализации методов аутентификации в рамках автоматизированной системы защиты

Статические и динамические методы биометрической аутентификации следует применять на точках доступа к стратегически важным ресурсам современного промышленного предприятия.

На точке доступа «Проходная» необходимо применение, как минимум, трёхфакторной аутентификации, причём с обоими видами биометрической аутентификации:

- метод на основе знания секрета;
- метод на основе владения материальным носителем;
- статический биометрический метод;
- динамический биометрический метод.

На точке «доступа автоматизированное рабочее место сотрудника предприятия» в зависимости от принадлежности к подразделению предприятия и выполняемым функциям необходимо применение, как минимум двухфакторной аутентификации, содержащей:

- метод на основе владения секретом, или на основе владения материальным носителем;
- динамической или статической биометрической аутентификации.

На точке доступа «ядро основной автоматизированной системы» методы аутентификации должны быть наиболее точными: обязательно наличие, как минимум двух методов статической и одного метода динамической биометрической аутентификации.

Выводы

Для достижения поставленной цели по оптимизации функционирования методов биометрической аутентификации в автоматизированных системах защиты в статье:

- рассмотрены и проанализированы современные методы биометрической аутентификации;
- разработана классификация статических и динамических методов биометрической аутентификации, выявлены их особенности и недостатки;
- предложен вариант оптимального совместного использования методов аутентификации в модуле автоматизированной системы защиты стратегических ресурсов предприятия от комплексных кибер-атак.

Новизна работы состоит в представленной структурной схеме функционирования модуля аутентификации, который включает в себя максимальное количество рационально взаимодействующих методов.

СПИСОК ЛИТЕРАТУРЫ

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие. М.: Академия, 2008. 256 с.
2. Karlova T.V., Bekmeshov A.Y., Kuznetsova N.M. ProtectiontheDataBanksinStateCriticalInformation-InfrastructureOrganizations // Proceedings of the 2019 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov, St. Petersburg, Russia: Saint Petersburg Electrotechnical University "LETI", 2019. P. 155–157.
3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных. М.: Горячая линия-Телеком, 2001. 148 с.
4. Мельников В. П., Клейменов С.А. , Петраков А.М. Информационная безопасность: учеб. пособие / под ред. С.А. Клейменова. М.: Академия, 2012. 336 с.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999. 376 с.
6. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие. М: Академия, 2006. 336 с.
7. Takada,T., Koike H. Awase-E: Image-basedAuthenticationforMobilePhonesusingUser'sFavoriteImagesinHuman-Computer / InteractionwithMobileDevicesandServices // Springer-Verlag. 2003. P. 347–351.
8. Хорев П.Б. Программно-аппаратная защита информации: учеб. пособие. М.: ФОРУМ: ИНФА-М, 2019. 352 с.
9. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. – URL: http://www.consultant.ru/documents/cons_doc_LAW_220885 (дата обращения: 30.01.2020).
10. Karlova T.V., Sheptunov S.A. , Kuznetsova N.M. Automation of Data Defence Processes in the Corporation Information Systems // Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov. St. Peterburg, Russia: Saint Petersburg Electrotechnical University "LETI". 2017. P. 199–202.
11. ATT&CK Matrix for Enterprise. URL: https://attacks. mitre.org (дата обращения: 30.01.2020).

1. Khorev P.B. *Methods and Means of Information Protection in Computer Systems*: manual. M.: Academy. pp. 256.
2. Karlova T.V., Bekmeshov A.Y., Kuznetsova N.M. ProtectiontheDataBanksinStateCriticalInformation-InfrastructureOrganizations // Proceedings of the 2019 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov, St. Petersburg, Russia: Saint Petersburg Electrotechnical University "LETI", 2019. P. 155–157.
3. Malyuk A.A., Pazizin S.V., Pogozhin N.S. Introduction into information protection in automated. M.: *Hot Line – Telecom*, 2001. pp. 148.
4. Melnikov V.P., Kleimyonov S.A., Petrakov A.M. *Information Safety*: manual / under the editorship of S.A. Kleimyonov. M.: Academy, 2012. 336 p.
5. Romanets Yu.V., Timofeev P.A., Shangin V.F. Information protection in computer systems and networks. M.: *Radio and Communications*, 1999. pp. 376.
6. Platonov V.V. Software-Hardware Means to Ensure Information Safety of Computer Networks: manual. M.: Academy, 2006. pp. 336.
7. Takada,T., Koike H. Awase-E: Image-basedAuthenticationforMobilePhonesusingUser'sFavoriteImagesinHuman-Computer / InteractionwithMobileDevicesandServices // Springer-Verlag. 2003. P. 347–351.
8. Khorev P.B. *Software-Hardware Information Protection*: manual. M.: FORUM: INFA-M, 2019. pp. 352.
9. The Federal Law "On Safety of Critical Information Infrastructure of the Russian Federation" of 26.07.2017 No.187-F3. - URL:

http://www.consultant.ru/documents/cons_doc_LAW_220885 (address date:30.01.2020).
10. Karlova T.V., Sheptunov S.A. , Kuznetsova N.M. Automation of Data Defence Processes in the Corporation Information Systems // Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov. St. Peterburg, Russia: Saint Petersburg Electrotechnical University "LETI". 2017. P. 199–202.
11. ATT&CK Matrix for Enterprise. URL: https://attacks. mitre.org (address date: 30.01.2020).

Ссылка для цитирования:
Кузнецова Н.М. , Карлова Т.В., Бекмешов А.Ю. Анализ и применение методов биометрической аутентификации в автоматизированной системе защиты ресурсов промышленного предприятия // Вестник Брянского государственного технического университета. 2020. № 8. С. 47 - 52. DOI: 10.30987/1999-8775-2020-8-47-52.

Статья поступила в редакцию 15.04.20.
Рецензент: к.т.н., доцент Брянского государственного технического университета
Рытов М.Ю.,
член редсовета журнала «Вестник БГТУ».
Статья принята к публикации 22.07.20.

Сведения об авторах:

Кузнецова Наталия Михайловна, к.т.н., доцент, Московский государственный технологический университет «СТАНКИН», тел.: 8-(903)-581-80-15, e-mail: knm87@mail.ru.
Карлова Татьяна Владимировна, д. соц. н., профессор, Институт конструкторско-технологической информатики РАН, тел.: 8-(903)-776-90-78, e-mail: karlova-t@yandex.ru.
Бекмешов Александр Юрьевич, к.т.н., доцент, Институт конструкторско-технологической информатики РАН, тел.: 8-(926)-582-34-35, e-mail: b-a-y-555@yandex.ru.

Kuznetsova Natalia Michailovna, Can. Sc. Tech., Assistant Prof., Moscow State Technological University “STANKIN”, phone: 8-903-581-80-15, e-mail: knm87@mail.ru.
Karlova Tatiana Vladimirovna, Dr. Sc. Sociol., Prof., Institute of Design-Technological Informatics of RAS, phone: 8-903-776-90-78, e-mail: karlova-t@yandex.ru.
Bekmeshov Alexander Yurievich, Can. Sc. Tech., Assistant Prof., Institute of Design-Technological Informatics of RAS, phone: 8-926-582-34-35, e-mail: b-a-y-555@yandex.ru.