УДК 004.056 DOI: 10.34759/trd-2020-114-18

Использование методов биометрической аутентификации в автоматизированных системах управления с использованием клавиатурного почерка

Соломатин М.С.*, Митрофанов Д.В.**

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина»,

ул. Старых Большевиков, 54а, Воронеж, 364064, Россия.

**e-mail: newmihei@gmail.com*

***e-mail: mitrofanovd@mail.ru*

Статья поступила 31.08.2020

Аннотация

В статье рассматривается информационная безопасность автоматизированных систем управления. Предлагается использовать системы биометрической аутентификации. Перспективным является использование анализа клавиатурного почерка оператора как один из элементов интеллектуального детектора системы защиты. Приведены три основных алгоритма аутентификации по клавиатурному почерку. Представлен алгоритм работы режима обучения и аутентификации.

Ключевые слова: автоматизированная система управления, информационная безопасность, информационная система, безопасность информационных систем, биометрическая аутентификация, клавиатурный почерк.

Введение

Развитие информационных технологий и их использование в системах различного назначения приводит к тому, что появляются новые виды уязвимостей

информационной безопасности таких систем. Для повышения безопасности информации необходимо постоянно совершенствовать системы и механизмы защиты [1, 2].

Не исключением являются и автоматизированные системы управления [3, 4]. Под автоматизированными системами управления будем понимать комплекс средств автоматизации, который имеет в своем составе программную и аппаратную части, и обученный персонал, предназначенный для управления различными процессами.

Как отмечено в [5], одним из способов защиты информации в автоматизированных системах управления является использование интеллектуального детектора, одной из подсистем которого является подсистема авторизации в системе.

Биометрическая аутентификация с использование клавиатурного почерка в автоматизированной системе управления

Авторизация – предоставление определённому лицу или группе лицправ на выполнение определённых действий, а также процесс проверки(подтверждения) данных прав при попытке выполнения этих действий [6].

При разграничении прав доступа в информационной системе пользователю необходимо представиться и подтвердить свою личность, так называемые идентификация и аутентификация [7]. В настоящее время существует и используется большое количество систем аутентификации. Все большую популярность приобретает биометрическая система аутентификации, обладающая

возможностью установить личность и права доступа пользователя по каким-либо биометрическим данным [8].

Возросшая популярность биометрических систем определяется их преимуществами:

– нет необходимости запоминать большие и сложные пароли;

– отпадает необходимость переноса каких-либо дополнительных устройств;

– снижается вероятность ошибок при аутентификации;

– нельзя передать свои биометрические данные другому лицу.

Среди недостатков таких систем можно выделить следующие:

– сложность разработки системы;

– сложность правильной настройки;

– высокая стоимость.

Одним из возможных способов классификации биометрических систем аутентификации является характеристики человека, которые можно разделить на динамические и статические [8].

Динамическими являются методы основаныена поведенческих особенностях конкретного человека: голос, рукописный почерк и, как его дальнейшее развитие, клавиатурный почерк. К статическим относятся теметоды, которые основаны на физиологических характеристиках человека: отпечаток пальца, радужная оболочка глаза, геометрия частей тела.

Поскольку большую часть времени в современном мире пользователь автоматизированной системы управления проводит за персональным компьютером,

более подробно рассмотрим его клавиатурный почерк [9]. Этот метод аутентификации относится к динамическим характеристикам человека и может меняться с течением времени. При использовании данного метода аутентификации нет необходимости в покупке дополнительного дорогостоящего оборудования. Используя обычную клавиатуру, которая идет в комплекте с персональным компьютером и специального программного обеспечения появляется возможность в считывании динамических характеристик пользователя.

К одному из недостатков использования аутентификации с использованием клавиатурного почерка можно отнести следующий: с улучшение навыков пользователя работы с клавиатурой изменяется и его клавиатурный почерк [10]. Системе необходимо постоянно проводить корректировку и обновлять свои базы данных, содержащие характеристики пользователя. Данную проблему можно решить, используя программный метод обновления эталона и постоянного переобучения.

Используя следующие динамические параметры, клавиатурный почерк пользователя можно описать с помощью:

– скорости ввода символов – количество введенных символов за определенный временной отрезок;

– динамики ввода символов – характеристика, учитывающая время между нажатиями клавиш клавиатуры;

– опечатки при вводе – характеристика, отражающая совершенные ошибки при вводе [12].

Как отмечено в работе [9], в настоящее время используется три основных алгоритма аутентификации по клавиатурному почерку:

1. Анализ во время ввода пароля.

2. Анализ на основании ввода дополнительного текстового фрагмента или фразы.

3. Постоянный скрытый мониторинг.

Используя первый алгоритм, мы получаем высокое быстродействие работы системы, т.к. для аутентификации необходимо просто ввести пароль заданной длины и сложности. Основным недостатком данного алгоритма можно считать слишком короткий пароль. Также при успешной аутентификации в системе оператор может покинуть рабочее место по служебной необходимости и не заблокировать систему. Этим может воспользоваться потенциальный нарушитель для выполнения каких-либо атак на информационную систему.

Второй алгоритм лишен недостатка на длину пароля, потому что требует ввода большего количества символов, но лишается быстродействия, потому что на ввод дополнительной фразы большого объема требуется много времени. Данный алгоритм эффективно применять, когда оператор мало отвлекается от выполнения своих обязанностей и почти все время находится на рабочем месте.

Алгоритм постоянного скрытого мониторинга является самым сложным в реализации и требовательным к ресурсам компьютера, но в то же время, он обеспечивает высокую точность определения потенциального нарушителя.

В основе работы всех трех алгоритмов лежит сравнение с эталонной моделью поведения, которая содержится в базе данных. Эта модель создается в так

называемом режиме обучения системы, во время работы которого собирается статистическая информация о клавиатурном почерке пользователя. Необходимо отметить, что эталонная модель может создаваться и на тестовых примерах, которые не имеют отношение к вводу настоящей информации в автоматизированной системе.

Во время работы режима обучения системы пользователь вводит определенные тестовые фразы, которые подготовлены заранее и должны меняться с течением времени. Выбор тестовых фраз является важным этапом, потому что необходимо собрать достаточное количество статистической информации, приближенной к реальной работе.

Эталонная модель поведения представляет собой динамические характеристики человека, которые в дальнейшем используются для сравнения с параметрами лиц, пытающихся получить на доступ к ресурсам.

После режима обучения, в период нормального функционирования системы, на этапе идентификации, рассчитанные на основе статистической информации оценки, сравниваются с эталонными, на основании чего делается вывод о совпадении или несовпадении параметров клавиатурного почерка.

Когда полученные в ходе работы статистические данные отличаются от эталонной модели поведения больше чем на заданное системой защиты значения, пользователь получает отказ к работе, а система защиты формирует предупреждающее сообщение.

Алгоритм режима обучения представлен на рисунке 1.

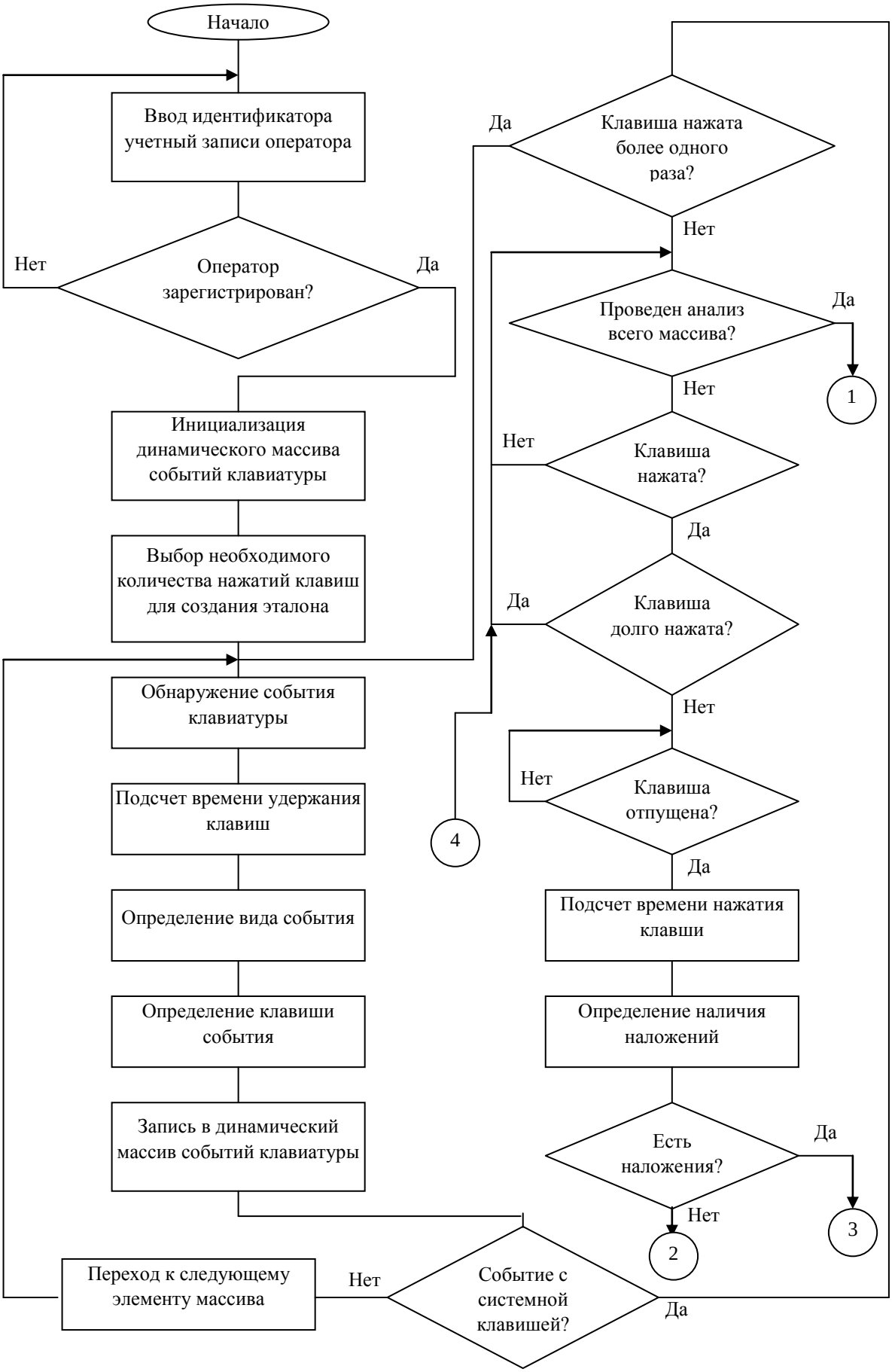

Рисунок 1 – Алгоритм режима обучения

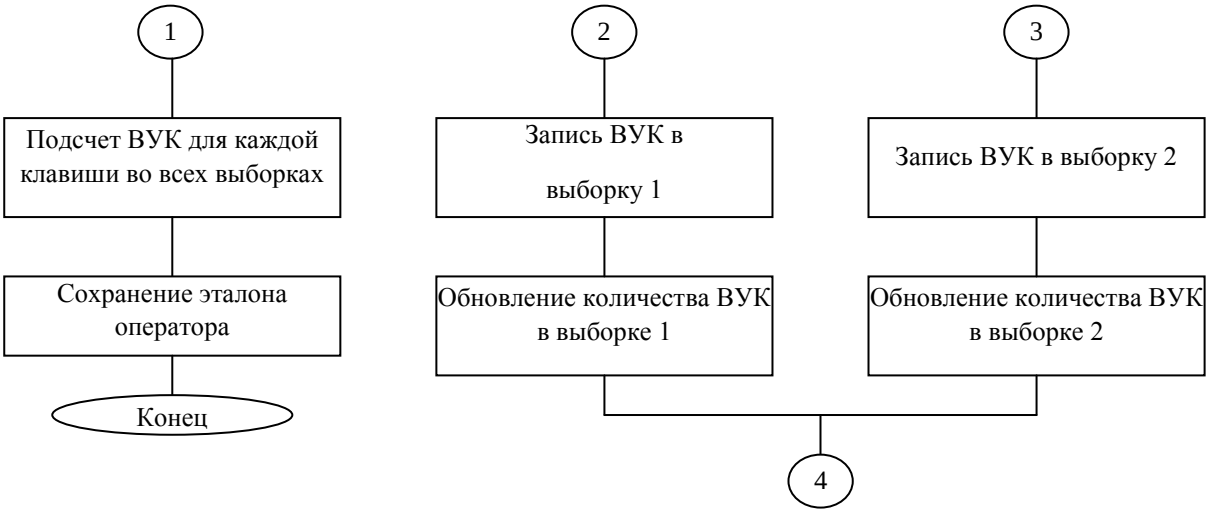

Рисунок 1 – Алгоритм режима обучения (окончание)

Для аутентификации с использованием клавиатурного почерка при вводе пароля следует обращать особое внимание на скорость и динамику ввода. Так же в [9] отмечено, что временные интервалы между нажатиями клавиш более точно характеризуют клавиатурный почерк оператора, чем время удержания клавиш (ВУК) [12].

Следует учитывать, что необходимо производить фильтрацию долгих нажатий клавиш от ввода подряд одинаковых букв, например, «мм» в слове «программа».

Рассмотрим алгоритм аутентификации. Обычно процессу авторизации предшествует процесс аутентификации – подтверждение подлинности, соответствия оператора предъявленному им идентификатору.

В данном алгоритме сравнение с эталонной моделью происходит на основании идентификатора, которым представился пользователь.

Алгоритм аутентификации представлен на рисунке 2.

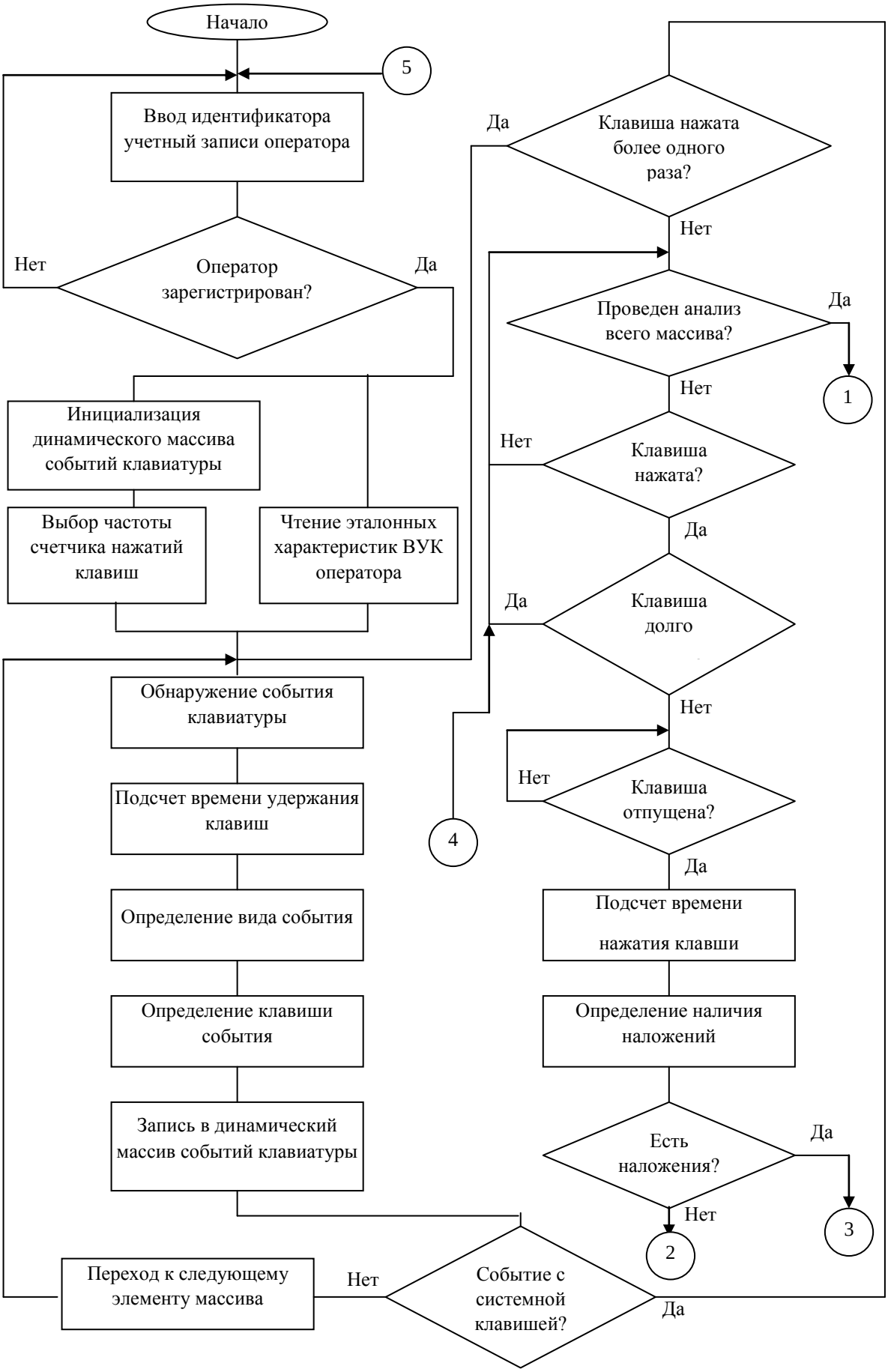

Рисунок 2 – Алгоритм аутентификации

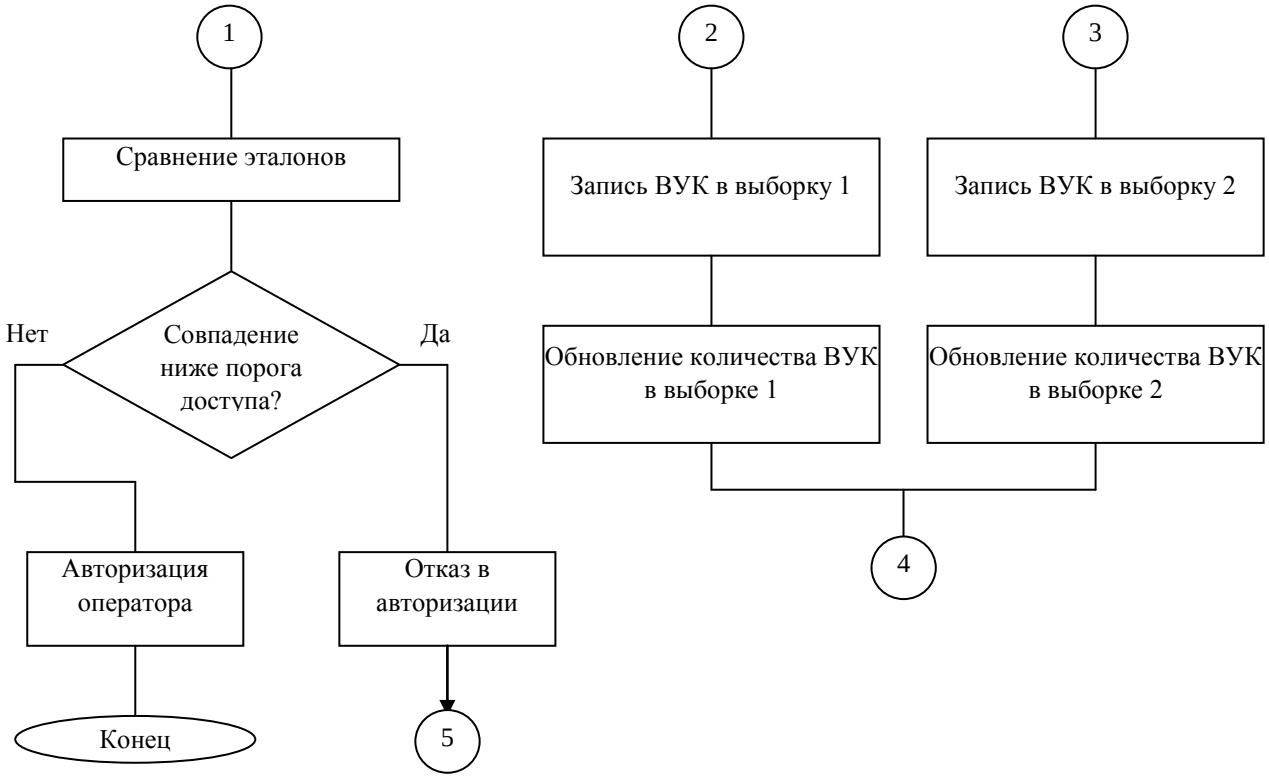

Рисунок 2 – Алгоритм аутентификации (окончание)

Выводы

Таким образом, для повышения защищенности информационных систем и автоматизированных систем управления предлагается использовать биометрическую аутентификацию на основе клавиатурного почерка пользователя, как реализации одной из функции интеллектуального детектора системы защиты информации. Приведено описание и характеристики клавиатурного почерка пользователя. Приведен алгоритм регистрации клавиатурного почерка и аутентификации в системе.

Библиографический список

1. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах». 2015. URL: https://fstec.ru/component/attachments/download/812

2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61798

3. Карантаев В.Г. Система защиты информации как составная часть АСУ ТП // Информатизация и системы управления в промышленности. 2017. № 2 (68). URL: https://isup.ru/articles/2/11118/

4. Чернов Д.В., Сычугов А.А. Современные подходы к обеспечению информационной безопасности АСУ ТП // Известия Тульского государственного университета. Технические науки. 2018. № 10. С. 58 – 64.

5. Соломатин М.С., Митрофанов Д.В. Модель интеллектуального детектора системы защиты автоматизированной системы управления // Труды МАИ. 2020. № 110. URL: http://trudymai.ru/published.php?ID=112926. DOI: 10.34759/trd-2020-110-16

6. Ходашинский И.А., Савчук М.В., Горбунов И.В., Мещеряков Р.В. Технология усиленной аутентификации пользователей информационных процессов // Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. № 2-3 (24). С. 236 – 248.

7. Информационная безопасность и защита информации. URL: https://sites.google.com/site/infobezcom/11-mehanizmy-informacionnoj-bezopasnosti/tema-12-identifikacia-i-autentifikacia

8. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Пензенский государственный университет, 2006. - 186 с.

9. Новиков А.А., Шарков А.Е., Сердюк В.А. Новые продукты активного аудита информационной безопасности // Тезисы докладов X юбилейной конференции «Методы и технические средства обеспечения безопасности информации». Санкт Петербург, 2002. С. 153 – 154.

10. Сухаревская Е.В. Аутентификация пользователей по клавиатурному почерку // Международный студенческий научный вестник. 2018. № 2. URL: https://eduherald.ru/ru/article/view?id=18132

11. Цанниева Г.А., Гасанова Н.Р. Клавиатурный почерк как способ аутентификации иидентификации пользователя // Материалы VIII Международной студенческой научной конференции «Студенческий научный форум», 2016. URL: http://scienceforum.ru/2016/article/2016029537

12. Клавиатурный почерк как средство аутентификации. 2012. URL: https://www.securitylab.ru/blog/personal/aguryanov/29985.php

13. Сабанов А.Г. Об уровнях строгости аутентификации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 2-1 (26). С. 134 – 139.

14. Бухарин В.В., Кирьянов А.В., Стародубцев Ю.И. Способ защиты информационно-вычислительных сетей от компьютерных атак // Труды МАИ. 2012. № 57. URL: http://trudymai.ru/published.php?ID=31145

15. Бухарин В.В., Кирьянов А.В., Стародубцев Ю.И., Трусков С.С. Метод обнаружения сетевого перехвата информационного трафика информационно-телекоммуникационной сети // Труды МАИ. 2012. № 57. URL: http://trudymai.ru/published.php?ID=31144

16. Филатов В.И., Борукаева А.О., Бердиков П.Г. Алгоритм анализа согласованности экспертных оценок параметров аппаратно-программного комплекса автоматизированного рабочего места // Труды МАИ. 2018. № 103. URL: http://trudymai.ru/published.php?ID=100781

17. Филатов В.И., Бонч-Бруевич А.М., Хохлачев Е.Н., Борукаева А.О., Бердиков П.Г. Формализация параметров модели адаптивной системы защиты автоматизированной системы управления связью // Труды МАИ. 2020. №112. URL: http://trudymai.ru/published.php?ID=116576. DOI: 10.34759/trd-2020-112-17

18. Скрыпников А.В., Хвостов В.А., Чернышова Е.В., Самцов В.В., Абасов М.А. Нормирование требований к характеристикам программных систем защиты информации // Вестник Воронежского государственного университета инженерных технологий. 2018. Т. 80. № 4 (78). С. 96 – 110.

19. Яшина А.М. Современные способы защиты информации и информационная безопасность // Труды международного симпозиума «Надежность и качество». - Пенза, Пензенский государственный университет, 2018. С. 104 – 106.

20. Жукова П.Н., Насонова В.А., Ходякова Н.В. О некоторых средствах защиты информационных систем от несанкционированного доступа // Проблемы правоохранительной деятельности. 2015. № 2. С. 83 – 88.

Biometric authentication methods application for automated control systems employing keyboard handwriting

Solomatin M.S.*, Mitrofanov D.V.**

Air force academy named after professor N.E. Zhukovskii and Yu.A. Gagarin,

54a, Starykh bol'shevikov, Voronezh, 394064, Russia

**e-mail: newmihei@gmail.com*

***e-mail: mitrofanovd@mail.ru*

Abstract

Information technologies development in many areas of human life activity led to the necessity of automated systems for any process control. The task of information protectiveness, which enters, processes and stored in these systems, becomes up-to-date as well.

Earlier, it was noted in the works that, in our opinion, application of the intellectual detector of the information protecting system in the automated control systems, was up-to-date.

One of the intelligent detector subsystems is the authentication subsystem within the information system. Let us take a closer look at the biometric authentication. These systems are based on unique biometric specifics of the particular person. They can be divided into dynamic ones, which are subjected to changes with time, and static, remaining unchanged.

They can be divided into dynamic, which are subject to change over time, and static, which remain constant.

With authentication in the automated control system, we suggest employing user's keyboard handwriting, which refers to the person's dynamic characteristics.

Under the keyboard handwriting we understand a set of dynamic characteristics of the working with the keyboard. The standard keyboard allows measuring the following timing characteristics: the time of holding the pressed key and the time interval between keystrokes.

With this authentication technique employing there is no need to purchase extra expensive equipment. It becomes possible to read user's dynamic characteristics, using a conventional keyboard that comes with a personal computer, and special software.

At present, three basic authentication algorithms based on the keystroke handwriting are being employed. These are analysis while password entering, analysis, based on entering extra text fragment or phrase, and constant covert monitoring. Each of the algorithms has its pros and contras. System development complexities, operation time, and requirements to the computer speed can be highlighted as the common differences.

Operation of each algorithm is based on comparison with the reference behavioral model.

During operation in the system training mode the user enters certain test phrases, which were prepared in advance and should be changing with the with the passage of time. The text phrases selection is an important stage, since it is necessary to collect sufficient amount of statistic information close to real operation.

After the learning mode, the estimates calculated based on statistical information are compared with the reference ones during the period of the system normal operation at the stage of identification. On their basis, a conclusion is made on the keyboard handwriting parameters match or mismatch.

When statistical data obtained in the course of work differs from the reference behavioral model by more than the value set by the protection system, the user gets a refusal to work, and protection system generates a warning message.

Thus, in our opinion, the user authentication application in automated control system employing the keyboard handwriting is prospective

Keywords: automated control system, information security, information system, information systems security, biometric authentication, keyboard handwriting.

References

1. *Metodicheskii dokument FSTEK Rossii "Metodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh"* (Threats determining techniques to information security in information systems). 2015. URL: https://fstec.ru/component/attachments/download/812

2. *Federal'nyi zakon "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" ot 27.07.2006 № 149-FZ* (On information, information technology and information protection). URL: http://www.consultant.ru/document/cons_doc_LAW_61798

3. Karantaev V.G. *Informatizatsiya i sistemy upravleniya v promyshlennosti*, 2017, no. 2 (68). URL: https://isup.ru/articles/2/11118/

4. Chernov D.V., Sychugov A.A. *Izvestiya Tul'skogo gosudarstvennogo universiteta, Tekhnicheskie nauki*, 2018, no. 10, pp. 58 – 64.

5. Solomatin M.S., Mitrofanov D.V. *Trudy MAI*, 2020, no. 110. URL: http://trudymai.ru/published.php?ID=112926. DOI**:** 10.34759/trd-2020-110-16

6. Khodashinskii I.A., Savchuk M.V., Gorbunov I.V., Meshcheryakov R.V. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2011, no. 2-3 (24), pp. 236 – 248.

7. *Informatsionnaya bezopasnost' i zashchita informatsii*. URL: https://sites.google.com/site/infobezcom/11-mehanizmy-informacionnoj-bezopasnosti/tema-12-identifikacia-i-autentifikacia

8. Ivanov A.I. *Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizhenii* (Biometric personality identification by the subconscious movements dynamics), Penza, Penzenskii gosudarstvennyi universitet, 2006, 186 p.

9. Novikov A.A., Sharkov A.E., Serdyuk V.A. *Tezisy dokladov X yubileinoi konferentsii "Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii"*, Saint Petersburg, 2002, pp. 153 – 154.

1. 10. Sukharevskaya E.V. *Mezhdunarodnyi studencheskii nauchnyi vestnik*, 2018, no. 2. URL: https://eduherald.ru/ru/article/view?id=18132

11. Tsannieva G.A., Gasanova N.R. *Materialy VIII Mezhdunarodnoi studencheskoi nauchnoi konferentsii "Studencheskii nauchnyi forum", 2016.* URL: http://scienceforum.ru/2016/article/2016029537

12. *Klaviaturnyi pocherk kak sredstvo autentifikatsii*. 2012. URL: https://www.securitylab.ru/blog/personal/aguryanov/29985.php

13. Sabanov A.G. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2012, no, 2-1 (26), pp. 134 – 139.

14. Bukharin V.V., Kir'yanov A.V., Starodubtsev Yu.I. *Trudy MAI*, 2012, no. 57. URL: http://trudymai.ru/eng/published.php?ID=31145

15. Bukharin V.V., Kir'yanov A.V., Starodubtsev Yu.I., Truskov S.S. *Trudy MAI*, 2012, no. 57. URL: http://trudymai.ru/eng/published.php?ID=31144

16. Filatov V.I., Borukaeva A.O., Berdikov P.G. *Trudy MAI*, 2018, no. 103. URL: http://trudymai.ru/eng/published.php?ID=100781

17. Filatov V.I., Bonch-Bruevich A.M., Khokhlachev E.N., Borukaeva A.O., Berdikov P.G. *Trudy MAI*, 2020, no. 112. URL: http://trudymai.ru/eng/published.php?ID=116576. DOI**:** 10.34759/trd-2020-112-17

18. Skrypnikov A.V., Khvostov V.A., Chernyshova E.V., Samtsov V.V., Abasov M.A. *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernykh tekhnologii*, 2018, vol. 80, no. 4 (78), pp. 96 – 110.

19. Yashina A.M. *Trudy mezhdunarodnogo simpoziuma "Nadezhnost' i kachestvo"*, Penza, Penzenskii gosudarstvennyi universitet, 2018, pp. 104 – 106.

20. Zhukova P.N., Nasonova V.A., Khodyakova N.V. *Problemy pravookhranitel'noi deyatel'nosti*, 2015, no. 2, pp. 83 – 88.