УДК 004.9
DOI: 10.17586/0021-3454-2023-66-6-449-456

АУТЕНТИФИКАЦИЯ ОПЕРАТОРА АРМ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА НА ОСНОВЕ КОМПЬЮТЕРНОГО ПОЧЕРКА

И. А. Саитов*, А. И. Саитов, М. М. Шарапов

Академия ФСО России, Орел, Россия
**soul1308@yandex.ru*

Аннотация. На примере системы динамической аутентификации оператора автоматизированного рабочего места критически важного объекта показаны пути повышения достоверности распознавания легитимности пользователя по отсутствию отклонений в поведении последнего. Рассмотрен вариант известного алгоритма идентификации компьютерного почерка. Исследованы направления совершенствования состава и методики профессионального психофизического отбора кандидатов на должность операторов автоматизированного рабочего места критически важных объектов.

Ключевые слова: *динамическая аутентификация, компьютерный почерк, легитимный пользователь, отклонения в поведении, распознавание образов, максимум апостериорной вероятности*

Ссылка для цитирования: *Саитов И. А., Саитов А. И., Шарапов М. М.* Аутентификация оператора АРМ критически важного объекта на основе компьютерного почерка // Изв. вузов. Приборостроение. 2023. Т. 66, № 6. С. 449—456. DOI: 10.17586/0021-3454-2023-66-6-449-456.

AUTHENTICATION OF A CRITICAL OBJECT WORKSTATION OPERATOR BASED ON COMPUTER HANDWRITING

I. A. Saitov*, A. I. Saitov, M. M. Sharapov

Academy of the Federal Security Service of Russia, Orel, Russia
**soul1308@yandex.ru*

Abstract. On the example of a system of dynamic authentication of an operator of a workstation of a critically important object, ways are shown to increase the reliability of recognizing the legitimacy of a user by the absence of deviations in his behavior. A variant of the well-known computer handwriting identification algorithm is considered. Directions for improving the composition and methods of professional psycho-physical selection of candidates for the position of operators of an automated workplace of critically important objects are studied.

Keywords: dynamic authentication, computer handwriting, legitimate user, behavior deviance, pattern recognition, maximum a posteriori probability

For citation: Saitov I. A., Saitov A. I., Sharapov M. M. Authentication of a critical object workstation operator based on computer handwriting. *Journal of Instrument Engineering.* 2023. Vol. 66, N 6. P. 449—456 (in Russian). DOI: 10.17586/0021-3454-2023-66-6-449-456.

Введение. Современная геополитическая ситуация характеризуется активизацией различных типов внешних и внутренних угроз национальной безопасности. В текущих условиях

объекты критически важной инфраструктуры* государства требуют повышенных мер по обеспечению защищенности [1—3]. В связи с этим разработка научно-технических предложений по совершенствованию систем контроля состояния критически важных объектов государства (КВОГ) является актуальной задачей.

Анализ инцидентов безопасности последних лет показал, что в настоящее время особенно актуальны** задачи:

1) пресечения несанкционированного доступа нелегитимных пользователей к автоматизированному рабочему месту (АРМ) оператора;

2) выявления (пресечения) злонамеренных действий лиц, обладающих правом доступа к этому АРМ.

Очевидно, что осуществление угроз безопасности путем использования уязвимостей КВОГ „внутренними нарушителями“ может привести к значительному ущербу для страны. Следовательно, актуально исследовать приемы, способы и алгоритмы идентификации состояния пользователей (операторов АРМ) в ходе выполнения ими служебных обязанностей („на лету“) по управлению КВОГ. Разрабатываемый инструментарий должен обеспечить распознавание как нелегитимных пользователей, так отклонения в поведении легитимных.

Общие положения. Системы доступа пользователей к АРМ КВОГ в качестве идентификаторов используют [4—6]:

— секретное знание (например, пароль);

— физические объекты, принадлежащие пользователям (smart-карты, флеш-накопители и т.п.);

— биометрические данные пользователей.

Часто эти средства используются на начальном этапе работы с АРМ, т.е. „при входе в систему“, для статической аутентификации. Такие средства просты в использовании, но ненадежны. Нелегитимный пользователь может получить доступ к АРМ в случае отсутствия легитимного на рабочем месте, после того как тот „вошел в систему“. Кроме того, средства статической аутентификации не способны „на лету“ распознавать как нелегитимных пользователей, так отклонения в поведении легитимных.

Динамическая аутентификация [4, 6] предполагает проверку характеристик пользователя во время его взаимодействия с АРМ, в частности, на основе работы с клавиатурой, манипуляторами „мышь“, „джойстик“ и пр. Следовательно, перспективны для распознавания как нелегитимных пользователей, так и отклонений в поведении легитимных системы динамической аутентификации на основе клавиатурного почерка (КП). КП — поведенческая биометрическая характеристика, представляющая собой параметрическое описание особенностей ввода оператором АРМ КВОГ данных с клавиатуры или манипуляций „мышью“.

Большинство систем динамической аутентификации (ДА) на основе КП предполагает „обучение с учителем“ [4—7]. При этом на этапе обучения формируется эталонный шаблон легитимного и без отклонений в поведении пользователя АРМ КВОГ в виде вектора биометрических признаков. Естественно, достоверность распознавания классов пользователей (например, легитимный/нелегитимный и/или норма/отклонение) зависит от качества обучения средств ДА, т.е. от качества обучающих примеров и эффективности алгоритма распознавания [4, 8, 9].

Классические алгоритмы аутентификации по КП используют в качестве эталонного вектора признаков легитимного пользователя АРМ множество признаков, полученных при выполнении работником определенных тестовых заданий. При этом данные о пользователе

* Приказ ФСТЭК России от 9 августа 2018 г. № 138 „Об утверждении Требований к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды“.

** http:\\infowatch.ru/report2016.

могут собираться локально (непосредственно на рабочем месте) или удаленно по технологии Web-сбора. При этом вне зависимости от способа получения данные будут принципиально неполными, неточными по причине стабильности психофизического состояния работника на определенном промежутке времени. Кроме того, для каждой операционной системы необходимо реализовывать собственный „сборщик“ со своими достоинствами и недостатками [4, 8].

При трудоустройстве претендент на должность в КВОГ проходит профессиональное психофизическое исследование, что существенным образом повышает достоверность эталонных признаков в формируемом векторе. Это достигается путем ввода специальных вопросов, тестов, заданий, направленных на сбор сведений в различных психофизических состояниях оператора.

Следовательно, обучение системы ДА на основе КП для оператора АРМ КВОГ потенциально позволяет повысить достоверность выявления как нелегитимных пользователей, так отклонений в поведении легитимных. Однако до настоящего времени отсутствуют учитывающие эти новые возможности современные методики и алгоритмы сбора данных, а также обучения системы ДА.

Решение задачи идентификации состояния оператора АРМ КВОГ на основе компьютерного почерка. В типовых системах ДА на основе КП при решении поставленной задачи при локальном сборе данных в ОС Windows формируются файлы:

1) динамической библиотеки-перехватчика (.dll), предназначенной для сбора параметров целевых событий;

2) исполняемой программы (.exe), предназначенной для управления данной библиотекой.

Например, данные об операторе АРМ, собранные в библиотеке $H(U_i)$, принято отображать в виде:

$$H(U_i) = (A_{i1}, A_{i2}, \ldots, A_{iN}); \quad A_{ij} = \text{«key}_{ij}, \text{type}_{ij}, t_{ij}\text{»},$$

где A_{ij} — элемент библиотеки; key_{ij} — код используемой клавиши; type_{ij} — тип произошедшего события (нажатие/отжатие); t_{ij} — временная метка, соответствующая данному событию; N — число событий.

Для обучения системы ДА требуется сначала определить состав вектора набора признаков оператора АРМ. Для этого следует выполнить следующие шаги.

1. *Разбиение времени работы оператора на временные окна*. При этом временное окно с неусредненными характеристиками пользователя может быть представлено в виде

$$W_{ij} = \text{«}A_{ij1}, A_{ij2}, \ldots, A_{ijs}\text{»}, \tag{1}$$

где s — размер временного окна.

Тогда множество временных окон оператора:

$$B(U_i) = (W_{i1}, W_{i2}, \ldots, W_{iM}), \tag{2}$$

где M — число временных окон.

Исследования показали: чем больше объем собранных данных, тем выше точность сформированного вектора эталонных характеристик оператора АРМ КВОГ.

2. *Расчет выявленных признаков для каждого временного окна*. Исследования показали, что в описанных условиях для ДА состояния пользователя во время его работы только с клавиатурой компьютера целесообразно учитывать признаки, представленные в таблице.

Основные характеристики КП оператора АРМ

№	Характеристика	Описание
1	Интервалы времени между нажатием клавиш	Средняя пауза между нажатиями клавиш при наборе текста
2	Среднее время удержания клавиши при наборе текста	Среднее время между нажатием и отпусканием клавиши при наборе текста
3	Скорость набора текста „нетто“	Чистая скорость набора текста без учета удаленных символов
4	Скорость набора текста „брутто“	Скорость набора с учетом удаленных символов
5	Степень отклонения ритма от среднего при наборе текста	Степень неравномерности набора в процентах, среднее отклонение паузы между нажатиями от среднего значения
6	Число исправлений при наборе текста	Процент исправленных символов по отношению к общему числу символов в тексте
7	Число перекрытий между клавишами при наборе текста	Число событий перекрытий — одна кнопка не опущена, но нажата уже другая
8	Частота нажатия клавиш	Число нажатий клавиш в единицу времени
9	Среднее время удержания группы клавиш при наборе текста	Среднее время между нажатием одной клавиши группы и последней клавиши группы во всем временном окне

3. *Формирование эталонной модели оператора АРМ* из признаков п. 2. На этом этапе формируется эталонный вектор признаков в классе „легитимный пользователь, состояние — норма (отсутствие отклонений)“.

4. *Решение задачи распознавания образов*. Данный этап является самым сложным и требует дополнительных исследований. Так, например, статистические методы распознавания подразумевают определение принадлежности наблюдаемого образа к тому или иному классу путем расчета расстояний в какой-либо метрике (Хэмминга, Евклида и пр.):

$$I = \sum_{i=1}^{F} (|C_i| - |D_i|); \tag{3}$$

$$I = \sqrt{\sum_{i=1}^{F} (C_i - D_i)^2}; \tag{4}$$

$$I = \sqrt{\sum_{i=1}^{F} \frac{(C_i - D_i)^2}{\sigma_i^2}}, \tag{5}$$

где C_i — вектор параметров КП легитимного пользователя, D_i — текущий вектор параметров КП пользователя АРМ, F — число анализируемых клавиш, σ_i^2 — среднеквадратическое отклонение C_i от D_i.

Для формального представления задачи распознавания образов наиболее часто используются ошибки первого и второго рода. Ошибка первого рода (P_1) — вероятность ошибочных отказов легитимному пользователю в допуске к АРМ (ложное выявление отклонений в поведении). Ошибка второго рода (P_2) — это вероятность допуска нелегитимного пользователя (ошибочный пропуск отклонений в поведении). Сравнения эталонного и текущего векторов параметров КП осуществляется с учетом заранее установленного порога. Проведенные исследования [4, 8, 9] показали, что вариации значения такого порога могут обеспечить высокий уровень достоверности выявления нелегитимного пользователя или отклонений в поведении ($P_2 \to 0{,}01$), однако это приводит к высокой вероятности ложного срабатывания ($P_1 \geq 0{,}45$). Естественно, такая система контроля состояния оператора АРМ КВОГ не обеспечивает заданной достоверности распознавания.

Анализ современных инструментов идентификации позволил определить, что параметрические методы распознавания в данных условиях более эффективны. Для реализации предлагаемого подхода требуется расчет дополнительных параметров (см. таблицу).

Так, отклонение от среднего в скорости набора может быть записано как

$$\alpha = \sqrt{\frac{\sum_{i=1}^{n-1}\left(\frac{t_i^{\text{pause}}}{t_{\max}^{\text{pause}}} - m^{\text{pause}}\right)^2}{n-2}}; \tag{6}$$

отклонение от среднего времени удержания

$$\beta = \sqrt{\frac{\sum_{i=1}^{n-1}\left(\frac{t_i^{\text{press}}}{t_{\max}^{\text{press}}} - m^{\text{press}}\right)^2}{n-2}}. \tag{7}$$

При этом математические ожидания (МО) времени паузы и нажатия соответственно

$$\overline{m}^{\text{pause}} = \frac{\sum_{i=1}^{n-1} \frac{t_i^{\text{pause}}}{t_{\max}^{\text{pause}}}}{n-1}; \qquad \overline{m}^{\text{press}} = \frac{\sum_{i=1}^{n} t_i^{\text{press}}}{n}; \tag{8}$$

$$\overline{s} = \frac{t_n^{\text{up}} - t_1^{\text{down}}}{60} v_{\max}, \tag{9}$$

где $t_i^{\text{down}}, t_i^{\text{up}}$ — время нажатия/отжатия клавиши, $t_i^{\text{press}} = t_i^{\text{up}} - t_i^{\text{down}}$ — время удержания клавиши, $t_i^{\text{pause}} = t_{i+1}^{\text{down}} - t_i^{\text{up}}$ — время между нажатиями, $v_{\max} = 900$ зн / мин — максимальная скорость набора.

Исследования показали, что число клавиш с перекрытиями и суммарное время перекрытий являются дополнительными признаками КП оператора в различных психологических состояниях. Факт перекрытия между клавишами i и $i+1$ выявляется, если:

$$t_i^{\text{down}} \le t_{i+1}^{\text{up}} \text{ и } t_{i+1}^{\text{down}} \le t_i^{\text{up}}. \tag{10}$$

При невыполнении условия (10) перекрытие клавиш отсутствует.

Среднее время перекрытий $\overline{t_c}$ и их среднеквадратическое отклонение d_c можно определить из

$$\overline{t_c} = \frac{t_c}{n_c \cdot t_{\max}^{\text{press}}}; \tag{11}$$

$$d_c = \sqrt{\frac{\sum_{i}^{n}\left(\frac{t_i^{\text{up}} - t_{i+1}^{\text{down}}}{t_{\max}^{\text{press}}} - \overline{t_c}\right)^2}{n_c - 1}}, \tag{12}$$

где t_c — суммарное время перекрытий, n_c — число клавиш с перекрытиями.

В результате получается новый (расширенный) вектор, используемый для ДА оператора АРМ КВОГ:

$$\mathbf{V} = \left\{t_1^{\text{press}}, \ldots, t_n^{\text{press}}, t_1^{\text{pause}}, \ldots, t_n^{\text{pause}}, \overline{m}^{\text{pause}}, \alpha, \overline{m}^{\text{press}}, \beta, \overline{s}, t_c, d_c\right\}. \tag{13}$$

Для эффективного функционирования системы ДА по конкретному пользователю необходимо L реализаций таких векторов $\mathbf{V} = \{V_1, V_2, \ldots, V_L\}$, при этом достаточность значения L должна выявляться путем решения отдельной задачи минимизации [4].

Обученная на расширенном векторе параметров (13) система ДА может использовать традиционный байесовский подход или его современные модификации [4] для принятия решения по классификации в пространствах „легитимный пользователь/нелегитимный пользователь“ и „норма/отклонение“.

Пусть заданы Q классов $K_1, K_2, \ldots, K_Q$ и $P(K_i|\mathbf{V})$, $i = 1, 2, \ldots, Q$, — апостериорная вероятность того, что пользователь, желающий получить доступ к системе, представляемый вектором признаков $\mathbf{V}$, принадлежит классу K_i. Для простоты сначала рассматривается два класса: K_1 — легитимный пользователь, K_2 — нелегитимный пользователь. Решающее правило: при максимуме апостериорной вероятности $P(K_1|\mathbf{V}) > P(K_2|\mathbf{V})$ — $\mathbf{V} \in K_1$, иначе $\mathbf{V} \in K_2$. Пусть $A_1, A_2, \ldots, A_n$ — полная группа несовместных событий и

$$\bigcup_{i=1}^{n} A_i = K \quad A_i \cap A_j = \varnothing, \text{ при } i \neq j.$$

$$P(A_i|B) = \frac{P(A_i) \cdot P(B|A_i)}{\sum_{i=1}^{n} P(A_i) \cdot P(B|A_i)},$$

где $P(A_i)$ — априорная вероятность события A_i, $P(B|A_i)$ — условная вероятность события B при условии, что произошло событие A_i.

Если $B \equiv K_i$, а $P(A)$ и $P(A|B)$ описываются плотностями $P(\mathbf{V})$ и $P(\mathbf{V}|K_i)$, то

$$P(K_i|\mathbf{V}) = \frac{p(\mathbf{V}|K_i) \cdot P(K_i)}{p(\mathbf{V})}.$$

В процессе классификации процедура сравнения $P(K_1|\mathbf{V})$ и $P(K_2|\mathbf{V})$ аналогична процедуре сравнения $P(\mathbf{V}|K_1) \cdot P(K_1)$ и $P(\mathbf{V}|K_2) \cdot P(K_2)$, следовательно, задача распознавания сводится к вычислению величин $P(\mathbf{V}|K_1)$, $P(K_1)$, $P(\mathbf{V}|K_2)$, $P(K_2)$. Практическое применение инструментария в виде программных продуктов [10, 11] показало, что с учетом (13) данных для определения вероятности принадлежности пользователя к каждому из классов достаточно для обеспечения $P_2 = 0{,}01$ при $P_1 \leq 0{,}22$.

Существенно сложнее распознать отклонения в поведении легитимного пользователя. При тех же исходных данных с учетом (13) достоверность распознавания отклонений поведения от нормы (усталость, опьянение, гнев), даже при ослабленных требованиях к ошибкам второго рода ($P_2 = 0{,}1$), приводит к высокому уровню ложных срабатываний ($P_1 \geq 0{,}4$). Однако дальнейшие исследования, в том числе [12, 13], показали необходимость модификации не столько средств распознавания, сколько способа сбора данных для обучения системы ДА, помещая пользователя в стрессовые ситуации [8, 9, 14]. Перспективно использование алгоритмов КП в составе полимодальной информационной системы с применением средств сбора аудио- и видеоданных (видеокамера, микрофон) [14, 15]. Примеры практического применения разработанного подхода с расширенным вектором параметров КП в составе комплексов защиты атомных электростанций с учетом разработанного программного инструментария [10, 11] продемонстрировали возможность повышения достоверности распознавания легитимности пользователя АРМ на 12—23 %.

Таким образом, динамическая аутентификация пользователя по КП перспективна для развития алгоритмов идентификации („на лету“) состояния операторов АРМ в ходе управления КВОГ. Расширение вектора параметров эталонного образа (КП легитимного пользовате-

ля) за счет учета перекрытия клавиш и отклонения от среднего при наборе позволило повысить достоверность распознавания в пространстве „легитимный пользователь/нелегитимный пользователь“. Однако для повышения достоверности распознавания отклонений в поведении легитимного пользователя требуется усовершенствовать систему контроля, дополнив ее многомодальным интерфейсом [4, 14, 15]. В связи с этим необходимо в кратчайшие сроки разработать „стрессовый“ компонент для совершенствования методики профессионального психофизического отбора кандидатов на замещение должностей операторов АРМ критически важных объектов государства.

Заключение. В результате исследования типовой системы динамической аутентификации оператора АРМ критически важного объекта выявлены пути повышения достоверности распознавания легитимности пользователя и отсутствия отклонений в его поведении за счет расширения составляющих вектора клавиатурного почерка. Предложены области применения многомодальных интерфейсов и пути совершенствования методики профессионального психофизического отбора кандидатов на замещение должности оператора АРМ критически важных объектов.

СПИСОК ЛИТЕРАТУРЫ

1. *Шнепс-Шнеппе М. А.* Телекоммуникации Пентагона: цифровая трансформация и киберзащита. М.: Горячая линия – Телеком, 2017. 272 с.
2. Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи. М.: Ассоциация документальной электросвязи, 2019. 108 с.
3. *Bely R. V., Harlanov A. S.* Analysis of global threats to Russia in the development of US space weapons systems as building a system of total military domination // Education. The science. Scientific personnel. 2020. P. 85—91.
4. *Никитин В. В., Басов О. О.* Подход к совершенствованию системы аутентификации пользователей автоматизированной системы // Информационные системы и технологии. 2018. № 5(109). С. 99—107.
5. *Березникер А. В.*, *Казачук М. А., Машечкин И. В., Петровский М. И.* Динамическая аутентификация пользователей на основе анализа работы с компьютерной мышью // Вестн. Московского университета. Сер. 15: Вычислительная математика и кибернетика. 2021. № 4. С. 3—16.
6. *Иванов А. И.* Биометрическая идентификация личности по динамике подсознательных движений. Пенза: Изд-во Пензенского гос. ун-та, 2000. 188 с.
7. *Саитов С. И., Будков В. Ю., Левоневский Д. К., Денисов А. В.* Моделирование сети передачи данных полимодальной системы контроля критически важных объектов государства // Вестн. Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления, 2021. Т. 17, № 1. С. 59—71.
8. *Шиверов П. К., Новосад Т. Г., Осипов М. Н.* Доверие в контексте анализа стойкости протоколов аутентификации // Ползуновский вестник. 2014. № 2. С. 248—250.
9. *Носов М. В., Басов О. О.* Оценивание психофизиологического состояния человека по сигналам различных каналов взаимодействия с техническими средствами автоматизированных рабочих мест // Тр. 4-й Междунар. науч.-практ. конф. „Современные инновации в науке и технике“. Курск, 2014. Т. 2. С. 72—75.
10. Св-во о рег. БД № 2017621143. База данных клавиатурного почерка для исследования психофизиологического состояния оператора / *С. И. Саитов, О. О. Басов, М. В. Носов.* 03.10.2017.
11. Св-во о рег. программ № 2018660834. Программа аутентификации пользователя по клавиатурному почерку / *С. И. Саитов, И. А. Саитов, А. А. Логвин.* 28.08.2018.
12. *Бобов М. Н.* Как организовать аутентификацию в сети взаимодействующих предприятий // Управление защитой информации. 2001. Т. 5, № 3. С. 267—273.
13. *Медриш М. А., Белявский Д. М., Дабринян С. С., Левова И. Ю.* и др. Цифровая идентификация объектов: технологии и не только. М.: Научное обозрение, 2016. 228 с.

14. *Саитов И. А., Басов О. О., Карпов А. А.* Методологические основы синтеза полимодальных инфокоммуникационных систем государственного управления: монография. Орел: Академия ФСО России, 2015. 270 с.

15. *Рындин А. В.* Метод приоритетной мультипотоковой передачи многомодальной информации. Дис. … канд. техн. наук. Таганрог: Южный Федеральный университет, 2022. 138 с.

Сведения об авторах

Игорь Акрамович Саитов — д-р техн. наук, профессор; Академия ФСО России; начальник факультета; E-mail: soul1308@yandex.ru

Андрей Игоревич Саитов — курсант; Академия ФСО России

Михаил Михайлович Шарапов — курсант; Академия ФСО России

Поступила в редакцию 17.01.2023; одобрена после рецензирования 14.03.2023; принята к публикации 27.04.2023.

REFERENCES

1. Shneps-Shneppe M.A. *Telekommunikatsii Pentagona: tsifrovaya transformatsiya i kiberzashchita* (Pentagon Telecommunications: Digital Transformation and Cyber Defense), Moscow, 2017, 272 p. (in Russ.)
2. *Metodicheskiye rekomendatsii po kategorirovaniyu ob"yektov kriticheskoy informatsionnoy infrastruktury, prinadlezhashchikh sub"yektam kriticheskoy informatsionnoy infrastruktury, funktsioniruyushchim v sfere svyazi* (Guidelines for Categorizing Critical Information Infrastructure Objects Owned by Critical Information Infrastructure Entities Operating in the Field of Communications), Moscow, 2019, 108 p. (in Russ.)
3. Bely R.V., Harlanov A.S. *Education. The science. Scientific personnel*, 2020, pp. 85–91.
4. Nikitin V.V., Basov O.O. *Information systems and technologies*, 2018, no. 5(109), pp. 99–107. (in Russ.)
5. Berezniker A.V., Kazachuk M.A., Mashechkin I.V., Petrovskiy M.I., Popov I.S. *Vestnik Moskovskogo Universiteta. Seria 15, Vycislitel'naa Matematika I Kibernetika*, 2021, no. 4, pp. 3–16. (in Russ.)
6. Ivanov A.I. *Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizheniy* (Biometric Identification of a Person by the Dynamics of Subconscious Movements), Penza, 2000, 188 p. (in Russ.)
7. Saitov S.I., Budkov V. Yu., Levonevsky D.K., Denisov A.V. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2021, no. 1(17), pp. 59–71. (in Russ.)
8. Shiverov P.K., Novosad T.G., Osipov M.N. *Polzunovskiy Vestnik*, 2014, no. 2, pp. 248–250. (in Russ.)
9. Nosov M.V., Basov O.O. *Sovremennyye innovatsii v nauke i tekhnike* (Modern Innovations in Science and Technology), Proceedings of the 4th International Scientific and Practical Conference, Kursk, 2014, vol. 2, pp. 72–75. (in Russ.)
10. Certificate on the state registration of the computer programs 2017621143, *Baza dannykh klaviaturnogo pocherka dlya issledovaniya psikhofiziologicheskogo sostoyaniya operatora* (Database of Keyboard Handwriting for the Study of the Psychophysiological State of the Operator), S.I. Saitov, O.O. Basov, M.V. Nosov, Priority 03.10.2017. (in Russ.)
11. Certificate on the state registration of the computer programs 2018660834, *Programma autentifikatsii pol'zovatelya po klaviaturnomu pocherku* (User Authentication Program by Keyboard Handwriting), S.I. Saitov, I.A. Saitov, A.A. Logvin, Priority 28.08.2018. (in Russ.)
12. Bobov M.N. *Upravleniye zashchitoy informatsii*, 2001, no. 3(5), pp. 267–273. (in Russ.)
13. Medrish M.A., Belyavsky D.M., Dabrinyan S.S., Levova I.Yu. *Tsifrovaya identifikatsiya ob"yektov: tekhnologii i ne tol'ko* (Digital Identification of Objects: Technologies and Not Only), Moscow, 2016, 228 p. (in Russ.)
14. Saitov I.A., Basov O.O., Karpov A.A. *Metodologicheskiye osnovy sinteza polimodal'nykh infokommunikatsionnykh sistem gosudarstvennogo upravleniya* (Methodological Foundations for the Synthesis of Polymodal Infocommunication Systems of Public Administration), Orel, 2015, 270 p. (in Russ.)
15. Ryndin A.V. *Metod prioritetnoy mul'tipotokovoy peredachi mnogomodal'noy informatsii* (Method of Priority Multistream Transmission of Multimodal Information), Candidate's thesis, Taganrog, 2022, 138 p. (in Russ.)

Data on authors

Igor A. Saitov — Dr. Sci., Professor; Academy of the Federal Security Service of Russia; Head of a Faculty; E-mail: soul1308@yandex.ru

Andrey I. Saitov — Cadet; Academy of the Federal Security Service of Russia

Mikhail M. Sharapov — Cadet; Academy of the Federal Security Service of Russia

Received 17.01.2023; approved after reviewing 14.03.2023; accepted for publication 27.04.2023.