УДК 004.056.53 DOI: 10.26102/2310-6018/2020.29.2.020

Реализация системы адаптивной аутентификации с применением ЭЭГ интерфейса

А.Ю. Исхаков[1], А.М. Смирнов[2]
[1]Институт проблем управления им. В.А. Трапезникова РАН, Москва, Российская Федерация
[2]МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Резюме: В работе предлагается методическое обеспечение для объектов критической информационной инфраструктуры, предусматривающее систематизацию основных шагов для формирования алгоритмов адаптивной аутентификации в том числе с применением биометрического фактора, заключающегося в проверке электроэнцефалограммы субъекта доступа. Предлагаемый подход устраняет недостатки существующих традиционных методов аутентификации, основанных на использовании явных способов проверки, связанных с тем, что для установления подлинности пользователя применяются опознавательные характеристики, которые могут быть скомпрометированы злоумышленниками. В ходе выполнения исследования была реализована подсистема аутентификации с помощью интерфейса мозг-компьютер. Несмотря на устойчивость к ошибкам второго рода, недостаточные результаты коэффициента ложного отказа в доступе, полученные на этапе проведения эксперимента, не позволяют осуществить «бесшовное» внедрение подобных механизмов биометрической аутентификации в действующие объекты критической информационной инфраструктуры. При этом, эффективность сформированных на основе предложенного в работе подхода адаптационных механизмов проверки пользовательского профиля свидетельствует о возможности их использования на реальных объектах с применением разносторонних факторов и критериев аутентификации. Таким образом, в рамках данной статьи был рассмотрен один из аспектов комплексного подхода по обеспечению безопасности функционирования технологических процессов, а также противодействию мошенничеству и хищению информации за счет формирования алгоритмов адаптивной аутентификации.

Ключевые слова: аутентификация, электроэнцефалограмма, нейроинтерфейс, критическая информационная инфраструктура, информационная безопасность.

Для цитирования: Исхаков А.Ю., Смирнов А.М. Реализация системы адаптивной аутентификации с применением ЭЭГ интерфейса. *Моделирование, оптимизация и информационные технологии.* 2020;8(2). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/05/IskhakovSmirnov_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.020

Implementation of an adaptive authentication system using an EEG interface

A.Y. Iskhakov[1], A.M. Smirnov[2]
[1]V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation
[2]Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract: The work offers methodological support for critical information infrastructure objects, which provides for the systematization of the basic steps for the formation of adaptive authentication

algorithms, including using a biometric factor, which consists in checking the electroencephalogram of the access subject. The proposed approach eliminates the drawbacks of existing traditional authentication methods based on the use of explicit verification methods related to the fact that authentication characteristics are used to authenticate the user, which can be compromised by attackers. During the research, an authentication subsystem was implemented using the brain-computer interface. Despite the resistance to errors of the second kind, the insufficient results of the false access denial coefficient obtained at the stage of the experiment do not allow for the "seamless" implementation of such biometric authentication mechanisms in existing objects of critical information infrastructure. At the same time, the effectiveness of the adaptive mechanisms for checking the user profile formed on the basis of the approach proposed in the work indicates the possibility of their use on real objects using diverse factors and authentication criteria. Thus, in the framework of this article, one of the aspects of an integrated approach to ensure the security of the functioning of technological processes, as well as combating fraud and theft of information through the formation of adaptive authentication algorithms, was considered.

Keywords: authentication, electroencephalogram, neurointerface, brain–computer interface, critical information infrastructure, information security.

For citation: Iskhakov A.Y., Smirnov A.M. Implementation of an adaptive authentication system using an EEG interface. *Modeling, Optimization and Information Technology*. 2020;8(2). Available from: https://moit.vivt.ru/wp-content/uploads/2020/05/IskhakovSmirnov_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.020 (In Russ).

Введение

Зачастую политика ограничения числа попыток ввода пароля при аутентификации в системах некоторых объектов критической информационной инфраструктуры (КИИ) не применяется либо устанавливается с большим пороговым значением. Это связано с результатом оценки рисков, которые определяют данную меру как опасную с точки зрения ошибок легитимного оператора и вследствие необходимости обеспечения непрерывности технологического процесса [1]. В связи с этим вызывают интерес методы адаптивной аутентификации, позволяющие по определенному набору признаков определить уровень риска тех или иных действий пользователя и выбрать соответствующий способ проверки. Очевидно, что при применении жестких ограничительных мер ложные срабатывания системы, возникающие вследствие подозрительных или ошибочных действий оператора, могут привести к нарушению производственного процесса, что в условиях промышленности и критических производств недопустимо [2]. Однако в разумных пределах подобные системы защиты информации позволят серьезнейшим образом улучшить эффективность мониторинга для операторов службы безопасности. Задача построения интеллектуальной системы оценки поведенческих признаков пользователя выходит за рамки данной статьи. В данной работе предпринимается попытка представить метод формирования системы адаптивной аутентификации (соответствующего алгоритма) и провести пробную интеграцию интерфейса мозг-компьютер в качестве одного из факторов для подобных проверок.

В последнее годы исследования в области развития биометрической аутентификации значительным образом расширились за счет методов и алгоритмов распознавании пользователей посредством оценки их уникальных параметров электроэнцефалограммы (ЭЭГ). ЭЭГ интерфейс в сравнении с традиционными биометрическими признаками (фотографиями лица, отпечатками пальцев, голоса, снимками радужной оболочки глаз) по праву обладает рядом достоинств с точки зрения надежности и приватности для пользователя [3]. Это связано с тем, что анализируемые сигналы не описывают никаких внешних особенностей человека. Они являются более устойчивыми к угрозам фальсификации, поскольку вероятность компрометации ЭЭГ

сигналов низкая в силу их уникальности, а задача синтеза является крайне сложной. Кроме того, при каждой попытке инициализации сеанса аутентификации системе нет необходимости проверять факт физического наличия живого субъекта и его дееспособного состояния. При этом в данном направлении до сих пор имеется ряд вопросов со стороны научного сообщества, требующих проведения многочисленных экспериментов: от общих задач выявления и апробации неизменяемых показателей и паттернов субъектов доступа в условиях возможных различий психофизиологического состояния до вопросов определения эффективных протоколов регистрации ЭЭГ.

Материалы и методы

Технологии снятия ЭЭГ в качестве поведенческих характеристик находят свое широкое применение в направлении обеспечения безопасности информации, при этом далеко не ограничиваясь задачами идентификации и аутентификации как отдельными подсистемами авторизации. Так в статье [4] рассматривается биометрическая криптосистема, реализующая доступ к ключевой информации пользователей посредством интерфейса мозг-компьютер. Алгоритмы проверки основаны на задаче дискретного логарифмирования и кодах Боуза-Чоудхури-Хоквингема [5]. Представленные эксперименты показывают, что предложенная система проверки как неотъемлемая составляющая биометрической криптосистемы является эффективной с показателем ошибок (ERR) 0,024. В работе [6] на основе результатов проведенных экспериментов установлена область применения нейросетевых преобразователей «Биометрия – код доступа» в современных криптографических приложениях. Авторами рассмотрены различные технологии выделения сигналов ЭЭГ, исследована эффективность различных математических методов обработки сигналов. Вышеперечисленные результаты позволили коллективу предложить подход к построению системы высоконадёжной биометрической аутентификации в соответствии с серией стандартов ГОСТ Р 52633, кардинально повысить эффективность идентификации на основе ЭЭГ в оценке $FAR = 10^{-12}$.

В то же время важно отметить, что любая система биометрической аутентификации должна обладать свойством стабильности используемых признаков. То есть эффективность применяемых алгоритмов не должна снижаться даже в случаях редких проверок субъектов доступа (спустя несколько недель или месяцев). Этот факт находит свое подтверждение в работе [7]. В данном исследовании эффективность системы биометрической идентификации подвергалась оценке в течение длительных промежутков времени (в частности, процент распознавания субъектов доступа снизился с 94.60% при первичных тестах до 78.20% спустя полгода тестирования). Кроме того, в исследовании [8] была выявлена схожая тенденция повышения общего уровня ошибок в механизме аутентификации на основе ЭЭГ (рост с 7.1% до 36.2% уже в течение 3 дней после инициализации профилей пользователей). Проблема снижения качества используемых паттернов распознавания профилей посредством различных классификаторов также находит свое подтверждение в [9-11].

Первичной задачей в рамках данного исследования заключалась в интеграции функционала биометрических проверок перед каждым сеансом авторизации. При инициализации подсистемы разграничения доступа от субъекта требуется проведение аутентификации на мобильном терминале посредством ввода графического пароля, состоящего из последовательности 4 команд (с применением зарегистрированных воображаемых состояний). При этом процесс проверки в общем виде включает в себя следующие этапы:

1. Снятие данных ЭЭГ у идентифицируемого;

2. Пространственная фильтрация;
3. Проверка полученного паттерна на заранее сформированном классификаторе;
4. Отработка базового алгоритма аутентификации.

Значительным недостатком предложенного метода, сдерживающим попытку его реализации в качестве единственного фактора аутентификации для всех информационных систем в исследуемом периметре внедрения, является сложность реализации поддерживающей его инфраструктуры. В связи с этим его внедрение возможно только в совокупности с дополнительными механизмами аутентификации [12-14]. На случай возникновения ошибок необходимо реализовать адаптивные механизмы проверки, учитывающих многочисленные параметры рабочей среды, характеризующие виртуальный профиль субъекта доступа.

При этом предлагается реализовать адаптивную подсистему анализа, принимающую решения о легитимности действий пользователя в течение всего сеанса работы по ряду различных характеристик: выявление несанкционированных изменений виртуального профиля субъекта доступа, изменение ЭЭГ при идентификации по сравнению с нейтральным состоянием идентифицируемого и др. (Рисунок 1).

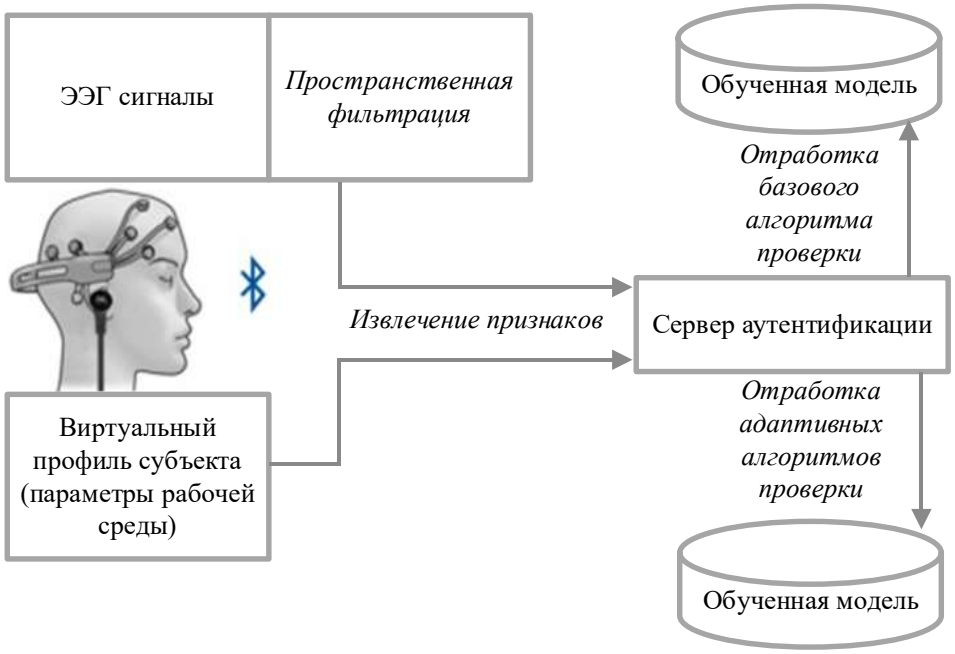

Рисунок 1 – Концептуальная схема предлагаемого подхода
Figure 1 – Conceptual scheme

Подход к построению адаптивной системы аутентификации

Проанализированные выше работы не предлагают унифицированного методического обеспечения для построения систем адаптивной аутентификации, а ограничиваются рассмотрением частных вопросов, касающихся проведения задач классификации признаков. Не менее важной задачей представляется формирование метода, который предусматривает систематизацию основных шагов по реализации алгоритмов на объекте КИИ для подсистемы адаптивной аутентификации, обеспечивая при этом возможности:

1) Детектировать инциденты информационной безопасности посредством анализа аутентификационного профиля пользователя;

2) Адаптивно подбирать дополнительный фактор аутентификации в зависимости от выявленных отклонений. Данное требование позволит учесть политики безопасности типовых объектов с системами промышленной автоматизации, которые не позволяют внедрить блокировку по *N* ошибкам оператора (невозможность приостановки процесса, например, в случае если оператор вводит ошибочный пароль).

Метод представлен ниже в виде пошагового описания выполняемых этапов.

Входные данные:

1) S – множество информационных систем, требующих внедрение аутентификации операторов:

$$S = \{s_1, s_2, ..., s_n\}, \quad (1)$$

где n – число таких информационных систем;

2) A' – множество возможных способов аутентификации;

Основные шаги:

Шаг 1. Провести аудит для каждой информационной системы $s_i \in S$;

Шаг 2. Определить множество C всех возможных признаков и характеристик оператора, доступных к сбору для каждой из сред:

$$\forall s_i \in S : \mathrm{C}_i = \{\mathrm{c}_i \mid \mathrm{c}_i - \text{признак оператора, доступный для сбора в информационной системе } s_i\} \quad (2)$$

Шаг 3. Определить множество возможных для систем $s_i \in S$ $(i = \overline{1,n})$ способов аутентификации A ($A \subset A'$) и перечень действий X_j для каждого из способов:

$$\forall a_j \in A : X_j = (x_{j1}, x_{j2}, ..., x_{jm}), \quad (3)$$

где m – число действий для способа аутентификации $a_j \in A$, так что последовательность X_j приводит к выполнению a_j ;

Шаг 4. Провести группировку соответствия «Признак → Перечень действий для его аутентификации», которая сформируется в обучающую выборку в виде кортежей:

$$\langle c_i, X_j \rangle = \langle c_i, (x_{j1}, x_{j2}, ..., x_{jm}) \rangle \quad (4)$$

Шаг 5. Используя методы машинного обучения (обозначаемые как единая функция F) провести обучение математической модели с обязательным этапом оптимизации набора признаков по степени их важности на принятие решений.

$$F : \langle c, X \rangle \to \langle \mathrm{P}, \langle C, \mathrm{Y} \rangle \rangle, \quad (5)$$

где P – профиль аутентификации, Y – перечень действий после оптимизации и ранжирования;

Шаг 6. Сформировать и задокументировать профиль аутентификации ($p_k \in P$) для объекта в виде последовательности действий Y:

$$\langle p_k, \langle c_k, y_j \rangle \rangle, \quad (6)$$

где k – порядковый идентификатор профилей аутентификации, i – идентификатор признака оператора в информационной системе, j – идентификатор для оптимизированного и ранжированного перечня действий для проверки признака c_i ;

Шаг 7. Формирование алгоритма адаптивной аутентификации для выбранного объекта на основе полученных профилей аутентификации.

Выходные данные:

1) кортежи вида $\langle \mathrm{P}, \langle C, \mathrm{Y} \rangle \rangle$, определяющие пары профилей аутентификации и оптимизированный и ранжированный набор признаков и действий для ее проведения;

2) алгоритм адаптивной аутентификации на основе полученных профилей, отличающийся возможностью определять набор признаков на основе доступных способов аутентификации конкретной системы с учетом анализа признаков, не прошедших проверку.

На Рисунке 2 представлены блок-схемы как предлагаемого метода, так и полученного алгоритма аутентификации в общем виде.

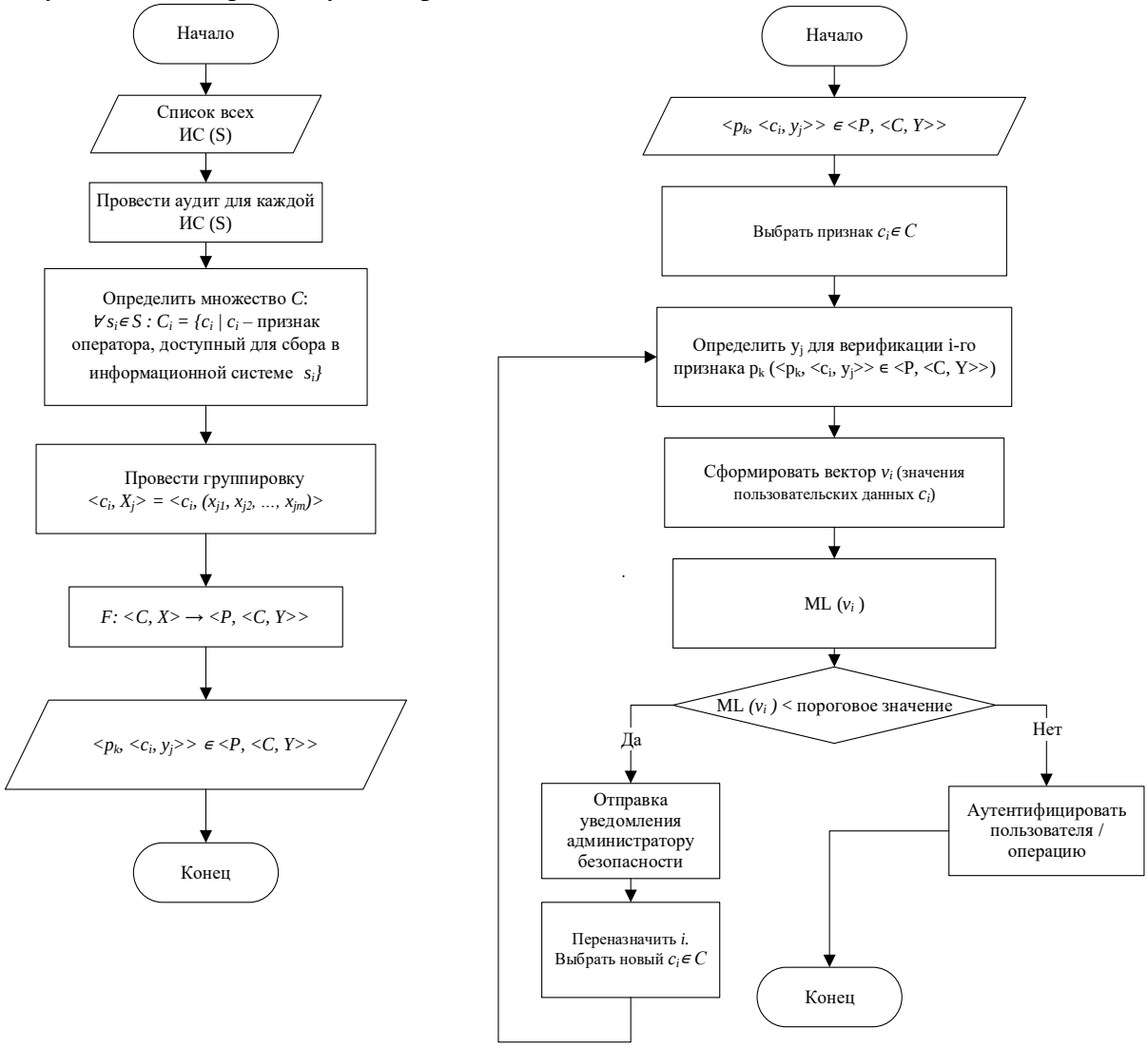

Рисунок 2 – Блок-схемы предлагаемого метода и полученного алгоритма аутентификации в общем виде

Figure 2 – Flowcharts of the proposed method and the obtained authentication algorithm in general form

Электроэнцефалограмма как фактор аутентификации

С целью отделения шумов от целевого сигнала был использован фильтр Баттерворта 8-го порядка. Это позволило сделать более плоским участок характеристики в полосе пропускания. Учитывая, что ЭЭГ здорового взрослого человека, находящегося в состоянии покоя, имеет два основных типа ритмов, характеризующихся частотой колебаний в 8—13 Гц и 14—30 Гц соответственно, в качестве нижней полосы пропускания было использовано значение 8 Гц, а в качестве верхней — 30 Гц.

На этапе обучения предлагается предоставить субъекту механизм проверки с помощью графического пароля (это позволит на первых этапах понимать насколько корректно отрабатывает биометрическая подсистема). В целях управления отрисовкой графического пароля было решено реализовать 4 состояния для однозначного определения направления движения пера: вверх, вниз, вправо и влево. Каждое из таких состояний задается пользователем при помощи воображаемых движений конечностями (возможно и нейтральное состояние) и регистрируется с помощью нейрогарнитуры. Для классификации состояний пользователя была использована многоклассовая классификация на основе данных ЭЭГ, модель обучения — многослойный перцептрон. В качестве математического аппарата использовались многослойные нейронные сети прямого распространения. Обучение осуществлялось алгоритмом обратного распространения [15]. В качестве векторов биометрических данных особое внимание отдавалось векторам данных, снятых с электродов, расположенных на затылочной области головы, в которой возникает наиболее сильный вызванный потенциал [16].

Алгоритм неоднократно обрабатывает элементы из обучающего множества $\left\{\left(x(n), d(n)\right)\right\}_{n=1}^{N}$ следующим образом:

1) Генерация методом конгруэнтных соотношений случайных равномерно распределенных чисел с математическим ожиданием 0 пороговых значений и весовых коэффициентов.

2) Пусть обучающая выборка представлена парой $\left(x(n), d(n)\right)$. Тогда индуцированное локальное поле нейрона *j i*-го слоя можно вычислить по формуле:

$$v_j^{(i)}(n) = \sum_{l=1}^{l_0} w_{jl}^{(i)}(n)\, y_l^{(i-1)}(n), \tag{7}$$

где $y_l^{(i-1)}(n)$ — выходной сигнал нейрона, расположенного в предыдущем слоя на текущей итерации *n*. Причем $y_0^{(i-1)}(n) = 1$, а $w_{jl}^{(i)}(n)$ – порог, примененный к нейрону.

Для определения выходного сигнала нейрона использована функция сигмоидального типа $\phi_j\left(v_j(n)\right)$. Пусть I – глубина сети, тогда $y_0^{(I)}(n) = o_j(n)$, а значение ошибки вычисляется следующим образом: $e_j(n) = d_j(n) - o_j(n)$.

3) Определение локальных градиентов узлов:

$$\delta_j^i(n) = e_j(n)\frac{\partial\phi\left(v_j^{(I)}\right)}{\partial v_j^{(I)}}. \tag{8}$$

4) Повторение вычислений, указанных в пунктах 2 и 3, до тех пор, пока не выполнится критерий останова: достаточно малая интенсивность изменений среднеквадратичной ошибки.

В рассматриваемой задаче классификации удобнее применить метод, основанный на представленном выше алгоритме – метод случайного изменения порядка следования примеров, подаваемых на вход многослойного персептрона от одной эпохи к другой. В качестве сигмоидальной функции рекомендуется использовать нелинейную функцию

гиперболического тангенса, так как она является антисимметричной и модель обучается быстрее.

В качестве оценки решения классификатора было использовано Байесовское решающее правило, обобщенное для апостериорной вероятности оценок. Случайный вектор относится к классу C_k, ($k=\overline{1,4}$) в том случае, если $F_k(x) > F_j(x)$ для всех *j*. Причем вектор-функция *F* минимизирует функционал эмпирического роста.

На следующем этапе решается вопрос легитимности пользователя. Осуществляется повторная проверка отделенных от шумов сигналов на попадание в указанный интервал частоты колебаний ритмов. Аутентификация считается успешно пройденной субъектом в том случае, если последовательность состояний, распознанных сетью, полностью совпадает с соответствующей последовательностью, однозначно определяющей графический пароль.

Реализация алгоритма адаптивной аутентификации с применением ЭЭГ

В рамках исследования оценки эффективности представленного ранее подхода к применению ЭЭГ интерфейса в задаче адаптивной аутентификации была использована восьмиканальная нейрогарнитура беспроводной регистрации ЭЭГ человека с сухими электродами Neuroplay-8C и программное обеспечение Cortex 1.8.0. В целях обеспечения аутентификации с помощью интерфейса мозг-компьютер был разработан прототип программного комплекса на языке C++ с использованием интегрированной кроссплатформенной среды разработки Qt версии 5.5.1. При этом задано следующее соответствие между состояниями пользователя и командами по управлению движением пера:

1) сосредоточение – вверх,
2) нейтральное состояние – вниз,
3) резкие воображаемые движения нижними конечностями – вправо,
4) резкие воображаемые движения рукам – влево.

Для получения информации о текущем состоянии пользователя, определяемом при помощи многослойного перцептрона, осуществлялся GET-запрос по протоколу HTTPS на серверное приложение. Графический интерфейс разработанного прототипа представлен на Рисунке 3.

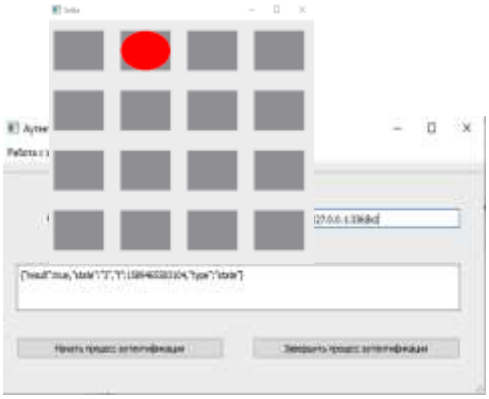

Рисунок 3 – Форма для управления запуском и остановом процесса аутентификации с применением графического пароля и нейроинтерфейса
Figure 3 – Form for managing the start and stop of the authentication process using a graphic password and BCI

При запуске процесса аутентификации старт осуществлялся из левого верхнего угла сетки. При первом несовпадающем состоянии с элементом заданной последовательности состояний аутентификация прерывается, пользователь объявляется нелегитимным, а администратору безопасности отправляется уведомление о возможном нарушителе. Для проверки и оценки качества разработанного прототипа была проведена серия экспериментов на десяти испытуемых. При этом для обучения было проведено 30 тестов, а затем по 30 контрольных тестов для каждого из испытуемых. С учетом используемой международной системы расположения электродов «10-20» при регистрации электроэнцефалограммы на Рисунках 4 и 5 приведены примеры диаграммы спектров для указанных электродов первого и третьего состояний в области альфа- (отмечены зеленым цветом), бета- (отмечены красным цветом), тета- (отмечены синим цветом), дельта- (отмечены сиреневым цветом), гамма- (отмечены оранжевым цветом) ритмов двух испытуемых.

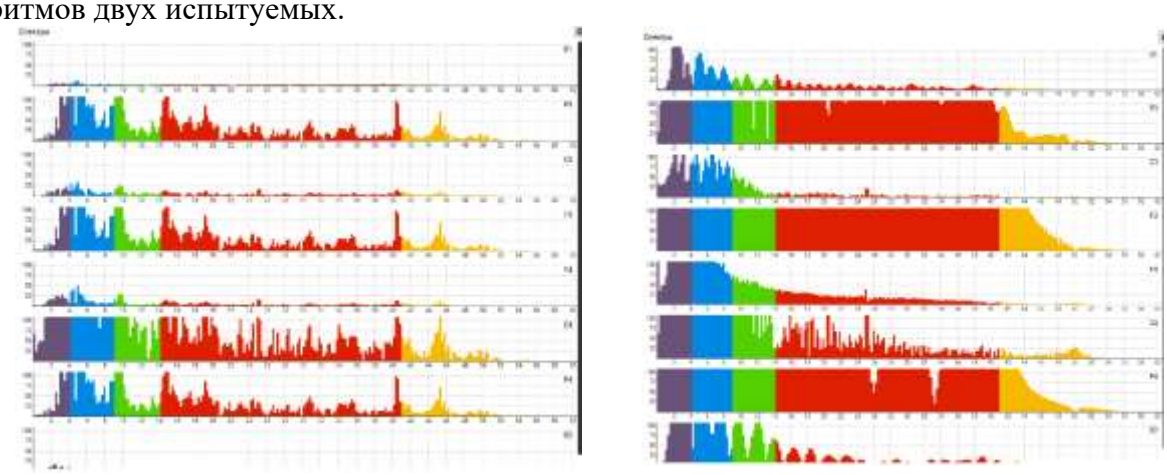

Рисунок 4 — Диаграмма спектров легитимного пользователя для состояний 1 (слева) и 3 (справа)

Figure 4 – Legitimate user spectrum chart for state 1 (left) and 3 (right)

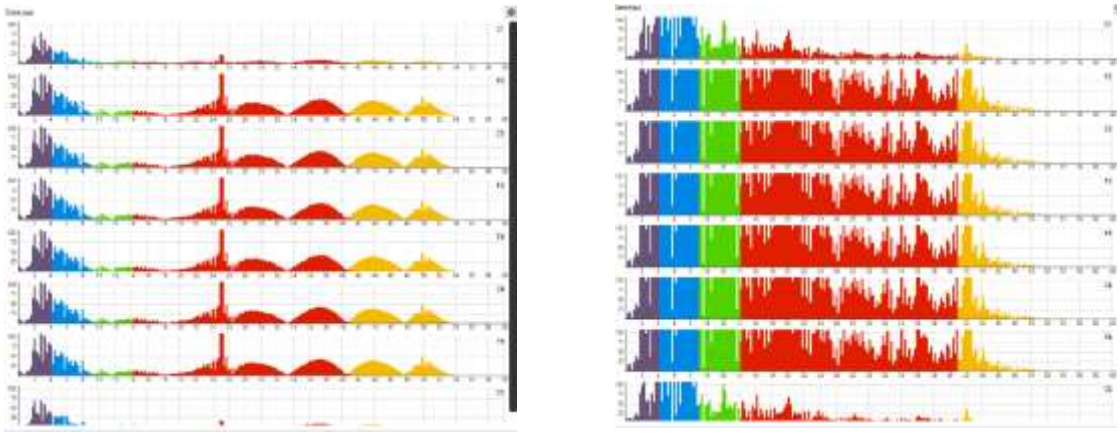

Рисунок 5 — Диаграмма спектров для одного из нелегитимных пользователей, имитирующих заранее известный код доступа (состояние 1 слева, состояние 3 справа)

Figure 5 – Spectrum chart for one illegitimate users imitating a previously known access code (state 1 on the left, state 3 on the right)

Таблица 1 — Сопоставление данных оценки применения нейроинтерфейса с учетом предложенного подхода

Table 1 – Compared data on the reliability of the use of the neural interface taking into account the proposed approach

Параметры используемой сети	Первая итерация с применением ЭЭГ		Адаптационные механизмы проверки		
	FRR	*FAR*	Количество запусков	% успешных авторизаций после 1-го алгоритма	% успешных авторизаций после 2-го алгоритма
1024 нейрона, N=5	0.2335	0,0001*	121	99%	1%
1024 нейрона, N=10	0.3921	0,0001*	185		

** В ходе проведения экспериментов FAR ошибок не зафиксировано. Поскольку данная величина носит вероятностный характер и в соответствии с рассмотренными исследованиями, принято* $FAR < 10^{-4}$.

Несмотря на абсолютную устойчивость к ошибкам второго рода, недостаточные результаты FRR, полученные с помощью предложенных выше алгоритмов, не позволяют осуществить «бесшовное» внедрение подобных механизмов биометрической аутентификации в действующую систему проверки и разграничения прав доступа. Это вызвано большим числом малоинформативных признаков и несимметричными функциями плотности вероятности, которые проблематично аппроксимировать известными законами распределения [17]. В связи с этим и с целью улучшения результатов требуется проведение дополнительных исследований с привлечением большего числа испытуемых и построением альтернативных классификаторов, в том числе с применением методов глубокого обучения [18]. При этом эффективность сформированных на основе предложенного в работе подхода адаптационных механизмов проверки пользовательского профиля показала свою эффективность, что свидетельствует о возможности его использования на реальных объектах КИИ с применением разносторонних факторов и критериев аутентификации.

Заключение

Обеспечение безопасности промышленных систем автоматизации и управления – сложная задача, требующая комплексного подхода, для решения которой необходимо учитывать и специфику промышленных систем, и международные и отечественные стандарты, а также требования регулирующих органов, направленные на повышение безопасности ключевых систем информационной инфраструктуры [19-20]. В рамках данной статьи был рассмотрен один из аспектов комплексного подхода по обеспечению безопасности функционирования технологических процессов, а также противодействию мошенничеству и хищению информации за счет реализации подсистемы адаптивной аутентификации.

Экспериментальная проверка доказывает эффективность представленного метода по формированию механизмов адаптивной аутентификации с учетом большого количества ошибок первого рода, выявленных при первичной апробации внедрения биометрического фактора проверки по ЭЭГ. Преимуществом предложенного подхода является возможность по определенному набору признаков определить уровень риска тех или иных действий пользователя и выбрать соответствующий способ аутентификации, что в свою очередь уменьшает возможность получения и использования защищаемых данных злоумышленником.

Благодарности

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-29-01156 мк и гранта Президента РФ для молодых российских ученых – кандидатов наук (МК-2421.2020.9).

ЛИТЕРАТУРА

1. Двойнишников Н.Э. Технологические особенности проблем обеспечения информационной безопасности автоматизированных систем управления, являющихся объектами критической информационной инфраструктуры. *Международный журнал прикладных наук и технологий «Integral»*. 2019;1:127-132.
2. Аракелян Э.К., Андрюшин А.В., Минзов А.П. Особенности систем информационной безопасности АСУТП ТЭС и АЭС. *Доклады БГУИР*. 2015;2:213-214.
3. Гончаров С.М., Вишняков М.С. Идентификация пользователей на основе электроэнцефалографии с использованием технологий «Интерфейс мозг-компьютер». *Доклады ТУСУР*. 2012;1-2(25):166-170.
4. Damasevicius R., Maskeliunas R., Kazanavicius E., Wozniak M. Combining Cryptography with EEG Biometrics. *Computational Intelligence and Neuroscience*. 2018:1867548.
5. Кузьмин О.В., Дружинин В.И. Коды Боуза–Чоудхури–Хоквингема в системах обнаружения и исправления ошибок при передаче данных. *Современные технологии. Системный анализ. Моделирование*. 2013;3(39):23-29.
6. Гончаров С. М., Боршевников А. Е. Нейросетевой преобразователь «Биометрия – код доступа» на основе электроэнцефалограммы в современных криптографических приложениях. *Вестник СибГУТИ*. 2016;1:17-22.
7. Hu B., Liu Q., Zhao Q., Qi Y., Peng H. A real-time electroencephalogram (EEG) based individual identification interface for mobile security in ubiquitous environment. *2011 IEEE Asia-Pacific Services Computing Conference*. 2011:436-441.
8. Marcel S., Millan J. del R. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2007;29;4:743–748.
9. Yang S., Deravi F. On the Usability of Electroencephalographic Signals for Biometric Recognition: A Survey. *IEEE Transactions on Human-Machine Systems*. 2017;47;6:958–969.
10. Rahman M.W., Gavrilova M. Overt mental stimuli of brain signal for person identification. *2016 International Conference on Cyberworlds*. 2016:197–203.
11. Chan H.-L., Kuo P.-C., Cheng C.-Y., Chen, Y.-S. Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition. *Frontiers in Neuroinformatics*. 2018;12:1–15.

12. Исхаков А.Ю., Мещеряков Р.В. Схемы аутентификации пользователя в СКУД с использованием QR кодов и передачи данных по технологии NFC. *Информационное противодействие угрозам терроризма*. 2014;22: 11-15.
13. Богданов Д.С., Клюев С.Г. Классификация и сравнительный анализ технологий многофакторной аутентификации в Веб-приложениях. *Моделирование, оптимизация и информационные технологии.* 2020;8(1).
14. Исхаков А. Ю., Исхакова А. О., Мещеряков Р. В., Бендрау Р., Мелехова О. Использование тепловой карты поведения пользователя в задаче идентификации субъекта инцидента информационной безопасности. *Труды СПИИРАН*. 2018; 6(61):147-171.
15. Хайкин С. Нейронные сети: полный курс, 2-е изд: М. : Издательский дом «Вильямс». 2006.
16. Лебедева Н. Н., Каримова Е.Д. Устойчивость паттернов ЭЭГ человека в различных задачах: проблема аутентификации личности. *Журнал высшей нервной деятельности им. И.П. Павлова,* 2020;70(1):40-49.
17. Сулавко А.Е., Самотуга А.Е., Стадников Д.Г., Пасенчук В.А., Жумажанова С.С. Биометрическая аутентификация на основе параметров электроэнцефалограмм. *Материалы III Международной научно-технической конференции Проблемы машиноведения*. 2019;2:375-384.
18. Евсютин О.О., Мещеряков Р.В., Шумская О.О. Стегоанализ цифровых изображений с использованием наивного Байесовского классификатора. *Материалы 10-й Всероссийской мультиконференции МКПУ-2017*. 2017:56-58.
19. Usmonov B., Evsutin O., Iskhakov A., Shelupanov A., Iskhakova A., Meshcheryakov R. The cybersecurity in development of IoT embedded technologies. *2017 International Conference on Information Science and Communications Technologies (ICISCT)*. 2017:1-4.
20. Исхаков С. Ю., Шелупанов А.А., Исхаков А.Ю. Имитационная модель комплексной сети систем безопасности. *Доклады ТУСУР*. 2014;2(32):82–86.

REFFERENCES

1. Dvojnishnikov N.E. Technological features of the problems of ensuring the information security of automated control systems that are objects of critical information infrastructure. *International Journal of Applied Sciences and Technologies "Integral"*. 2019;1:127-132.
2. Arakelyan E.K., Andryushin A.V., Minzov A.P. Features of information security systems for process control systems of thermal and nuclear power plants. *Doklady BGUIR*. 2015;2:213-214. (In Russ.)
3. Goncharov S.M., Vishnyakov M.S. User identification based on electroencephalography data using «Brain Computer Interface» technology. *Proceedings of Tomsk State University of Control Systems and Radioelectronics*. 2012:1-2(25):166-170. (In Russ.)
4. Damasevicius R., Maskeliunas R., Kazanavicius E., Wozniak M. Combining Cryptography with EEG Biometrics. *Computational Intelligence and Neuroscience*. 2018:1867548.
5. Kuzmin O.V., Druzhinin V.I. Bose – Chaudhuri – Hocquenghem codes in systems of detection and correction of errors when transferring data. *Modern technologies. System analysis. Modeling.* 2013;3(39):23-29. (In Russ.)
6. Goncharov S., Borshevnikov A. Neural network transformer "Biometry – access code" based on the electroencephalogram in modern cryptographic applications. *Vestnik SibGUTI*. 2016;1:17-22. (In Russ.)

7. Hu B., Liu Q., Zhao Q., Qi Y., Peng H. A real-time electroencephalogram (EEG) based individual identification interface for mobile security in ubiquitous environment. *2011 IEEE Asia-Pacific Services Computing Conference*. 2011:436-441.
8. Marcel S., Millan J. del R. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2007;29;4:743–748.
9. Yang S., Deravi F. On the Usability of Electroencephalographic Signals for Biometric Recognition: A Survey. *IEEE Transactions on Human-Machine Systems*. 2017;47;6:958–969.
10. Rahman M.W., Gavrilova M. Overt mental stimuli of brain signal for person identification. *2016 International Conference on Cyberworlds*. 2016:197–203.
11. Chan H.-L., Kuo P.-C., Cheng C.-Y., Chen, Y.-S. Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition. *Frontiers in Neuroinformatics*. 2018;12:1–15.
12. Iskhakov A.Y., Meshcheryakov R.V. Patterns user authentication in the ACS using QR codes and data technology NFC. *Information counteraction to threats of terrorism*. 2014;22:11-15. (In Russ.)
13. Bogdanov D.S., Klyuev S.G. Classification and comparative analysis of technologies of multifactor authentication in Web applications. *Modeling, optimization and information technology*. 2020;8(1). (In Russ.)
14. Iskhakov, A. Y., Iskhakova, A. O., Meshcheryakov, R. V., Bendraou, R., Melekhova, O. Application of User Behavior Thermal Maps for Identification of Information Security Incident. *SPIIRAS Proceedings*. 2018;6(61):147-171.
15. Haikin S. Neural Networks: a complete course, 2nd ed.– M.: Williams Publishing House. 2006. (In Russ.)
16. Lebedeva N.N., Karimova E.D. Stability of human EEG patterns in different tasks: the personality authentication problem. *Neuroscience and Behavioral Physiology*, 2020;70(1):40-49. (In Russ.)
17. Sulavko A.E., Samotuga A.E., Stadnikov D.G., Pasenchuk V.A, Zhumazhanova S.S. Biometric authentication based on electroencephalogram parameters. *Materials of the III International Scientific and Technical Conference Problems of Engineering.* 2019;2:375-384. (In Russ.)
18. Evsutin O.O., Meshcheryakov R.V., Shumskaya O.O. Steganalysis of digital images with use of the naive Bayes classifier. *Materials of the 10th All-Russian Multi-Conference MKPU-2017.* 2017:56-58. (In Russ.)
19. Usmonov B., Evsutin O., Iskhakov A., Shelupanov A., Iskhakova A., Meshcheryakov R. The cybersecurity in development of IoT embedded technologies. *2017 International Conference on Information Science and Communications Technologies (ICISCT)*. 2017:1-4.
20. Iskhakov S.Yu., Shelupanov A.A., Iskhakov A.Y. Engineering of imitation model of a complex network of security systems. *Proceedings of Tomsk State University of Control Systems and Radioelectronics*. 2014;2(32):82–86.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Исхаков Андрей Юнусович, кандидат технических наук, старший научный сотрудник Института проблем управления им. В.А. Трапезникова РАН, Самара, Российская Федерация.
e-mail: iskhakovandrey@gmail.com
ORCID: 0000-0002-6603-265X

Andrey Y. Iskhakov, PhD, Associate professor, «Higher Mathematics And Economic-Mathematical Methods» Department, Samara State University Of Economics , Samara, Russian Federation.

Смирнов Антон Михайлович, студент МГТУ им. Н. Э. Баумана, Москва, Российская Федерация.
e-mail: smirnovanton.m@mail.ru

Anton M. Smirnov, student, Bauman Moscow State Technical University, Moscow, Russian Federation,