Для цитирования: *А.Р. Абзалов, И.И. Кашапов, А.Ю.Орлов, И.Р. Мамлеев. Аутентификация пользователей на основе трехступенчатой модели клавиатурного почерка. Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47(3): 39-48. DOI:10.21822/2073-6185-2020-47-3-39-48*
For citation: *A.R. Abzalov, I.I. Kashapov, A.Yu. Orlov, I.R. Mamleev. User authentication based on the three-stage keyboarding model. Herald of Daghestan State Technical University. Technical Sciences. 2020; 47 (3): 39-48. (In Russ.) DOI:10.21822/2073-6185-2020-47-3-39-48*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 004.059
DOI:10.21822/2073-6185-2020-47-3-39-48

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ТРЕХСТУПЕНЧАТОЙ МОДЕЛИ КЛАВИАТУРНОГО ПОЧЕРКА

А.Р. Абзалов, И.И. Кашапов, А.Ю. Орлов, И.Р. Мамлеев
Казанский национальный исследовательский технический университет
им. А.Н. Туполева,
420111, г. Казань, ул. Карла Маркса, 10, Россия

Резюме. Цель. *В статье предложена трехступенчатая модель, которая позволяет увеличить эффективность аутентификации при реализации систем дистанционного обучения, не только в системах автоматического прокторинга, но и в сложных информационных системах критически важных объектов.* ***Метод.*** *Увеличение эффективности аутентификации пользователей происходит за счёт увеличения точности аутентификации по клавиатурному почерку.* ***Результат.*** *Предложенная модель поможет осуществить процесс разграничения доступа для мошенников и легальных пользователей, путём приспосабливания к малейшим изменениям параметров клавиатурного почерка, что позволяет увеличить точность аутентификации. Во время тестирования один из тестируемых пользователей был аутентифицирован при помощи сравнения девиаций, в то время как другие три пользователя были аутентифицированы при помощи критерия χ^2. Оставшиеся пользователи не смогли пройти процедуру аутентификацию на всех этапах системы.* ***Вывод.*** *Проведено экспериментальное исследование, результаты которого показали высокую способность предложенной модели разграничения доступа для легальных пользователей и злоумышленников с учетом незначительных изменений параметров динамики нажатия клавиш, и повысить точность аутентификации пользователей. Достоверность аутентификации пользователей на практике составила 97,5%.*

Ключевые слова: *дистанционное обучение, клавиатурный почерк, биометрия, аутентификация, автоматический прокторинг*

USER AUTHENTICATION BASED ON THE THREE-STAGE KEYBOARDING MODEL

A. R. Abzalov, I.I. Kashapov, A.Yu. Orlov, I.R. Mamleev
A.N. Tupolev Kazan National Research Technical University,
10 Karl Marx St., Kazan 420111, Russia

Abstract. Objective. *The article offers a three-stage model that allows increasing the effectiveness of authentication in the implementation of distance learning systems, not only in automatic proctoring systems but also in complex information systems of critical objects.* ***Methods.*** *Increasing the effectiveness of user authentication is achieved by increasing the accuracy of authentication using keyboarding.* ***Results.*** *The proposed model will help to implement the process of access differentiation for fraudsters and legal users, by adapting to the slightest changes in the keyboarding parameters, which allows increasing the authentication accuracy. During testing, one of the tested users was authenticated using a deviation comparison, while the other three users were authenticated using the χ^2*

criterion. The remaining users were not able to complete the authentication procedure at all stages of the system. ***Conclusion.*** *The results of an experimental study showed the high ability of the proposed model of access control for legitimate users and attackers with some minor changes in the parameters of the keystrokes dynamics, improving the accuracy of user authentication. The user authentication reliability in practice was 97.5%.*

Keywords: *distance learning, keyboarding, biometrics, authentication, automatic proctoring*

Введение. Несмотря на то, что задачи аутентификации и идентификации пользователей при работе в информационных системах, в том числе дистанционного обучения, достаточно изучены, они все еще остаются актуальными. Ранее созданные решения основываются на ограниченном количестве средств и методов, таких как: электронные замки, а также технологии биометрической аутентификации и идентификации. Не так давно широкое распространение получил метод аутентификации, основанный на клавиатурном почерке, иначе говоря, характерном наборе произвольного текста или парольной фразы на клавиатуре.

Данный принцип аутентификации пользователей заключается в возможности анализа временных промежутков между нажатиями клавиш при вводе пароля. Эффект клавиатурного почерка создается благодаря осуществлению большинства манипуляций с клавиатурой на бессознательном уровне. У каждого подготовленного пользователя, при многократном вводе одного и того же пароля, формируется автоматический стереотип действий.

Анализируемыми параметрами клавиатурного ввода являются: временные интервалы между нажатиями соседних клавиш, а также время нажатия каждой клавиши. В работах [1-5] приведены результаты исследований идентификации пользователей по клавиатурному почерку. Точность идентификации составляет более 97%. Помимо того, существует множество иностранных исследований.

Примером может служить работа Е. Флиора и К. Ковальского и разработанная ими система идентификации, основанная на клавиатурном почерке. В результате их работы только 3 из 8 пользователей были идентифицированы верно. А вероятность распознавания соответственно равна 37,5%. В то же время, Н. Д'Лим и Дж. Миталл получили результат в 12,5%, что соответствует лишь 1 распознанному пользователю из 8.

Постановка задачи. Большинство современных систем аутентификации позволяют весьма точно определить конкретного пользователя, однако достигается это простой связкой логин и пароль. Аутентификация же пользователей по клавиатурному почерку не требует дополнительных привязок к пользователю, однако имеет при этом существенным недостатком – низкую точность. В работе представлена трехступенчатая модель увеличения точности аутентификации по клавиатурному почерку, чьей основной задачей, помимо прочих, также является увеличение эффективности аутентификации в том числе и на сложных критически важных системах.

Методы исследования.

1. ***Исследование современных решений аутентификации пользователей с использованием систем автоматизированного прокторинга***

1.1 Автоматизированный прокторинг.

Центр тестирования – реальное место в физическом мире, где проходит первичная аутентификация пользователей, а затем и текущая, промежуточная или итоговая аттестация с применением технических средств тестирования. В центре тестирования проводится компьютерное тестирование, в процессе которого специальные средства наблюдения фиксируют местоположение и действия пользователя.

Существуют автоматизированные контрольные системы онлайн тестирования, которые позволяют выявлять так называемый «маскарад» или подмену тестируемого (ProctorEdu, Экзамус и др.). В таких системах обязательно присутствие человека – проктора, в чьи обязанности входит слежение за процессом и выявление нарушений в режиме реального времени.

Пользователей верифицируют в два этапа: система сверяет фотографию, которую поль-

зователь загружал во время подачи заявки на онлайн тестирование, с пользователем, находящимся перед камерой. Система делает фотографию пользователя непосредственно перед онлайн тестированием и сравнивает её с эталоном. Однако данные системы прокторинга имеют недостатки: производительность зависит от количества прокторов, которые находятся онлайн или просматривают видеозаписи, при оценивании результатов тестирования происходит задержка по времени (нужно время, чтобы просмотреть видеозаписи, в случае асинхронного прокторинга,), сложно организовать работу большого количества прокторов, также проктор может оказаться недобросовестным или необязательным, что может сказаться на качестве процесса. Стоит отметить, что, несмотря на указанные недостатки, подобные системы, в настоящее время, применяются в комплексных системах прокторинга, в частности, большинством американских вузов.

Данное решение очень эффективно, но для его использования требуются материальные затраты на технические средства, для найма административного персонала, затраты на помещение, в которых будут организовываться центры тестирования. Также данное решение не позволяет принимать участие в работе путём дистанционного метода и дает возможность для «подтасовки» результатов самого тестирования.

В европейских странах, в связи с европейским менталитетом, законодательством и т.п., вопросы аутентификации пользователей в системах тестирования специалистами предметной области подробно не рассматриваются по причине отсутствия понимания возможного сговора о подмене легитимного пользователя для сдачи экзаменов (зачетов).

1.2 Физиологическая биометрия.

Данное решение позволяет аутентифицировать пользователей на основе их физиологических данных (отпечатки пальцев, радужная оболочка, структура лица, и др.) с учетом развития систем искусственного интеллекта, нанотехнологий и т.п. Надежность такого решения заметна только на методах идентификации пользователей, которые берут за основу распознавание радужной оболочки глаз [5-8], иные способы по мнению авторов работ Е. Флиорома и К. Ковальского, а также Н. Д'Лима и Дж. Миталла не подтвердили своей надежности.

1.3 Поведенческая биометрия.

Приведенное решение дает возможность аутентифицировать пользователей на основе их уникальных поведенческих характеристик (клавиатурный почерк, голосовой ритм, походка, характер подписи). В работах К. Ковальского, Е. Флиорома, Шарипова Р.Р. и Катасёва А.С. [9] был предложен метод на основе коэффициента корреляции (1), для сравнения напечатанных данных.

$$r = \sum_i^n (k_i * t_i) / \sqrt{\sum_{i=1}^{n} k_i^2 * \sum_{i=1}^{n} t_i^2} \qquad (1)$$

k_i - вектор длины $i = \underline{1,n}$, отражает разницу между отпусканием предыдущей и последующим нажатием следующей клавиши в эталонной подписи; t_i - вектор длины $i = \underline{1,n}$, в нем сохраняются интервалы времени между нажатиями клавиш. Стоит отметить, что приведенное решение эффективно только при работе с небольшими объемами данных.

Авторами работ [4, 8, 10] была предложена модель, основывающаяся на нейронной сети, которая учитывает частоту нажатия клавиш, движение мыши, время задержки нажатия клавиш и скорость набора текста [11].

По результатам исследований было выявлено, что пользователи были успешно аутентифицированы в тех случаях, когда различие между текущими данными и сохраненным шаблоном было менее 10%. Данная модель содержит в себе модуль, обновляющий шаблон, каждый раз, в случае, если аутентификация была пройдена успешно.

Пользователь в момент прохождения аутентификации может находиться в разном физическом и психологическом состоянии, и это может серьезно повлиять на ее результаты. В рабо-

те предполагается, что клавиатурный почерк человека – фактор достаточно стабильный, ограничения не рассматривались.

Одной из будущих задач ставится разработка метода, который, для повышения точности, будет основываться на уровне логического сравнения. Его назначение заключается в создании более качественного эталона, в котором бы могли учитываться индивидуальные особенности пользователей и отклонения, возникающие в связи с эмоциональным фоном пользователей. Именно такой метод позволит в будущем разработать непрерывную систему аутентификации пользователей, отслеживающую в том числе, и эмоциональный фон сотрудников критически важных объектов.

В работе представлена трехступенчатая модель увеличения точности аутентификации, заключающаяся в трех последовательных этапах:

1) Аутентификация на базе эталонных и текущих параметров пользователя;
2) Аутентификация с помощью сопоставления параметров пользователя с соответствующими классами: легальные и нелегальные пользователи;
3) Постоянная автоматическая адаптация критериев класса легального пользователя на базе рекуррентных вычислений.

2. Трехступенчатая модель аутентификации пользователей по клавиатурному почерку.

В информационных системах, находящихся в режиме онлайн, предлагается следующая трехступенчатая модель аутентификации. На рис.1 представлена схема трехступенчатой модели системы аутентификации пользователей.

Рис. 1. Трехступенчатая модель аутентификации пользователей
Fig. 1. Three-step user authentication model

Перед тем, как начать пользоваться системой автоматического прокторинга, пользователь должен авторизоваться в системе (ввести логин, пароль и другие параметры). Далее, успешно пройдя авторизацию, пользователь должен пройти аутентификацию, для чего измеряются клавиатурные параметры пользователя, формируются эталоны по данным измерениям и выполняется процесс сравнения данных параметров пользователя по критерию сравнения центров распределения двух совокупностей при условии, что распределение параметров клавиатурного почерка будет подчиняться нормальному гауссовскому закону (стандартное отклонение) и проверке соответствия на критерий Хи-квадрат (χ^2). В случае если на первом этапе пользователю не удалось пройти аутентификацию, то на втором этапе происходит решение классовой задачи, чтобы сравнить текущие данные с данными классов пользователей.

На третьем этапе данные пользователя обновляются на основе рекуррентного процесса. На рис. 2 приведена структурная схема трехступенчатой модели аутентификации пользователей.

Рис. 2. Детализация трехступенчатой модели аутентификации пользователей
Fig.2. Detailing a three-step user authentication model

Обсуждение результатов. Рассмотрим каждый уровень разработанной модели подробнее. На статистическом этапе измеряются временные параметры клавиатурного почерка у пользователей, а также формируются эталоны для каждого пользователя. Они представляют из себя измерение среднеквадратических отклонений (СКО) и средних значений. После этого анализируются стандартные отклонения между эталонными значениями и входными данными. По формуле (2) вычисляется стандартное отклонение временных параметров работы пользователей на клавиатуре.

$$S = \sqrt{\frac{1}{N}\sum_{i=1}^{n}\left(x_i - \overline{x_j}\right)^2} \qquad (2)$$

N - размер выборки временных параметров, S - стандартное отклонение, x_i - текущее значение выборки, а $\overline{x_j}$ - среднее значение параметров.

Полученное значение S сравнивается с ранее сохраненным стандартным отклонением, рассчитанным на основе собранных данных каждого конкретного пользователя. В случае, когда разница между этими значениями незначительна, пользователь проходит проверку, иначе осуществляется проверка критерия χ^2.

Прохождение теста χ^2 используется для опровержения или подтверждения гипотезы. В качестве гипотезы для теста в предлагаемой системе принимается предположение о том, что «Пользователь легальный». В данном тесте предполагается одна степень свободы, так как возможны только два результата: пользователь либо легален, либо нелегален. Степень свободы используется при выборе критических значений в статистической таблице [12]. Значение выбирается исходя из желаемой точности. Для предложенной системы было выбрано значение, при котором уровень достоверности составлял 97,5%. Данный уровень показывает вероятность то-

го, что решение об отклонении или принятии гипотезы верно.

Для доказательства верности гипотезы необходимо сохраненное среднее значение атрибута передавать как ожидаемое значение, а среднее значение входного атрибута – как наблюдаемое. Целью теста будет определение того, является разница между входным и сохраненным средними значениями следствием случайности или же она получена в результате иных особенностей. Ниже приведена формула (3) [12], где χ^2 – критерий Хи-квадрат, $\overline{x_j}$ – наблюдаемое среднее значение времени, а L_i – ожидаемое значение (среднее эталонное значение):

$$\chi^2 = \sum \frac{(\overline{x}_j - L_i)^2}{L_i} \quad (3)$$

Для принятия гипотезы, значение χ^2 должно быть меньше или равно критического значения, выбранному из статистической таблицы [2]. Если значение χ^2 больше критического значения, то пользователь отклоняется. В ином случае, пользователь принимается с вероятностью 97,5%. Начинается следующая ступень модели аутентификации.

На этапе классификации, фиксируется последовательность классифицируемых признаков пользователей в процессе формирования априорного словаря классов. При этом самым основным в этом процессе остается выбор адекватного правила классификации характеристик. Эти правила должны соответствовать требованиям, предъявляемым к системе распознавания, зависящих от возможных решений, принимаемых системой управления при распознавании неизвестных ранее характеристик. После этого происходит определение параметров классов посредством разделения характеристик почерка на классы $L_1,...L_m$. В пространстве наборных необходимо определить характеристик области S_i, $i=1, ..., m$, эквивалентные классам. Рассмотренный выше пример представлен на рис. 3.

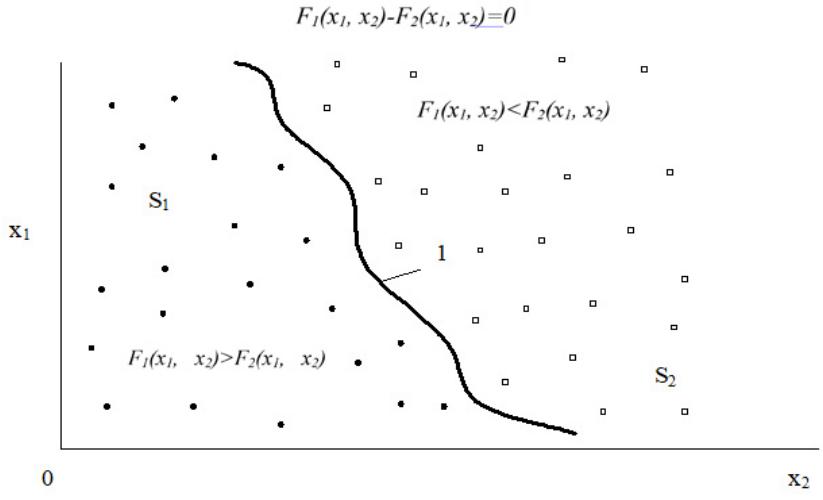

Рис. 3. Разбиение классов пользователей
Fig. 3. Classification of user classes

Таким образом, становится возможным определение границ областей S_i, соответствующих классам L_i, по которым принимается решение.

На рис. 3 представлено соответствующего разбиения. Легальные пользователи находятся в области, параметры незарегистрированных или случайных пользователей – в области S2. 1 – решающая граница. Задав разделяющие функции, можно проверить выполнения условий:

Если $F_1(x_1, x_2)>F2(x_1, x_2)$ – то пользователь идентифицируется, как легальный, и если $F_1(x_1, x_2)<F_2(x_1, x_2)$ - то это параметры пользователя, который распознается как «чужой» и будет игнорироваться системой. Иначе, если пользователь распознается, как «свой», параметры и S обновляются, в соответствии с рекуррентными отношениями (4) (5):

$$\bar{x}_j = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (4),$$

где N – количество наблюдений, $\overline{x_j}$ - среднее значение параметров конкретного пользователя, x_i - текущее значение параметров конкретного пользователя.

$$S = \frac{1}{N-1} \cdot \sum_{i=1}^{N} \left| x_i - \bar{x}_j \right| \quad (5),$$

где S – среднеквадратичное отклонение (новое).

Экспериментальная часть. В качестве проверки трехступенчатой модели, были проведены статистические расчеты и экспериментальное исследование. Была выбрана экспериментальная группа из 8 студентов ИКТЗИ (институт компьютерных технологий и защиты информации) КНИТУ-КАИ, все из них владеют десятипальцевым слепым набором на клавиатуре. Первым этапом испытуемым предлагалось авторизоваться на web-сайт, созданный под цели эксперимента. В результате чего были сформированы эталоны данных пользователей. При авторизации студенты вводили свои ФИО, специальность, год обучения, направление их подготовки, после чего перенаправлялись на другую страницу. Далее студентами осуществлялся ввод готовых текстов, которые представляли собой заранее подготовленные предложения, заранее не известные тестируемой группе.

После чего, введённые данные тестируемой группы были собраны на стороне клиента из web-формы: при печати символов на клавиатуре студентами, программа-обработчик обрабатывала любое нажатие и отпускание любой клавиш. Программа написана на языке JavaScript и для обработки применялись встроенные функции Keydown, т.е. событие «нажатие клавиши» и Keyup – событие «отпускание клавиши».

```
public static void KeyDUP(string[] args)
    {
        Form1.KeyDown += KeyDownOrUp;
        Form1.KeyUp += KeyDownOrUp;
        Form1.KeyPress += KeyDownOrUp;
        string text;
        protected void KeyDownOrUp(Object sender,KeyEventArgs e)
        {
            text = e.GetType() + " key=" + (e.GetType() == "KeyPress" ? e.KeyChar :
e.KeyCode) + DateTime.Now;
        }
    }
```

Алгоритм программы устанавливал первую временную метку при нажатии клавиши и вторую временную метку при ее отпускании. Далее вычисляется разница во времени между метками, и, соответственно, определяется время удержания клавиши. Также алгоритм с помощью встроенных функций фиксирует код нажатой клавиши в кодировке ASCII и её значение. В результате все полученные данные: код клавиши, ее имя, время задержки и время отпускания клавиши передается на сервер, где происходит дальнейшая обработка данных. Передача информации происходит с помощью JS-функции, использующей AJAX запросы.

Сбор информации на сервере является следующим этапом работы системы. Web сервер был организован на базе Apache HTTP Server 2.2, а также OS Linux Mint. При передаче данных, скрипт, на языке PHP, на стороне сервера запрашивал базу данных, которая была реализована на MySQL, для проверки, не были ли сохранены какие-либо предыдущие данные, такие как

нажатые клавиши, для текущего пользователя. В случае если такие данные уже были в базе данных, то обработчик выбирал из них последние три и использовал их временные метки, чтобы рассчитать временные интервалы диграфов, триграфов и квадграфов, путём разности значений временных меток.

Во время эксперимента статистические данные были поделены на две группы:

1. Эталонные данные;
2. Данные для обработки.

Был выбран такой параметр, как время удержания клавиш студентами, потому что этот параметр был наиболее информативен в нашем случае. Но данное утверждение при работе с большим объёмом данных может быть неверно.

По результатам тестов [19 – 21] для каждого из студентов были рассчитаны и построены стандартные девиации эталонных и текущих данных. В табл. 1 представлены результаты всех 8 тестируемых пользователей. Также был рассчитан критерий χ^2 для отдельно взятого тестируемого пользователя. По данным таблицы видно, что пользователь №6 был аутентифицирован при помощи сравнения стандартных девиаций его эталона и данных, потому что разница в этой девиации составила меньше 3-х, что и было в процессе аутентификации первым шагом.

Таблица 1. Значение девиации и критерий хи-квадрат
Table 1. The value of deviation and the chi-square criterion

Студент Student	Данные Facts		
	Значение девиации (эталонные данные) Deviation value (reference data)	Значение девиации (измеренные) Deviation value (measured)	Критерий Хи-квадра Criterion Chi-square
1	86	32	28.7
2	169	41	31.42
3	63	9	5.95
4	62	48	51.41
5	162	35	11.84
6	39	38	13.86
7	42	12	4.82
8	105	118	63.31

Пользователи под номерами № 3, 5 и 7 были аутентифицированы посредством критерия χ^2: значения критерия оказалось меньше критического значение 12,71. Исходя из результатов, можно сделать вывод, что с уверенностью в 97,5% пользователи аутентифицировались верно. Результаты расчётов показывают также, что на этапе сопоставления статистических значений параметров клавиатурного почерка проверку подлинности прошли 50% пользователей.

Первоначальной целью было убедиться в том, что предложенная модель аутентификации способна разграничить доступ легальных и нелегальных пользователей с учетом постоянных адаптаций к изменениям параметров клавиатурного почерка. Такие адаптации должны позволить повысить точность аутентификации.

В итоге сравнением методом девиаций был аутентифицирован один из пользователей, трое других - методом подсчета критерия χ^2. Все остальные тестируемые не были аутентифицированы ни на одном из этапов системы. Это может быть объяснено недостаточным количеством исходных данных для идентификации. Для доказательства принципиальной работоспособности модели представленной выборки достаточно, и есть все основания предполагать, что при увеличении объема выборки процент успешного распознавания будет увеличиваться.

Вывод. В результате проделанного исследования была получена информация о том, что решение в половине случаев было принято уже на статистическом этапе трехступенчатой модели аутентификации, вероятность точности которой выше, по сравнению с некоторыми известными решениями.

При создании больших информационных систем проблемы с эффективностью достаточно быстро оптимизируются путем увеличения количества исходных данных, при этот простота алгоритмов легко может позволить снизить нагрузки на вычислительные мощности крупномасштабных систем. Помимо прочего, важным дополнением к сравнению наборных характеристик оказалось применение критерия χ^2, ввиду возможности анализировать статистические вариации. Это, в том числе отражается и в результате эксперимента, в котором трое из восьми пользователей были аутентифицированы уже на первом этапе, с использованием оценки критерия χ^2.

Библиографический список:

1. Глова В.И., Катасев А.С., Абзалов А.Р. Модель локализации искажений и подтверждения авторства исходных текстов программ // Вестник Казанского государственного технического университета им. А.Н. Туполева. 2008. № 3. С. 84-87.
2. Добровинский Д.С., Ловецкий И.В., Попов М.А. Прокторинг как инструмент развития дистанционного образования // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. 2018. С. 27-32.
3. Тумбинская М.В. Поддержка принятия решений и моделирование обеспечения защиты информации в информационных системах интернет-банкинга // Вестник компьютерных и информационных технологий. 2015. №7 (133). С. 33-39.
4. Тумбинская М.В., Баянов Б.И., Рахимов Р.Ж., Кормильцев Н.В., Уваров А.Д. Анализ и прогнозирование вредоносного сетевого трафика в облачных сервисах // Бизнес-информатика. 2019. № 1. С. 71-81.
5. R.R. Sharipov, M.V. Tumbinskaya, A.R. Abzalov Analysis of users keyboard handwriting based on Gaussian reference signals // International Russian Automation Conference. RusAutoCon. 2019.
6. Тумбинская М.В. Системный подход к обеспечению защиты от нежелательной информации в социальных сетях // Вопросы кибербезопасности. 2017. №2 (20). С. 30-44.
7. Тумбинская М.В. Модель защищенной информационной системы интернет-банкинга // Прикладная информатика. 2015. № 5 (59). С. 62-72.
8. Шарипов Р.Р., Сафиуллин Н.З. Аппаратурный анализ клавиатурного почерка с использование эталонных гауссовских сигналлов // Вестник Казанского государственного технического университета им. А.Н. Туполева, 2006. № 2. С. 21-23.
9. Шарипов Р.Р., Катасёв А.С. Система распознавания клавиатурного почерка пользователей на основе полигауссового алгоритма // Вестник Казанского государственного энергетического университета. 2016. № 4 (32). С. 45-59.
10. Тумбинская М.В. Обеспечение защиты от нежелательной информации в социальных сетях // Вестник Мордовского университета. 2017. Т. 27. № 2. С. 264-288.
11. Мухаматханов Р.М., Михайлов А.А., Баянов Б.И., Тумбинская М.В. Классификация DDos-атак на основе нейросетевой модели // Прикладная информатика. 2019. № 1 (79). С. 96-103.
12. Берман Г.Н. Сборник задач по курсу математического анализа. Москва: Наука, 1977 416 с.

References:

1. Glova V.I., Katasev A.S., Abzalov A.R. Model' lokalizatsii iskazheniy i podtverzhdeniya avtorstva iskhodnykh tekstov programm // Vestnik Kazanskogo gosudarstvennogo tekhnicheskogo universiteta im. A.N. Tupoleva. 2008. № 3. S. 84-87. [Glova V.I., Katasev A.S., Abzalov A.R. Model for localization of distortions and confirmation of authorship of source codes of programs // Bulletin of Kazan State Technical University. A.N. Tupolev. 2008. No. 3. S. 84-87.(In Russ)]
2. Dobrovinskiy D.S., Lovetskiy I.V., Popov M.A. Proktoring kak instrument razvitiya distantsionnogo obrazovaniya // Nauchno-tekhnicheskoye i ekonomicheskoye sotrudnichestvo stran ATR v XXI veke. 2018. S. 27-32. [Dobrovinsky D.S., Lovetsky I.V., Popov M.A. Proctoring as a tool for the development of distance education // Scientific, technical and economic cooperation of the Asia-Pacific countries in the XXI century. 2018.S. 27-32. .(In Russ)]
3. Tumbinskaya M.V. Podderzhka prinyatiya resheniy i modelirovaniye obespecheniya zashchity informatsii v informatsionnykh sistemakh internet-bankinga // Vestnik komp'yuternykh i informatsionnykh tekhnologiy. 2015. №7 (133). S. 33-39. [Tumbinskaya M.V. Decision support and modeling of information security in information systems of Internet banking // Bulletin of computer and information technologies. 2015. No. 7 (133). S. 33-39. .(In Russ)]
4. Tumbinskaya M.V., Bayanov B.I., Rakhimov R.ZH., Kormil'tsev N.V., Uvarov A.D. Analiz i prognozirovaniye vredonosnogo setevogo trafika v oblachnykh servisakh // Biznes-informatika. 2019. № 1. S. 71-81. [Tumbinskaya M.V., Bayanov B.I., Rakhimov R.Zh., Kormiltsev N.V., Uvarov A.D. Analysis and prediction of malicious network traffic in cloud services // Business Informatics. 2019.No. 1.P. 71-81. .(In Russ)]

5. R.R. Sharipov, M.V. Tumbinskaya, A.R. Abzalov Analysis of users keyboard handwriting based on Gaussian reference signals // International Russian Automation Conference. RusAutoCon. 2019.
6. Tumbinskaya M.V. Cistemnyy podkhod k obespecheniyu zashchity ot nezhelatel'noy informatsii v sotsial'nykh setyakh // Voprosy kiberbezopasnosti. 2017. №2 (20). S. 30-44. [Tumbinskaya M.V. A systematic approach to ensuring protection against unwanted information in social networks // Cybersecurity Issues. 2017. No. 2 (20). S. 30-44. (In Russ)]
7. Tumbinskaya M.V. Model' zashchishchennoy informatsionnoy sistemy internet-bankinga // Prikladnaya informatika. 2015. № 5 (59). S. 62-72. [Tumbinskaya M.V. Model of a secure information system for Internet banking // Applied Informatics. 2015. No. 5 (59). S. 62-72. (In Russ)]
8. Sharipov R.R., Safiullin N.Z. Apparaturnyy analiz klaviaturnogo pocherka s ispol'zovaniye etalonnykh gaussovskikh signallov // Vestnik Kazanskogo gosudarstvennogo tekhnicheskogo universiteta im. A.N. Tupoleva, 2006. № 2. S. 21-23. [Sharipov R.R., Safiullin N.Z. Instrumental analysis of keyboard handwriting using standard Gaussian signals. Bulletin of Kazan State Technical University. A.N. Tupolev, 2006. No. 2. S. 21-23. .(In Russ)]
9. Sharipov R.R., Katasov A.S. Sistema raspoznavaniya klaviaturnogo pocherka pol'zovateley na osnove poligaussovogo algoritma // Vestnik Kazanskogo gosudarstvennogo energeticheskogo universiteta. 2016. № 4 (32). S. 45-59. [Sharipov R.R., Katasev A.S. A system for recognizing the keyboard handwriting of users based on the poly-Gaussian algorithm // Bulletin of Kazan State Power Engineering University. 2016. No. 4 (32). S. 45-59. (In Russ)]
10. Tumbinskaya M.V. Obespecheniye zashchity ot nezhelatel'noy informatsii v sotsial'nykh setyakh // Vestnik Mordovskogo universiteta. 2017. T. 27. № 2. S. 264-288. [Tumbinskaya M.V. Providing protection against unwanted information in social networks // Bulletin of the Mordovian University. 2017.Vol. 27.No. 2.P. 264-288. (In Russ)]
11. Mukhamatkhanov R.M., Mikhaylov A.A., Bayanov B.I., Tumbinskaya M.V. Klassifikatsiya DDos-atak na osnove neyrosetevoy modeli // Prikladnaya informatika. 2019. № 1 (79). S. 96-103. [Mukhamatkhanov R.M., Mikhailov A.A., Bayanov B.I., Tumbinskaya M.V. Classification of DDos attacks based on a neural network model // Applied Informatics. 2019. No. 1 (79). S. 96-103.(In Russ)]
12. Berman G.N. Sbornik zadach po kursu matematicheskogo analiza. Moskva: Nauka, 1977 416c. [Berman G.N. Collection of problems for the course of mathematical analysis. Moscow: Nauka, 1977 416c. (In Russ)]

Сведения об авторах:

Абзалов Айрат Ринатович, старший преподаватель, кафедра систем информационной безопасности, e-mail:kai.abzalov@mail.ru, ORCID 0000-0002-2832-2840

Кашапов Ильназ Ильгизович, студент, e-mail: exkashapov@mail.ru, ORCID 0000-0002-2352-6545

Орлов Артемий Юрьевич, студент, e-mail: tyoomsday@gmail.com, ORCID 0000-0002-1041-4499

Мамлеев Искандер Раушанович, студент, e-mail: iskandr3567@mail.ru, ORCID 0000-0003-2364-8507

Information about the authors:

Airat R. Abzalov, Senior Lecturer, Department of Information Security Systems, e-mail: kai.abzalov@mail.ru, ORCID 0000-0002-2832-2840

Ilnaz I. Kashapov, student, e-mail: exkashapov@mail.ru, ORCID 0000-0002-2352-6545

Artemy Yu. Orlov, student, e-mail: tyoomsday@gmail.com, ORCID 0000-0002-1041-4499

Iskander R. Mamleev, student, e-mail: iskandr3567@mail.ru, ORCID 0000-0003-2364-8507

Конфликт интересов.
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 30.05.2020.
Принята в печать 18.07.2020.

Conflict of interest.
The authors declare no conflict of interest.
Received 30.05.2020.
Accepted for publication 18.07.2020.