ПРОЕКТИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Строкань О.В., Коротыш Д.В.

ФГБОУ ВО «Мелитопольский государственный университет имени А.С. Макаренко», Мелитополь, e-mail: korotish13zzz@gmail.com

Со стремительными темпами развития информационных технологий, растет и количество информационных угроз. В современном мире одной из наиболее распространенных и актуальных угроз безопасности информационных систем общего и специального назначения является угроза утечки данных, которая постоянно растет пропорционально интенсивности использования информационных технологий. Большинство данных покидает сети компаний из рук сотрудников организаций, где используются цифровые технологии хранения и обработки данных. Поэтому обеспечение контроля доступа сотрудника компании к ресурсам информационной системы организации позволит значительно повысить уровень безопасности данных компании.

Одним из способов защиты информации является пользовательская аутентификация. Аутентификация пользователя – процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных. [1]. Стандартные средства аутентификации в виде логина и пароля не могут обеспечить необходимую степень защиты, поскольку всегда существует вероятность кражи или взлома пароля. Поэтому все более популярными становятся биометрические методы аутентификации: распознавание голоса; распознавание радужки глаза; распознавание личности; сканирование отпечатков пальцев; распознавание клавиатурного почерка. Одним из самых эффективных является метод распознавания клавиатурного почерка [2].

Под понятием «клавиатурный почерк» понимается поведенческая биометрическая характеристика, состоящая из паттернов ритма и динамики, характерных для этого оператора при наборе текста [2, 3]. Клавиатурный почерк является уникальным для каждого человека стилем ввода символов, которые описываются динамикой ввода символов из клавиатуры и наличием ошибок, характерных для каждого человека. Динамика нажатия клавиш, которая представляет ритмы набора текста, которые пользователь выполняет, печатая на клавиатуры, обеспечивают высокий уровень безопасности, а также имеют преимущества в практическом применении, т.к. недорогая реализация этого метода – важный показатель по сравнению со сканированием отпечатков пальцев, которые требуют дополнительного оборудования для аутентификации [3]. Для усовершенствования средств анализа параметров клавиатурного почерка, предназначенных для распознавания личности пользователя, применяется современная технология нейросети.

Повысить эффективность данного метода можно за счет разработки соответствующего программного обеспечения.

Для создания системы аутентификации по клавиатурному почерку необходимо собрать достаточное количество данных о пользовательских наборах текста. Источниками данных могут быть:

- специализированные базы данных: в научных работах и открытых источниках существуют базы данных, содержащие информацию о клавиатурном почерке разных пользователей. Такие базы могут быть использованы для обучения модели, однако их актуальность и полнота могут быть ограничены;

- сбор данных в реальном времени: для обеспечения актуальности данных можно использовать методы сбора информации о клавиатурном почерке в реальном времени, например, через специализированные приложения или веб-сервисы.

На рисунке 1 приведена последовательность функционирования системы аутентификации пользователей на основе клавиатурного почерка.

Для систем биометрической аутентификации, которые базируются на динамических характеристиках людей, характерны режимы функционирования идентификации и обучения, которые предназначены для формирования биометрического профиля пользователя на основе параметров клавиатурного почерка. В режиме идентификации система проводит анализ параметров клавиатурного почерка на предмет соответствия зарегистрированного профиля оператора с известными профилями.

В наше время на рынке существует множество систем аутентификации по клавиатурному почерку. В таблице 1 представлена сравнительная характеристика наиболее распространенных из них.

Главным недостатком рассмотренных готовых решений по распознаванию клавиатурного почерка является точности аутентификации от объема и качества данных, сложность внедрения и использования. Для устранения указанных недостатков предлагается спроектировать интеллектуальную систему аутентификации пользователей по индивидуальному электронному почерку, направленное на защиту информации от несанкционированного доступа.

На начальном этапе проектирования разработана диаграмма вариантов использования интеллектуальной системы (рис. 2) [8].

Рис. 1. Последовательность функционирования системы аутентификации пользователей на основе клавиатурного почерка

Таблица 1

Сравнительная характеристика аутентификации по клавиатурному почерку

Название	Характеристика	Достоинства	Недостатки
BioHashing [4]	Использует комбинацию из биометрических данных пользователя и криптографического хеширования для создания уникального идентификатора	- высокая степень защиты данных; - устойчивость к подделке.	- возможность атак по стороннему каналу; - сложность внедрения и использования.
TypingDNA [5]	Использует алгоритмы машинного обучения для определения уникальных особенностей набора текста пользователя	- простота интеграции с веб-сервисами и приложениями; - поддержка множества языков и платформ.	- точность и скорость аутентификации могут зависеть от качества и объема доступных данных; - возможность подделки в случае недостаточно уникальных текстов.
KeyTrac [6]	Основана на анализе клавиатурного почерка	- легкость интеграции с различными платформами; - поддержка множества языков.	- точность аутентификации также зависит от объема и качества данных; - возможность подделки при недостаточно уникальных текстов.

Главными пользователями системы распознавания личности пользователей по клавиатурному почерку являются: administrator (Администратор); monitor (Монитор); user (Пользователь). В функции Administrator входит управление программной частью системы – настройка на работу, проверка работоспособности, управление базами данных системы, а именно формирование значений входных и нормативных величин. User сотрудник является основным пользователем системы. В его функции входит только работа по ПК, система сама распознает имеет ли он право. Monitor создает диалоговое окно системы и пользователя.

Основными элементами интеллектуальной системы распознавания клавиатурного почерка являются: устройство считывания биометрической характеристики; образец, который только считали; блок по обработке считанных биометрических данных; контрольный шаблон биометрической характеристики; база данных, хранящая эталонные шаблоны пользователей; сам эталонный шаблон; блок для сравнения контрольного и эталонного образцов.

Устройство считывания характеристик представляет собой клавиатуру персонального компьютера. Процесс представления свойства сводится к вводу текста. Образец представляет собой два набора временных интервалов: время удержания клавиши, интервал между нажатием клавиши, измеренные при вводе текста.

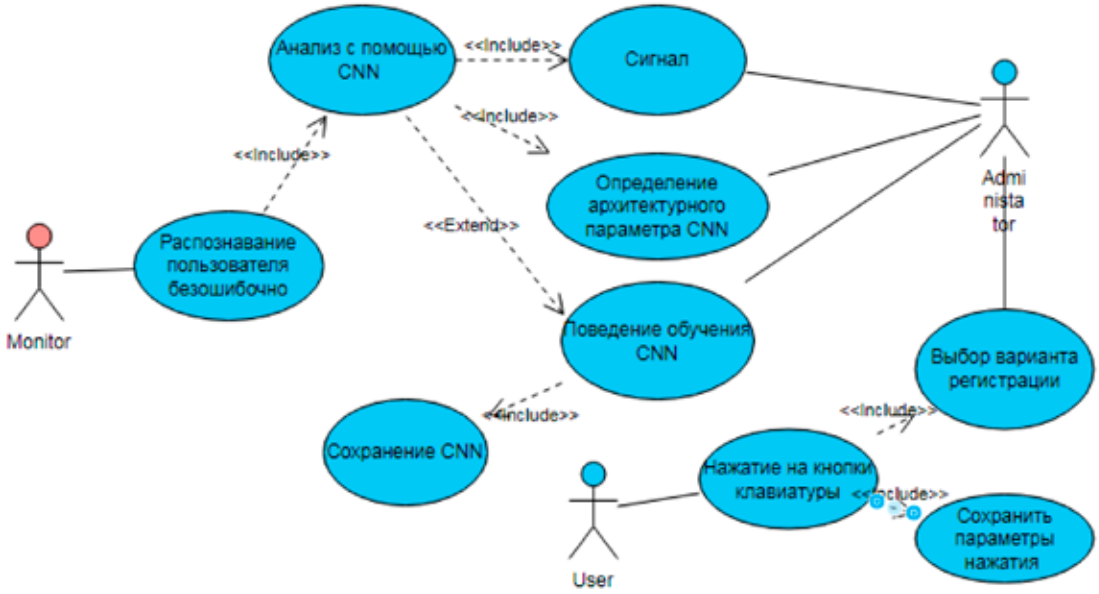

Рис. 2. Диаграмма вариантов использования системы распознавания личности пользователей с клавиатурным почерком

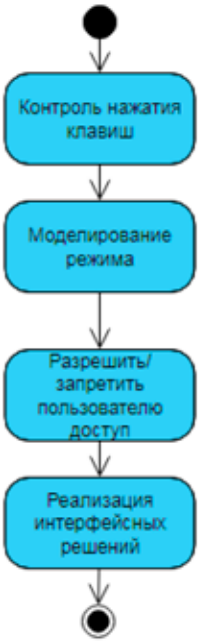

Рис. 3. Диаграмма состояний интеллектуальной системы

Блок по обработке считанных биометрических данных выполняет формирование контрольного шаблона из полученного образца. Контрольный шаблон – представляется для сравнения с эталонным шаблоном при прохождении аутентификации. База данных – набор текстовых файлов, содержащих эталонные шаблоны пользователей. База формируется в обучающем режиме. Эталонный шаблон – набор массивов характеристик временных зарубок. Формируется при работе пользователя в режиме обучения. Сохраняется в базе данных системы. Блок сравнения реализует методики анализа клавиатурного почерка.

На рисунке 3 приведена диаграмма состояний разрабатываемой системы распознавания пользователя. Системы распознавания пользователя по клавиатурному почерку имеет целью обеспечение обеспечения высокого уровня защиты информации и данных. При разработке программного обеспечения системы в первую очередь необходимо разработать последовательность действий его выполнения – алгоритм. Для этого определяется исходное состояние системы, входные данные, а также определяются выходные управляющие сигналы и управляющие воздействия.

Разработаный способ проектирования системы распознавания личности пользователя по клавиатурному почерку основан на процедуре представления параметров клавиатурного почерка в виде подходящей для анализа сверточной нейронной сети и нейросетевой модели типа SqueezeNet, приспособленной к анализу параметров клавиатурного почерка.

Список литературы

1. Дорожнин А. Идентификация, аутентификация и авторизация – в чем разница? [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/identification-authentication-authorization-difference/29123/ (дата обращения: 10.05.2023).

2. Alghamdi S., Elrefaei L. Dynamic user verification using touch keystroke based on medians vector proximity. In Computational Intelligence, Com-munication Systems and Networks (CICSyN). IEEE. 2015. P. 121-126.

3. Hayreddin Ç., Shambhu U. Sensitivity analysis in keystroke dynam-ics using convolutional neural networks 2017 IEEE Workshop on Information Forensics and Security (WIFS) 4-7 Dec. 2017. P. 1-6.

4. Teixeria T., Fairhurst M., Santos R. Investigating keystroke dynamics in the password domain for user authentication: Benchmarking available datasets and algorithms // Computers & Security. 2020. Vol. 92. P. 101760.

5. Typing D.N.A. Typing biometrics authentication API. [Электронный ресурс]. URL: https://www.typingdna.com/ (дата обращения: 10.05.2023).

6. Key Trac. Keystroke Biometrics for User Identification and Authentication. [Электронный ресурс]. URL: https://www.keytrac.net/ (дата обращения: 10.05.2023).

7. Соколов Д.А. Использование клавиатурного почерка для проверки подлинности в распределенных системах с мобильными клиентами // Безопасность информационных технологий. 2010. № 2. С. 50-53.

8. А.с. 105640. Навчальне видання «Управління ІТ-проєктами: лабораторний практикум» / Строкань О.В., Мірошниченко М.Ю. Украина; дата регистрации 18.06.2021.

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ УПРАВЛЕНИЯ ЗАПАСАМИ

Чепурной М.П., Барышевский С.О.

ФГБОУ ВО «Мелитопольский государственный университет имени А.С. Макаренко», Мелитополь, e-mail: maxchepurnoi@yandex.ru, solbar16@gmail.com

В условиях рыночной экономики все более актуальным становится вопрос о поиске инструментов анализа и прогнозирования экономических процессов. Одним из способов принятия управленческих решений является использование методов имитационного моделирования.

Моделирование систем управления запасами, наряду с моделированием систем массового обслуживания, можно назвать «классическими задачами имитационного моделирования» [1].

Имитационное моделирование проводится в тех случаях, когда исследователь имеет дело с такими математическими моделями, которые не позволяют заранее вычислить или предсказать результат. В этом случае для предсказания поведения реальной сложной системы необходимо провести эксперимент, имитация на модели при заданных исходных параметрах [2, с.125].

Имитационное моделирование можно представить, как обычные итерационные вычисления, выполняемые с помощью расчетных программ или табличного процессора; такие вычисления можно выполнить и без компьютера, с привлечением арифметических действий, вспомогательных таблиц [3].

Одним из направлений имитационного моделирования является моделирование случайной величины [4].

В данной работе мы предлагаем рассмотрение примера имитационного моделирования управления запасами с помощью моделирования случайной величины.

Моделируется некоторая случайная величина. Сначала из опытных данных определяется количество появлений возможных значений этой величины в единицу времени. По частотам вычисляются вероятности, по значениям этих вероятностей – кумулятивные вероятности. Зная кумулятивные вероятности, устанавливаем соответствие между случайными числами и значениями случайной величины. Берем несколько случайных чисел из специальной таблицы, восстанавливаем по ним значения случайной величины и определяем нужные нам характеристики [4, с. 88].

Пример. Начальный запас 11 единиц, стоимость подачи заказов C_0 = 25 рублей/заказ, стоимость хранения C_h = 12 рублей/единицу в день, одна упущенная продажа C_b = 120 рублей. При наличии на складе не более 5 единиц подается заказ на 11 единиц. Считаем, что все заказы подаются и выполняются в начале рабочего дня.

Из предыдущего опыта известно (наблюдение велось в течение 100 рабочих дней).

Спрос в день	0	1	2	3	4	5
Частота	10	15	25	20	20	10

Время выполнения заказа, дни	1	2	3
Частота	3	30	15

Покажем, как заполняются Таблица 1 и Таблица 2.

Как заполнять 3-й и 4-й столбцы вполне понятно. Так как у чисел в столбце «Кумулятивная вероятность» после запятой меняются два знака, то случайные числа группируем по два. Заполняется последний столбец сверху вниз.

Таблица 1

Спрос в день

Спрос в день	Частота	Вероятность	Кумулятивная вероятность	Случайные числа
0	10	0,1	0,10	00 – 09
1	15	0,15	0,25	10 – 24
2	25	0,25	0,50	25 – 49
3	20	0,2	0,7 0	50 – 69
4	20	0,2	0,90	70 – 89
5	10	0,1	1,00	90 – 99
Сумма	100			