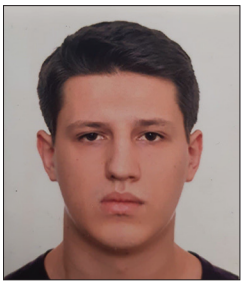
активно опиралось на корейские промышленные конгломераты — чеболей. Каждый из чеболей выбирает определенные отрасли промышленности и отвечает за развитие технопарков, региональных инновационных кластеров в выбранных отраслях. Такие меры были основаны на разнообразном и главное успешном опыте по запуску инновационных технологий не только на отечественных рынок, но и на глобальные мировые рынки, а также опыте управление инновационными центрами. Это дало возможность создания новых рабочих мест и использовать разработки для модернизации традиционных промышленных отраслей.

Опыт Республики Корея в сфере развития инноваций и становления креативных индустрий очень ценен. Он четко показывает, насколько важна роль структурированного продуманного плана и правильно поставленной государственной экономической политики. Но также важно отметить глубоки смысл проведенных реформ и цели осуществляемой работы на сегодняшний день. План реализации креативной экономики несет в себе глобальные цели, а именно изменение менталитета целой нации, отношение к инновациям, нововведениям, творчеству, открытой позиции к выражению идей и взращиванию качества, которое является необходимым в современном стремительно развивающимся мире — умение поиска креативных решений насущих проблем.

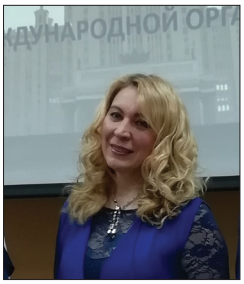
Список литературы:

1. Официальный сайт ООН [Электрон. ресурс]. — Режим доступа: https://www.un.org/ru/sections/observances/international-years/index.html.
2. World economic forum: "The skills are needed to thrive in the Fourth Industrial Revolution" [Электрон. ресурс]. — Режим доступа: https://www.weforum.org/agenda/2016/01/the-10-skills-you-need-to-thrive-in-the-fourth-industrial-revolution/.
3. **Financial Times** "South Korea set to transform telecoms with nationwide 5G launch" [Электрон. ресурс]. — Режим доступа: https://www.ft.com/content/948df1de-56a3-11e9-91f9-b6515a54c5b1.
4. Официальный сайт MSIP [Электрон. ресурс]. — Режим доступа: http://english.msip.go.kr/web/main/main.do.
5. Business Korea Magazine [Электрон. ресурс]. — Режим доступа: www.Businesskorea.co.kr.
6. Introduction to Creative Economy & The 3rd Science and Technology Basic Plan in Korea. Korea Institute of S&T Evaluation and Planning (KISTEP) [Электрон. ресурс]. — Режим доступа: http://www.nif. kz/pdf/park_eng.pdf.

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ



Павленко Александр Александрович
Студент кафедры «Информационная безопасность» Московского политехнического университета



Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Аннотация. В данной статье рассматриваются вопросы обеспечения безопасности с помощью программных решений, основанных на алгоритмах машинного обучения для определения манеры ввода текста с клавиатуры, обзор положительных и отрицательных сторон технологии.

Ключевые слова: машинное обучение, нейронные сети, информационная безопасность, системы защиты, биометрическая аутентификация.

Absract. This article discusses security issues using software solutions based on machine learning algorithms for determining the manner of entering text from the keyboard, an overview of the positive and negative aspects of the technology.

Keywords: machine learning, neural networks, information security, security systems, biometric authentication.

Введение

Биометрия в современных системах обеспечения безопасности определяется как автоматизированное использование биологических свойств для идентификации личности. Эти свойства позволяют людям идентифицировать нескольких людей в зависимости от их физических и поведенческих характеристик, а их правильное использование позволяет автоматизированным системам распознавать патерны поведения для обеспечения безопасности. В последствии возникновения таких потребностей была основана новая область исследований, и, как следствие, результаты этих исследований были интегрированы во многие новые области. Этого следовало ожидать из-за растущего спроса на безопасность и преимуществ биометрических систем; биометрические характеристики нельзя украсть, потерять или забыть. В этом смысле любые уникальные детали человеческого тела будут использоваться в качестве биометрических данных для создания неповторимых идентификационных ключей. Можно утверждать, что данные методы обеспечивают безопасность на основе того, чем Вы владеете, а не тем, что знаете (пароль, ПИН-код) или тем, что имеете (смарт-карта, токен). В этом направлении было разработано несколько систем на основе различных физиологических и поведенческих особенностей, которые включают отпечаток пальца, лицо, радужную оболочку, сетчатку, голос, нажатие клавиш, ухо, геометрия руки, подпись и походка[2]. Биометрические системы основаны на вводе данных из нескольких источников, начиная с датчиков различного типа, которые используются для сбора биометрических данных. На заключительном этапе система принимает решение, которое связывает полученные и уже имеющиеся биометрические характеристики о личности.

Цели и задачи исследования

Целью данной работы является изучение и анализ биометрического метода аутентификации на основе машинного обучения для определения уникального поведения пользователя при наборе текста на клавиатуре, оценка актуальности данного метода в информационной безопасности.

Результаты

Идея аутентификации пользователей по манере набора текста не нова, однако успехов в этой области удалось достичь лишь в последние несколько лет с развитием алгоритмов машинного обучения. «Считывание» динамики нажатия клавиш основывается на поиске закономерностей при нажатии на клавиши во время обычного клавиатурного ввода. Компания TypingDNA использовала эти достижения для разработки технологии распознавания шаблонов набора на основе искусственного интеллекта. Утверждается, что ее точность превышает 99% и может достигать даже 99,9% при наличии достаточно большого объема данных о характере набора текста конкретным пользователем [1]. Технология предусматривает запись небольших блоков информации, характеризующих процесс набора текста пользователем с учетом времени его перемещения с одной клавиши на другую и продолжительности удержания клавиш при нажатии. Таким образом создаются уникальные шаблоны набора, содержащие до 320 различных признаков. Для работы данного алгоритма необходимо применение вероятностно-статистического метода, то есть сбор статистики из выборки временных значений. Непосредственно элементом выборки является время удержания клавиши. Эталонное представления пользователя создается в режиме обучения.

Такой вид аутентификации относится к биометрическим методам, а значит, к самым удобным, ведь для подтверждения личности не требуется запоминать никакой информации и носить с собой специализированные устройства многофакторной аутентификации, достаточно набрать на клавиатуре фразу, система определяет манеру печати пользователя и сравнивает её с имеющимися в базе.

К сожалению, такой метод не лишен недостатков. Существует множество факторов, способных привести к изменению характеристик поведения при вводе текста с клавиатуры. К примеру, поведение может зависеть от времени суток, настроения и самочувствия пользователя. Так же нельзя исключать возможные травмы кистей рук, способные влиять на нормальную манеру печати. Именно поэтому для нормального функционирования системы необходима как можно более подробная биометрическая модель и периодические корректировки эталонных моделей поведения. Тем не менее, с учетом всего этого уже существуют программные решения, учитывающие огромное количество факторов и возможных проблем. В таких сложных системах используются параллельно несколько алгоритмов определения, основанных на нейронных сетях для максимизации точности работы системы защиты. Однако, данный метод аутентификации достаточно прост в реализации и внедрении. К тому же, такая система обойдется дешевле, чем аналоги. Так же она удобна для пользователя, которому просто необходимо ввести контрольную фразу, либо пароль.

На сегодняшний день существует три алгоритма биометрической аутентификации по клавиатурному почерку [2]:

1) алгоритм, анализирующий клавиатурный почерк во время ввода пароля;

2) алгоритм, анализирующий клавиатурный почерк после ввода дополнительного текстового фрагмента или фразы;

3) алгоритм, который постоянно производит скрытый мониторинг клавиатурного почерка пользователя;

Первый алгоритм не самый надежный, так как вследствие относительно маленькой длины пароля, системе может не хватить собранных данных для принятия решения о личности пользователя. Второй алгоритм выглядит более надежно, но даже он проверяет клавиатурный почерк лишь на начальной стадии авторизации. Третий способ отлично подходит для предотвращения несанкционированного доступа к информации, если сотрудник отошел от рабочего места и не заблокировал устройство или не вышел из системы. В комплексной системе проверки аутентификации имеет место использование сразу нескольких алгоритмов проверки пользователя.

Заключение

Данная технология уже смогла добиться большой точности, тем не менее мало кто сталкивался с данным методом аутентификации пользователей в связи со сравнительно небольшой распространенностью. Так же технология, в отличии от привычных сенсоров для считывания отпечатков пальцев и камер для сканирования лица не требует аппаратных средств, кроме клавиатуры, что является большим плюсом. Этот метод может быть эффективно использован в бюджетных системах и в веб решениях в качестве элемента многофакторной аутентификации из-за того, что не требует специальных аппаратных приспособлений для функционирования.

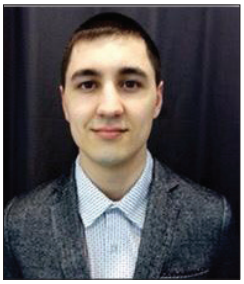
Список литературы

1. **Лучан К.** Биометрия текстового ввода.
2. **Yunbin Deng**, **Yu Zhong**. Keystroke Dynamics User Authentication Using Advanced Machine Learning Methods.
3. **Сухаревская Е.В.** Аутентификация пользователя по клавиатурному почерку.
4. https://www.osp.ru/cw/2017/3/13051677.
5. https://www.bigdataschool.ru/bigdata/biometrics-methods.html.
6. https://www.eduherald.ru/ru/article/view?id=18132.
7. https://www.osp.ru/lan/2012/02/13012841.
8. http://sciencegatepub.com/books/gcsr/gcsr_vol2/GCSR_Vol2_Ch2.pdf.
9. http://www.m-hikari.com/ces/ces2018/ces33-36-2018/p/hernandezCES33-36-2018-2.pdf.

ГИДРОДИНАМИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДЕТОНАЦИИ ВНУТРИ ОБОЛОЧНОГО УСТРОЙСТВА СЛОЖНОЙ ФОРМЫ[1]

Рыбакин Борис Петрович
Доктор физико-математических наук, профессор кафедры газовой и волновой динамики МГУ имени И.М. Ломоносова

Кравченко Марина Николаевна
Кандидат физико-математических наук, доцент кафедры нефтегазовой и подземной гидромеханики РГУ нефти и газа (НИУ) имени И.М. Губкина



Садринов Дмитрий Рафаэльевич
Студент РГУ нефти и газа (НИУ) имени И.М. Губкина

[1] Работа выполнена при поддержке гранта Российского Фонда Фундаментальных Исследований №18-07-01303А.