УДК 681.3:004.056.5

Мазниченко Наталья Ивановна
Национальный юридический университет имени Ярослава Мудрого
(Харьков, Украина)

ИСПОЛЬЗОВАНИЕ ДИНАМИЧЕСКИХ БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В СЕТИ

Аннотация. *Проанализированы возможности идентификации пользователя по особенностям клавиатурного почерка и динамике работы с мышью во время ввода пароля при работе в сетевых приложениях и сервисах. Представлены сценарии клиент-серверной реализации систем биометрической идентификации по динамическим биометрическим признакам. Рассмотрены особенности каждого сценария для обоснованного выбора в конкретных ситуациях.*

Ключевые слова: *биометрические технологии, информационная безопасность, идентификация пользователей компьютерных систем*

Maznichenko Natalia
Yaroslav Mudryi National Law University
(Kharkov, Ukraine)

USE OF DYNAMIC BIOMETRICS FOR USER IDENTIFICATION IN NETWORK

Abstract. *Possibilities of user identification are analyses on the features of the keystroke dynamics and dynamics of work with a mouse during the input of password during work in network applications and services. The scenarios of client-server realization of the systems of biometric authentication are presented on dynamic biometric signs. The features of every scenario are considered for a reasonable choice in certain situations.*

Keywords: *biometric technologies, informative safety, authentication of users of the computer systems*

Постановка проблемы. Биометрические системы идентификации личности на сегодняшний день активно используются во многих областях [1, с. 128]: компьютерная безопасность, электронная коммерция, системы управления и контроля доступом в помещения, системы гражданской идентификации и автоматизированные дактилоскопические системы (АДИС) и т.д. В последнее время в связи с актуальностью проблемы безопасности информации, хранящейся, обрабатываемой и передаваемой в компьютерных система и сетях, все больше внимания уделяется совершенствованию существующих систем безопасности и поиску новых решений в этой области. Начиная с 2001 года значительно вырос интерес к биометрическим технологиям для проверки идентичности пользователей компьютерных систем. Однако возможности использования данных технологий в сети Интернет значительно ограничивается в связи с необходимостью в использовании дорогостоящих дополнительных устройств. Следует отметить, что с недавнего времени некоторые мобильные устройства оснащаются

возможностью проверки отпечатка пальца, однако, данные устройства все еще недостаточно популярны и не могут быть использованы для проверки пользователей в сетевых приложениях. Поэтому удачным решением представляется возможность проверки пользователей посредством использования таких устройств, как клавиатура и манипулятор «мышь». Основное преимущество этого подхода – то, что он не требует дополнительных устройств, которые в большинстве своем достаточно дорогостоящие и не приспособлены для использования в мобильных устройствах. Еще одно преимущество состоит в том, что пользователь может проверяться не только во время ввода логина и пароля, а и непрерывно на протяжении всего сеанса роботы с определенным приложением или сервисом.

Анализ литературы. В течение трех последних десятилетий достаточно большое количество исследований было проведено для анализа возможности использования динамики нажатия клавиш (клавиатурного почерка) для проверки пользователей во время ввода логина и пароля и при наборе свободных текстов [2, 3, 4, 5, 6, 7, 8].

Современные системы идентификации по клавиатурному почерку распознают пользователя с достаточно высокой надежностью (около 0,9-0,95).

Некоторые исследователи клавиатурного почерка предлагают использовать образцы клавиатурного почерка злоумышленника (незарегистрированного пользователя) для повторного переобучения классификатора, что позволило увеличить точность систем идентификации по клавиатурному почерку до 10% [9, 10, 11].

Также в последнее время в некоторых работах для проверки пользователей было предложено использовать такую биометрическую характеристику как особенность работы пользователей с манипулятором «мышь» [12, 13, 14].

Существующие исследования мониторинга манипулятора «мышь» при работе пользователя показывают надежность распознавания 0,8-0,9.

Некоторые ученые для идентификации пользователей предлагают использовать особенности работы пользователя с несколькими устройствами ввода (клавиатура, компьютерная мышь, графический планшет, джойстик и т. п.), для чего был введен термин «информационный почерк» [15, 16, 17].

Невзирая на возросший интерес и достижения в создании и использовании систем идентификации пользователя по динамическим биометрическим характеристикам все еще существуют некоторые проблемы, которые не позволяют сделать данную технологию распространенной, особенно при работе в сети.

Цель статьи. Проанализировать возможность использования динамических биометрических характеристик для обеспечения дополнительного уровня безопасности при работе пользователей в сети за счет увеличения точности идентификации.

Изложение основного материала. В настоящее время работа пользователей в большинстве сервисов, приложений, услуг в сети Интернет должна быть персонифицирована, т.е. пользователь должен сначала зарегистрироваться (приобрести идентификационные признаки), а при последующих попытках доступа должен указать эти признаки (авторизация).

На сегодняшний день в большинстве приложений и сервисов пользователь идентифицируется логином и паролем [18, с. 217]. Использование одного и того же пароля для нескольких сервисов (приложений) увеличивает уязвимость для идентификационных признаков. Постоянный рост оперативных услуг Интернет, в которых пользователи проверяются именем пользователя и паролем, все чаще приводит к опасности кражи идентификационных данных. Кража идентификационных признаков пользователей компьютерных систем может иметь несколько целей: использование их злоумышленником для осуществления банковских афер, для получения товаров и услуг (финансовая цель или составляющая); возможность выдать себя за другого с целью совершения преступления (криминальная составляющая); возможность присваивания возможностей другого пользователя в повседневной жизни (identity cloning); использование деловой (коммерческой) репутации другого пользователя для получения соответствующей выгоды и преимуществ (бизнес-составляющая).

В этой статье рассмотрим проблему кражи идентификационных признаков пользователя компьютерных систем (стационарных и мобильных) с целью доступа к локальным и сетевым ресурсам.

В данном случае кража идентификационных признаков может использоваться, во-первых, чтобы обратиться к ценной (важной, конфиденциальной) информации, хранящейся на персональных компьютерах или мобильных устройствах. Во-вторых, чтобы получить доступ к услугам, предоставляемым через глобальную сеть (например, Интернет) или локальную внутреннюю сеть организаций.

Поэтому, для подтверждения идентичности истинного пользователя целесообразно использовать дополнительные средства безопасности. Потенциально положительные решения в данном случае можно найти в использовании динамических биометрических технологий.

Динамические биометрические системы по проверке пользователей, основанные на их взаимодействии с компьютером посредством клавиатуры и мыши, могут использоваться в нескольких направлениях:

1) Проверка при регистрации входа. Каждый раз, когда пользователь регистрируется на собственном локальном компьютере или сервисе в локальной сети или Интернете с помощью набора логина пользователя и пароля − эти действия дополнительно контролируются и проверяются за счет динамической биометрической характеристики данного пользователя.

2) Непрерывная проверка. После того, как пользователь получает доступ к компьютеру или сетевому сервису, его взаимодействие с клавиатурой и действия с манипулятором «мышь» непрерывно контролируются с целью постоянной проверки на идентичность во время всего сеанса работы.

3) Сброс пароля. Когда пользователь забыл пароль для логина, он может попросить выполнить проверку по динамической биометрической характеристике вместо непосредственного обращения к администратору.

Процесс идентификации пользователей по биометрическим признакам предполагает два этапа:

– режим обучения, в котором формируется база данных биометрических шаблонов зарегистрированных пользователей;

– режим идентификации пользователя при попытке доступа, т.е. сравнение его образца биометрической характеристики с имеющимся шаблоном в базе данных зарегистрированных пользователей, на основе которого пользователю либо предоставляется доступ, либо отказывается в доступе.

Все биометрические системы, использующие динамические биометрические характеристики, работают практически по одинаковой схеме, что проиллюстрировано на рисунке 1 [19, с. 34]:

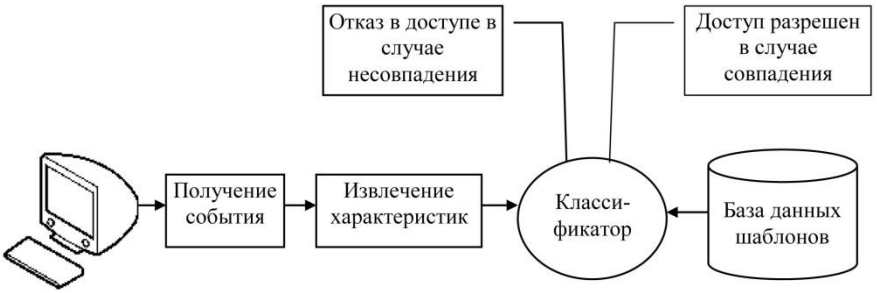


Рис. 1. Типичная структура динамической биометрической идентификации пользователя.

Данная структура включает несколько компонентов:

1) получение события – обрабатывается действие пользователя с устройством ввода (клавиатура, мышь);

2) извлечение характеристик − уникальная информация извлекается из полученного действия и составляется биометрический образец;

3) классификатор − сравнение сохраненного ранее в базе данных шаблона с представленным образцом (на основе определенного математического метода), в результате чего выносится решение о разрешении/запрете доступа;

4) база данных шаблонов (образцов) динамических характеристик зарегистрированных пользователей, которые были получены на этапе обучения биометрической системы идентификации.

Существуют четыре математических подхода к решению задачи распознавания [5, с. 123]:

– статистические алгоритмы;

– на основе нейросетевых алгоритмов.

– на базе теории распознавания образов и нечеткой логики;

– вероятностные и комбинированные алгоритмы;

Наиболее распространенными являются статистический метод и метод на основе нейросетевых алгоритмов.

Методы проверки основаны, обычно, на фиксированном или свободно-набираемом тексте. Последние могут использоваться для проверки пользователей в непрерывном режиме.

Динамические биометрические характеристики в системах

идентификации пользователей для обеспечения дополнительной защиты можно использовать в следующих вариантах:

1) Локальный компьютер (например, настольный компьютер, портативный компьютер, сервер), в котором все компоненты процесса проверки осуществляются на самом компьютере и никакая коммуникация с внешним миром не требуется.

2) Веб-обозреватель, в котором различные сетевые технологии используются для приобретения характеристик, а все остальные задачи выполняются на сервере. При этом используются только те действия с клавиатурой и мышью, которые связаны с веб-обозревателем.

3) Клиент-серверная реализация, в которой часть компонентов проверки находятся на клиентском компьютере, а часть − на сервере. Здесь некоторые действия реализуются на уровне клиентского компьютера, затем полученные данные отправляются на сервер.

Клиент-серверные системы идентификации пользователей по динамическим биометрическим характеристикам можно реализовать по нескольким сценариям. Рисунок 2 представляет три варианта реализации структуры динамической биометрической идентификации, которая была представлена на рисунке 1.

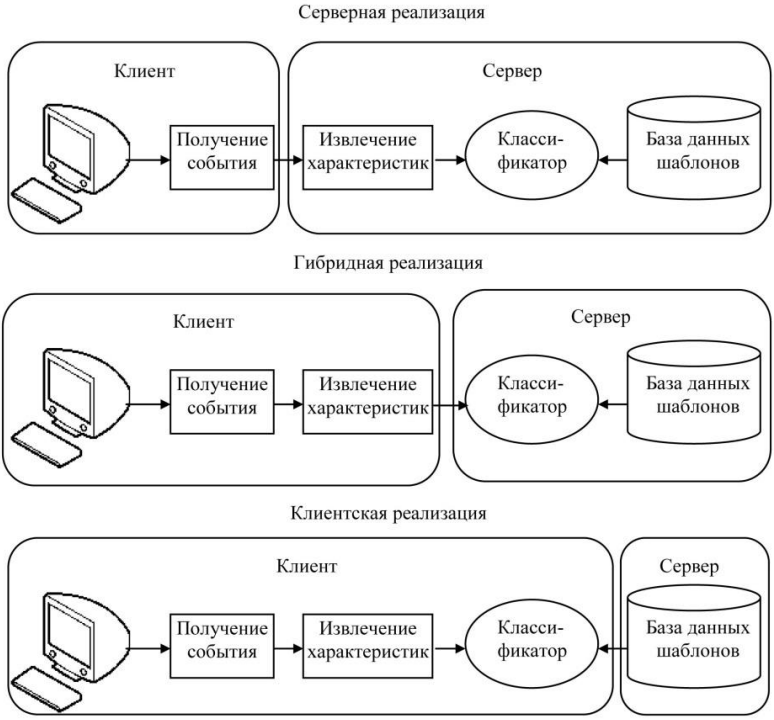


Рис. 2. Сценарии реализации клиент-серверных систем биометрической идентификации, основанные на динамических характеристиках.

Рассмотрим подробнее каждую из представленных реализаций.

1) Серверная реализация. В данном случае единственное действие, реализуемое на клиентском компьютере – получение событий от устройств ввода (клавиатура, мышь). Затем полученные данные передаются на сервер. Все остальные процессы (выделение признаков и непосредственно идентификация) выполняются на сервере.

К преимуществам данной реализации следует отнести легкость в обновлении системы, т.к. оно требуется чаще всего только на сервере. Но следует отметить и следующие особенности: такая реализация требует качественной и скоростной коммуникации между клиентским компьютером и сервером; биометрические данные пользователя, полученные на клиентском компьютере включают личную информацию, требующую защиты при передаче.

2) Гибридная реализация. В данной реализации на клиентском компьютере осуществляется извлечение биометрической характеристики от действий пользователя с клавиатурой или/и мышью. Затем полученные характеристики пересылаются на сервер, где и происходит процесс идентификации.

3) Клиентская реализация. В данном случае база данных биометрических признаков зарегистрированных пользователей загружается с сервера на клиентский компьютер, а затем все процессы проверки полностью выполняются на клиентском компьютере.

Как видим, разные сценарии реализации клиент-серверной системы динамической биометрической идентификации пользователей требуют разного объема вычислительных действий, выполняемых на клиентском компьютере.

Выводы.

Невзирая на большой потенциал данных технологий, хотелось бы остановиться на ряде проблем, которые требуют решения и которые препятствуют более широкому их распространению. Первой важной проблемой следует отметить разное аппаратное обеспечение компьютерных систем, на которых может работать пользователь (стационарный домашний компьютер, портативный компьютер, компьютер в интернет-кафе и так далее). Особенно это касается работы пользователя с сетевыми сервисами и приложениями. Разные компьютеры могут иметь разные устройства ввода (клавиатура, манипулятор «мышь»). Эта ситуация может значительно влиять на точность идентификации пользователя, потому эта проблема требует дальнейшего исследования. Другой важный аспект, который влияет на точность идентификации, может быть вызван разными состояниями пользователя на протяжении дня. Возможным решениям в данном случае представляется исследование динамических характеристик пользователя на протяжении длительного времени (например, на протяжении дня). Еще одной проблемой в применении представленной технологии является конфиденциальность и возможность ее нарушения. Дело в том, что некоторые пользователи не желают предоставлять свои динамические биометрические характеристики для сбора, побаиваясь их возможной кражи. В данном случае предлагается заранее информировать пользователей об использовании данных и получить предварительное согласие. Необходимо также отметить,

что большинство работ по исследованию динамических биометрических характеристик используют относительно небольшие наборы данных для оценки, которые не могут адекватно отображать требования, которые предъявляются к сетевым приложениям и сервисам, где может работать огромное количество пользователей. Анализ публикаций, посвященных идентификации пользователей на основе динамических характеристик, позволяет сделать вывод об использовании указанных характеристик для проверки пользователя, в основном, только во время введения парольной фразы при входе в систему или запуске приложений или сервисов. Однако работ, где бы рассматривался непрерывный мониторинг работы пользователя во время всего сеанса работы с компьютером, практически нет.

В заключении хотелось бы отметить, что решение указанных проблем позволит использовать динамические биометрические характеристики для повышения точности и надежности идентификации пользователей и повысить уровень безопасности при работе пользователей с сетевыми сервисами и приложениями и послужит дополнительным уровнем защити идентификационных данных пользователя от кражи их злоумышленником.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Н.И. Мазниченко. Области применения и принципы построения биометрических систем / Вестник Национального технического университета «Харьковский политехнический институт”: сб. науч. раб. – Тематический выпуск «Информатика и моделирование» – Х.: НТУ “ХПИ”. – 2007. – № 19. – 202 с. – С. 127-132.
2. Скубицкий А. В. Анализ применимости метода реконструкции динамических систем в системах биометрической идентификации по клавиатурному почерку // «Инфо-коммуникационные технологии». – 2008. – Т. 6, № 1. – С. 51-53.
3. Чалая Л.Э. Модель идентификации пользователей по клавиатурному почерку // «Искусственный интеллект». – 2004, № 4. – С. 811-817.
4. Брюхомицкий Ю.А., Казарин М.Н. Метод биометрической идентификации пользователя по клавиатурному почерку на основе разложения Хаара и меры близости Хэмминга // Известия ТРТУ. – Таганрог: Изд-во ТРТУ, 2003. – № 4(33). – С. 141-149.
5. Salil P. Banerjee, Damon L. Woodard. Biometric Authentication and Identification using Keystroke Dynamics: A Survey // Journal of Pattern Recognition Research 7 (2012), pp. 116-139.
6. Mrs. D. Shanmugapriya, Dr. G. Padmavathi. A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges // International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009, pp. 115-119.
7. Иванов В. Г. Сжатие изображений на основе компенсации контуров при вейвлет-преобразовании / В. Г. Иванов, М. Г. Любарский, Ю. В. Ломоносов // Проблемы управления и информатики. – 2006. – № 3. – С. 89 – 101.
8. Yu E., Cho S.: Keystroke Dynamics Identity Verification - Its Problems and Practical Solutions. Computer and Security 23(5) (2004), pp. 428-440.
9. Hyoun-joo Lee, Sungzoon Cho. Retraining a Novelty Detector with Impostor Patterns for Keystroke Dynamics-Based Authentication // ICB, volume 3832 of Lecture Notes in Computer Science, pp. 633-639, 2006.

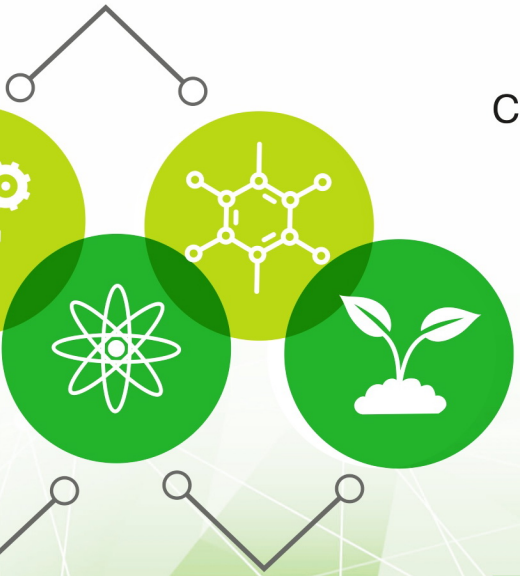
10. Hyoun-joo Lee, Sungzoon Cho. Retraining a keystroke dynamics based authenticator with impostor patterns // Computers & Security, vol. 26, no. 4, pp. 300-310, 2007.
11. Lee H., Cho S. SOM-based Novelty Detection Using Novel Data. // Proceedings of Sixth International Conference on Intelligent Data Engineering and Automated Learning, Lecture Notes in Computer Science 3578 (2005), pp. 359-366.
12. Диденко С.М. Шапцев В.А. Исследование динамики работы пользователя с манипулятором мышь // Математическое и информационное моделирование. – Тюмень: Изд-во ТюмГУ, 2004. – С.57-65.
13. Gorad B. J., Kodavade D. V. «User Identity Using Mouse Signature, IOSR Journal of Computer Engineering», Volume 12, Issue 4, Jul.–Aug. 2013, pp. 33-36.
14. Clint Feher, Yuval Elovici, Robert Moskovitch, Lior Rokach, Alon Schclar, «User identity verification via mouse dynamics», Information Sciences 201 (2012), pp. 19-36.
15. Бушуев С.И., Авраменко В.С. Аутентификация пользователей в автоматизированных системах на основе информационного почерка // Проблемы современной геополитики / Сборник трудов 1-й Международной науч.-практ. конф. «Проблемы современной геополитики. Продление НАТО на Восток — проблемы безопасности России и стран СНГ». – СПб.: Балтийский гос. техн. ун-т "ВОЕНМЕХ". – 1999 г. – С. 53-59.
16. Власов А.Н. Способ представления координатной составляющей информационного почерка пользователя // Материалы международной науч. конф. по мягким вычислениям. – СПб: Изд-во Политехнического университета, 2003. – Т. 1. – С. 116-119.
17. Диденко С.М., Шапцев В.А. Методика отображения информационного почерка пользователя // Вестник кибернетики. – Тюмень: Изд-во ИПОС СО РАН, 2005. – С.74-79.
18. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів // Системи обробки інформації. Випуск 6 (113). – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – 320 с. – С. 215-223.
19. Gorad B. J., Kodavade D. V. «User Identity Using Mouse Signature, IOSR Journal of Computer Engineering», Volume 12, Issue 4, Jul.–Aug. 2013, Pp. 33-36.

ISSN 2524-0986

iScience

АКТУАЛЬНЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ В СОВРЕМЕННОМ МИРЕ

СБОРНИК НАУЧНЫХ ТРУДОВ



Выпуск 2(34)
Часть 1

Переяслав-Хмельницкий
2018

АКТУАЛЬНЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ В СОВРЕМЕННОМ МИРЕ

ВЫПУСК 2(34)
Часть 1

Февраль 2018 г.

СБОРНИК НАУЧНЫХ ТРУДОВ

Выходит –12 раз в год (ежемесячно)
Издается с июня 2015 года

Включен в наукометрические базы:

РИНЦ http://elibrary.ru/title_about.asp?id=58411
Google Scholar
https://scholar.google.com.ua/citations?user=JP57y1kAAAAJ&hl=uk
Бібліометрика української науки
http://nbuviap.gov.ua/bpnu/index.php?page_sites=journals
Index Copernicus
http://journals.indexcopernicus.com/++++,p24785301,3.html

Переяслав-Хмельницкий

«Актуальные научные исследования в современном мире» ISCIENCE.IN.UA
Выпуск 2(34) ч. 1 ISSN 2524-0986

УДК 001.891(100) «20»
ББК 72.4
А43

Актуальные научные исследования в современном мире // Сб. научных трудов - Переяслав-Хмельницкий, 2018. - Вып. 2(34), ч. 1 – 131 с.

Языки издания: українська, русский, english, polski, беларуская, казақша, o'zbek, limba română, кыргыз тили, Հայերեն

Сборник предназначен для научных работников и преподавателей высших учебных заведений. Может использоваться в учебном процессе, в том числе в процессе обучения аспирантов, подготовки магистров и бакалавров в целях углубленного рассмотрения соответствующих проблем. Все статьи сборника прошли рецензирование, сохраняют авторскую редакцию, всю ответственность за содержание несут авторы.

УДК 001.891(100) «20»
ББК 72.4
А43

СОДЕРЖАНИЕ

СЕКЦИЯ: СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Ерошенко Ольга Артуровна,
Прасол Игорь Викторович (Харьков, Украина)
ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ МИОГРАФИЧЕСКИХ СИГНАЛОВ МЫШЦ ДЛЯ ЗАДАЧ ЭЛЕКТРОТЕРАПИИ..... 5

Мазниченко Наталья Ивановна (Харьков, Украина)
ИСПОЛЬЗОВАНИЕ ДИНАМИЧЕСКИХ БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В СЕТИ... 10

Місюра Владислав Олександрович,
Корнійчук Віктор Іванович (Київ, Україна)
ПОТОКОВЕ МОВЛЕННЯ ВІДЕО ФАЙЛІВ У PEER-TO-PEER МЕРЕЖАХ ЗА ДОПОМОГОЮ WEBRTC..... 18

Моренцов Евгений Иванович (Киев, Украина)
ПРОГРАММНАЯ ІНЖЕНЕРИЯ: ОТ ТЕХНОЛОГИИ ПРОГРАММИРОВАНИЯ К МЕТАТЕХНОЛОГИИ..... 24

Сімоненко Андрій Валерійович, Поляков Денис Олександрович (Київ, Україна)
ПОПЕРЕДНЯ ОБРОБКА ДАНИХ ДЛЯ МАШИННОГО ПЕРЕКЛАДУ..... 31

Поліщук Андрій Олександрович,
Романчук Ростислав Олександрович (Київ, Україна)
ПРИХОВУВАННЯ ІНФОРМАЦІЇ ВИКОРИСТОВУЮЧИ АУДІО СТЕГАНОГРАФІЮ..... 36

Коломиец Алина Дмитриевна, Лейбович Лев Иссахарович
НУК им. адмирала Макарова (Николаев, Украина)
К ВОПРОСУ МОДЕЛИРОВАНИЯ ИСТЕЧЕНИЯ НАГРЕТОЙ ВОДЫ ЧЕРЕЗ СОПЛО ЛАВАЛЯ..... 42

Абдурахманова Нигора Нурмахамадовна,
Абдурахманов Абдуазиз Абдугаффорович (Ташкент, Узбекистан)
ПРИМЕНЕНИЕ МЕТОДОВ ИНТЕЛЛЕКТУАЛИЗАЦИИ В СИСТЕМАХ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ..... 50

Соколов В. Ю. (Київ, Україна)
СТАНОВЛЕННЯ БІБЛІОТЕЧНОЇ ВАЛЕОЛОГІЇ ТА ШЛЯХИ ПОКРАЩЕННЯ ВАЛЕОЛОГІЧНОГО СУПРОВОДУ ІНФОРМАЦІЙНО-БІБЛІОТЕЧНОЇ ДІЯЛЬНОСТІ..... 56

СЕКЦИЯ: ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

Діхтярук Микола Миколайович, Ярецька Наталія Олександрівна (Хмельницький, Україна)
КОНТАКТНА ВЗАЄМОДІЯ НЕСКІНЧЕНОГО СТРИНГЕРА З ОДНІЄЮ ТА ДВОМА ПОПЕРЕДНЬО НАПРУЖЕННИМИ СМУГАМИ..... 75