Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2020-24-2-108-121

Вариант разграничения доступа к информационным ресурсам на основе неявной аутентификации

А. Л. Марухленко [1] ✉, А. В. Плугатарев [1], М. О. Таныгин [1], Л. О. Марухленко [1], М. Ю.Шашков [1]

[1] ФГБОУ ВО «Юго-Западный государственный университет»
ул. 50 лет Октября 94, г. Курск 305040, Российская Федерация

✉ e-mail: proxy33@mail.ru

Резюме

Цель исследования. *Цель работы заключается в построении модели системы для эффективной аутентификации мобильных пользователей на основе общедоступных данных пользователя и его поведенческих факторов, а также в исследовании алгоритмов вычисления порогового значения, значения при котором аутентификация пользователя мобильного устройства считается успешной.*

Методы. *В процессе анализа поведенческих факторов пользователя, которого необходимо аутентифицировать при взаимодействии мобильных устройств, предложены следующие методы вычисления порогового значения. Предложено использование динамических методов определения пороговой величины аутентификации пользователей, основанных на стандартном отклонении и вычислении совокупного среднего балла. Метод, основанный на стандартном отклонении, основан на том, что система делит совокупный поток оценок на несколько блоков одинаково длины, где первый блок используется для обучения, а вычисленный порог используется во втором блоке. Данная последовательность действий повторяется непрерывно, то есть предыдущий блок предоставляет результаты обучения для вычисления порога для текущего блока. Метод вычисления совокупного среднего балла, где вместо использования единого значения общего балла в качестве входных данных, система использует среднее значение текущего блока в качестве входных данных, а новый вычисленный порог используется в качестве порога принятия решения для следующего блока. Предложена математическая модель, обеспечивающая балансирование между скоростью и надёжностью аутентификации мобильных пользователей.*

Результаты. *Итогом проведенных исследований является разработка эффективного построения системы для вычисления порогового значения успешной аутентификации пользователя мобильного устройства на основе поведенческих особенностей, и адаптирующаяся к изменению поведенческих факторов пользователя. Проведены экспериментальные исследования и сравнения с аналогами, подтверждающие полноту и корректность, а также различные вариации предложенных решений.*

Заключение. *Предложенный метод неявной аутентификации для управления мобильным доступом легко реализуем, прост в использовании и адаптивен к изменениям входящих данных. Также предложены варианты вычисления порогового значения, при котором неявная аутентификация считается успешно пройденной.*

Ключевые слова: *разграничение доступа; системный анализ; распознавание; неявная аутентификация; сетевое взаимодействие.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Вариант разграничения доступа к информационным ресурсам на основе неявной аутентификации / А. Л. Марухленко, А. В. Плугатарев, М. О. Таныгин, Л. О. Марухленко, М. Ю.Шашков // Известия Юго-Западного государственного университета. 2020; 24(2): 108-121. https://doi.org/10.21869/2223-1560-2020-24-2-108-121.

Поступила в редакцию 25.02.2020 *Подписана в печать 07.04.2020* *Опубликована 20.04.2020*

Option of Control of Access to Information Resources Based on Implicit Authentication

Anatoliy L. Marukhlenko [1] ✉, Aleksey V. Plugatarev [1], Maksim O. Tanygin [1], Leonid O. Marukhlenko [1], Maksim Yu. Shashkov [1]

[1] Southwest State University
50 Let Oktyabrya str. 94, Kursk 305040, Russian Federation

✉ e-mail: proxy33@mail.ru

Abstract

Purpose of reseach *is to build a model of a system for effective authentication of mobile users based on public data of the user and his behavioral factors as well as to study algorithms for calculating the threshold value at which the authentication of a mobile device user is considered successful.*

Methods. *When analyzing the behavioural factors of a user who needs to be authenticated when interacting with mobile devices, application of the following methods for calculating the threshold value are proposed: dynamic methods for determining the threshold value of user authentication based on the standard deviation and the calculation of the aggregate mean score; the method based on the standard when the system divides the aggregate flow of estimates into several blocks of the same length, where the first block is used for training, and the calculated threshold is used in the second block (this sequence of actions is repeated continuously, that is, the previous block provides training results for calculating the threshold for the current block); a method for calculating the aggregate mean score, where instead of using a single total score as input, the system uses the mean value of the current block, and the new calculated threshold is used as the threshold for decision making for the next block. A mathematical model that balances the speed and reliability of mobile users authentication is proposed.*

Results. *The result of the research is the development of an effective system for calculating the threshold value of successful authentication of a mobile device user based on behavioural features which adapts to changes of the user's behavioural factors. Experimental studies and comparisons with analogs confirming the completeness and correctness were carried out as well as various variants of the proposed solutions.*

Conclusion. *The proposed method of implicit authentication for mobile access control is easy to implement, easy to use, and adaptive to changes in input data. Options for calculating the threshold value at which implicit authentication is considered successful are also proposed.*

Keywords: *control access; system analysis; identification; implicit authentication; network interconnection.*

Conflict of interest. *The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Marukhlenko A. L., Plugatarev A.V., Tanygin M.O., Marukhlenko L.O., Shashkov M. Yu. Option of Control of Access to Information Resources Based on Implicit Authentication // *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2020, 24(2): 108-121 (In Russ.). https://doi.org/10.21869/2223-1560-2020-24-2-108-121.

Received 25.02.2020 *Accepted 07.04.2020* *Published 20.04.2020*

***

Введение

Мобильные устройства стали незаменимыми в повседневной жизни, предоставляя удобный доступ к онлайн-сервисам, многие из которых включают денежные транзакции и хранение или передачу конфиденциальных данных [1]. В результате они становятся все более привлекательными для злоумышленников, которые могут поставить под угрозу безопасность и конфиденциальность данных, доступ к которым хранится на мобильных устройствах [2-3]. Мобильные устройства особенно уязвимы для потери или физической кражи, поэтому важно иметь эффективный контроль доступа и строгие защитные меры, которые постоянно защищают устройства. Контроль доступа обычно включается аутентификацией пользователя, проверка пользователя на легитимность [4].

Аутентификация с одноразовыми паролями очень неудобна и легко теряется [5]. Аутентификация, включающая биометрические характеристики, такие как лицо и радужная оболочка глаза, отпечаток пальца, голос или речь являются вычислительно дорогими для устройств с ограниченным объемом памяти и энергопотреблением [6].

В целях защиты конфиденциальности пользователей на мобильных устройствах в данной статье предлагается управляемая событиями схема неявной аутентификации. Неявная аутентификация – перспективная альтернатива традиционным методам аутентификации [7]. Например, предложены схемы, основанные на шаблонах поведения пользователя. Баланс между адаптивностью и практической осуществимостью все еще остается проблемой [8-11]. В данной этой статье предлагается управляемая событиями схема, которая включает в себя осведомленность о поведении пользователя через данные повседневного взаимодействия с телефоном.

Чтобы обеспечить работу в режиме реального времени в статье рассматриваются функции поведения пользователя для профилирования пользователей и применяются совокупные оценки и пороговые вычисления для неявной схемы аутентификации [12]. В статье исследуются несколько методов вычисления порогового балла использования схемы для того, чтобы определить уровень доверия текущего пользователя.

Предлагаемая схема предназначена для: работы полностью в фоновом режиме. Затем, полученные значения можно использовать для активации контроля доступа с явной аутентификацией [13].

Данная задача решается в целях защиты конфиденциальности пользователей на мобильных устройствах. В данной статье предлагается управляемая событиями схема неявной аутентификации. Необходимо исследовать несколько методов использования схемы

для распознавания законного поведения пользователя [14]. Исследуемые методы вычисляют совокупную оценку и пороговое значение в режиме реального времени. Чтобы определить уровень доверия текущего пользователя используются данные, полученные в результате предыдущих взаимодействий пользователя с устройством [15]. Разработанная схема должна работать полностью в фоновом режиме, иметь минимальный период получения порогового значения, иметь высокую скорость распознавания пользователей для неявной аутентификации и оперативно обнаруживать ошибки, которые могут использоваться для запуска контроля доступа с явной аутентификацией.

Материалы и методы

1. Метод определения доверительности источника

Предложенная схема аутентификации пользователя моделирует профиль пользователя посредством данных, собранных из повседневного поведения пользователя. Алгоритм оценки применяется для вычисления уровня доверия текущего подключения. Порог принятия решения адаптивно вычисляется, ниже которого явный процесс аутентификации может быть запущен или активирован для обеспечения контроля доступа [16].

Предлагаемый подход использует данные, полученные из событий повседневных пользовательских действий или моделей поведения. Он основан на общедоступных данных, которые могут быть извлечены из большинства телефонов, для создания профиля пользователя. Будем рассматривать следующие источники информации для неявной схемы аутентификации:

1) входящие / исходящие SMS;

2) входящий / исходящий телефонный звонок;

3) история браузера;

4) WIFI история.

Функции, используемые для моделирования профиля пользователя, могут быть представлены следующим образом:

$$F=(f_1+f_2+f_3+..+f_n). \quad (1)$$

Функции для вычисления оценки для каждого источника представлены в виде:

$$Sc=(S_1+S_2+S_3+..+S_n). \quad (2)$$

Таким образом, совокупный балл N, рассчитанный по этой модели, может быть представлен как

$$N= \sum_{i=0}^{n} S_i(f_i). \quad (3)$$

SMS – сообщения. Каждый раз, когда происходит пересылка SMS-сообщения, система записывает время и отображает номер телефона. Каждому входящему и исходящему номеру телефона присваивается приоритетное значение, рассчитываемое из:

$$K_T=120+(48\times OT)-t, \quad (4)$$

где OT – обозначает общее количество раз, когда событие произошло; t – время между текущим вычислением и последним вычислением (в часах). С помощью

приведенного выше выражения поддерживается кэш наиболее значимых событий, поскольку любое значение, меньшее нуля, удаляется из списка [17]. OT инициализируется нулем для любого числа, удаленного из списка. Кроме того, формула позволяет удалить из кэша числа, которые были неактивны более недели. Каждый раз, когда происходит новое SMS-событие, система проверяет, были ли выполнены следующие условия при расчете балльной оценки:

Условие 1: система ищет, находится ли этот номер в верхних 5 позициях в списке значений приоритета.

Условие 2: система проверяет, появляется ли этот номер в списке контактов пользователя.

Оценка определяется следующим образом:

$$S_T=\sum S_{условия}.$$

Звонки. Расчёт ведётся так же, как и в случае SMS-активности, за исключением того, что в расчёт берётся продолжительность телефонного звонка. Долгосрочный вызов является показателем нормального использования, и это принимается в рассмотрение при подсчете баллов.

История браузера. Система извлекает историю браузера и записывает доменное имя каждого посещенного URL. Аналогично функциям SMS и вызовов, список приоритетов поддерживается на основе формулы

$$K_B=72+(8\times OT)-t, \quad (5)$$

где OT представляет общее количество посещений URL; t –интервал в часах между последним посещением и текущим посещением. Кэш наиболее релевантных URL-адресов поддерживается путем удаления отрицательных значений из списка, а OT для удаленного URL-адреса сбрасывается в ноль. Оценка истории браузера вычисляется путем проверки того, сколько недавно посещенных доменов находятся в верхних 6 позициях в списке значений приоритета. Оценка определяется следующим образом:

$$S_B=\sum S_{доменов}\ . \quad (6)$$

История WIFI. Система записывает идентификатор набора услуг (SSID) подключенной точки доступа и продолжительность каждого соединения. Список значений приоритета также вычисляется аналогично

$$K_{wf}=100+(18\times OT)-t\ , \quad (7)$$

где OT обозначает общее количество раз, когда пользователь подключался к определенной точке доступа, а t (в часах) обозначает интервал между временем последнего соединения и текущим временем [18]. Соединения продолжительностью менее двух минут не включаются в вычисления, чтобы избежать использования автоматических коротких соединений с точками доступа. Каждый раз, когда устанавливается новое соединение WIFI, система определяет оценку для истории WIFI, прове

ряя, находится ли она в топ-5 из списка значений приоритета, а затем вычисляет оценку следующим образом:

$$S_B=\sum S_{соединений}\ . \quad (8)$$

2. Метод вычисления порогового значения, основанный на оценке среднеквадратичного отклонения

Для вычисления порогового значения в данной системе будем использовать динамические методы определения пороговой величины. Один из подходов основан на оценке стандартного отклонения (рис. 1). Система делит совокупный поток оценок на несколько блоков одинаковой длины ($block_1$, …, $block_n$) длины L. Первый блок используется для обучения, а вычисленный порог используется во втором блоке. Этот шаблон повторяется непрерывно, то есть предыдущий блок предоставляет результаты обучения для вычисления порога для текущего блока. Оценка скорости распознавания данным методом представлена на рис. 1.

3. Метод вычисления порогового значения совокупного среднего балла

Также стоит уделить внимание методу вычисления совокупного среднего балла. Пороговое значение вычисляется по формуле

$$\Pi=\alpha*Z_{t-1}+(1-\alpha)*\Pi_{t-1},\quad t<1. \quad (9)$$

Вместо использования единого значения общего балла в качестве входных данных для определения значения порога, система использует среднее значение текущего блока (размер блока b может быть скорректирован в реализации) в качестве входных данных. Новый вычисленный порог используется в качестве порога принятия решения для следующего блока. Например, если исходный индекс AS (совокупного балла) текущего блока равен k, размер блока задается значением b. Значение выражается следующим образом:

$$Z=\frac{\sum_{i=k}^{i=k+b} AS_i}{b}\ . \quad (10)$$

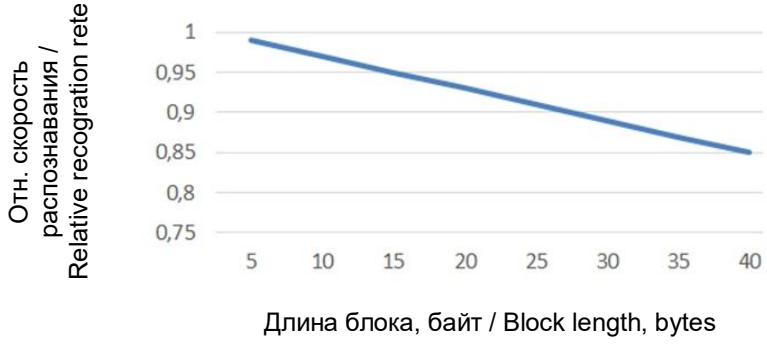

Рис. 1. Зависимость скорости распознавания пользователя от величины блока при использовании метода стандартного отклонения

Fig. 1. Dependence of the user identification rate on the block size when using the standard deviation method

Далее новый вычисленный порог используется в качестве обнаружения порога для следующего блока от AS_{k+b+1} до AS_{k+2b+1}.

Результаты и их обсуждение

1. Результат исследования зависимости скорости аутентификации от различных параметров

Баланс между адаптивностью и практической осуществимостью является одной из задач данного исследования, поэтому необходимо исследовать зависимость скорости аутентификации пользователя от различных параметров.

На рис. 1 показано, что скорость распознавания пользователей уменьшается с увеличением размера блока. Это связано с алгоритмом стандартного отклонения, который дает порогу больше места для того, чтобы наверстать изменение оценки, когда размер блока меньше [19]. Результат показывает, что блок небольшого размера достигает лучшей производительности при распознавании пользователя.

На рис. 2 показана восходящая динамика скорости распознавания пользователя при увеличении коэффициента. В методе вычисления совокупного балла коэффициент α представляет степень взвешивания. Чем выше α, тем быстрее удаляется старшее наблюдение (порог). Следовательно, высокое значение α подразумевает наиболее высокий уровень распознавания пользователей.

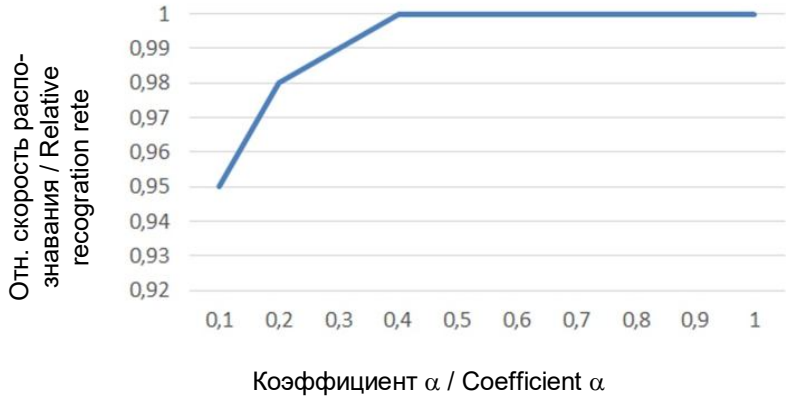

Рис. 2. Зависимость скорости распознавания пользователя от коэффициента α

Fig. 2. Dependence of the user identification rate on coefficient α

2. Сравнение с методом биометрической аутентификации в мобильных взаимодействиях

Надёжным методом также является применение биометрических моделей аутентификации в мобильном оборудовании для вычисления порога. В основе этого метода находится индуктивный подход – это построение теории, основанной на уже имеющихся данных. Зависимость успешной аутентификации от точности данных схематично представлено на рис. 3 [20].

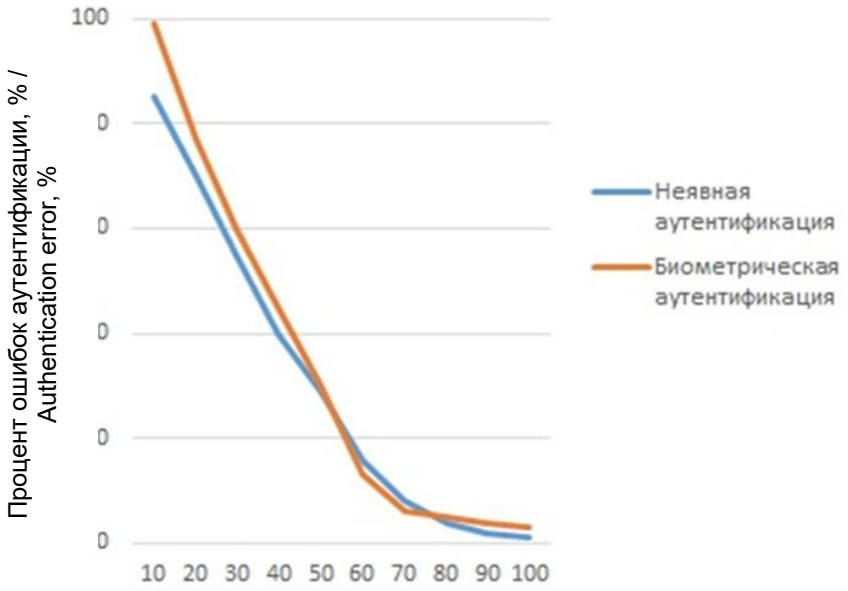

Рис. 3. Зависимость успешной аутентификации от предоставляемой точности данных

Fig. 3. Dependence of successful authentication on provided data accuracy

Также следуя из вышеизложенного, на рисунке схематично представлен график зависимости точности аутентификации от входной информации.

Из рис. 3 следует, что применение биометрических моделей требует высокой точности исходных данных. Предлагаемый метод при условии разбиения информационного потока на маленькие блоки более эффективен. При защите более ценной информации предлагаемый метод сравним с биометрической аутентификацией, однако предложенный метод аутентификации вполне достаточно использовать для защиты данных от злоумышленников в повседневной жизни.

Выводы

В данной статье предложена и оценена управляемая событиями схема неявной аутентификации для управления мобильным доступом. Схема предназначена для прозрачной и адаптивной работы путем вычисления совокупных баллов (указывающих на уровень доступа пользователя). Результаты показывают, что выполнимо и практично создать эффективную систему неявной аутентификации из легкодоступных повседневных телефонных данных, с помощью которых вычисляется пороговое значение, при котором неявная аутентификация считается успешно пройденной.

Список литературы

1. Intuitive security policy configuration in mobile devices using context profiling / A. Gupta, M. Miettinen, N. Asokan, M. Nagy // In Privacy, Security, Risk and Trust (PASSAT), 2012 International.

2. Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors / H. G. Kayacik, M. Just, L. Baillie, D. Aspinall, N. Micallef // In Proceedings of the Third Workshop on Mobile Security Technologies (MoST), 2014.

3. "ePet: when cellular phone learns to recognize its owner / M. Tamviruzzaman, S. I. Ahamed, C. S. Hasan, C. O'brien // In Proceedings of the 2nd ACM workshop

4. Анализ потенциальных уязвимостей и современных методов защиты многопользовательских ресурсов / А.Л. Марухленко, Л.О. Марухленко, Е.Е. Конорева, М.О. Таныгин // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции / отв. ред. В. Г. Андронов. Курск, 2018. С. 136-140.

5. Организация системы сетевого мониторинга и оценки состояния информационной безопасности объекта / А.Л. Марухленко, К.Д. Селезнёв, М.О. Таныгин, Л.О. Марухленко // Известия Юго-Западного государственного университета. 2019. Т. 23. № 1. С. 118-129. http:// doi.org/10.21869/2223-1560-2019-23-1-118-129.

6. Progressive Authentication: Deciding When to Authenticate on Mobile Phones / O. Riva, C. Qin, K. Strauss, D. Lymberopoulos // In USENIX Security Symposium. 2012. P. 301-316.

7. Комплексная оценка информационной безопасности объекта с применением математической модели для расчета показателей риска / А.Л. Марухленко, А.В. Плугатарев, Л.О. Марухленко, М.А. Ефремов // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8. № 4 (29). С. 34-40.

8. Casa: context- aware scalable authentication / E. Hayashi, S. Das, S. Amini, J. Hong, I. Oakley // In Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM, 2013. P. 3-13.

9. Марухленко А.Л., Мирзаханов П.С., Марухленко С.Л. Мониторинг и имитационное моделирование процессов взаимодействия абонентов вычислительной сети // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2012. № 2-3. С. 236-241.

10. Установление доверительного канала обмена данными между источником и приёмником информации с помощью модифицированного метода одноразовых паро-

лей / М.О. Таныгин, Х.Я. Алшаиа, В.А. Алтухова, А.Л. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8. № 4 (29). С. 63-71

11. Программный модуль для оценки криптостойкости симметричных методов шифрования с использованием параллельных вычислений / А.Л. Марухленко, Л.О. Марухленко, А.В. Плугатарев, В.П. Добрица // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения сборник научных статей по материалам II Всероссийской научно-практической конференции / отв. ред. В. Г. Андронов. Курск, 2018. С. 33-38.

12. Таныгин М.О., Берлизева В.А., Алшаиа Х.Я.А. Алгоритм обратимых преобразования для контроля аутентичности пакетов в сетях с низкой пропускной способностью // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам III Всероссийской научно-практической конференции / отв. ред. В. Г. Андронов. Курск, 2019. С. 169-173.

13. Вариант организации защищенной системы контроля версий и обновления программного обеспечения для компиляции дистрибутивов / А.Л. Марухленко, Н.К. Зарубина, А.А. Шамина, И.И. Марухленко // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: материалы 1 Всероссийской научно-практической конференции: в 2 ч. / отв. ред. В. Г. Андронов. Курск, 2017. С. 190-196.

14. Blerton Abazi, Besnik Qehaja, Edmond Hajrizi. Application of biometric models of authentication in mobile equipment. IFAC-PapersOnLineVolume 52, Is. 252019. P. 543-546.

15. Марухленко А.Л., Мирзаханов П.С. Программный комплекс для моделирования процесса передачи и обработки сетевых потоков данных // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2012. № 2-3. С. 175-180.

16. Ефремова Е.О., Калугин Е.В. Адаптивный алгоритм аутентификации источника сообщений // Прикладная математика и информатика: современные исследования в области естественных и технических наук: материалы V Международной научно-практической конференции (школы-семинара) молодых ученых. Тольятти, 2019. С. 38-42.

17. Пат. 2541131 Российская Федерация, МПК G06K9/62. Способ динамической биометрической аутентификации личности по особенностям почерка / Добрица В.П., Милых В.А., Лапина Т.И., Лапин Д.В.; заявитель и патентообладатель Юго-Западный государственный университет. № 2013128214/08; заявл. 19.06.2013; опубл. 27.12.2014, Бюл. № 36.

18. Администрирование информационных систем / Д.О. Бобынцев, Л.А. Лисицин, А.Л. Марухленко, С.А. Кужелева; Юго-Зап. гос.ун-т. Курск, 2019. 201 с.

19. Безопасность информационных систем / А.Л Марухленко., М.О. Таныгин, М.А. Ефремов, А.Г. Спеваков; Юго-Зап. гос.ун-т. Курск, 2019. 210 с.

20. Разработка защищенных корпоративных систем на базе клиент-серверной технологии / М.А. Ефремов, Ю.А. Халин, А.Л. Марухленко, Л.О. Марухленко; Юго-Зап. гос.ун-т. Курск, 2018. С. 176.

References

1. Gupta A., Miettinen M., Asokan N., Nagy M. Intuitive security policy configuration in mobile devices using context profiling. In Privacy, Security, Risk and Trust (PASSAT), 2012 International.

2. Kayacik H. G., Just M., Baillie L., Aspinall D., Micallef N. Data driven authentication: On the effectiveness of user behavior modeling with mobile device sensors. In Proceedings of the Third Workshop on Mobile Security Technologies (MoST), 2014.

3. Tamviruzzaman M., Ahamed S. I., Hasan C. S., O'brien C. ePet: when cellular phone learns to recognize its owner. In Proceedings of the 2nd ACM workshop.

4. Marukhlenko A.L., Marukhlenko L.O., Konoreva E.E., Tanygin M.O. [Analysis of potential vulnerabilities and modern methods of protecting multi-user resources]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya. Sbornik nauchnykh statei po materialam II Vserossiiskoi nauchno-prakticheskoi konferentsii* [Infocommunications and space technologies: state, problems and solutions The collection of scientific articles based on the materials of the II All-Russian scientific-practical conference]. Kursk, 2018, pp. 136-140 (In Russ.).

5. Marukhlenko A.L., Seleznev K.D., Tanygin M.O., Marukhlenko L.O. Organizatsiya sistemy setevogo monitoringa i otsenki sostoyaniya informatsionnoi bezopasnosti ob"ekta [Arrangement of the System of Network Monitoring and Assessment of the State of Information Security of an Objecı]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*, 2019, vol. 23, no. 1, pp. 118-129 (In Russ.) http:// doi.org/10.21869/2223-1560-2019-23-1-118-129.

6. Riva O., Qin C., Strauss K., Lymberopoulos D. Progressive Authentication: Deciding When to Authenticate on Mobile Phones. In USENIX Security Symposium, 2012, pp. 301-316.

7. Marukhlenko A.L., Plugatarev A.V., Marukhlenko L.O., Efremov M.A. Kompleksnaya otsenka informatsionnoi bezopasnosti ob"ekta s primeneniem matematicheskoi modeli dlya rascheta pokazatelei riska [A comprehensive assessment of the information security of an object using a mathematical model for calculating risk indicators]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika,*

informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing Engineering, Information Science. Medical Instruments Engineering, 2018, vol. 8, no. 4 (29), pp. 34-40 (In Russ.).

8. Hayashi E., Das S., Amini S., Hong J., Oakley I. Casa: context-aware scalable authentication." In Proceedings of the Ninth Symposium on Usable Privacy and Security, ACM, 2013, pp. 3-13.

9. Marukhlenko A.L., Mirzakhanov P.S., Marukhlenko S.L. Monitoring i imitatsionnoe modelirovanie protsessov vzaimodeistviya abonentov vychis-litel'noi seti [Monitoring and simulation modeling of processes of interaction between subscribers of a computer network]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing Engineering, Information Science. Medical Instruments Engineering,* 2012. no. 2-3, pp. 236-241 (In Russ.).

10. Tanygin M.O., Alshaya Kh.Ya., Altukhova V.A., Marukhlenko A.L. Ustanovlenie doveritel'nogo kanala obmena dannymi mezhdu istochnikom i priemnikom informatsii s pomoshch'yu modifitsirovannogo metoda odnorazovykh parolei [Establishing a confidence channel for exchanging data between a source and a receiver of information using the modified one-time password method]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing Engineering, Information Science. Medical Instruments Engineering,* 2018, vol. 8, no. 4 (29), pp. 63-71 (In Russ.).

11. Marukhlenko A.L., Marukhlenko L.O., Plugatarev A.V., Dobritsa V.P. [A software module for assessing the cryptographic strength of symmetric encryption methods using parallel computing]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya sbornik nauchnykh statei po materialam II Vserossiiskoi nauchno-prakticheskoi konferentsii* [Infocommunications and space technologies: state, problems and solutions. The collection of scientific articles based on the materials of the II All-Russian Scientific and Practical Conference]. Kursk, 2018, pp. 33-38 (In Russ.).

12. Tanygin M.O., Berliseva V.A., Alshaya Kh.Ya.A. [Reversible conversion algorithm to control packet authenticity in networks with low bandwidth]. *INFOkommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya sbornik nauchnykh statei po materialam III Vserossiiskoi nauchno-prakticheskoi konferentsii* [INFO communications and space technologies: state, problems and solutions. The collection of scientific articles based on the materials of the III All-Russian scientific-practical conference]. Kursk, 2019, pp. 169-173 (In Russ.).

13. Marukhlenko A.L., Zarubina N.K., Shamina A.A., Marukhlenko I.I. [A variant of organizing a secure version control system and software updates for compiling distributions]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya. Materialy 1 Vserossiiskoi nauchno-prakticheskoi konferentsii.* [Infocommunications and space technologies: state, problems and ways of solving. Materials of the 1st All-Russian Scientific and Practical Conference]. Kursk, 2017, pp. 190-196 (In Russ.).

14. Blerton Abazi, Besnik Qehaja, Edmond Hajrizi. Application of biometric models of authentication in mobile equipment. IFAC-PapersOnLineVolume 52, is. 252019, pp. 543-546.

15. Marukhlenko A.L., Mirzakhanov P.S. Programmnyi kompleks dlya modelirovaniya protsessa peredachi i obrabotki setevykh potokov dannykh [A software package for modeling the process of transmitting and processing network data streams]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing Engineering, Information Science. Medical Instruments Engineering,* 2012, no. 2-3, pp. 175-180 (In Russ.).

16. Efremova E.O., Kalugin E.V. [Adaptive message source authentication algorithm]. *Prikladnaya matematika i informatika: sovremennye issledovaniya v oblasti estestvennykh i tekhnicheskikh nauk. Materialy V Mezhdunarodnoi nauchno-prakticheskoi konferentsii (shkoly-seminara) molodykh uchenykh.* [Applied mathematics and computer science: modern research in the field of natural and technical sciences. Materials of the V International scientific-practical conference (school-seminar) of young scientists]. Tolyatti, 2019, pp. 38-42 (In Russ.).

17. Dobritsa V.P., Milykh V.A., Lapina T.I., Lapin D.V. *Sposob dinamicheskoi biometricheskoi autentifikatsii lichnosti po osobennostyam pocherka* [The method of dynamic biometric authentication of personality according to the features of handwriting]. Patent RF, 2541131 C2, 02/10/2015. Application No. 2013128214/08 of 06/19/2013 (In Russ.).

18. Bobyntsev D.O., Lisitsin L.A., Marukhlenko A.L., Kuzheleva S.A. *Administrirovanie informatsionnykh sistem* [Administration of information systems]. Kursk, 2019, 201 p. (In Russ.).

19. Marukhlenko A.L., Tanygin M.O., Efremov M.A., Spevakov A.G. *Bezopasnost' informatsionnykh sistem* [Security of information systems]. Kursk, 2019, 210 p. (In Russ.).

20. Efremov M.A., Khalin Yu.A., Marukhlenko A.L., Marukhlenko L.O. *Razrabotka zashchishchennykh korporativnykh sistem na baze klient-servernoi tekhnologii* [Development of secure corporate systems based on client-server technology]. Kursk, 2018, 176 p. (In Russ.).

Информация об авторах / Information about the Authors

Марухленко Анатолий Леонидович,
кандидат технических наук, доцент кафедры информационной безопасности,
ФГБОУ ВО «Юго-Западный государственный университет»,
г. Курск, Российская Федерация,
e-mail: proxy33@mail.ru

Anatoliy L. Marukhlenko, Cand. of Sci. (Engineering), Associate Professor of Information Security Department,
Southwest State University,
Kursk, Russian Federation,
e-mail: proxy33@mail.ru

Плугатарев Алексей Владимирович,
магистрант кафедры информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет»,
г. Курск, Российская Федерация,
e-mail: aplugatarev@bk.ru

Aleksey V. Plugatarev, Master Student of Information Security Department,
Southwest State University,
Kursk, Russian Federation,
e-mail: aplugatarev@bk.ru

Таныгин Максим Олегович,
кандидат технических наук, заведующий кафедрой информационной безопасности,
ФГБОУ ВО «Юго-Западный государственный университет»,
г. Курск, Российская Федерация,
e-mail: tanygin@yandex.ru

Maksim O. Tanygin, Cand. of Sci. (Engineering), Head of Information Security Department, Southwest State University,
Kursk, Russian Federation,
e-mail: tanygin@yandex.ru

Марухленко Леонид Олегович,
ст. преподаватель кафедры информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет»,
г. Курск, Российская Федерация,
e-mail: leonid.marukhlenko@mail.ru

Leonid O. Marukhlenko, Senior Lecturer of Information Security Department,
Southwest State University,
Kursk, Russian Federation,
e-mail: leonid.marukhlenko@mail.ru

Шашков Максим Юрьевич, магистрант, кафедры информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет»,
г. Курск, Российская Федерация,
e-mail: dmax2019@yandex.ru

Maksim Yu. Shashkov, Master Student of Information Security Department,
Southwest State University,
Kursk, Russian Federation,
e-mail: dmax2019@yandex.ru