

7. Lobo, A., Vivec, J. (2001). Port users perspective of the container transshipment business. Proceedings of the International Conference on Port and Maritime R&D and technology. Singapore.
8. Fisk, R., Brown, S., Bitner, M. (1993). Tracking the Evolution of Services Marketing Literature. Journal of Retailing, 69 (1).
9. Astashkin, V. A. (2004). Sovershenstvovanie funkcionirovanija transportno – jekspeditorskih predpriyatij, Moscow, 142.
10. Zeithaml, V.; In: Donnelly, J. H., George, W. R. (1981). How Consumer Evaluation Processes Differ Between Goods and Services. Marketing of Services, 186–190.

Надійшла (received) 10.10.2014

УДК 004.32; 004.48; 004.45; 004.82

Ж. Ю. ЗЕЛЕНЦОВА, инженер, Одесский национальный экономический университет;

Е. О. ЙОНА, соискатель, Одесский национальный экономический университет

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ОРГАНИЗАЦИИ СИСТЕМ ЕДИНОГО ВХОДА. ЧАСТЬ 2: ОРГАНИЗАЦИЯ ЕДИНОГО ДОСТУПА В ПОДСЕТИ

Предлагается технологическое решение задачи идентификации пользователей при их доступе к мультисервисным системам. Показывается, что решение может привести к снижению количества применяемых адаптивных (интеллектуальных) методик процесса IAM в современных ИТ-платформах. Акцентируется внимание на том, что предлагаемый подход актуален для решения проблемы гипер-подключенности в подсетях, для которых характерно большое количество данных, устройств и пользователей.

Ключевые слова: системы единого входа, организация доступа, Single Sign-On, iGenotype, e-passport

Введение. Технология единого входа SSO (англ.: *Single Sign-On* [SSO]) – одна из технологий, относящихся к широкому классу систем управления идентификацией и доступом пользователей (англ.: *Identity management and access* [IAM]) к ресурсам информационных систем и сетей. Основное отличие SSO от других технологии состоит в совмещении процессов идентификации (ID) и аутентификации (AuthN) с единой точкой отказа [1]. Эту технологию на сегодняшний день реализует ряд производителей VMware, Google, Pay Pal. Ими отмечается ряд проблемных вопросов и уязвимостей архитектурного уровня, которые непременно будут оказывать значительное влияние на процесс развития информационных систем при текущих признаках цифровой вселенной (англ.: *Digital Universe* [DUn]), о чём свидетельствует стабильный росте количества пользователей, устройств, данных, а также при расширении сервисных возможностей сети [2-4]. Основные положения по этому вопросу, изложены в [5].

Целью работы является разработка предложений по созданию модели системы идентификации и обеспечения доступа с единым входом, которая может быть адаптирована к текущим особенностям современных сервисных структур, что готовятся к повсеместному использованию рядом производителей ИТ-систем.

Результаты исследования: Организация и модель SSO. Предлагаемая к анализу тема рассматривалась в рамках задачи организации единого входа в

сервисной подсети [6]. Как подчеркивается в [6-9], для современной сетевой инфраструктуры свойственно большое количество пользователей, устройств и данных. Стремительно растет количество низкопроизводительных устройств типа *Internet of Things* [IoT] или «интернет-вещей». Исследование особенностей организации систем единого входа и общая модель представления данных и идентификации в сервисных подсетях, приведены авторами в [5]. Учитывая это, рассмотрим организацию характера доступа.

Согласно модели IAM, процесс, который следует после идентификации IdM, это процесс предоставления доступа AM (англ.: *Access Management* [AM]), который часто называют процессом *управления доступом*. Суть его состоит из совмещения AuthN и AuthZ. При этом доступ в мультисервисную подсеть может быть организован двумя способами.

Основной способ состоит в разделении процесса идентификации на два этапа. Первый из них предполагает распознавание пользователя в сервисной подсети. После этого пользователь может осуществить вход в подключенные сервисы, что организовывается с помощью встроенного менеджера паролей.

Эффективная функциональность систем с такой процедурой доступа в составе глобальных платформ спорна, т.к. множество точек доступа порождает такое же количество уязвимостей и, в целом, снижает безопасность системы.

Второй способ, который на сегодняшний день получает активное внедрение, состоит в применении методики единого входа – Single Sign-On. При этом предполагается, что предложенная в [5] «бесшовная» архитектура сервисных подсетей имеет соответствующие интерфейсы интеграции. Кроме того, подразумевается, что пользователи работают в пределах облачных структур. В таком случае, прежде всего, «облако»-обертка может встраивать новый сервис и подключаться к шине сервисов в программно-конфигурируемой сети топологии «cloud-to-cloud». Эта сеть предоставляет сервисный слой виртуализации, который доступен пользователям, посредством интеграционного интерфейса. Учитывая это, в интеграционных настройках кросс-системы интеграционной платформы, пользователем должны быть установлены параметры доступа к сервису. Эти «пользовательские» параметры идентификации будут автоматически согласованы с внутрисистемными моделями идентификации интеграционной платформы. Далее доступ во все сервисы будет установлен автоматически.

Далее предлагаемая двухэтапная модель идентификации

$$IAM = IAM_{pub} + IAM_{pers}$$

не противоречит изложенному подходу, что подтверждается анализом на рис. 1, на котором приведена диаграмма деятельности по идентификации и обеспечению доступа к сервисным подсетям.

По оценке Forrester Research – независимой аналитической компании, которая занимается исследованиями рынка информационных технологий, общий тренд продуктов IAM предполагает интеллектуальную обработку информации с упрощением процесса доступа. Но при этом особо отмечается, что должны быть соблюдены все параметры безопасности и организацией единого входа во все сервисные подсистемы [6-10]. Продукты, подобные IAM, оценены компанией, как лучшие на рынке. Отмечается, что они готовы к внедрению и предлагаются

такими производителями, как Aveksa, CA Technologies, Courion, Dell, IBM, NetIQ, Oracle, Ping Identity, и SecureAuth.

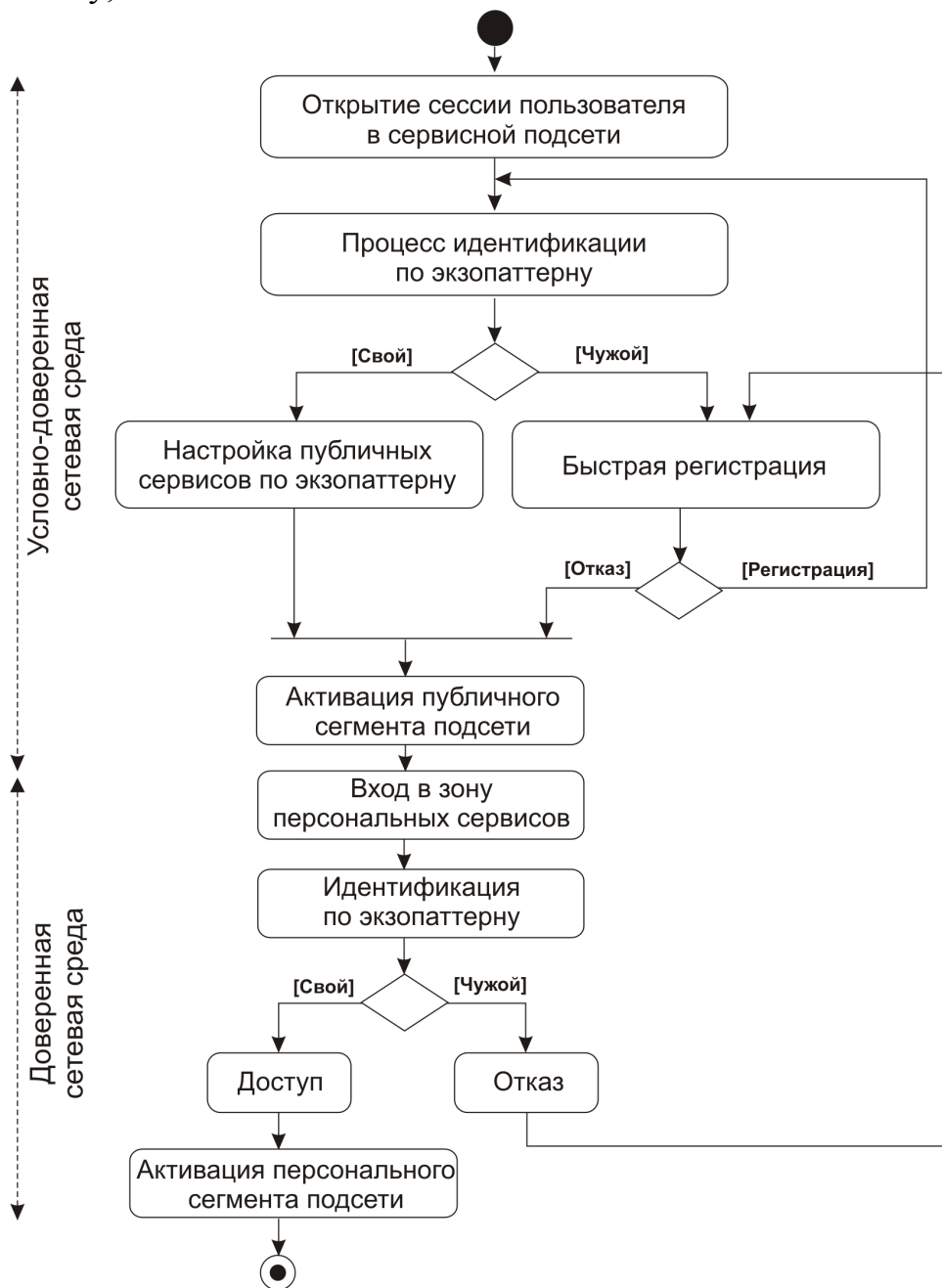


Рис. 1 – Диаграмма деятельности по двухэтапной идентификации по эндо- и экзопаттернам [5] и обеспечении доступа в подсети в условно-доверенные и доверенные сетевые сегменты на основе доступных данных о пользователе

Следующая проблема по отношению к AuthN и AuthZ – интеллектуальность. Учёт параметров интеллектуальности, это достаточно общая оценка методики идентификации, т.к. прежде всего, речь идет об обработке косвенных данных, а именно – внешних паттернов идентификации, на основании которых проводится предварительное распознавание [11]. Традиционно рабочие паттерны объединяются в модели – роли, предполагающие избирательность и гибкость идентификации и организации доступа. Эти методы известны как *метод управления доступом* на основе ролей (англ. *Role Based Access Control [RBAC]*).

Они применяются при использовании метода мандатного доступа (англ. *Mandatory access control* [MAC]). Последний метод, например, рекомендован Федеральной службой по техническому и экспортному контролю РФ для систем, которые оперируют данными, относящимися к государственной тайне [12].

Для реализации отмеченных целей могут быть применены методы распознавания на базе нечеткой логики. При этом адаптивность может быть обеспечена на основе использования марковских процессов принятия решений [13].

Как было показано в модели *iGenotype* [5], для каждого пользователя характерно наличие ряда собственных персональных и мобильных устройств, которые могут быть идентифицированы в мультисервисной системе по тем или иным признакам по отношению к владельцу. Это же положение можем распространить на данные специальных типов, т.е на официальные, социальные, виртуальные, а также на данные, которые описывают «цифровую тень» и «цифровой след».

Представим предлагаемую модель представить в виде математического словесного описания:

Модель *iGenotype* связанных данных пользователя может быть представлена в виде кортежа длины «3» – $iG : \langle IO, Dev, Data_{iG} \rangle$, где IO – набор официальной информации о сетевом пользователе, Dev – связанные устройства, $Data_{iG}$ – связанные с пользователем сетевые данные. По аналогии определим связанные с устройствами данные $iG_{dev} : \langle Dev, IO_{dev}, Data_{Dev} \rangle$, где $IO_{dev}, Data_{Dev}$ – данные, связанные с устройством. Также введём определение о сетевых данных и связанных с ним устройствах и владельцах – $iG_{data} : \langle Data, IO_{data}, Dev_{data} \rangle$. В общем случае это может быть описано, как $\langle Dev, iG_{dev} \rangle$ и $\langle Data, iG_{data} \rangle$.

Удовлетворение требований внутренних паттернов идентификации может быть применено в защищенной зоне интеграционной платформы с высоким уровнем доверия, например, в интерфейсе финансовых сервисов. Двухуровневый подход управлением доступом пользователя в зонах низкого и высокого уровня доверия разрешает и проблему организации безусловного доступа в сеть «в любой точке мира, с любого устройства и любого человека». При этом такой подход упрощает доступ к любым публичным сегментам. В общем виде его можно считать модификацией комплекса, состоящего из мандатного и ролевого подходов.

Отметим, что интерфейсы единого входа часто называют сетевой экосистемой. Это также подразумевает дружелюбность интерфейса по отношению к пользователю. Очевидно, что, несмотря на возможности полного контроля действий пользователя в сети и решения проблемы охраны правопорядка в сети, должны существовать определенные правовые рамки, которые обеспечат неприкосновенность личной жизни как одну из основ демократического сообщества.

Выводы. Рассмотрены цифровые возможности обеспечения функций государства в интернет-сегменте, которые относятся к идентификации и аутентификации пользователей при их доступе к государственным облачным

структурам. Кроме того, следует отметить, что вопрос также актуален для зон социальных отношений нового поколения, которые оформились в отдельную общественную структуру в последние десятилетия. С целью организации SSO, предложена модель идентификации и предоставления доступа в сервисных подсетях «облачного» типа с единым входом благодаря «сквозным» вычислениям с использованием адаптивных методик идентификации. При этом учтено, что рассматриваемые подсети являются частным случаем более широкого класса систем, так как конвергентная инфраструктура подразумевает «бесшовную» архитектуру.

Предложенный подход связанных данных о пользователях на основе эндо- и экзопаттернов, с учётом результатов из [5], могут унифицировать процесс идентификации в сервисных подсетях и свести его к определенным SLA-запросам в сервис-ориентированной архитектуре. Это позволит применить его в государственных подсетях, где развиваются новые модели доставки сервисов: Government to Citizens & Citizens to Government, Government to Businesses & Businesses to Government, Government to Employees, Government to Government. Подход может быть применён для сетевых е-паспортов пользователей.

Список литературы: 1. The Hyperconnected World: A New Era of Opportunity, White Paper, Akamai [Электронный ресурс] // Портал : akamai.com. – Режим доступа \www/ URL: http://www.akamai.com/dl/akamai/hyperconnected_world.pdf. – Заглавие с контейнера, доступ свободный, 13.12.2013. 2. Зеленцова, Ж. Ю. Конвергенция глобальной сети как новый этап развития: обзор инфраструктурных решений и технологий с целью нахождения решений для повышения безопасности обработки данных при облачных вычислениях [Текст] / Ж. Ю. Зеленцова, Н. Ф. Казакова // Інформаційна безпека. — 2013. — № 4 (12). — С. 23-40. 3. Зеленцова, Ж. Інфраструктурні рішення та технології підвищення безпеки обробки даних при хмарних обчисленнях [Текст] / Ж. Зеленцова, Н. Казакова // Захист інформації і безпека інформаційних систем : III міжнар. наук.-техн. конф., 5-6 червня 2014 р. : матер. конф. — Львів, НУ «Львівська політехніка. — С. 58-59. 4. Луговой, А. В. Эра мегаданных. Состояние и эволюция мирового информационно-вычислительного пространства [Текст] / А.В. Луговой А.В, Ж.Ю. Зеленцова, О.В. Луговая // Вісник Кременчуцького національного університету імені Михайла Остроградського. – 2012. – Вип.1/2012 (72). Часть 1. – С.36-42. 5. Зеленцова, Ж. Ю. Исследование особенностей организации систем единого входа. часть 1: модель представления данных и идентификации в сервисных подсетях [Текст] // Ж. Ю. Зеленцова, Е. О. Йона // Вісник національного технічного університету "ХПІ". — 2014. — № 40(1083). — С. 66-74. 6. Global Internet Traffic Projected to Quadruple by 2015, Press Release, Cisco, 2011 [Электронный ресурс] // Портал : cisco.com. – Режим доступа \www/ URL: <http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003>. – Заглавие с экрана, доступ свободный, 26.09.2013. 7. Internet of things: \$8.9 trillion market in 2020, 212 billion connected things, ZDNet, October 3, 2013 [Электронный ресурс] // Портал : zdnet.com. – Режим доступа \www/ URL: <http://www.zdnet.com/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things-7000021516/>. – Заглавие с экрана, доступ свободный, 12.12.2013. 8. Florentine Sh., Olavsrud Th. Forecast for Cloud Computing, CIO, December 2013 [Электронный ресурс] // Портал : cio.com. – Режим доступа \www/ URL: http://www.cio.com/article/745155/2014_Forecast_for_Cloud_Computing. – Заглавие с экрана, доступ свободный, 18.03.2014. 9. Identity management solution that automates and streamlines access governance [Электронный ресурс] // Портал : Dell. – Режим доступа \www/ URL: <http://software.dell.com/products/identity-manager/>. – Заглавие с экрана, доступ свободный, 30.12.2013. 10. Cser An., Maler E., Balaouras St., Belanger H. The Forrester Wave™: The Forrester Wave™: Identity And Access Management Suites, Q3 2013 [Электронный ресурс] // Портал : forrester.com. – Режим доступа \www/ URL:

<http://www.forrester.com/The+Forrester+Wave+Identity+And+Access+Management+Suites+Q3+2013/fulltext/-/E-RES99281>. – Заглавие с контейнера, доступ платный, 16.03.2014. **11.** Haggard J. History of SSO - a perspective from the original front lines, SingleSign-OnSummit, 2008 [Электронный ресурс] // Портал : [ssosummit.com](http://www.ssosummit.com). – Режим доступа \www/ URL: <http://www.ssosummit.com/ssosummit/upload/2008-SSOSummit-John-Haggard-Presentation.pdf>. – Заглавие с контейнера, доступ свободный, 18.03.2014. **12.** Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ от 30 марта 1992 г. [Электронный ресурс] // Портал : ФСТЭК. – Режим доступа \www/ URL: <http://fstec.ru/component/content/article/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g>. – Заглавие с экрана, доступ свободный, 28.12.2013. **13.** Казакова, Н. Ф. Автоматизация процессу адаптации информационных систем до инцидентов информационной безопасности [Текст] / Н. Ф. Казакова, С. В. Вавилов // Информационная безопасность. — Луганськ : СНУ ім. В. Даля. — 2013. — №4(12). — С. 49-56. — ISSN 2224-9613.

Bibliography (transliterated): **1.** The Hyperconnected World: A New Era of Opportunity, White Paper, Akamai. http://www.akamai.com/dl/akamai/hyperconnected_world.pdf. **2.** Zelencova, Zh. Ju., Kazakova, N. F. (2013). Konvergencija global'noj seti kak novyj jetap razvitija: obzor infrastrukturyh reshenij i tehnologij s cel'ju nahozhdenija reshenij dlja povyshenija bezopasnosti obrabotki dannyh pri oblachnyh vychislenijah. Informacijna bezpeka, 4 (12), 23-40 (in russian). **3.** Zelencova, Zh. Ju., Kazakova, N. F. (2014). Infrastrukturi rishennja ta tehnologii pidvishhennja bezpeki obrobki danih pri hmarnih obchislennjah. Zahist informacii i bezpeka informacijnih sistem, Ukraine, Lviv, National University «Lviv Polytechnic», 2014.06.06, proc. of conf., 58-59 (in ukrainian). **4.** Lugovoj, A. V., Zelencova, Zh. Ju., Lugovaja, O. V. (2012). Jera megadannyh. Sostojanie i jevoljucija mirovogo informacionno-vychislitel'nogo prostranstva. Visnyk Kremenchuc'kogo nacional'nogo universytetu imeni Myhajla Ostrogradskogo, 1 (72), v. 1, 36-42 (in russian). **5.** Zelencova, Zh. Ju., Jona, E. O. (2014). Issledovanie osobennostej organizacii sistem edinogo vhoda. Chast' 1: Model' predstavlenija dannyh i identifikacii v servisnyh podsetjah (2014). Visnik nacional'nogo tehničnogo universitetu "HPI", 40 (1083), 66-74 (in russian). **6.** Global Internet Traffic Projected to Quadruple by 2015, Press Release, Cisco, 2011. <http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003>. **7.** Internet of things: \$8.9 trillion market in 2020, 212 billion connected things, ZDNet, October 3, 2013. <http://www.zdnet.com/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things-7000021516/>. **8.** Florentine, Sh., Olavsrud, Th. Forecast for Cloud Computing, CIO, December 2013. http://www.cio.com/article/745155/2014_Forecast_for_Cloud_Computing. **9.** Identity management solution that automates and streamlines access governance. <http://software.dell.com/products/identity-manager/>. **10.** Cser, An., Maler, E., Balaouras, St., Belanger, H. The Forrester Wave™: The Forrester Wave™: Identity And Access Management Suites, Q3 2013. <http://www.forrester.com/The+Forrester+Wave+Identity+And+Access+Management+Suites+Q3+2013/fulltext/-/E-RES99281>. **11.** Haggard, J. History of SSO – a perspective from the original front lines, SingleSign-OnSummit, 2008. <http://www.ssosummit.com/ssosummit/upload/2008-SSOSummit-John-Haggard-Presentation.pdf>. **12.** Avtomatizirovannye sistemy. Zashchita ot nesankcionirovannogo dostupa k informacii. Klassifikacija avtomatizirovannyh sistem i trebovanija po zashchite informacii. Rukovodjashchij dokument ot 30 marta 1992 g. <http://fstec.ru/component/content/article/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g> (in russian). **13.** Kazakova, N. F., Vavilov, Je. V. (2013). Avtomatyzacija procesu adaptacii informacijnyh sistem do incydentiv informacijnoi' bezpeky. Informacijna bezpeka, 4(12), 49-56 (in ukrainian).

Надійшла (received) 10.10.2014