

**Список літератури:** 1. Кочнев, Ф. П. Управление эксплуатационной работой железных дорог: Учеб. пособие для вузов [Текст] / Ф. П. Кочнев, И. Б. Сотников. – М.: Транспорт, 1990. – 424 с. 2. Лаврухін, О. В. Формування критерію безпеки для оцінки транспортної події – прийняття поїзда на зайняту колію [Текст] / О. В. Лаврухін // Інформаційно-керуючі системи на залізничному транспорті. Науково-технічний журнал. – 2011. – Вип. 2. – С. 102–108. 3. Орловский, С. А. Игры в нечётко определённой обстановке [Текст] / С. А. Орловский // Ж.: вычисл. матем. и матем. физ. – 1976. – Вип. 16. – С. 1427–1435. 4. Орловский, С. А. Проблемы принятия решений при нечёткой исходной информации [Текст] / С. А. Орловский. – М.: Наука. Главная редакция физико-математической литературы, 1981. – 208 с. 5. Орловский, С. А. Об одной задаче принятия решений в нечётко определённой обстановке [Текст] / С. А. Орловский. – Вопросы прикладной математики. – Иркутск, 1976. – 208 с. 6. Mamdani, E. H. Advances in the linguistic synthesis of fuzzy controllers [Text] / E. H. Mamdani // Int. J. of Man – Machine Studies. – 1976. – Vol. 8. – P. 669–678. 7. Лаврухін, О. В. Формування моделей і методів інтелектуальної автоматизованої технології оперативного планування та управління поїздопотоками [Текст] / О. В. Лаврухін // Тези 74-ї міжнародної науково-практичної конференції УкрДАЗТ. – 2012. – Вип. 129. – С. 258. 8. Zadeh, L. A. Fuzzy orderings [Text] / L. A. Zadeh. – Inf. Sci. – 1971. – Vol. 3. – P. 177–200. 9. Zadeh, L. A. Fuzzy logic and approximate reasoning [Text] / L. A. Zadeh // Synthese. – 1975. – Vol. 80. – P. 407–428. 10. Мелихов, А. Н. Ситуационные советующие системы с нечёткой логикой [Текст] / А. Н. Мелихов, Л. С. Бернштейн, С. Я. Коровин. – М.: Наука. Гл. ред. Физ.-мат.-лит., 1990. – 272 с.

**Bibliography (transliterated):** 1. Kochnev, F. P., Sotnikov, I. B. (1990). Upravlenie jekspluatacionnoj rabotoj zheleznyh dorog: Ucheb. posobie dlja vuzov. Moscow: Transport, 424. 2. Lavruhin, O. V. (2011). Formuvannja kriteriju bezpeki dlja ocinki transportnoj podii – priijnattja poizda na zajnjatu koliju. Informacijno-kerujuchi sistemi na zaliznichnomu transporti. Naukovo-tehnichnij zhurnal, 2, 102–108. 3. Orlovskij, S. A. (1976). Igry v nechjotko opredeljonnoj obstanovke. Zh.: vychisl. matem. i matem. fiz., 16, 1427–1435. 4. Orlovskij, S. A. (1981). Problemy prinjatija reshenij pri nechjotkoj ishodnoj informacii. Moscow: Nauka. Glavnaja redakcija fiziko-matematicheskoy literatury, 208. 5. Orlovskij, S. A. (1976). Ob odnoj zadache prinjatija reshenij v nechjotko opredeljonnoj obstanovke. Voprosy prikladnoj matematiki. Irkutsk, 208. 6. Mamdani, E. H. (1976). Advances in the linguistic synthesis of fuzzy controllers. Int. J. of Man – Machine Studies, 8, 669–678. 7. Lavruhin, O. V. (2012). Formuvannja modelej i metodiv intelektual'noj avtomatizovanoj tehnologii operativnogo planuvannja ta upravlinnja poizdopotokami. Tezi 74 mizhnarodnoi naukovo-praktichnoi konferencii UkrDAZT, 129, 258. 8. Zadeh, L. A. (1971). Fuzzy orderings. Inf. Sci., 3, 177–200. 9. Zadeh, L. A. (1975). Fuzzy logic and approximate reasoning. Synthese, 80, 407–428. 10. Melihov, A. N., Bernshtejn, L. S., Korovin, S. Ja. (1990). Situacionnye sovetujushhie sistemy s nechjotkoj logikoj. Moscow: Nauka. Gl. red. Fiz.-mat.-lit., 272.

*Надійшла (received) 25.08.2014*

**УДК 004.32; 004.48; 004.45; 004.82**

**Ж. Ю. ЗЕЛЕНЦОВА**, инженер, ОНЭУ, Одесса;  
**Е. О. ЙОНА**, соискатель, ОНЭУ

## **ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ОРГАНИЗАЦИИ СИСТЕМ ЕДИНОГО ВХОДА. ЧАСТЬ 1: МОДЕЛЬ ПРЕДСТАВЛЕНИЯ ДАННЫХ И ИДЕНТИФИКАЦИИ В СЕРВИСНЫХ ПОДСЕТЯХ**

С ростом количества сервисов в глобальной сети возникает необходимость их агрегации. Показано, что существует несколько подходов «бесшовного» объединения сервисов в пользовательском сегменте сети. Отмечено, что остается открытым вопрос организации единого доступа к сетевым сервисам. Обосновывается необходимость введения систем идентификации и обеспечения доступа с единым входом. Рассмотрена модель представления данных, что сочетает фиксацию сведений о пользователях, их устройствах и действиях в глобальной сети.

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

© Ж. Ю. ЗЕЛЕНЦОВА, Е. О. ЙОНА, 2014

**Введение.** Глобальная вычислительная среда становится все более разнообразной по количеству предоставляемых сервисов. В результате возникает необходимость их интеграции в рамках единой пользовательской платформы, подразумевающей поддержку единого входа. В рамках этой проблемы нужно рассматривать архитектурные особенности интеграционных систем, т.к. существует ряд ограничений и требований безопасности, которые должны быть учтены при разработке сервисов идентификации. Также интенсивно развивается сетевая инфраструктура, что подразумевает изменение и архитектурных принципов.

**Цель работы.** Целью работы является обоснование систем идентификации и обеспечения доступа с единым входом (англ.: *Single Sign-On* [SSO]), адаптированных к текущим особенностям сервисных систем. Такие системы предложены целым рядом производителей и готовятся к повсеместному использованию.

**Результаты исследования: модели идентификации и представления персональной информации в мультисервисных системах.** Технология единого входа SSO – одна из технологий, относящихся к широкому классу систем управления идентификацией и доступом пользователей (англ.: *Identity management and access* [IAM]). Основное отличие технологии SSO 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 систем при текущих признаках цифровой вселенной (англ.: *Digital Universe*) – при росте количества пользователей, устройств, данных, а также при расширении сервисных возможностей сети.

Предлагаемая здесь к анализу тема рассматривалась в рамках задачи организации единого входа в сервисной подсети [2]. Как подчеркивается в [2-5], для современной сетевой инфраструктуры свойственно большое количество пользователей, устройств и данных. Стремительно растет количество низкопроизводительных устройств типа Internet of Things (IoT) или «интернет-вещей». По версии IDC, количество уникальных подключений в 2020 году достигнет 212 млрд. [6]. Нарастание количества подключений будет происходить в четырех сервисных сегментах: *мобильных технологий, медиа, «облачных» сервисов и средств безопасности*. Также в своем отчете компания Akamai, подчеркивает необходимость разработки hyper-connected платформ, ориентированных на обслуживание большого количества уникальных подключений, которое будет характерно для сервисных платформ в среднесрочной перспективе [1].

Относительно сегментации пользователей, эксперты отмечают последующую сегментацию сервисных сетей, что подразумевает формирование различий в восприятии потребителей между государственными, «облачными» и частными внедрениями [7]. Т. о., исследование процесса развития направления сервисных подсетей, агрегирующих определенное количество сервисов, работающих с большим количеством пользователей посредством устройств и генерирующих данные, является актуальным и востребованным.

Архитектурные особенности мультисервисной платформы, о которой ведется речь, отмечены на рис. 1.

Как следует из рис. 1 и показано в [3-5], платформа имеет сервис-ориентированную архитектуру (англ.: *Service-Oriented Architecture* [SOA]). Она представляет собой набор высокопроизводительных и низкопроизводительных ресурсов, объединенных между собой посредством слоя виртуализации разных интеграционных уровней. Зона высокопроизводительных ресурсов объединена с зоной низкопроизводительных ресурсов (устройствами пользователей) с помощью слоя сопряжения – «облачного» слоя. Каждое облако является отдельным сервисом или представляет собой платформу сервисов PaaS. Сервисы между собой взаимно-интегрированы с помощью технологии программно-конфигурируемых сетей (англ.: *Software-defined Networking* [SDN]) с топологией «cloud-to-cloud». Подсеть предусматривает интеграцию сервисов-«облаков» в один интерфейс, которые могут быть слабосвязными. При этом обеспечивается

«бесшовное» подключение сервисов различных поставщиков решений. Сервисы-«облака» предоставляют услуги конечному пользователю посредством интеграционного интерфейса пользователя и подключаются по типу Plug-In. Для подключения большого количества сервисов запросы унифицированы по принципу SLA-запросов (англ.: *Service Level Agreement* [SLA]).

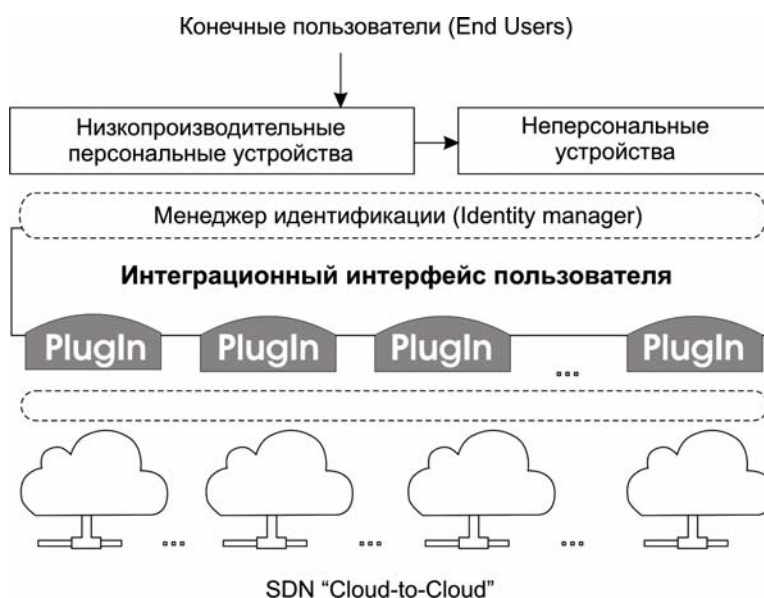


Рис. 1 – Архитектура сервисной подсети «облачного» типа

Интеграционная сервисная платформа с приведенной архитектурой может управлять идентификацией и доступом с помощью менеджера идентификации (англ.: *Identity Manager*), основанного на технологии единого входа SSO и обеспечивающего идентификацию пользователя в различных сервисных составляющих, подключенных к подсети (рис. 1). Решение, касающееся менеджера идентичностей, использовано из Dell One Identity [8].

В совокупности системы управления идентификацией (англ.: *Identity-Management Systems*) управляют процессом цифровой идентификации устройств посредством выявления данных о пользователях с помощью аппаратных и программных методов. Сам процесс идентификации может значительно отличаться в зависимости от архитектурных особенностей сетевых сред, а проектирование систем доступа должно учитывать архитектурные особенности и технологические тренды, предполагающие изменения процесса доступа к сервисным платформам.

Процесс управления учетными записями и доступом IAM классически состоит из нескольких подпроцессов [9]:

– управления идентификацией и учетными записями (англ.: *Identity Management* [IdM]), состоящего из управления жизненным циклом идентичностей и администрирования учетных записей;

– управления доступом (англ.: *Access Management* [AM]), состоящего из аутентификации [AuthN] и авторизации [AuthZ];

– контроллинга, управления рисками и соответствия требованиям (англ.: *Governance, Risk and Compliance* [GRC]), состоящего из сбора информации для аудита, отчета о действиях (Actionable reports), оценки и контроля рисков (Risk Management), соответствия государственным и корпоративным стандартам (Compliance).

Существует целый ряд технологий, которые могут быть использованы как составляющие систем IAM. Так, это: системы контроля доступа (англ.: *Access Control*); цифровые удостоверения (англ.: *Digital Identities*); менеджеры паролей (англ.: *Password Managers*), агрегирующие пароли разных систем и обеспечивающие «быстрый» доступ с идентифицированных устройств; системы единого входа (англ.: *Single Sign-on*); маркеры безопасности (англ.: *Security Tokens*), система глобальной идентификации OpenID.

Идентификация в теоретических и практических моделях строится на получении некоторой модели с набором идентифицирующих атрибутов [10]. К идеальным моделям относят модель «чистой идентичности» (англ.: *Pure Identity*). На практике обычно рассматривают только некоторые аспекты идентичности в рамках построенной агрегирующей семантической модели – такой подход не подразумевает совпадение полного набора параметров.

Семантическая модель, в свою очередь, состоит из внешних и внутренних паттернов. Модель «чистой идентичности» связана только внутренними паттернами, т. е. не зависит от работы приложения в котором проходит идентификация и других факторов. На практике применяются несколько моделей определения идентичности, обеспечивая разброс параметров. В результате снижается погрешность распознавания при выполнении условий упрощения доступа.

В рамках глобальных платформ, о которых идет речь [3-5], рассматривается сетевой сервис OpenID, обеспечивающий единую идентификацию пользователей в социальных средах: в качестве основного атрибута идентификации выступает адрес электронной почты – e-mail. Этот адрес является основным идентификатором в социальных сетях: идентификация не подразумевает полной персональной идентичности личности. Для критически важных приложений имеются специализированные базы, включая базу персональной информации (англ.: *Personal identifying information* [PII]), созданную в США на основе официальных данных и используемую системами идентификации с высоким уровнем доверия. В других странах существуют Единые реестры или другие подобные структуры, которые подразумевает всю совокупность национальных данных с целью использования в электронных приложениях, прежде всего, связанных с сервисами госуслуг.

Очевидно, что любая сервисная подсеть подразумевает регистрацию пользователей. Обычно основным идентификатором является e-mail пользователя, но это не исключает применение дополнительных методов «скрытой

идентификации», упрощающей процесс распознавания. Современная электронная система должна обеспечить одновременно интуитивную простоту регистрации и предполагать минимальный объем вводимых данных при условии максимально полной идентификации пользователей – так называемый интеллектуальный доступ к сервисам. При описании такой модели идентификации предполагается, что именно внешний паттерн идентификации будет иметь большое значение в определении идентичности пользователя. Подход наиболее применим для систем, где пользователь должен сам заботиться о безопасности персональных данных, а система выполняет только надзорную роль. В критически важных системах функция безопасности в полной мере отслеживается системой: применяются, например, цифровые удостоверения и биометрические данные, поэтому внешние паттерны идентификации имеют второстепенное значение.

Понятие персональной информации определяет стандарт NIST Special Publication 800-122 – подразумевается «любая информация, которая помогает отличить или проследить личность человека – такая как: имя, номера кредитных карт, идентификационные номера или номера социального страхования, дата и место рождения, фамилия матери, биометрические данные, а также сопряженная информация медицинского, образовательного, финансового и квалификационного характера» [11]. В России и Украине использование персональных данных, в соответствии с законами о персональных данных (в Украине – Закон «О защите персональных данных» от 01.06.2010, №2297-VI, в России – Закон РФ «О персональных данных» от 26.06.2006, №152-ФЗ) предполагает ведение соответствующего реестра пользователей, что создает определенные сложности для каждой отдельной фирме и создает прецедент создания государственного сервиса единого реестра идентификации со скрыванием данных о пользователях.

В контексте идентификации в сервисных подсетях и развитии систем глобальной идентификации необходимо упомянуть о двух понятиях, описывающих новые типы сетевых данных. Речь идет о *цифровом следе* (англ.: *Digital Footprint*) и о *цифровой тени* (англ.: *Digital Shadow*). Эти данные возникают в результате активных и пассивных действий пользователя в электронных сервисах [12]. Поэтому они могут быть включены в множество «связных» персональных данных неофициального характера – внешние паттерны идентификации. Фактически все данные о пользователях в сети могут быть консолидированы, представлены в виде метаданных и, впоследствии, использованы в качестве атрибутов идентификации и внешних паттернов персональной идентификации в глобальных системах.

Такой подход – введение метаданных пользователей – потребует особого формата организации данных, по своей логике отличных от классического представления данных в SQL, возможностей процедурного расширения PLPG SQL, а также методов хранения в реляционных хранилищах. В целом, на основании внешних и внутренних паттернов идентификации может быть создана модель *цифрового паспорта* человека (англ.: *Digital Passport* или *E-Passport*), включающая в себя целый набор образцов для идентификации и видов слабосвязных данных внешних паттернов, которые могут быть отнесены к определенной персоне.

Идея введения E-Passport не нова. Аппаратная реализация электронных паспортов активно применяется в Великобритании и ЕС. Они выдаются в Великобритании с 2006 года и представляют собой информацию о персоне и машиносчитываемую биометрическую фотографию [13]. В некоторых странах применяются автоматизированные полосы паспортного контроля, которые фиксируют передвижения владельцев электронных паспортов ЕС: это классический пример создания «цифровой тени» человека при консолидации данных.

Используемая в Великобритании технология NM Passport отличается от технологической реализации, требующейся при проведении идентификации в глобальных сетевых платформах и сервисных подсетях с высоким уровнем доверия. Наличие такого чипа обеспечивает установление условно-полной идентичности, но исключает связывание сетевых персональных, косвенных данных и устройств пользователя. Новые подходы, подразумевающие связывание данных, пользователей и устройств, требуются в глобальной сети, в том числе, для решения проблемы больших данных (англ.: *Big Data*) и для *реализации основополагающей функции* государства – *охрана правопорядка*, также предполагающую правоохранительную деятельность в социально-общественных средах, к которым относится Интернет. Связывание позволяет одновременно уменьшить полезную емкость цифровой вселенной (англ.: *Digital Universe*) [13] и отслеживать действия пользователей в сети с целью правового контроля.

По сути, рассматривая связные данные о пользователе, имеющие персональный характер, в рамках некоторого массива метаданных, называемого Е-Паспортом, говорится о процессе виртуализации пользователей, который может быть рассмотрен не только в рамках идентификации. В данном случае должны быть затронуты новые технологические решения. Речь идет о дополненной, смешанной и виртуальной реальности. Очевидно, что массив данных о пользователе может быть структурно расширен, иметь публичную и непубличную зону данных. Эти данные могут поддаваться коррекции при условии соответствия уровня мандатного доступа к редактируемому массиву.

В рамках решения предлагается использовать модель iGenotype, связывающую устройства и данные с владельцем. Этот подход, предполагающий связывание данных, устройств и пользователей, может быть согласован с моделями доставки сервисов (англ.: *Delivery Models*), упоминаемых компанией Cisco, позволяющими унифицировать пользовательские запросы и обрабатывать их в составе SLA-запросов (англ.: *Service Level Agreement* [SLA]): «пользователь-пользователь» – People-to-People (P2P), «машина-машина» – Machine-to-Machine (M2M), «пользователь-машина» – People-to-Machine (P2M) (рис. 2).

Унификация запросов, снижает сложность любой сервисной системы, а также позволяет описать процесс предоставления сервисов в рамках современного подхода доставки сервисов по SLA-запросам. С целью дальнейшего анализа, представим это в виде математических описаний так, как это представлено ниже.

Задача идентификации и управления доступом IAM в сервисной подсети описывается целевой функцией  $IAM(\cdot)$ . Область определения системы задается входными (набором атрибутов идентификации и доступа) и выходными данными

$X_n \times S_n \subseteq Z$  при наборе ограничений  $g_n$ . На выходе функциональной группы получаем множество состояний системы  $\{s_n\}$ .

Система IAM может быть представлена в качестве оупорядоченного кортежа длины «3»:

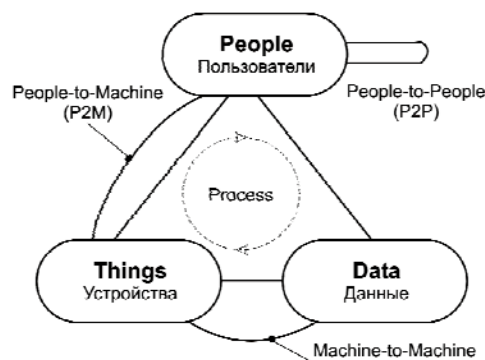
$IAM : \langle IdM, AM, GRC \rangle$  при условии, что  $IAM : IdM \rightarrow AM \rightarrow GRC$  условию. Для  $IdM$  существует набор атрибутов идентификации  $A = \{a_i\}$ , формирующих набор нечетких правил-паттернов идентификации  $\{\tilde{p}(a_i)\}$ .

Задачу идентификации пользователей подсети можно разбить на две части: идентификацию по внешним и по внутренним атрибутам:  $IdM(t+1) = IdM_{endo} + IdM_{ekzo}(t)$ . Эндонаттерн относится к неизменным атрибутам идентификации, экзонаттерн зависит от времени. Таким образом, информационная емкость эндонаттерна (состоит из официальных, биометрических и др. неизменных данных) будет постоянной  $C_{Pendo}^U = const$ , информационная емкость экзонаттерна (цифровая тень и след) изменяется в зависимости от сетевой активности пользователей  $C_{Pekzo}^U(t+1) \neq C_{Pekzo}^U(t)$ . После идентификации  $IdM$  система должна предоставить доступ (выполнить процесс  $AM$ ) к ресурсам подсети, которые разделим на зону публичных сервисов и зону персональных сервисов. Так как каждому процессу  $IdM$  соответствуют определенные процессы  $AM$  (предоставления доступа) и  $GRC$  (контроллинга рисков), можно говорить о двухэтапном процессе  $IdM / AM / GRC$  в подсети  $IAM = IAM_{pub} + IAM_{pers}$ .

**Выводы.** Рассмотрены цифровые возможности обеспечения одной из функций государства в интернет-сегменте – охрана правопорядка. Речь идет о зонах социальных отношений нового поколения, которые оформились в отдельную общественную структуру в последние десятилетия. При этом рассмотрена модель представления данных, которая будет сочетать в себе фиксацию данных о пользователях, их устройствах и действиях в глобальной сети наряду с сохранением конфиденциальности персональной информации и защитой частной жизни. Предложен подход, который позволяет создать защищенные государственные депозитарии связанных официальных и неофициальных данных о сетевых пользователях, а также избавиться от необходимости особого режима обработки персональных данных для каждой отдельной организации, на сегодняшний день нормированного законодательно. Рассмотрен один из вариантов решения проблемы больших данных с использованием модели



Модель консолидации данных о пользователях Network Cloud Cube-2



Модель доставки сервисов Cisco

Рис. 2 – Модель iGenotype и новые модели доставки сервисов [14, 15]

iGenotype связывания данных в сети, так как в этом случае снижается информационная емкость за счет сокращения объема неструктурированной информации. Предложен метод двухэтапной идентификации на основе эндо- и экзопаттерна в публичную и доверенную зоны сервисных подсетей. Такой подход может быть применен в ряде сервисов электронных госуслуг для обеспечения высокого уровня безопасности, и в развлекательных сервисных подсетях – для монетизации отдельных развлекательных сегментов. Предложена модель связывания данных, которая предполагает расширение ряда унифицированных SLA-запросов в контексте развиваемых моделей доставки сервисов (People-to-People [P2P], Machine-to-Machine [M2M], People-to-Machine [P2M]).

**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](http://www.akamai.com/dl/akamai/hyperconnected_world.pdf). — Заглавие с контейнера, доступ свободный, 13.12.2013. 2. 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. 3. 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. 4. 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. 5. Казакова, Н. Ф. Дослідження та застосування в системах захисту інформації кореляційного критерію подібності графічних структур [Текст] / Н. Ф. Казакова., О. О. Фразе-Фразенко // Системи обробки інформації. — 2014. — Т. 2, № 2(118). — С. 246. 6. 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. 7. Florentine, Sh. Forecast for Cloud Computing, CIO, December 2013 [Электронный ресурс] / Sh. Florentine, Th. Olavsrud // Портал : cio.com. — Режим доступа \www/ URL: [http://www.cio.com/article/745155/2014\\_Forecast\\_for\\_Cloud\\_Computing](http://www.cio.com/article/745155/2014_Forecast_for_Cloud_Computing). — Заглавие с экрана, доступ свободный, 18.03.2014. 8. 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. 9. Shapiro, VI. Решение Dell One Identity – от менеджмента идентичностей до управления и контроля доступа, Dell Security Software – IAM [Электронный ресурс] / VI. Shapiro // Портал : eiseverywhere.com. — Режим доступа \www/ URL: [https://www.eiseverywhere.com/file\\_uploads/ba9e74372c8f2370ab447b10810122a6\\_DellOneIdentitySolution-Russian\\_1\\_v3.pdf](https://www.eiseverywhere.com/file_uploads/ba9e74372c8f2370ab447b10810122a6_DellOneIdentitySolution-Russian_1_v3.pdf). — Заглавие с экрана, доступ свободный, 18.02.2014. 10. Казакова, Н. Ф. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки [Текст] / Н. Ф. Казакова, Е. А. Плешко, К. Б. Айвазова // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2013. — Т. 1, № 15(204). — С. 172-181. 11. McCallister, Er. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Recommendations of the National Institute of Standards and Technology, Special Publication 800-122, NIST, April 2010 [Электронный ресурс] / Er. McCallister, T. Grance, K. Scarfone // Портал : csrc.nist.gov. — Режим доступа \www/ URL: <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>. — Заглавие с контейнера, доступ свободный, 16.03.2014. 12. Луговой, А. В. Эра мегаданных. Состояние и эволюция мирового информационно-вычислительного пространства [Текст] / А. В. Луговой, Ж. Ю. Зеленцова, О. В. Луговая // Вісник Кременчуцького

національного університету імені Михайла Остроградського. — 2012. — Т. 1, № 1/2012 (72). — С. 36-42. **13.** HM Passport Office [Электронный ресурс] // Портал : gov.uk. — Режим доступа \www/ URL: <https://www.gov.uk/government/organisations/hm-passport-office>. — Заглавие с экрана, доступ свободный, 30.01.2014. **14.** Модель iGenotype – виртуализация устройств, данных и пользователей [Электронный ресурс] // Портал : network-cloud-cube-2.ru. — Режим доступа \www/ URL: <http://www.network-cloud-cube2.ru/model-igenotype>. — Заглавие с экрана, доступ свободный, 28.03.2014. **15.** 2013 Cisco Annual Security Report, Cisco [Электронный ресурс] // Портал : cisco.com. — Режим доступа \www/ URL: [https://www.cisco.com/web/offer/gist\\_ty2\\_asset/Cisco\\_2013\\_ASR.pdf](https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf). — Заглавие с контейнера, доступ свободный, 13.12.2013.

**Bibliography (transliterated):** **1.** The Hyperconnected World: A New Era of Opportunity, White Paper, Akamai. [http://www.akamai.com/dl/akamai/hyperconnected\\_world.pdf](http://www.akamai.com/dl/akamai/hyperconnected_world.pdf). **2.** Global Internet Traffic Projected to Quadruple by 2015, Press Release, Cisco, 2011. <http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003>. **3.** 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). **4.** Zelencova, Zh. Ju., Kazakova, N. F. (2014). Infrastrukturni 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). **5.** Kazakova, N. F., Frazefrazenko, O. O. (2014). Doslidzhennja ta zastosuvannja v systemah zahystu informacii' koreljacijnogo kryteriju podobnosti grafichnyh struktur. Systemy obrobky informacii', 2(118), v. 2, 246 (in ukrainian). **6.** 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/>. **7.** Florentine, Sh., Olavsrud, Th. (2014). Forecast for Cloud Computing, CIO, December 2013 [http://www.cio.com/article/745155/2014\\_Forecast\\_for\\_Cloud\\_Computing](http://www.cio.com/article/745155/2014_Forecast_for_Cloud_Computing). **8.** Identity management solution that automates and streamlines access governance. <http://software.dell.com/products/identity-manager/>. **9.** Shapiro, Vl. Reshenie Dell One Identity – ot menedzhmenta identichnostej do upravlenija i kontrolja dostupa, Dell Security Software – IAM. [https://www.eiseverywhere.com/file\\_uploads/ba9e74372c8f2370ab447b10810122a6\\_DellOneIdentitySolution-Russian\\_1\\_v3.pdf](https://www.eiseverywhere.com/file_uploads/ba9e74372c8f2370ab447b10810122a6_DellOneIdentitySolution-Russian_1_v3.pdf) (in russian). **10.** Kazakova, N. F., Pleshko, E. A., Ajvazova, K. B. (2013). Mizhnarodna reglamentacija pravovogo reguljuvannja ta standartyzacii' audytu informacijnoi' bezpeky. Visnyk Shidnoukrai'ns'kogo nacional'nogo universytetu imeni Volodymyra Dalja, 15(204), v. 1, 172-181 (in ukrainian). **11.** McCallister, Er., Grance, T., Scarfone, K. (2014). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Recommendations of the National Institute of Standards and Technology, Special Publication 800-122, NIST, April 2010. <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>. **12.** Lugovoj, A. V., Zelencova, Zh. Ju., Lugovaja, O. V. (2012). Jera megadannyh. Sostojanie i jevoljucija mirovogo informacionno-vychislitel'nogo prostranstva. Visnik Kremenchuc'kogo nacional'nogo universytetu imeni Mihajla Ostrograds'kogo, 1/2012 (72), v. 1, 36-42. **13.** HM Passport Office. <https://www.gov.uk/government/organisations/hm-passport-office>. **14.** Model' iGenotype – virtualizacija ustrojstv, dannyh i pol'zovatelej. <http://www.network-cloud-cube2.ru/model-igenotype> (in russian). **15.** 2013 Cisco Annual Security Report, Cisco. [https://www.cisco.com/web/offer/gist\\_ty2\\_asset/Cisco\\_2013\\_ASR.pdf](https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf).

Поступила (received) 22.08.2014