

УДК 681.321

Ю. Л. ПОНОЧОВНИЙ<sup>1</sup>, А. А. ФУРМАНОВ<sup>2</sup>, В. С. ХАРЧЕНКО<sup>2</sup><sup>1</sup> *Полтавский национальный технический университет им. Юрия Кондратюка, Украина*<sup>2</sup> *Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина*

## СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ И ТЕНДЕНЦИИ ИХ РАЗВИТИЯ

*Рассмотрен состав и взаимодействие стандартообразующих организаций в сфере облачных технологий. Показано состояние нормативных документов по 10 ключевым направлениям стандартизации информационной безопасности. Определены базовые направления стандартизации в соответствии с категориями облачных услуг. Рассмотрены стандарты, представляющие ролевую модель пользователей участников облачных услуг. Проведен анализ и определены тенденции в развитии стандартов, такие как: расширение спектра облачных услуг, укрупнение категории «безопасность», расширение спектра возможных угроз информации, рост числа стандартообразующих организаций – участников.*

**Ключевые слова:** *облачные технологии, информационная безопасность, стандартообразующие организации, тенденции развития стандартов.*

### Введение. Постановка задачи

Эффективное внедрение современных информационных технологий: Web-, Cloud-, IoT- (Internet of Things) и пр. невозможно без соответствующих нормативных документов, описывающих правовые нормы, проблемы, риски и способы их минимизации. Разработка и внедрение международных стандартов в области безопасности информационных технологий необходимы для повышения доверия к онлайн-операциям, смягчения последствий кибер-инцидентов и обеспечения безопасной совместимости среди торговых партнеров. Такие стандарты особенно важны в современном информационном пространстве, где продукты, процессы и услуги разрабатываются и поставляются по всему земному шару посредством последовательных операций, которые скрывают от потребителя особенности облачной инфраструктуры провайдера. Многие стандарты, которые сегодня вынужденно применяются к облачным вычислениям, были разработаны для «дооблачных» технологий, таких как веб-сервисы, платежные системы. Поэтому идет активная разработка стандартов и руководств, предназначенных для облачных вычислений [1].

Для сферы облачных вычислений особую роль имеют международные стандарты, поскольку потребители и провайдеры облачных услуг часто находятся в разных странах. Во многих странах мира разрабатываются стандарты и руководства, содержащие рекомендации по использованию облачных вычислений, которые опережают по срокам внедре-

ния соответствующие международные стандарты.

Каждый год в открытом доступе появляются новые работы, посвященные обзору и текущему состоянию стандартов в сфере облачных вычислений. В процессе работы над материалом данной статьи были проанализированы источники [1-7]. В отличие от обзорного представления данных работ, **целью данной статьи** является выявление тенденций в развитии стандартов в сфере информационной безопасности облачных вычислений.

На основе анализа проектов и принятых международных и национальных стандартов были выделены тенденции расширения стандартообразующих организаций, видов облачных услуг, участников облачных услуг, угроз информации в облачных технологиях. Также акцентируется внимание на расширение категории «безопасность» в аспекте защиты активов.

### 1. Состав и особенности взаимодействия стандартообразующих организаций в сфере облачных технологий

Согласно существующей классификации стандартообразующих организаций и органы имеют следующую иерархию уровней:

- международный (ISO/IEC [8, 9, 25, 26], ITC [10-18, 27]);
- межгосударственный (форумы и консорциумы [3, 5]);
- региональный (европейские органы ETSI, CEN/CENELEC [4]);

– национальный (государственные законы и стандарты, ведомственные нормативные документы, руководства, инструкции и пр. [2, 6, 24]).

В сфере стандартизации облачных технологий государственные границы теряют ограничительную роль, так как актеры - участники процесса предоставления услуг часто находятся в разных странах, а то и на разных континентах.

В силу актуализации вопросов информационной безопасности и отсутствия международных стандартов по сертификации элементов облачной инфраструктуры, эти элементы (дата-центры, каналы и сети коммуникаций и т.д.) используют сертификаты безопасности стандартов смежных направлений (как международных, так и других стран).

«Ансамбль» международных организаций, которые занимаются стандартами в сфере информационной безопасности [2] представлен на рис. 1. Стоит отметить, что в каждой стране дополнительно существуют региональные организации и ведомства, отвечающие за разработку нормативных документов в сфере информационной безопасности. На рис. 2 представлена схема взаимодействия международных и региональных стандартообразующих организаций в сфере облачных технологий [4].

В табл. 1 приведены реквизиты организаций с указанием адресов их сайтов.

Состояние разработки стандартов по информационной безопасности в сфере Cloud Computing по ключевым 10-ти направлениям проиллюстрировано в табл. 2 [2].

## 2. Стандартизация категорий облачных услуг

Традиционно облачные услуги имеют обозначение «X»aaS («услуга» as a service, «X» как сервис). Изначально облачная парадигма включала три вида услуг [19,20]: IaaS, PaaS, SaaS. В табл.3 даны определения этих услуг согласно различных источников [8,23]. Начиная с 2013 года в стандартах начали фигурировать названия новых видов облачных услуг:

- сеть как услуга (network as a service (NaaS)): категория облачной услуги, в которой возможность, предоставляемая потребителю облачной услуги, относится к возможностям транспортного соединения и связанным с ним сетевым возможностям [18];
- подключение как услуга: вид облачной услуги по предоставлению возможности организации межоблачного взаимодействия между облачными серверами [23].

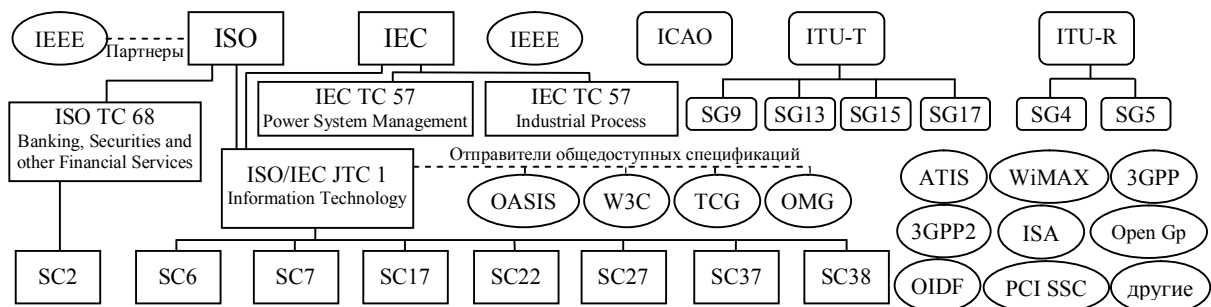


Рис. 1. Международные организации, принимающие участие в разработке международных стандартов в области информационной безопасности облачных технологий

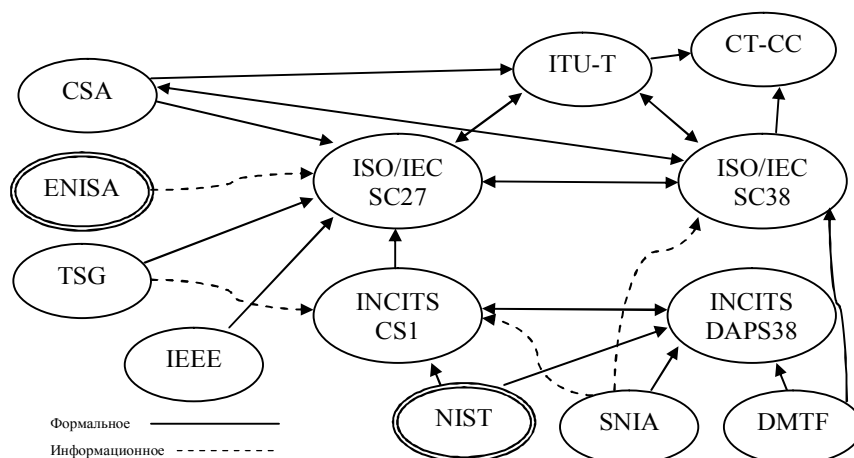


Рис. 2. Схема взаимодействия между региональными и международными стандартообразующими организациями

Таблица 1

Реквизиты стандартообразующих организаций (Standards Developing Organizations, SDO)

SDOs	Полное название организации	Веб-адресс
ISO	International Organization for Standardization Международная организация по стандартизации	http://www.iso.org
IEC	International Electrotechnical Commission Международная электротехническая комиссия	http://www.iec.ch
IETF	Internet Engineering Task Force Открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, занимающееся развитием протоколов и архитектуры Интернет	http://www.ietf.org
ICAO	International Civil Aviation Organization Международная организация гражданской авиации	http://www.icao.int
ITU	International Telecommunication Union Международный союз электросвязи	http://www.itu.int
OASIS	Organization for the Advancement of Structured Information Standards Консорциум, который управляет разработкой, конвергенцией и принятием промышленных стандартов электронной коммерции.	http://www.oasis-open.org
W3C	World Wide Web Consortium Консорциум Всемирной паутины	http://www.w3.org/
TCG	Trusted Computing Group Организация разработки и продвижения стандартов аппаратных и программных средств для обеспечения безопасности компьютерных систем	trustedcomputinggroup.org
OMG	Object Management Group Консорциум, занимающийся разработкой и продвижением объектно-ориентированных технологий и стандартов	http://www.omg.org
ATIS	Alliance for Telecommunications Industry Solutions Альянс для решений телекоммуникационной индустрии	http://www.atis.org/
ISA	International Society of Automation Международная Ассоциация Автоматизации	http://www.isa.org
WiMAX	Worldwide Interoperability for Microwave Access Forum Организация продвижения и развития технологии WiMAX	http://www.wimaxforum.org/
3GPP/3GPP2	3rd Generation Partnership Project Консорциум, разрабатывающий спецификации для мобильной телефонии	http://www.3gpp.org http://www.3gpp2.org
OIDF	OpenID Foundation Открытый стандарт децентрализованной системы аутентификации	http://openid.net
PCI SSC	Payment Card Industry Security Standards Council Совет по стандартам безопасности индустрии платежных карт	http://pcisecuritystandards.org
CSA	Cloud Security Alliance	https://cloudsecurityalliance.org
DMTF	Distributed Management Task Force	https://www.dmtf.org
ENISA	European Network and Information Security Agency	https://www.enisa.europa.eu
ETSI	European Telecommunications Standards Institute	http://www.etsi.org
IEEE	Institute of Electrical and Electronics Engineers Институт инженеров электротехники и электроники	https://www.ieee.org
INCITS	International Committee for Information Technology Standards	http://www.incits.org
NIST	National Institute for Standards and Technology	http://www.nist.gov
SNIA	Storage Networking Industry Association	http://www.snia.org

Таблица 2

Состояние разработки стандартов по информационной безопасности в сфере Cloud Computing

№ п/п	Направление стандартизации	Разработчики стандартов	Состояние для Cloud Computing	Примеры стандартов направления (не Cloud)
1	Cryptographic Techniques криптографические методы	IEEE ISO TC 68 ISO/IEC JTC 1 W3C	Стандарты доступны	ISO/IEC 18033 IEEE 1363 ISO/IEC 29192
2	Cyber Incident Management Управление инцидентами	ISO/IEC JTC 1 ITU-T PCI	Стандарты разрабатываются	ISO/IEC 27035 ITU-T X.1056
3	Identity Management Управление идентификацией	FIDO Alliance IETF; OASIS OIDF ISO/IEC JTC 1 ITU-T; W3C	Стандарты доступны	
4	Information Security Management Systems Системы управления информационной безопасностью	ATIS IEC ISA ISO/IEC JTC 1 OASIS ISO TC 223	Стандарты разрабатываются	ISO/IEC 27000
5	IT System Security Evaluation Оценка информационной безопасности ИТ-систем	ISO/IEC JTC 1	Стандарты разрабатываются	ISO/IEC 19790:2015 ISO/IEC 24759:2014 ISO/IEC TR 30104:2015 ISO/IEC 15408-3
6	Network Security Сетевая информационная безопасность	3GPP; 3GPP; IEC IETF; IEEE ISO/IEC JTC 1 ITU-T WiMAX Forum	Стандарты не разрабатываются	ISA/IEC-62443

Окончание табл. 2

№ п/п	Направление стандартизации	Разработчики стандартов	Состояние для Cloud Computing	Примеры стандартов направления (не Cloud)
7	Security Automation & Continuous Monitoring Автоматизированный и непрерывный мониторинг информационной безопасности	IETF ISO/IEC JTC 1 TCG	Стандарты разрабатываются	
8	Software Assurance гарантированное сопровождение ПО	IEEE ISO/IEC JTC 1 TCG	Стандарты не разрабатываются	ISO/IEC 19770-2
9	Supply Chain Risk Management Управление рисками/цепочками рисков	ISO/IEC JTC 1 The Open Group IEC TC 65	Стандарты разрабатываются	
10	System Security Engineering Система инженерии информационной безопасности	IEC ISA ISO/IEC JTC 1	Стандарты не разрабатываются	ISO/IEC 21827:2008 ISA/IEC-62443

Таблица 3

## Определение базовых видов облачных услуг

Вид услуги	Определение по «Проект ГОСТ» [23]	Определение по ISO17788:2014 [8]
Инфраструктура как услуга (infrastructure as a service (IaaS))	Вид облачной услуги по предоставлению возможности использования части инфраструктуры облачного сервера потребителем услуги для собственных нужд	Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, являются возможности инфраструктуры. Примечание – потребитель облачной услуги не осуществляет контроль или управление в отношении внутренних физических или виртуальных ресурсов, но осуществляет контроль над операционными системами, запоминающими устройствами и развернутыми приложениями, которые используют физические и виртуальные ресурсы. Потребитель облачной услуги может также иметь ограниченную возможность контроля над определенными компонентами сети (например, брандмауэрами хост-компьютеров).
Платформа как услуга (platform as a service (PaaS))	Вид облачной услуги по предоставлению возможности запуска в инфраструктуре облачного сервера собственных программ, созданных в облачной среде разработки для дальнейшего предоставления их в качестве облачной услуги «программное обеспечение как услуга». Примечание: потребителю не предоставляется возможность контроля или управления инфраструктурой облачного сервера.	Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю услуги, являются возможности платформы.
Программное обеспечение как услуга (software as a service (SaaS))	Вид облачной услуги по предоставлению возможности использования прикладного программного обеспечения, размещенного на облачном сервере. Примечание: Потребителю не предоставляется возможность контроля или управления обеспечивающей работу программ облачной инфраструктуры.	Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, являются возможности приложения.

– рабочее место как услуга (desktop as a service (DaaS)): вид облачной услуги по предоставлению возможности использования виртуального рабочего стола, предоставляемого поставщиком облачных услуг по модели аутсорсинга [23].

С принятием в 2014 году международного стандарта ISO17788 [8] регламентировано 7 репре-

зентативных категорий облачных услуг:

- Communications as a Service (CaaS);
- Compute as a Service (CompaaS);
- Data Storage as a Service (DSaaS);
- Infrastructure as a Service (IaaS);
- Network as a Service (NaaS);
- Platform as a Service (PaaS);

– Software as a Service (SaaS).

В приложении А данного стандарта приводится сравнительная таблица, в которой перечислены дополнительные категории облачных услуг:

- Database as a Service;
- Desktop as a Service;
- Email as a Service;
- Identity as a Service;
- Management as a Service;
- Security as a Service;

В проекте национального стандарта [23], помимо перечисленных, представлены также услуги:

- аппаратное обеспечение как услуга (HaaS);
- безопасность как услуга (SecaaS);
- бизнес–процесс как услуга (BPaaS);
- данные как услуга (DaaS);
- доверие как услуга (TaaS);
- облачная среда разработки как услуга (SDPaaS);
- общение как услуга (CaaS);
- подключение как услуга (NaaS);
- прозрачность как услуга (TraaaS);
- рабочее место как услуга (WaaS).

Детальный анализ данных нормативных документов указывает на рассогласование в аббревиатурах (рабочее место как услуга: DaaS в [8, 9, 13] и WaaS в [23]) и названиях (Compute as a Service [8, 10] и Hardware as a Service [23]) одних и тех же услуг. Это связано с рассогласованием времени разработки документов: судя по истории проект национального стандарта был подготовлен в 2013 году, а международный стандарт был официально принят в 2014 г.

В табл. 4 выполнено сведение категорий облачных услуг и стандартов их описывающих, и представленных в хронологическом порядке.

В проекте [23] имеется интересный подпункт (3.31) – Все как услуга: концепция, заключающаяся в предоставлении поставщиком облачных услуг всех возможных видов облачных услуг потребителю, получающему право легитимного использования любой облачной услуги, при наличии только доступа к сети связи общего пользования.

Международный стандарт ISO 17788 [8] также не ограничивает список новых облачных услуг, так что в будущем стоит ожидать расширение списка услуг и согласования их названий и обозначений.

### 3. Стандартизация участников процесса предоставления облачных услуг

Первый нормативный документ, регламентирующий понятие облачных технологий [19] не содержал информации об участниках процесса пре-

доставления услуг. В дальнейшем специалисты NIST [22] определили 2 типа участников:

- cloud provider,
- cloud consumer;

а в NIST SP 800-146:2012 [20] – определены cloud consumer, cloud provider, также понятие client, и здесь же указывается на сложность определения ролей и ответственности в облачной модели, упоминается «брокер».

Таблица 4

Хронология представления видов услуг в нормативных документах

	NIST800-144:2011	NIST800-145:2011	NIST800-146:2012	ITU.T Y3501:2013	Проект ГОСТ (2013)	ISO 17788:2014	ITU.T Y3500:2014
IaaS	*			*	*	*	*
PaaS	*			*	*	*	*
SaaS	*			*	*	*	*
NaaS				*	*	*	*
WaaS / DaaS				*/-	*/-	*/-	*/-
CaaS					*	*	*
HaaS / CompaaS					*/-	*/-	*/-
SecaaS					*	*	*
BPaaS					*	*	*
DaaS / DSaaS					*/-	*/-	*/-
TaaS					*	*	*
SDPaaS					*	*	*
TraaaS					*	*	*
Database as a Service						*	*
Email as a Service						*	*
Identity as a Service						*	*
Management as a Service						*	*

Специалисты этого же института в другом нормативном документе NIST SP 500-291:2011 [6], а также в [21] определили более сложную модель взаимодействия, включающую:

- Cloud Consumer Person,
- Cloud Provider Person,
- Cloud Auditor,
- Cloud Broker,
- Cloud Carrier;

и представленную на рис. 3.

Упрощенная модель взаимодействия была принята в проекте национального стандарта [23], в котором определены стороны поставщика и потребителя облачной услуги.

Международный стандарт ISO 17789 [9] вводит расширенную классификацию актеров облачного рынка, представленную на рис. 4.

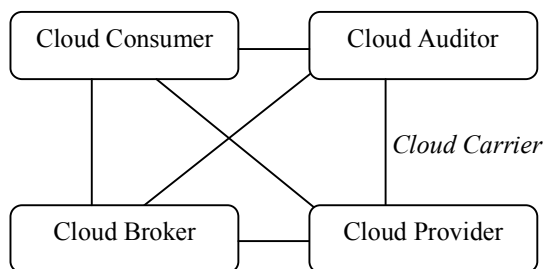


Рис. 3. Модель взаимодействия участников процесса предоставления облачных услуг согласно NIST SP 500-291:2011 [6]

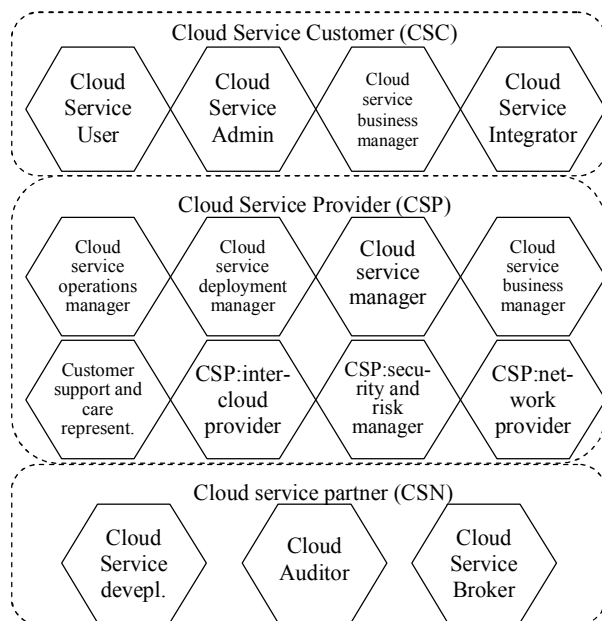


Рис. 4. Роли участников процесса предоставления облачных услуг согласно ISO 17789:2014 [9]

Ролевая модель, принятая в ISO 17788:2014 [8], распространилась на другие стандарты, поэтому в новом руководстве ITU.T X1601:2014 [18] рассматриваются следующие определения участников:

– потребитель облачной услуги (cloud service customer): сторона (физическое лицо или организация), которая состоит в деловых отношениях применительно к использованию облачных услуг;

– партнер облачной услуги (cloud service partner): партнер, участвующий в поддержке деятельности либо поставщика облачной услуги либо потребителя облачной услуги или же оказывает помощь в этой деятельности;

– поставщик облачной услуги (cloud service provider): сторона, которая предоставляет облачные услуги;

– пользователь облачной услуги (cloud service user): лицо, связанное с потребителем облачной услуги, которое пользуется облачными услугами;

– группа внутренних пользователей (tenant):

группа пользователей облачной услуги, совместно использующих доступ к набору физических и виртуальных ресурсов.

Следует отметить, что роль «tenant» также была введена в ISO 17788:2014 [8].

#### 4. Стандартизация угроз в сфере предоставления облачных услуг

В проекте национального стандарта [23] в отдельном разделе описаны угрозы безопасности информации (УБИ), характерные для поставщиков (15 видов угроз) и потребителей (7 видов угроз) облачных услуг. В последующем эти виды угроз категоризованы для каждого вида облачных услуг. Так, для базовых видов услуг распределение видов угроз представлено в табл. 5.

В международном нормативном документе ITU.T X1601:2014 [18] рассматривается ограниченное количество угроз безопасности для потребителей облачной услуги (CSC) (3 вида угроз) и для поставщиков облачной услуги (CSP) (2 вида угроз). При этом вводится новая категория «проблемы» безопасности, характерная для провайдеров и партнеров облачных услуг. Количество видов проблем безопасности для поставщиков облачной услуги (CSP) – 10; для партнеров облачной услуги (CSN) – 3.

#### 5. Расширение категорий стандартного определения безопасности (security)

Нельзя не отметить, что свойство «security» в последнее время претерпевает изменения в стандартных определениях. С одной стороны, постепенно расширяется наполнение категории «security» подсвойствами. Так к тройке базовых составляющих: конфиденциальности, целостности, доступности в последних редакциях нормативных документов [8, 25] все чаще добавляют такие подсвойства, как:

- аутентичность,
- подотчётность,
- невозможность отказа от авторства,
- надёжность.

Более того, в стандарте [26] «security» определяется как состояние защиты информационных активов, а конфиденциальность, целостность и доступность приводятся как частный пример этих активов.

На данный момент основные нормативные документы сферы облачных вычислений оперируют с базовыми подсвойствами «security».

С другой стороны, в последнее время понятие «security» рассматривается с позиции защиты не

Таблица 5

Угрозы безопасности информации для базовых видов облачных услуг [23]

	Угрозы безопасности информации	IaaS	Paas	SaaS
УБИ для потребителей облачных услуг	1) УБИ, связанные с неопределённостью ответственности;	+	+	+
	2) УБИ, связанные с потерей управления;	+	+	+
	3) УБИ, связанные с потерей доверия;	+	+	+
	4) УБИ, связанные с привязкой к провайдеру облачных услуг	+	+	+
	5) УБИ, связанные осуществлением незащищённого от НСД доступа со стороны потребителей облачных услуг;	+	+	+
	6) УБИ, связанные с недостатком управления информацией/облачными ресурсами;	+	+	+
	7) УБИ, связанные с потерей и утечкой данных.			+
УБИ для поставщиков облачных услуг	1) УБИ, связанные с неопределённостью при распределении ответственности;	+	+	+
	2) УБИ, связанные с несогласованностью политик безопасности;	+	+	+
	3) УБИ, связанные с непрерывной модернизацией;	+	+	+
	4) УБИ, связанные с приостановкой оказания услуг вследствие технических сбоев;	+	+	+
	5) УБИ, связанные с невозможностью миграции образов виртуальных машин из-за несовместимости аппаратного и ПО;	+	+	+
	6) УБИ, связанные с лицензионными политиками;	+	+	+
	7) УБИ, связанные с конфликтом юрисдикций различных стран;	+	+	+
	8) УБИ, связанные с осуществлением незащищённого администрирования облачных услуг;	+	+	+
	9) УБИ, связанные с общедоступностью инфраструктуры;	+	+	+
	10) УБИ, связанные с использованием технологий виртуализации;	+	+	+
	11) УБИ, связанные с нарушением доступности облачного сервера;	+	+	+
	12) УБИ, связанные с недобросовестностью поставщиков облачных услуг;		+	+
	13) УБИ, связанные со злоупотреблениями со стороны поставщиков облачных услуг;	+	+	+
	14) УБИ, связанные со злоупотреблениями со стороны потребителей облачных услуг.	+	+	

только информации (information security). В руководстве [27] дано определение кибербезопасности (cybersecurity), как набора инструментальных средств, стратегии, принципов обеспечения безопасности, гарантий безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя.

В разработках NIST также встречаются термины «network security», «Control system security», «IT security». Такие тенденции расширения категории «security» не могут не отразиться в нормативных документах сферы облачных вычислений, поскольку облачные инфраструктуры напрямую поддерживают сетевые, управляющие и информационные технологии.

### Заключение

В статье анализируется современное состояние отрасли стандартизации безопасности облачных вычислений. Выделены основные международные и региональные органы стандартизации, отмечена их роль в разработке стандартов по ключевым направлениям безопасности облачных вычислений.

Рассмотрены основные тенденции развития стандартов: расширение видов облачных услуг, участников процесса предоставления облачных услуг, угроз безопасности этим участникам. Также рассмотрено расширение стандартной категории «security» в направлениях наполнения подсвойствами и охвата различного класса систем (cyber-, network-, control system-).

Направлениями дальнейших исследований являются трассировка покрытия актуальных требований безопасности нормативными документами и выявление новых тенденций в их развитии.

### Литература

1. Храмовская, Н. Стандарты и руководства по использованию облачных вычислений [Текст] / Н. Храмовская // *Information Management*. – 2013. – № 3. – С. 12-21
2. NISTIR 8074 Volume 2 (Draft) Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity [Electronic resource] // National Institute of Standards and Technology. – Access mode: [http://csrc.nist.gov/publications/drafts/nistir-8074/nistir\\_8074\\_vol1\\_draft\\_report.pdf](http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf). – 24.11.2015.

3. D:A-5.1 Report on A4Cloud contribution to standards. Version 1.1. Deliverable Lead Organisation [Electronic resource] // Cloud Accountability Project (CSA). – Access mode: [http://www.a4cloud.eu/sites/default/files/D15.1\\_Report\\_on\\_A4Cloud\\_contribution\\_to\\_standards.pdf](http://www.a4cloud.eu/sites/default/files/D15.1_Report_on_A4Cloud_contribution_to_standards.pdf). – 24.11.2015.
4. Hibbard, E. A. Latest in Cloud Computing Standards [Electronic resource] // Eric A. Hibbard. – Access mode: <http://www.slideshare.net/rnewton/summary-cloudstandardseahv2130225>. – 24.11.2015.
5. Cisco Global Cloud Index: Forecast and Methodology, 2014-2019. White Paper [Electronic resource] // Cisco. – Access mode: [http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud\\_Index\\_White\\_Paper.pdf](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf). – 24.11.2015.
6. NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap [Text]. – impl. 01.07.2011. – Gaithersburg : National Institute of Standards and Technology, 2011. – 76 p.
7. ITU-T. FG Cloud TR. Version 1.0. (02/2012). Part 6: Overview of SDOs involved in cloud computing. [Electronic resource] // Switzerland, Geneva. – Access mode: [http://www.itu.int/dms\\_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P6-PDF-E.pdf](http://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P6-PDF-E.pdf). – 24.11.2015.
8. ISO/IEC 17788:2014 Information technology - Cloud computing - Overview and vocabulary [Text]. – impl. 15.10.2014. – Brussels : European Committee for Electrotechnical Standardization, 2014. – 16 p.
9. ISO/IEC 17789:2014 Information technology - Cloud computing - Reference architecture [Text]. – impl. 10.10.2014. – Brussels : European Committee for Electrotechnical Standardization, 2014. – 53 p.
10. Recommendation ITU-T Y.3500. Information technology - Cloud computing - Overview and vocabulary [Text]. – impl. 13.08.2014. – Geneva : International Telecommunication Union, 2014. – 18 p.
11. Recommendation ITU-T Y.3501. Cloud computing framework and high-level requirements [Text]. – impl. 22.05.2013. – Geneva : International Telecommunication Union, 2013. – 26 p.
12. Recommendation ITU-T Y.3502. Information technology - Cloud computing - Reference architecture [Text]. – impl. 13.08.2014. – Geneva : International Telecommunication Union, 2014. – 62 p.
13. Recommendation ITU-T Y.3503. Requirements for desktop as a service [Text]. – impl. 22.05.2014. – Geneva : International Telecommunication Union, 2014. – 34 p.
14. Recommendation ITU-T Y.3510. Cloud computing infrastructure requirements [Text]. – impl. 22.05.2013. – Geneva : International Telecommunication Union, 2013. – 28 p.
15. Recommendation ITU-T Y.3511. Framework of inter-cloud computing [Text]. – impl. 09.03.2014. – Geneva : International Telecommunication Union, 2014. – 46 p.
16. Recommendation ITU-T Y.3512. Cloud computing - Functional requirements of Network as a Service [Text]. – impl. 29.08.2014. – Geneva : International Telecommunication Union, 2014. – 36 p.
17. Recommendation ITU-T Y.3513. Cloud computing - Functional requirements of Infrastructure as a Service [Text]. – impl. 29.08.2014. – Geneva : International Telecommunication Union, 2014. – 26 p.
18. Рекомендация МСЭ-Т X.1601. Основы безопасности облачных вычислений [Текст]. – введ. 24.01.2014. – Женева : Международный союз электросвязи, 2014. – 32с.
19. NIST Special Publication 800-145. The NIST Definition of Cloud Computing [Text]. – impl. 01.11.2011. – Gaithersburg : National Institute of Standards and Technology, 2011. – 7 p.
20. NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations [Text]. – impl. 10.05.2012. – Gaithersburg : National Institute of Standards and Technology, 2012. – 81 p.
21. NIST Special Publication 500-299. NIST Cloud Computing Security Reference Architecture. Working Document. [Electronic resource] // National Institute of Standards and Technology. – Access mode: [http://bigdatawg.nist.gov/\\_uploadfiles/M0007\\_v1\\_3376532289.pdf](http://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf). – 24.11.2015.
22. NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing. [Text]. – impl. 01.12.2011. – Gaithersburg : National Institute of Standards and Technology, 2011. – 80 p.
23. Проект ГОСТ Р Защита информации. Требования по защите информации, обрабатываемой с использованием технологий "Облачных вычислений". Основные положения [Электронный ресурс] // Техэксперт. – Режим доступа: <http://docs.cntd.ru/document/1200102839>. – 24.11.2015.
24. Department of defense (DoD). Cloud computing security requirements guide (SRG). Version 1, Release 1. – impl. 12.01.2015. – Developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD), 2015. – 152 p.
25. ISO/IEC 27000:2014. Информационные технологии. Методы обеспечения защиты. Системы управления защитой информации. Общий обзор и словарь [Текст]. – введ. 15.01.2014. – Женева : Международная организация по стандартизации, 2014. – 44 с.
26. ISO/IEC 15408-1:2009. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model [Text]. – impl. 15.12.2009. – Brussels : European Committee for Electrotechnical Standardization, 2014. – 64 p.
27. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности [Текст]. – введ. 18.04.2008. – Женева : Международный союз электросвязи, 2008. – 64 с.



*Поступила в редакцію 12.09.2015, рассмотрена на редколлегии 18.11.2015*

## СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ХМАРНИХ ТЕХНОЛОГІЙ ТА ТЕНДЕНЦІЇ ЇХ РОЗВИТКУ

*Ю. Л. Поночовний, А. А. Фурманов, В. С. Харченко*

Розглянуто склад і взаємодія стандартоутворюючих організацій у сфері хмарних технологій. Показано стан нормативних документів за 10-ма ключовими напрямками стандартизації з інформаційної безпеки. Визначено базові напрямки стандартизації відповідно до категорій хмарних послуг. Розглянуто стандарти, що представляють рольову модель користувачів учасників хмарних послуг. Проведено аналіз та визначено тенденції у розвитку стандартів, такі як: розширення спектру хмарних послуг, укрупнення категорії «безпека», розширення спектру можливих загроз інформації, зростання числа стандартоутворюючих організацій - учасників.

**Ключові слова:** хмарні технології, інформаційна безпека, стандартоутворюючі організації, тенденції розвитку стандартів.

## INFORMATION SECURITY STANDARDS FOR CLOUD COMPUTING AND ITS TRENDS

*Yu. L. Ponochovniy, A. A. Furmanov, V. S. Kharchenko*

The composition and interaction of the standard-developing organizations in the field of cloud computing were considered. Displaying the state of normative documents on 10 key areas of information security standardization. The basic directions of standardization in accordance with the cloud services categories was defined. Standards which represent a participant-user role model of cloud services were considered. The analysis and trends identifying of standards (such as the range of cloud-based services expanding, integration of the "security" category, the range of possible informational threats expanding, the growth of standard-developing organizations – participants) were made.

**Keywords:** cloud computing, information security, the standard-developing organizations, the trends of standards.

**Поночовний Юрій Леонидович** – канд. техн. наук, ст. науч. сотр., доцент кафедри комп'ютерної інженерії, Полтавський національний технічний університет ім. Юрія Кондратюка, Полтава, Україна, e-mail: pnch1@rambler.ru.

**Фурманов Алексей Аркадиевич** – канд. техн. наук, доцент кафедри комп'ютерних систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: A.Furmanov@mail.ru.

**Харченко Вячеслав Сергеевич** – д-р техн. наук, профессор, заслуженный изобретатель Украины, заведующий кафедрой компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: V.Kharchenko@khai.edu.