|  |  |  |
| --- | --- | --- |
| itu_logo | **Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-16)Хаммамет, 25 октября – 3 ноября 2016 года** | C:\Users\gaspari\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\logos-02.png |
|  |  |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | **Документ 58-R** |
|  | **24 октября 2016 года** |
|  | **Оригинал: английский** |
|  |
| Директор БСЭ |
| Выводы третьего Глобального симпозиума по стандартам |
|  |
|  |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем отчете кратко представлены выводы третьего Глобального симпозиума по стандартам. |

Выводы третьего Глобального симпозиума по стандартам

На третьем Глобальном симпозиуме по стандартам, Хаммамет, Тунис, 24 октября 2016 года, собрались вместе авторитетные эксперты из сферы стандартизации для обсуждения вопросов о том, как работа в области стандартов может оптимальным образом включать аспекты безопасности, конфиденциальности и доверия.

# 1 Введение

Глобальные симпозиумы по стандартам (ГСС) проводятся для обсуждения на высоком уровне политики в области стандартизации, в ходе которых изучается развивающаяся динамика в сфере информационно-коммуникационных технологий (ИКТ) и связанные с этим последствия для технической стандартизации. ГСС проводится в начале Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ), которая проходит в МСЭ раз в четыре года. Предыдущие симпозиумы состоялись в Йоханнесбурге в 2008 году и Дубае в 2012 году.

Тема ГСС-12 – *Стандартизация на пересечении сектора ИКТ с другими секторами, такими как здравоохранение, коммунальное хозяйство и транспорт −* оказалась весьма своевременной, и выводы Симпозиума обеспечили полезное руководство для работы МСЭ в области стандартизации, проводимой в период 2013−2016 годов. ГСС-12 затрагивал вопросы безопасности, конфиденциальности и доверия, касающиеся инфраструктуры и услуг ИКТ, при обсуждении таких тем, как беспроводная передача медицинских данных, хранение данных о передвижении соединенных автотранспортных средств, а также сбор потребительских данных интернет-магазинами розничной торговли. В таких условиях необходимы стандартизированные системы для гарантии того, чтобы услуга имела надежные атрибуты безопасности и чтобы были защищены потребности пользователей в области безопасности и конфиденциальности.

На третьем Глобальном симпозиуме по стандартам (ГСС-16) обсуждалось, как заинтересованные стороны могли бы работать сообща над разработкой международных систем безопасности, конфиденциальности и доверия. На Симпозиуме собрались вместе ведущие эксперты в областях безопасности, конфиденциальности и доверия, представляющие правительства, регуляторные органы, органы по стандартам и отрасль. Участники обменялись мнениями о том, какими, по их представлениям, будут ключевые элементы таких систем, а также каким из этих элементов будет уделяться первоочередное внимание в соответствующей работе МСЭ по стандартизации, которая будет проводиться в период с 2017 по 2020 годы.

С приветственными замечаниями выступил **Е.П. Мохамед Ануар Мааруф**, Министр технологий связи и цифровой экономики Тунисской Республики. Со вступительными замечаниями выступили Генеральный секретарь МСЭ **Хоулинь Чжао** и Директор Бюро стандартизации электросвязи МСЭ **Чхе Суб Ли**. Симпозиум проходил под председательством **Монги Марзуга**, бывшего Министра ИКТ Туниса.

После открытия ГСС-16 были проведены три сессии, на которых к теме Симпозиума подошли с точки зрения регулирования и политики, отрасли и стандартизации. В разделе 2 настоящего отчета тема ГСС-16 рассматривается в контексте системы Организации Объединенных Наций (ООН), а затем в разделе 3 подытоживаются ключевые выводы и рекомендации, сделанные на каждой из сессий Симпозиума. Подробное резюме всех обсуждений на ГСС-16 включено в Дополнение I.

Окончательная программа, биографии ораторов и доклады приводятся по адресу: <http://itu.int/en/ITU-T/wtsa16/gss/>.

В соответствии с Резолюцией 122 (Пересм. Гвадалахара, 2010 г.) и Резолюцией 1272 (ИЗМ) Совета МСЭ выводы ГСС-16, изложенные в этом отчете, передаются на рассмотрение ВАСЭ-16.

# 2 Безопасность, конфиденциальность и доверие в сфере ИКТ − контекст ООН

ИКТ предоставили миллиардам людей возможность обмениваться цифровой информацией в глобальном масштабе. Использование этих технологий, которые в существенной степени основаны на технических стандартах, привнесло множество проблем, связанных с конфиденциальностью и безопасностью связи и, в конечном счете, с доверием конечных пользователей к ИКТ.

МСЭ занимается этой проблемой как в качестве организации по разработке стандартов, цель которой состоит в разработке обеспечивающих конфиденциальность добровольных международных стандартов в области ИКТ[[1]](#endnote-1), так и в качестве межправительственной организации, мандат которой заключается в укреплении доверия и безопасности при использовании ИКТ[[2]](#endnote-2). Всемирная встреча на высшем уровне по вопросам информационного общества возложила на МСЭ ответственность за то, чтобы действовать в качестве содействующей организации по Направлению деятельности C.5, работая вместе с Государствами − Членами МСЭ и другими заинтересованными сторонами в целях укрепления "*надежности и безопасности с помощью взаимодополняющих и взаимоусиливающих инициатив в сфере безопасности при использовании ИКТ и инициатив или руководящих принципов в отношении прав на неприкосновенность частной жизни, защиту данных и прав потребителей*".

Нормативная международная база для защиты конфиденциальности представлена в основном договорами в области прав человека, такими как Всеобщая декларация прав человека ООН 1948 года[[3]](#endnote-3) и Международный пакт о гражданских и политических правах ООН 1966 года[[4]](#endnote-4), и оба этих договора содержат положения о праве на конфиденциальность/частную жизнь (Ст. 12 и 17, соответственно). Но эти международные договоры не относятся явным образом к цифровой обработке личной информации, и в контексте системы ООН эта концепция рассматривалась лишь в форме не имеющего обязательной силы руководящего документа, а именно Руководящих принципов ООН 1990 года по регламентации компьютеризованных картотек, содержащих данные личного характера[[5]](#endnote-5).

Хотя ряд международных договоров юридически обязательного характера содержат положения о праве на конфиденциальность – например, Конвенция Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера[[6]](#endnote-6), Европейская конвенция о защите прав человека и основных свобод[[7]](#endnote-7) и Американская конвенция о правах человека[[8]](#endnote-8) – эти правовые документы были разработаны и приняты на региональной, а не на всеобщей основе. Многие из этих региональных соглашений основаны на одних и тех же основополагающих принципах конфиденциальности, таких как концепция осознанного согласия частного лица и адекватность мер безопасности, введенных до обработки личной информации[[9]](#endnote-9).

Различные заинтересованные стороны призывали к тому, чтобы уделять повышенное внимание необходимости общего глобального понимания вопросов обработки личной информации. Например, Международная конференция уполномоченных по вопросам защиты данных и конфиденциальности обратилась с призывом к a) Организации Объединенных Наций подготовить юридически обязательную "*всеобщую конвенцию* *о защите частных лиц в отношении обработки данных личного характера*"; b) международным организациям "*обязаться соблюдать принципы, совместимые с основными международными документами, посвященными вопросам защиты данных и конфиденциальности*"; и c) производителям аппаратного и программного обеспечения "*разрабатывать продукты и системы, включающие технологии, которые повышают конфиденциальность*"[[10]](#endnote-10).

Генеральная Ассамблея ООН учла этот призыв в ходе своей 68-й сессии (2013 г.), приняв резолюцию "Право на неприкосновенность личной жизни в цифровой век", в которой содержится призыв ко всем государствам − членам ООН "*уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации*"[[11]](#endnote-11). Согласно этой резолюции Совет ООН по правам человека назначил Специального докладчика, мандат которого включает, среди прочего, представление докладов о предполагаемых нарушениях права на конфиденциальность, в том числе в связи с проблемами, возникающими вследствие новых технологий.

# 3 Основные выводы ГСС-16

## 3.1 Принципы регулирования для обеспечения безопасности, конфиденциальности и доверия

*Напоминая, что конфиденциальность и защита данных являются важнейшими ценностями для отдельных лиц и обществ и что Всеобщая декларация прав человека закрепляет конфиденциальность в качестве одного из основополагающих прав;*

*отмечая, что сейчас почти во всех сферах жизни используются инфраструктура и услуги ИКТ, и поэтому, если степень доверия к ним нельзя будет сохранить, это окажет на них отрицательное воздействие; и*

*признавая тревожную тенденцию в области утечки данных и инцидентов с безопасностью, которая оказывает отрицательное воздействие на доверие со стороны людей,*

*ГСС выделил следующие меры*:

− использовать **международные системы**, которые содержат базовые принципы безопасности, конфиденциальности и доверия, и создать механизмы внедрения этих принципов;

− содействовать приверженности **принципам обеспечения конфиденциальности на этапе проектирования, оценке воздействия конфиденциальности и разработке** **технологий повышения конфиденциальности** (PET), которые, когда они интегрированы в инфраструктуру и услуги ИКТ, максимально сокращают обработку информации, позволяющей установить личность;

− создать средства для **обмена между государственным и частным секторами информацией** об угрозах инфраструктуре и услугам ИКТ, примерами передового опыта и стратегиями смягчения последствий таких угроз;

− мобилизовать международное сообщество и создавать партнерства для **развития национального потенциала** по защите от кибератак, увеличивая возможности стран по обнаружению инцидентов в сфере безопасности и по принятию скоординированных ответных мер на такие инциденты;

− установить баланс между необходимостью защиты конфиденциальности частных лиц и поощрения **использования данных инновационным образом**, чтобы задавать направление цифровой экономике. При принятии во внимание при проектировании новых технологий и услуг передовой опыт в области безопасности и конфиденциальности делает их привлекательными для потребителей и вносит вклад в совершенствование сети в целом;

− участвовать в разработке **международных стандартов для решения глобальных вопросов**, признавая, что при кибератаках государственные границы не соблюдаются и что нарушение конфиденциальности и безопасности ставит под угрозу доверие к ИКТ, а также что необходимы системы безопасности, стандартизированные на международном уровне, для гарантии того, что атрибуты безопасности услуги являются надежными и что потребности пользователей в области безопасности и конфиденциальности защищены в разных странах;

− содействовать разработке **стандартов для** "**деидентификации**" **личных данных** и **переносимости данных**, стандартов, способных вносить вклад в укрепление защиты потребителей и расширение возможностей выбора в отношении способности потребителей подписываться на услуги ИКТ и отказываться от их получения.

## 3.2 Как отрасль оправдывает ожидания конечных пользователей в отношении безопасности, конфиденциальности и доверия

*Вновь подтверждая огромный потенциал информационно-коммуникационных технологий и оцифровки для улучшения нашей жизни и совершенствования общества;*

*признавая, что нарушение безопасности, несоблюдение конфиденциальности в инфраструктуре и услугах ИКТ и отсутствие к ним доверия могут создавать серьезные угрозы для бизнеса и репутации компании; и*

*призывая к разработке реализуемых международных стандартов,*

*ГСС выделил следующие меры*:

− Поддерживать принципы **прозрачности** и **технологической целостности** и содействовать их внедрению. Признается, что не может быть доверия без прозрачности, и у пользователей должна быть возможность знать, как используются их данные, и решать, давать или не давать разрешение на такое использование. Технологическая целостность подкрепляет необходимость надежной защиты инфраструктуры и услуг ИКТ, поддерживая меры по обеспечению конфиденциальности и исключая вероятность скрытых функциональных возможностей, чтобы предотвратить несанкционированные изменения информации и обеспечить доверие к точности, полноте и надежности информации.

− Смягчать риски, создаваемые **ботнетами IoT**, с использованием стандартов безопасности. Растет количество сообщений о случаях злоупотребления устройствами интернета вещей (IoT) в рамках масштабных распределенных атак типа отказ в обслуживании (DDoS). Такие атаки могут привести к утечкам данных и значительному экономическому ущербу и ущербу репутации затронутых организаций. Необходимо изучить возможные пути использования прогресса в таких областях, как упрощенная криптография и стандартизированные методы обеспечения безопасности, для достижения высоких уровней безопасности при ограниченных вычислительных мощностях.

− Оценить воздействие **квантовых вычислений** на безопасность, конфиденциальность и доверие, а также исследовать **безопасные технологии для квантовых вычислений**. Хотя квантовые вычисления могут еще находиться на ранних стадиях своего развития, широко признается, что как только использование таких технологий станет практически целесообразным, традиционные методы шифрования, которые в настоящее время обеспечивают защиту онлайновых платежей, банковских транзакций, сообщений электронной почты и телефонных разговоров, скоро могут стать недостаточными. Настало время для оценки воздействия квантовых вычислений, а также для изучения, проверки, стандартизации и подготовки перехода к новым системам безопасности, которые могут выдерживать квантовые атаки, задолго до того, как наши системы станут уязвимыми перед такими атаками.

## 3.3 Подход органов по стандартам к вопросам безопасности, конфиденциальности и доверия

*Признавая важнейшую роль, которую играют стандарты в обеспечении безопасности, защите конфиденциальности инфраструктуры и услуг ИКТ и укреплении доверия к ним;*

*подчеркивая, что безопасность, конфиденциальность и доверие являются устоявшимися областями работы многих международных органов по стандартам, которые занимаются областями ИКТ и других технологий; и*

*призывая к стандартизации для решения проблем безопасности, конфиденциальности и доверия,*

*ГСС выделил следующие меры*:

− Поддержать подход "**обеспечения конфиденциальности на этапе проектирования**", уделяя должное внимание соображениям конфиденциальности в ходе разработки стандартов. Обеспечению конфиденциальности на этапе проектирования могут способствовать стандарты, обладающие характеристиками конфиденциальности и защиты данных, и стандарты также могут играть роль в обеспечении функциональной совместимости между характеристиками конфиденциальности.

− Понимать значение **программного обеспечения с открытыми исходными кодами** при решении проблем в областях безопасности, конфиденциальности и доверия. Программное обеспечение и стандарты с открытыми исходными кодами вносят взаимодополняющие вклады в рост отрасли ИКТ и инновации в этой отрасли. Сложность программного обеспечения возрастает, и, хотя сообщество разработчиков программного обеспечения с открытыми исходными кодами и сообщество стандартизации сотрудничают во многих областях, следует приложить дополнительные усилия для содействия обмену результатами работы между этими сообществами и тем самым обеспечить внедрение программного обеспечения высокого качества при высокой степени безопасности.

− **Укреплять сотрудничество** между органами по разработке стандартов при разработке международных сетей для безопасности, конфиденциальности и доверия, признавая их мандаты и сильные стороны и используя имеющиеся результаты работы. Органы по разработке стандартов должны придерживаться надлежащих процедур, принципов широкого консенсуса, прозрачности, сбалансированности и открытости при разработке стандартов; они должны быть привержены принципам технических достоинств, функциональной совместимости, конкуренции, инноваций и выгод для всех; наличия стандартов для всех и добровольного принятия стандартов. Органам по разработке стандартов следует также сотрудничать для решения проблемы неравенства между развивающимися и развитыми странами в способности получать доступ к стандартам, касающимся безопасности, конфиденциальности и доверия к инфраструктуре и услугам ИКТ, и внедрять эти стандарты, а также на равной основе участвовать в их разработке.

Дополнение I

Подробное резюме обсуждений, прошедших на ГСС-16

(Настоящее Дополнение не является неотъемлемой частью настоящего отчета)

Подробное резюме сделанных на ГСС‑16 докладов будет включено в Пересмотр 1 настоящего документа.

Примечания

1. См., например, Рекомендацию МСЭ-Т X.1171 "Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров". [↑](#endnote-ref-1)
2. См., например, Резолюцию 130 (Пересм. Пусан, 2014 г.) о роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий. [↑](#endnote-ref-2)
3. <http://www.un.org/en/universal-declaration-human-rights/>. [↑](#endnote-ref-3)
4. <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>. [↑](#endnote-ref-4)
5. <http://www.un.org/documents/ga/res/45/a45r095.htm>; Документ ООН E/CN.4/1990/72 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement>. [↑](#endnote-ref-5)
6. <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>. [↑](#endnote-ref-6)
7. <http://www.echr.coe.int/Documents/Convention_ENG.pdf>. [↑](#endnote-ref-7)
8. <https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm>. [↑](#endnote-ref-8)
9. См., например, Принципы конфиденциальности АТСЭ и нормативно-правовую базу ЕС по вопросам конфиденциальности, на которые в определенной степени повлияли Руководящие принципы ОЭСР, регулирующие неразглашение и трансграничные потоки личных данных; <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. [↑](#endnote-ref-9)
10. Декларация Монтрё Международной конференции уполномоченных по вопросам защиты данных и конфиденциальности, <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf>. [↑](#endnote-ref-10)
11. Резолюция 68/167 ГА ООН, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>. [↑](#endnote-ref-11)