|  |  |  |  |
| --- | --- | --- | --- |
| 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** | | **Пересмотр 1 Документа 58-R** | |
|  | | **27 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. Пересмотр 1 настоящего документа включает резюме всех сделанных ГСС докладов, в Дополнении 1. |

Выводы третьего Глобального симпозиума по стандартам

На третьем Глобальном симпозиуме по стандартам, Хаммамет, Тунис, 24 октября 2016 года, собрались 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/](http://itu.int/en/ITUT/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 C5, 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)

**Сессия 1: Приветствие и основные выступления**

**Е.П. Мохамед Ануар Мааруф**, министр технологий связи и цифровой экономики Тунисской Республики [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Maarouf) ] горячо приветствовал всех участников и выразил признательность членам МСЭ за выбор Хаммамета, Тунис, в качестве места проведения Глобального симпозиума по стандартам (ГСС) и Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ). Он отметил необходимость формирования доверия к инфраструктуре и услугам ИКТ, признавая важность темы ГСС‑16: *Безопасность, конфиденциальность и доверие в области стандартизации*.

В своей вступительной речи Председатель ГСС‑16 **Монги Марзуг** (бывший министр ИКТ Туниса) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) ] приветствовал всех участников и пожелал им приятного пребывания в Хаммамете. Он отметил роль Туниса в формировании информационного общества и описал важную роль, которую информационно-коммуникационные технологии (ИКТ) играют в нашей повседневной жизни сегодня и будут и далее играть в будущем. Он подчеркнул значение открытых, безопасных, защищенных и надежных услуг ИКТ для мирового развития во всех областях (таких, как здравоохранение, финансы, коммунальные службы, интернет вещей (IoT)). В связи с этим он отметил, что стандартизация должна играть важную роль в укреплении безопасности ИКТ, защите конфиденциальности и создании доверия к услугам ИКТ среди граждан, органов государственного управления и компаний. Он отметил, что цель третьего ГСС заключается в представлении и обсуждении вкладов в обеспечение безопасности, конфиденциальности и доверия к инфраструктуре и услугам ИКТ трех основных заинтересованных сторон: органов государственного управления и регуляторных органов; отрасли; и органов стандартизации; а также в представлении выводов и рекомендаций по этим темам ВАСЭ‑16.

Г-н **Хоулинь Чжао** (Генеральный секретарь МСЭ) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Zhao) ] поблагодарил принимающую ГСС и ВАСЭ Тунисскую Республику за ее поддержку деятельности МСЭ. Описывая позитивный вклад предыдущих сессий ГСС, он показал, как ГСС формирует международную платформу для обсуждения политики в области стандартизации, организуя встречу лидеров государственного и частного секторов для обсуждения того, каким образом техническая стандартизация должна реагировать на меняющиеся приоритеты в секторе ИКТ. Все выводы и рекомендации ГСС-08 и ГСС‑12 внесли существенный вклад в программу работы МСЭ в области стандартизации. Он также отметил, что доверительная среда ИКТ придаст уверенность пользователям и предприятиям, которые смогут использовать потенциал ИКТ в полном объеме, и что стандартизация ИКТ играет важную роль в осуществлении мандата МСЭ "укреплять доверие и безопасность при использовании ИКТ". В заключение он выразил свою признательность всем ораторам, ведущим и участникам за их вклад в работу ГСС-16.

В своем приветственном обращении г-н **Чхе Суб Ли** (Директор Бюро стандартизации электросвязи МСЭ) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) ] рассказал о том, что будущие сети должны будут поддерживать огромный объем приложений ИКТ и чрезвычайно широкий спектр услуг. Миллиарды соединенных устройств, вещей и предметов позволят системам взаимодействовать и получать друг от друга сведения, создавая интеллектуальные экосистемы, которые будут корректировать свои действия в интересах эффективности. В следующем поколении связи появятся приложения в областях от передачи голоса и изображения до промышленных роботов, интеллектуального транспорта, дистанционной хирургии, виртуальной реальности и многого другого. Г-н Ли отметил, что вследствие этого роста уровня сложности ИКТ и небывалого уровня их повсеместного распространения потребуются существенные преобразования в инфраструктуре и услугах сетей. Поскольку общества находятся на пути к миру, в котором практически все аспекты экономической и социальной активности будут зависеть от ИКТ, нам необходимо создать инфраструктуру и услуги ИКТ, которые заслуживали бы нашего доверия. Он отметил роль технических стандартов в предупреждении появления "бункеров" данных в различных секторах нашей экономики и сообщил, что эксперты, участвующие в деятельности в области стандартизации, проводят работу с целью оказания поддержки развитию совместно используемой комплексной экосистемы данных.

**Сессия 2: Регуляторные принципы для безопасности, конфиденциальности и доверия**

В ходе этой сессии рассматривались регуляторные принципы для безопасности, конфиденциальности и доверия, и ее вел г-н **Билель Джамусси** (руководитель Департамента исследовательских комиссий Бюро стандартизации электросвязи МСЭ) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) ].

В своем основном выступлении **Джон Эдвардс** (уполномоченныйпо вопросам конфиденциальности, Новая Зеландия, и председатель Исполнительного комитета Международной конференции уполномоченных по вопросам защиты данных и конфиденциальности) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) ] признал постепенное, но ускоряющееся движение в сторону консенсуса между организациями, ранее занимавшими различные позиции, к консенсусу, в соответствии с которым конфиденциальность становится одним из определяющих вопросов нашей эпохи. Г-н Эдвардс отметил, что Генеральная Ассамблея ООН на своей 68-й сессии (2013 г.) приняла резолюцию, озаглавленную "*Право на неприкосновенность личной жизни в цифровой век*", содержащую призыв ко всем Государствам – Членам ООН "*уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации*". Он рассказал о работе организации, которую он представляет, Международной конференции уполномоченных по вопросам защиты данных и конфиденциальности (ICDPPC), и предложил ряд идей для повышения доверия на основе применения принципов конфиденциальности и, может быть, разработки стандартов в секторе электросвязи, в том числе:

– содействовать приверженности принципам обеспечения конфиденциальности на этапе проектирования, оценке воздействия конфиденциальности и разработке технологий повышения конфиденциальности;

– обеспечивать, чтобы доступ к сетям, системам, контенту, связи и метаданным со стороны агентов государства обеспечивался только в соответствии с законным разрешением и только в случаях, когда такой доступ необходим и пропорционален;

– содействовать прозрачности в отношении доступа к личным данным и их использования для целей, помимо тех, для которых субъект этих данных дал свое согласие;

– разрабатывать соответствующие стандарты и гарантии и содействовать им в целях "деидентификации" личных данных и для предупреждения реидентификации лиц на основе набора деидентифицированных данных;

– разрабатывать стандарты для обеспечения 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;

– обеспечивать, чтобы граждане и потребители продолжали пользоваться прозрачностью в качестве основы, на которой принимаются затрагивающие их решения.

В своем выступлении **Виктор Мануэль Мартинес Ванегас** (директор по вопросам международной политики, Федеральный институт электросвязи, Мексика) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS_IFT_Draft_Presentation.pdf) ] подошел к теме ГСС в глобальном масштабе, обсудил инициативы, осуществляемые на региональном уровне, и представил национальный контекст для безопасности, конфиденциальности и доверия к ИКТ.

Он отметил, что развитие и распространение ИКТ оказывают положительное воздействие на экономический и социальный рост, но что имеются также угрозы и проблемы, которые могут подвергнуть опасности эти преимущества. Безопасность, конфиденциальность и доверие стали ключевыми элементами, которые следует изучать надлежащим образом. Выступающий привел выдержки из относящихся к теме публикаций, деклараций и соглашений, в том числе Генеральной Ассамблеи Организации Объединенных Наций, примеры деятельности МСЭ-Т и МЭК в области стандартизации, выдержки из Доклада об информационной экономике ЮНКТАД, в котором говорится: "*безопасность и доверие необходимы для создания благоприятной среды для электронной коммерции*". Г-н Мартинес Ванегас указал, что в его регионе, Латинской Америке и Карибском бассейне, аудитория интернета растет самыми быстрыми темпами в мире и что обеспечение безопасности, конфиденциальности и доверия к ИКТ является обязательным условием социально-экономического развития в регионе. Он также подчеркнул, что опыт региона показывает, что ни одна страна в одиночку не может обеспечить безопасность своих сетей и что сотрудничество является необходимым.

**Илиас Чантсос** (старший директор по связям с государственными организациями, регион Европы, Ближнего Востока, Африки, Азии и Тихого океана и Японии, советник по вопросам глобальной защиты важнейшей инфраструктуры и конфиденциальности, компания Symantec, Соединенные Штаты Америки) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) | [исходный документ](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/InternationalCyberNorms_Ch10%20-%20Symantec.pdf) ] рассказал о том, как политические и регуляторные стимулы влияют на технический прогресс и, в свою очередь, испытывают его воздействие. Он привел в качестве одного из наиболее ярких примеров этой динамики Общий регламент ЕС о защите данных. Существующей Директиве о конфиденциальности уже более 20 лет, и ее необходимо существенно изменить, чтобы отразить эволюцию или революцию, которую претерпели технологии и другие факторы, такие как социальные сети. В свою очередь, при использовании технологий и социальных сетей теперь придется соблюдать новый Регламент, что коренным образом изменит то, как государственные и частные организации будут управлять своими данными, в том числе защищать персональные данные от кибератак. Г-н Чантсос представил также концепцию технологической целостности, которая поддерживает необходимость в надежной безопасности инфраструктуры и услуг ИКТ, утверждая меры конфиденциальности и отвергая перспективы скрытых функциональных возможностей, чтобы не допустить несанкционированных изменений информации и установить доверие к точности, полноте и достоверности информации.

**Джеймс М. Килаба** (генеральный директор Регуляторного органа связи Танзании (TCRA)) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSSWTSA2016-Kilaba.pdf) ] отметил, что проблемы безопасности и конфиденциальности, вызванные технологическим сдвигом с того времени, когда лишь немногие персональные компьютеры были подключены к интернету, до сегодняшних средств, обеспечивающих связь любого человека, любой вещи в любом месте и в любое время. Он описал инициативы, предпринимаемые на национальном и региональном уровнях для защиты конфиденциальности, безопасности данных и инфраструктур ИКТ. Они включают: создание Национальной группы реагирования на нарушения компьютерной защиты (TZ-CERT), которая используется для распространения среди различных заинтересованных сторон знаний, информации и навыков в области кибербезопасности; осуществление DNSSEC в системе регистрации наименований доменов; и обсуждение проблем кибербезопасности в Восточноафриканской организации связи (EACO). Г-н Килаба напомнил о едином подходе к решению этих проблем, отметив необходимость согласования международных стандартов для оказания поддержки развивающимся странам.

**Шауки Гаддэ** (президент Национального органа по защите личной информации, Тунис) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Gaddes) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS-Gaddes.pdf) ] рассказал о ведущей роли Туниса в гарантировании посредством Конституции защиты конфиденциальности и личных данных (Статья 24, 2014 г.), доступа к сетям информации и связи (Статья 32, 2004 г.) и доступа к государственным документам (вступит в силу в 2017 г.). Он отметил, что Тунис придает большое значение формированию доверия между гражданами, частным сектором и правительством.

**Сессия 3: Как отрасль оправдывает ожидания конечных пользователей в отношении безопасности, конфиденциальности и доверия**

**Илиас Чантсос** (старший директор по связям с государственными организациями, регион Европы, Ближнего Востока и Африки, Азии и Тихого океана и Японии, советник по вопросам глобальной защиты важнейшей инфраструктуры и конфиденциальности, компания Symantec, Соединенные Штаты Америки) был ведущим сдвоенной сессии по теме соблюдения отраслью регуляторных принципов и оправдания ожиданий конечных пользователей в отношении безопасности, конфиденциальности и доверия.

**Аммар Алькассар** (главный исполнительный директор, Rohde & Schwarz Cybersecurity, Германия) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Alkassar) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-1201601024_ITU%20GSS16_ALKASSAR_2.pptx) ] представил тенденции в области ИКТ, которые существенно изменят наш мир. Он рассказал о том, что кибербезопасность будет одним из основных определяющих факторов этих перемен, и о том, что ее значение в будущем возрастет. Г-н Альксассар отметил, что инструменты в сфере безопасности, используемые в настоящее время, во многом не соответствуют защищаемым экономическим ценностям. Он указал на необходимость определения новых комплексов стандартов ввиду изменения парадигмы в сфере безопасности ИТ для противостояния условиям все более изощренных угроз. По мнению компании Rohde & Schwarz, это изменение парадигмы окажется под угрозой в отношении следующих элементов: реализации принципа "безопасность на этапе проектирования", использования упреждающих, а не последующих мер; использования контроля потока информации, а не контроля доступа; и освобождения пользователей от невыполнимых обязательств, когда речь идет о кибербезопасности. Он отметил, что сообщество ИКТ может внести существенный вклад в этой области, в особенности благодаря своей деятельности в области стандартизации, а также в налаживании контактов между традиционным сообществом электросвязи и новыми участниками сферы ИКТ.

**Томас Кремер** (член Совета директоров по вопросам конфиденциальности данных, Отдел по юридическим вопросам и контролю за соблюдением законодательства, Deutsche Telekom, Германия) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kremer) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Deutsche%20Telekom%20-%20final.pptx) | [исходный документ](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Getting%20out%20of%20the%20digital%20trust%20trap%20-%20deutsche%20telekom.pdf) ] подчеркнул, что прозрачность является предпосылкой доверия. Люди должны иметь возможность узнавать, как используются их данные, и осознанно решать, принимать ли такое использование. Вместе с тем одной прозрачности недостаточно, если компании собираются выполнять свои обязательства в цифровой области. Г‑н Кремер призвал создавать системы, которые бы надежно анонимизировали данные при всех сценариях использования, которые не требуют непосредственного личного участия. Он назвал шифрование еще одним способом получения доверия клиентов, особенно применительно к конфиденциальным данным, например о состоянии здоровья. Deutsche Telekom считает, что любое предложение о предоставлении органам власти "запасных ключей" или "служебных входов" в защищенные системы будет контрпродуктивным и подорвет усилия по укреплению безопасности, поскольку эти средства скоро попадут в руки злоумышленников. Г-н Кремер призвал находить "умные", удобные в употреблении и своевременные решения в области кибербезопасности. По мере появления новых технологий (IoT, машинного обучения, квантовых вычислений и т. п.) атаки будут становиться все более изощренными. Требуются стандартизованные способы выявления рисков и атак и смягчения их последствий.

**Дэвид Фрэнсис** (сотрудник по вопросам европейской кибербезопасности, Huawei Technologies, Китай) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Francis) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Huawei%20-%20final.pptx) ] разъяснил, чтó предусматривает защита конфиденциальности и безопасности с точки зрения поставщика технологий. Он рассказал о политических мерах и процедурах, используемых в такой компании, как Huawei Technologies, для обеспечения безопасности продукции и ее способности к восстановлению, что в конечном счете способствует защите конфиденциальности и данных конечного пользователя. К числу основных элементов, которые следует учитывать при комплексном подходе, относятся: защищенные устройства; архитектура – сеть составляется из множества сложных продуктов; и люди, которые внедряют условия, управляют ими, повышают их уровень, фиксируют и оценивают их. Г-н Фрэнсис затронул вопрос необходимости управления глобальной цепочкой поставок, на которую сектор ИКТ в полной мере полагается в отношении смягчения угроз безопасности, роли прозрачности и глобальных стандартов, а также необходимости международного сотрудничества для укрепления кибербезопасности во всем мире.

**Г-жа Джая Балу** (старший сотрудник по вопросам информационной безопасности, KPN, Нидерланды) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Baloo) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-4ITU-GSS-Tunesia.pdf) ] рассказал о стремительном развитии квантовых технологий – от квантовых вычислений до квантовой криптографии. Наличие квантового компьютера создаст риск в сфере безопасности для стран и компаний, полагающихся на асимметричную криптографию (RSA, ECC). В качестве реакции необходимо принимать постквантовые решения, которые могут состоять из трех этапов. Во-первых, можно увеличивать длину ключа существующих алгоритмов шифрования. Во-вторых, можно использовать распределение квантовых ключей для конкретных критических точек в сетях. В-третьих, можно создавать и поддерживать будущие защищенные постквантовые алгоритмы шифрования. Глобальное сообщество информационной безопасности успешно осуществляет инновации в связи с квантовыми технологиями. Вместе с тем существует опасность того, что это создаст новый разрыв в цифровой безопасности между странами, которые обладают финансовыми и научными ресурсами, позволяющими использовать квантовый компьютер для расшифровки криптографии других стран, тогда как их собственная связь будет защищена, и теми, кто не в состоянии ни атаковать, ни защищаться.

**Джеймс Сноу** (специалист по вопросам стратегии в сфере безопасности и соблюдения законодательства, Google, Соединенные Штаты Америки) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Snow) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Google-final.pptx) | [исходный документ](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GoogleExecSummary_2016.pdf) ] отметил, что Google считает одним из основных приоритетов получение и сохранение доверия потребителей посредством обработки данных в защищенной, надежной и соответствующей законодательству среде. Безопасность и конфиденциальность имеют для Google решающее значение, и поэтому компания вкладывает значительные средства в защиту данных потребителей. Это предусматривает использование защищенных серверов и сетевой инфраструктуры специального назначения, а также шифрование данных пользователей, размещенных на диске, хранимых на резервных носителях, передаваемых по интернету или передаваемых из одного центра обработки данных в другой.

Г-н Сноу отметил, что доверие потребителей начинается с понимания, и понимание можно создать только благодаря прозрачности, например путем предоставления подробной документации, аудиторских отчетов и сертификатов. Google сознает значение международного сотрудничества и использует для безопасности и конфиденциальности ряд международных стандартов, в том числе:

– ISO 27001:2013, Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования;

– ISO 27017:2015, Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для управления информационной безопасностью услуг облачных вычислений на основе стандарта ISO/IEC 27002;

– ISO 27018:2014, Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность (PII), в публичных облаках, выступающих в роли обработчиков PII; и

− SOC 2/SOC 3 − Основа аудита для не связанных с конфиденциальностью принципов, к которым относятся безопасность, наличие, целостность обработки и конфиденциальность.

**Юэцзинь Ду** (вице-президент по вопросам безопасности, Alibaba Group, Китай) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Du) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Yuejin-DU.pptx) ] рассказал о значении безопасности и конфиденциальности в инфраструктуре, которую Alibaba предоставляет своим клиентам для технологий коммерции и передачи данных. Так, Alibaba предоставляет своим партнерам продукты информационной безопасности и распространяет стандарты посредством Альянса безопасности экосистемы электронной коммерции (EESA), который был создан Alibaba в июле 2016 года. В рамках EESA Alibaba и ее партнеры могут использовать существующие модели обнаружения рисков для рассмотрения и выявления угроз и совместной работы в целях укрепления безопасности и защиты конфиденциальности в экосистеме электронной коммерции путем реализации созданных альянсом стандартов.

**Бернар Бенуа** (генеральный управляющий, WhiteNoise/Kudelski Security, Швейцария) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Benoit) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Kudelski%20-%20final.pdf) ] рассказал о возможных расхождениях в интересах пользователей, поставщиков услуг и органов государственного управления и о том, что существующие сети электросвязи имеют изъяны в сфере безопасности и поэтому неспособны гарантировать безопасность и конфиденциальность связи. Для укрепления безопасности и конфиденциальности в не пользующихся доверием сетях он предложил масштабируемый компонент безопасности аппаратного обеспечения на основании подхода over-the-top, который работает независимо от лежащих в основе сетей и протоколов. Г‑н Бенуа напомнил аудитории о необходимости не привязанных к платформам решений со стандартизованными интерфейсами, способными удовлетворять применимые требования законного перехвата, не ставя под угрозу технологическую целостность посредством служебных входов, запасных ключей и т. п.

**Сессия 4: Подход органов по стандартам к вопросам безопасности, конфиденциальности и доверия**

В ходе сессии 4 анализировались подходы, применяемые различными организациями по разработке стандартов (ОРС) в отношении безопасности, конфиденциальности и доверия. Сессию вел **Тони Эид** (главный редактор Telecom Review) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Eid) ].

**Софи Кливио** (директор по вопросам политики в области стандартизации и технической политики Международной организации по стандартизации (ИСО)) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Clivio) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/ISO%20-%20final.PPTX) ] изложила общий межотраслевой подход ИСО к вопросам безопасности, конфиденциальности и доверия. Она обратила внимание на работу комитетов ИСО по вопросам безопасности и способности к восстановлению; по управлению рисками; по цепочке блоков транзакций и электронным технологиям распределенного реестра; а также на совместную деятельность ИСО/МЭК в области информационной безопасности и конфиденциальности в Объединенном техническом комитете по информационным технологиям (ОТК1 ИСО/МЭК). Ключевыми областями, охваченными деятельностью ОТК1, являются управление безопасностью информации, управление шифрованием и безопасностью, управление определением идентичности и технологии защиты конфиденциальности; биометрия; карты и персональная идентификация; управление информационными технологиями; механизмы обеспечения безопасности, конфиденциальности и доверия для облачных вычислений, больших данных и IoT. Г‑жа Кливио отметила, что ИСО и ее стандарты присутствуют в различных отраслях экономики, включая здравоохранение, транспорт (например, авиацию, интеллектуальные транспортные системы, морскую технологию), энергетику, строительство, обрабатывающую промышленность (включая аддитивное производство), и что были заключены соглашения о сотрудничестве с организациями, удовлетворяющими потребности и особые запросы этих отраслей.

**Франс Вреесвик** (генеральный секретарь и главный исполнительный директор Международной электротехнической комиссии (МЭК)) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vreeswijk) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEC%20-%20final.pptx) ] рассказал о том, как МЭК объединяет усилия всех заинтересованных сторон в области электротехники для укрепления доверия к безопасным и эффективным продуктам и системам посредством использования международных стандартов МЭК и систем оценки соответствия МЭК. МЭК опубликовала свыше 200 стандартов по кибербезопасности, уделяя особое внимание защите важнейших инфраструктур, таких как производство и распределение электроэнергии, водопользование и управление отходами, больницы и здравоохранение, производство и центы обработки данных, от киберуязвимостей и кибератак. МЭК также проводит большую работу для обеспечения безопасности и защищенности всего электрического и электронного оборудования, которое делает возможным сбор данных или применение протоколов доступа и управления. Так, сюда относятся датчики, медицинские устройства, носимые на себе "умные" устройства, а также технологии вычислений и хранения данных. Международные стандарты МЭК представляют собой ключевые факторы совершенствования обеспечения способности к восстановлению, управления рисками и эффективности.

МЭК тесно сотрудничает с ИСО в Объединенном техническом комитете по информационным технологиям (ОТК1 ИСО/МЭК) в таких областях, как управление безопасностью информации, управление определением идентичности, криптография и идентификация в целях безопасности, технологии конфиденциальности, биометрия; карты и персональная идентификация, облачные вычисления, большие данные и многое другое. МЭК постоянно взаимодействует с МСЭ, совместно с ИСО, в рамках Всемирного сотрудничества по стандартам.

Г-н Вреесвик призвал расширять сотрудничество между всеми организациями, занимающимися разработкой стандартов, для решения проблем безопасности, конфиденциальности и доверия. По сути ни одна организация сама по себе не сможет обеспечить все стандарты, необходимые в этой области.

**Карен Маккабе** (старший директор по вопросам технической политики и международным делам Ассоциации стандартов IEEE (IEEE-SA)) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#McCabe) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEEE-final.pptx) ] подчеркнула, что стандарты должны играть решающую роль в содействии обеспечению безопасности и конфиденциальности и в формировании доверия к ИКТ. Чтобы выполнить эту функцию, передовой опыт должен использоваться с учетом комплекса принципов, предусматривающих в рамках мирового сообщества добровольное сотрудничество между всеми заинтересованными сторонами и создающих благоприятные условия для достижения высокого уровня технических навыков, обеспечения глобальной функциональной совместимости и инноваций. Эти принципы включают: прямое участие; надлежащие процедуры; широкий консенсус; наличие баланса; прозрачность; всеобщую открытость; согласованность; аспект развития. Оратор отметила, что открытый процесс − это полезная практика в отношении безопасности, поскольку анализ силами многих экспертов может помочь выявить возможные недочеты и повысить качество разрабатываемых стандартов. Прозрачность процессов разработки открытых стандартов способствует укреплению доверия к платформам, услугам и продуктам, основанным на этих стандартах и придерживающимся их. Кроме того, открытые стандарты создают условия для широкого распространения технологий по защите конфиденциальности и укреплению безопасности, так как они способствуют обеспечению функциональной совместимости. В заключение выступающая отметила, что открытые стандарты активизируют процесс инноваций, которые могут помочь найти решения проблем безопасности, конфиденциальности и доверия.

IEEE имеет в своем портфеле широкий выбор стандартов − от вопросов безопасности, конфиденциальности и доверия для серии стандартов сетей IEEE 802 до вопросов шифрования в серии IEEE 1363 (при уделении особого внимания алгоритмам на основе инфраструктуры открытых ключей (PKI)), в серии IEEE 1619 и многие другие. Отраслевая группа по безопасности соединений (ICSG) IEEE − это группа хозяйствующих субъектов, занимающихся вопросами компьютерной безопасности и собравшихся, для того чтобы объединить свои ресурсы и опыт в борьбе с неуклонным и быстрым ростом угроз компьютерной безопасности. Еще одним усилием, предпринятым недавно, стала инициатива IEEE в области интернета, имеющая целью повысить влияние и престиж организации в вопросах разработки глобальной политики в сфере технологий в областях управления использованием интернета, разработки политики в отношении кибербезопасности и конфиденциальности, обеспечивая консенсус в твердых научно-технических знаниях и руководстве процессом. Глобальная инициатива IEEE об учете этических факторов при проектировании автономных систем и ее Специальный комитет по вопросам этики, общества и технологий изучают новые стандарты и решения, сертификаты и кодексы поведения, а также проблему достижения консенсуса в вопросе реализации интеллектуальных технологий с позиции этики, включая системы искусственного интеллекта и автономные системы.

Далее г-жа Маккабе призвала вовлечь новое поколение специалистов в вопросах конфиденциальности, безопасности и этики из различных областей знаний в процессы разработки стандартов и включить вопросы конфиденциальности, безопасности и этики в сами открытые стандарты, чтобы способствовать укреплению доверия к ИКТ.

**Ашок Ганеш** (директор по вопросам инноваций CEN-CENELEC) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Ganesh) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/CEN-CENELEC-final.pptx) ] подчеркнул, что во всех отраслях промышленности происходят серьезные преобразования, поскольку там внедряются новые технологии и подходы (например, интернет вещей, облачные вычисления, робототехника, сенсорные технологии), что коренным образом меняет их процессы, системы и даже бизнес-модели. Эти традиционные вертикальные отрасли промышленности (например, обрабатывающая промышленность, энергетика, транспорт), не являвшиеся ранее важными пользователями ИКТ и цифровых технологий, ищут поддержки и решений в области стандартизации для проведения этих преобразований. Г-н Ганеш отметил, что ОРС, такие как ИСО, МЭК, а также CEN и CENELEC в Европе, имеют значительную зону влияния в этих вертикальных отраслях и желают выработать свои подходы, чтобы удовлетворить эти потребности, связанные с ИКТ/цифровыми технологиями. Внедрение этих технологий предполагает использование систем для промышленных предприятий и производственных процессов, а также создание, обработку и хранение большого объема данных и обмен ими. Г-н Ганеш отметил, что проблема, стоящая перед организациями по стандартизации, многогранна: сохранить участие традиционных заинтересованных сторон, привлечь заинтересованные стороны в сфере ИКТ/цифровых технологий и изменить собственные подходы, чтобы быть в состоянии предоставлять напрямую и опосредованным путем решения по стандартизации в постоянно усложняющейся и быстро развивающейся области. Первоочередная задача для ОРС заключается в сосредоточении основного внимания на потребностях и приложениях различных секторов, включая изучение связи между кибербезопасностью и функциональной безопасностью, надежностью продукта, защитой данных и конфиденциальностью.

**Рейнхард Шолль** (заместитель Директора Бюро стандартизации электросвязи МСЭ) [ [биография](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Scholl) | [презентация](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Reinhard-final.pptx) ] напомнил всем участникам о симпозиуме по кибербезопасности, прошедшем в качестве сопутствующего мероприятия ВАСЭ-04 во Флорианополисе, Бразилия. Итогами мероприятия стали 11 основных выводов, большинство из которых сохраняют свою актуальность; например: "Безопасность должна быть встроенной, а не дополнительной характеристикой", "Заинтересованным сторонам следует совместно пользоваться информацией" и "Стандартизация должна быть важнейшей частью глобальных усилий в области кибербезопасности".

Для характеристики сложившейся ситуации оратор привел несколько цифр по количеству известных киберинцидентов в сетевой инфраструктуре МСЭ. По его мнению, безопасность и конфиденциальность не являются взаимоисключающими. Он также пояснил, что работа МСЭ в области укрепления доверия и безопасности при использовании ИКТ продолжала активизироваться в стремлении содействовать развитию более безопасных сетевых инфраструктур, услуг и приложений. Он представил проведенную в последнее время работу МСЭ в областях безопасности и доверия, включая отчет, в котором подчеркивается важность и необходимость доверия в контексте ИКТ и вводятся соответствующие понятия и основные характеристики доверия. В числе идей, обсуждаемых в отчете, "индекс доверия" – величина, в которой несколько относящихся к доверию показателей сводятся в единое контрольное значение. Индекс доверия может использоваться для сопоставления доверия среди заинтересованных сторон при создании новых взаимоотношений в сфере доверия или цепочки создания стоимости в сфере доверия.

Г-н Шолль отметил, что членами Союза была начата работа, для того чтобы изучить, в том числе, требования, возможности и сценарии услуг для обеспечения доверия; структуру архитектуры для надежных сетей электросвязи; технические решения для обеспечения доверия; обеспечение доверия при анализе больших данных; и управление межоблачным доверием. Соответствующие усилия МСЭ‑Т в области стандартизации охватывают такие области, как кибербезопасность; управление безопасностью; архитектура и структура безопасности; противодействие спаму; управление определением идентичности; и защита информации, позволяющей установить личность.

Г-н Шолль также рекомендовал изучить вопрос о том, какой вклад сообщество разработчиков программного обеспечения с открытыми исходными кодами может внести в разработку стандартов, касающихся безопасности, конфиденциальности и доверия к инфраструктуре и услугам ИКТ. Он отметил, что следует предпринимать дополнительные усилия для обмена результатами работы между сообществом разработчиков программного обеспечения с открытыми исходными кодами и сообществом стандартизации, обеспечивая тем самым внедрение высококачественных стандартов и программного обеспечения.

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)