**Парламентское собрание Союза Беларуси и России**

**Постоянный Комитет Союзного государства**

**Оперативно-аналитический центр**
**при Президенте Республики Беларусь**

**Государственное предприятие «НИИ ТЗИ»**

**Полоцкий государственный университет**


# КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

**УДК 004(470+476)(061.3)**
**ББК 32.81(4Беи+2)**

**ISBN 978-985-531-564-4**

третий способ проверяет ссылки на источник, указанный в публикуемых записях. На случай, если пользователь распространяет записи о своей странице в другой социальной сети, чтобы данная информация была доступна всем его друзьям.

четвертый способ подходит для выявления пользователей, тщательно скрывающих свою личность, и основан на принципе ближайшего окружения пользователя: среди друзей пользователя находятся те, кто указал ссылку на свой профиль в другой социальной сети, и уже в указанной социальной сети находятся все общие друзья этих пользователей.

Однако анализ всех составляющих портрета пользователя социальной сети показал, что существующие методы идентификации используют далеко не все возможные ресурсы и не учитывают некоторых особенностей, которые бы позволили однозначно идентифицировать пользователя, как одно физическое лицо.

**Список литературы**

1 Социальные сети в России, зима 2015-2016 Цифры, тренды, прогнозы[веб-сайт] – URL:https://blog.br-analytics.ru/socialnye-seti-v-rossii-zima-2015-2016-cifry-trendy-prognozy.

2 Щюц А. Структура повседневного мышления // Социологические исследования.

3 Будаев Э. В., Чудинов А. П. Методологические грани политической метафорологии.

4 Kats E., Lasarfeld P. Personal influence. New York : FreePress, 1955

5 Green S. Twitter and Russian protest: memes, networks and mobilization // Центр изучения интернета и общества:[веб-сайт] – URL: http://www.newmediacenter.ru/ru/2012/05/22/твиттер-и-российский-протест-мемы-сет.

6 Бергер П., Лукман Т. Социальное конструирование реальности : трактат по социологии знания. М. : Медиум, 1995. 323 с.

7 Paridhi J., Ponnurangam K., Anupam J. Identifying Users across Multiple Online Social Networks.

# ВОПРОСЫ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ И КАЧЕСТВА ОЦЕНОК БЕЗОПАСНОСТИ ИТ

Ю.И. ИВАНЧЕНКО

*НИИ прикладных проблем математики и информатики БГУ*

В окружающем нас мире все большее место занимают ИТ. Каждый из нас вынужден принимать решение использовать ли и насколько использовать их в своей деятельности. И этот выбор основывается на нашем доверии к конкретным ИТ или услугам, предоставляемым с их помощью. Следует особо подчеркнуть, что это доверие должно быть не религиозным, а осознанным, т.е. основанным на знаниях и надежных свидетельствах, качественных оценках.

Вместе с тем, быстрые темпы обновления знаний и, соответственно, изменений технологий и средств информатизации вместе с непрерывно усиливающейся зависимостью бизнеса, обороноспособности, общественной жизни и т.д. от информационных технологий, объективно не позволяют своевременно получить такие свидетельства, которые позволяли бы сформировать осознанный приемлемый уровень доверия.

Современная воспитательно-образовательная парадигма (деградация классического образования) не оставляет надежды на улучшение ситуации в части обретения

субъектами информационных отношений знания необходимого для осознанного принятия решения.

С учетом сказанного становится очевидной необходимость выработки новых подходов к обеспечению (в первую очередь кадрового) информационной безопасности.

Эти новые подходы необходимо сформулировать в расчете на предотвращение (недопущение, упреждение) событий безопасности. Это по нашему мнению возможно путем:

1) воспитания культуры информационной безопасности в максимально широкой общественной среде, причем начинать это воспитание следует с момента когда ребенок получает доступ к современному средству коммуникации;

2) создания профессиональных институтов (центров, ассоциаций) высочайшей квалификации, способных выполнять роль ведущих (локомотивов) в решении не только текущих или уже известных проблем информационной безопасности, но и (а может быть и в большей степени) будущих.

Культура информационной безопасности формируется на базе достаточной совокупности согласованных правовых норм, знания и исполнения их субъектами информационных отношений. Там же где регулирование посредством правовых норм неуместно должны быть и работать этические нормы.

Важнейшим из упомянутых институтов является институт оценки, поскольку даже использование своих средств защиты требует оценки их возможностей, а большинство государств никогда не сможет обеспечивать свою безопасность и безопасность своих граждан в информационной сфере с помощью только собственных доверенных средств информатизации и защиты информации. Поэтому проблемы оценки будут только обостряться и дополнительную остроту им будет придавать «капитализация» (от слова – капитализм) всех сфер нашей жизни. И здесь вновь важнейшим элементом выступает доверие. Стороны информационных отношений должны доверять оценкам друг друга, а это невозможно без согласованной политики в области оценки соответствия, обеспечивающих правовых норм, и единообразного технического регулирования (включая требования, критерии и методики), наличия взаимно признаваемых компетенций в данной области деятельности и, наконец, взаимной прозрачности механизмов и процедур оценивания.

Взаимное признание компетенций экспертов-оценщиков требует согласования деятельности в таких областях как правовое регулирование, образовательная деятельность, сертификация (проверка и подтверждение квалификации) экспертов-оценщиков, аккредитация организаций и др.

В качестве первых шагов для решения обозначенных проблем, по нашему мнению, необходимы:

гармонизация законодательства (по меньшей мере, государств ЕАЭС) в области информационных технологий в целом (на основе, например, модельного законодательства);

активизация деятельности в ISO в части издания стандартов ISO на русском языке;

перевод и ввод в действие международных стандартов по информационной безопасности и оценке соответствия как межгосударственных, обеспечение их доступности по примеру http://protect.gost.ru (в рамках, например, Межгосударственного Совета по стандартизации, метрологии и сертификации);

гармонизация процедур оценки в области информационных технологий на межгосударственном уровне и создание (например, в рамках ЕАЭС) открытой, прозрачной системы оценки соответствия;

создание электронного общедоступного русскоязычного глоссария (в перспективе информационно-поискового тезауруса), который позволит всем создавать более качественные документы: НПА, ТНПА, техническую, программную, эксплуатационную документацию и т.п.

объединение усилий по исследованию проблем обеспечения безопасности информационных технологий и поиску путей их решения.

# О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЮЗНОМ ГОСУДАРСТВЕ

Э.П. КРЮКОВА, А.М. ЛАСИЦА

*Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»*

В рамках Научно-исследовательской работы «Исследование особенностей, разработка организационно-правовых основ по формированию систем и механизмов обеспечения безопасности данных персонального и иного охраняемого характера, не составляющих государственные секреты (тайну), в том числе на критически важных объектах Союзного государства» (шифр «Норма»), выполненной по мероприятию 5 программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011 – 2015 годы, утвержденной постановлением Совета Министров Союзного государства от 20 апреля 2012 г. № 6, разработано Положение о порядке обработки, использования и защиты персональных данных в Союзном Государстве.

Положение разработано на основе Директивы Европейского союза 2012 [1] года и распространяется на обработку персональных данных, выполняемую полностью или частично автоматизированными информационными системами, а также иными средствами, которые являются частью системы хранения персональных данных или предназначены для создания части такой системы.

В Положении устанавливаются нормы, отсутствующие или расширяющие положения национальных законодательств государств-участников Союзного государства, касающиеся категорирования персональных, принципов и условий их обработки, порядка сбора и организация доступа к персональным данным, обязанностей по обеспечению и порядку защиты персональных данных при хранении, обработке и трансграничной передаче, полномочий и обязанностей независимых надзорных органов, порядка выполнения мер по защите персональных данных и средств правовой защиты, ответственности и санкций, особых ситуаций при обработке персональных данных.

**Список литературы**

1. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).