BSA проанализировала законодательство стран Евросоюза в области кибербезопасности

12 Март, 2015 - Grayling |
ИТ: софт

Анализ законодательства и политик стран Евросоюза в области кибербезопасности выявил разобщенность нормативных сводов и недостаточную подготовленность государств-членов к распространению виртуальных угроз.

В рамках обзора, опубликованного сегодня Ассоциацией производителей программного обеспечения BSA | The Software Alliance, осуществляется комплексная оценка национальных законов, а также правил и политик в 28 странах-участницах Евросоюза по 25 критериям, которые считаются наиболее важными для обеспечения эффективной защиты от угроз кибербезопасности. Основной задачей обзора является предоставление государствам-участникам Евросоюза возможности для оценки подготовленности своих политик по ключевым метрикам и параметрам, а также обозначение ключевых элементов необходимых для укрепления юридической основы обеспечения национальной кибербезопасности

«При внимательном изучении имеющихся в странах Европы механизмов защиты от киберугроз обнаруживается весьма неоднородная картина. Большинство стран-участниц Евросоюза отдают высокий приоритет проблемам кибербезопасности, однако несоответствия в их подходе к обеспечению безопасности оставляют единый рынок незащищенным от этих угроз, — отмечает Томас Буэ (Thomas Boué), директор ассоциации BSA по связям с госструктурами в странах Европы, Ближнего Востока и Африки. — Директива Евросоюза по сетевой и информационной безопасности могла бы помочь обеспечить более высокий фундаментальный уровень кибербезопасности и повысить устойчивость к киберугрозам, если бы она была направлена на повышение подготовленности наиболее важных элементов инфраструктуры Евросоюза к подобным угрозам и предусматривала создание гармонизированных процессов ведения отчетности и публикации информации в масштабах всего единого рынка».

В числе основных результатов анализа:

- Большинство государств-членов Евросоюза признают вопрос обеспечения кибербезопасности одним из ключевых национальных приоритетов, особенно в отношении критически важной инфраструктуры.
- Наличие существенных расхождений в государственных политиках в области кибербезопасности, а также в юридических механизмах и операционных возможностях различных государств-членов Евросоюза обуславливают наличие значительных пробелов в общей системе обеспечения кибербезопасности в Европе.
- Почти во всех государствах-членах Евросоюза были созданы команды оперативного реагирования для разрешения инцидентов в области кибербезопасности, однако заявленная

миссия и квалификации этих команд могут существенно отличаться от страны к стране.
- Вызывает беспокойство отсутствие систематического подхода к организации частно-государственного партнёрства и взаимодействия по вопросам обеспечения кибербезопасности между правительствами государств-членов Евросоюза и неправительственными организациями и международными партнёрами.

В докладе содержится призыв к государствам-членам Евросоюза сосредоточить свои усилия на четырёх ключевых аспектах для создания эффективной нормативно-правовой базы в области кибербезопасности:

- Создать и обеспечить функционирование комплексной нормативно-правовой платформы на базе национальной стратегии кибербезопасности, которая будет дополняться планами в области кибербезопасности по отдельным секторам.
- Учредить оперативные органы с четким распределением обязанностей, которые будут отвечать за обеспечение оперативной компьютерной безопасности, реагировать на чрезвычайные ситуации и иные инциденты.
- Способствовать формированию атмосферы доверия и организовывать сотрудничество с частным сектором, негосударственными организациями и международными партнёрами.
- Вести просветительскую работу и повышать уровень осведомлённости об угрозах для кибербезопасности и о первоочередных мерах для их устранения.

В то же время, результаты анализа предупреждают европейские правительства о необходимости избегать протекционистских режимов, которые подрывают основы кибербезопасности, а вовсе не способствуют её усилению. В частности, государствам-членам Евросоюза следует:

- Избегать ненужных или необоснованных требований, которые могут ограничивать выбор или увеличивать стоимость продукции, в том числе требований в отношении специфических сертификаций для отдельных стран или требований к проведению испытаний; избегать требований к уровню локализации; требований в отношении раскрытия конфиденциальной информации, в том числе исходных кодов или ключей шифрования, а также избегать введения ограничений в отношении принадлежности прав на интеллектуальную собственность иностранным компаниям.
- Воздержаться от манипулирования стандартами, и, наоборот, способствовать внедрению технических стандартов, признанных на международном уровне и разрабатываемых участниками отрасли.
- Избегать правил в отношении локализации данных, обеспечивать свободное перемещение данных между рынками.
- • Избегать преференций для локальных технологий, что может сдерживать развитие конкуренции с иностранными продуктами и препятствовать глобальным инновациям.

С полным текстом обзора законодательства всех 28 странах и подробными выводами по каждому государству-члену Евросоюза можно ознакомиться на сайте BSA по адресу: www.bsa.org/EUcybersecurity.