# Кибербезопасность

**В 1988 году ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА НАСЕЛЕНИЕМ** находилось в стадии своего становления, и Регламент международной электросвязи (РМЭ), составленный в тот год, еще не содержал четких положений, касающихся кибербезопасности. Однако в нем содержится (в Статье 9) упоминание недопустимости "технического ущерба", добавленное в качестве ответной меры на один из первых элементов вредоносного программного обеспечения, компьютерный червь Morris, блуждавший в то время. Спустя десятилетия, значение защиты кибербезопасности чрезвычайно выросло и будет учитываться при пересмотре РМЭ. Имеются предложения добавить или изменить статьи в этом договоре, чтобы включить в него элементы, связанные с безопасностью, в том числе меры по противодействию спаму.

Количество кибератак увеличивается, а сами они становятся все более изощренными. В то же время растет наша зависимость от интернета и других сетей, необходимых для получения важнейших услуг и информации. Согласно информации компании, занимающейся вопросами безопасности, McAfee, в 2011 году было выявлено самое большое за всю историю количество скрытых угроз. В частности, сообщалось, что в настоящее время в мире блуждает не менее 70 миллионов различных элементов вредоносного программного обеспечения, а смартфоны превратились в одно из средств их распространения. Анализ показывает, что как минимум 70% сообщений электронной почты – это спам.

Между тем "умные" электросети, облачные вычисления, сети средств промышленной автоматики, интеллектуальные транспортные системы, электронное правительство и электронный банкинг – и это далеко не полный перечень типов инфраструктур – становятся взаимосвязанными. Сбой в одной из них может затронуть другие. Наряду с повышением удобств и эффективности возрастает и уязвимость в отношении кибератак[1].

Вместе с тем на международном уровне еще не принято согласованное определение кобербезопасности. Это сдерживает усилия по защите, которые должны быть предприняты как на национальном, так и на международном уровне, учитывая тот факт, что сети и компьютерные системы в настоящее время не имеют границ.

Инциденты, связанные с информационно-коммуникационными технологиями (ИКТ) обычно рассматриваются в рамках существующих национальных уголовных кодексов, которые зачастую не соответствуют глобальным тенденциям. У нас еще нет общего международного стандарта соответствующих преступлений: должно ли к таким преступлениям относиться нарушение авторских прав на программное обеспечение, например, помимо распространения детской порнографии, финансовое мошенничество, а также атаки отказа в обслуживании? Ответ может заключаться в согласовании национальных законов и установлении нормативно-правовых баз, на которых можно было бы развивать международное сотрудничество. Однако некоторые полагают, что это не требуется или это должно осуществляться только на региональном уровне.

Законы являются не единственной или самой оперативной ответной мерой на кибератаки. Технические решения могут быть дополнены стандартами, которые позволяют обеспечить функциональную совместимость и соответствие мерам безопасности. Это особенно важно в условиях взаимозависимости сетей в современном мире. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) опубликовал около 300 стандартов, касающихся кибербезопасности. МСЭ помогает также развивающимся странам в этой области и поддерживает создание групп реагирования на компьютерные инциденты или CIRT. В своей Глобальной программе кибербезопасности [2] МСЭ содействует развитию международного сотрудничества.

Эта работа является составной частью мандата МСЭ как ведущей организации по координации международных усилий по "укреплению доверия и безопасности при использовании ИКТ" – задачи, порученной ему лидерами Всемирной встречи на высшем уровне по вопросам информационного общества, состоявшейся в 2003 и 2005 годах.

---

[1] См. также Краткую базовую информацию, касающуюся ВКМЭ, "Защита важнейшей национальной инфраструктуры".

[2] См. www.itu.int/osg/csd/cybersecurity/gca/.