Секция «Масс-медиа в России и мире»

План "Вижипират" - новый этап развития системы кибербезопасности во Франции

Чикишев Николай Анатольевич

Аспирант

Московский государственный университет имени М.В.Ломоносова, Факультет журналистики, Кафедра зарубежной журналистики и литературы, Москва, Россия

E-mail: kuormasto@gmail.com

Становление цифровой экономики в развитых странах сопряжено с проблемами в области информационной безопасности. С ростом использования различных информационных систем в сферах производства повышается риск их противоправного использования и уязвимость для кибератак.

За время работы нового социалистического правительства во Франции (с 2012 года) одним из главных направлений цифровой политики государства стала безопасность информационных систем. Актуальность нормирования этой сферы очевидна, если учесть масштаб инцидентов. Серьезной проблемой для французских властей была кража финансовой информации министерств экономического блока в марте 2011 года [1]. Последний громкий пример - кибератаки во время нападения на редакцию "Шарли Эбдо" в январе 2015 года. Объектом атак оказались около 19 000 французских сайтов, среди которых были как медиа, так и сайты другой тематики [2].

Упомянутое событие стало поводом применить обновленную контртеррористическую программу "Вижипират" [3], созданную с целью предвидеть и предотвращать угрозы, которые в первую очередь связаны с терроризмом.

Программа "Вижипират" была принята в 1991 году и периодически обновлялась правительством исходя из современных вызовов, угрожающих безопасности государства. С внедрением в производство электронных информационных систем возникла необходимость создания единого центра, отвечающего за кибербезопасность на государственном уровне. В 2009 году разрозненные дирекции и департаменты были объединены в Национальное агентство безопасности информационных систем (ANSSI) [4]

Увеличение числа кибератак вынудило французские власти регламентировать общие правила в сфере безопасности информационных систем. В 2014 году основные положения "Вижипират" были коренным образом пересмотрены, и правительство Жан-Марка Эро обнародовало программу "Задачи кибербезопасности" [5]. В ней предельно конкретно описаны цели, стоящие перед государственными органами, бизнесом и обществом, с рекомендациями для их достижения.

Документ является следующим этапом в формировании законодательной базы для цифровой экономики Франции. Исходя из современных вызовов киберпространства, в программе "Задачи кибербезопасности" французское правительство считает важным подчеркнуть независимость агентов сферы и необходимость их сотрудничества в борьбе с киберпреступностью. Одними из главных проблем нормирования отрасли являются стремительные технологические изменения и уровень компетентности надзорных органов: развитие IT-отрасли всегда опережает ее осмысление регламентирующими институтами. Выход авторы документа видят в возросшей ответственности пользователей информационных систем: именно они должны отвечать за своевременное обновление систем кибербезопасности. С другой стороны, из положений программы следует решение правительства контролировать данную сферу, руководствуясь задачами обеспечить общественное спокойствие и уменьшить число угроз в национальном масштабе.

***

Противоречивость подходов к решению проблем цифровой экономики порождают широкие дискуссии во французском обществе. Мы выделили несколько тем, которые предполагают различные пути развития системы кибербезопасности:

1) нормирование: каков уровень ответственности участников и насколько отрасль должна быть регламентирована? Стремление государства на законодательном уровне стать контролирующим институтом в киберсфере сегодня входит в противоречие с политикой крупных бизнес-игроков (особенно если они транснациональны: примером может послужить ситуация вокруг налогообложения);

2) кооперация: каким образом должно происходить сотрудничество между участниками? Независимость и автономность в области кибербезопасности наносит вред ее общему уровню. Однако прерогатива решений остается сегодня в руках пользователей информационных систем, открытость деятельности которых ограничена;

3) масштаб: каков территориальный приоритет? Трансграничность киберпространства распространяет его проблемы на все государства, и для успешной борьбы с вызовами сферы необходим единый подход, который подразумевает международный уровень выработки решений. Но различия в становлении цифровой экономики в разных регионах бывают большими, что приводит к совершенно отличным путям развития данной сферы.

Источники и литература

1) Фокус на кибербезопаность = Focus sur la cyber-sécurité/ Prévention des Risques Majeurs; - Режим доступа: http://www.risques.gouv.fr/menaces-terroristes/focus-cyber-securite, свободный. – Загл. с экрана. – Яз. франц.

2) Кибератаки продолжаются против французских сайтов = Les cyberattaques se poursuivent contre les sites web français/ Le journal du Geek; - Режим доступа: http://www.journaldugeek.com/2015/01/15/charlie-hebdo-les-cyberattaques-se-poursuivent-contre-les-sites-web-francais/, свободный. – Загл. с экрана. – Яз. франц.

3) План «Вижипират» = Le plan Vigipirate/ Prévention des Risques Majeurs; - Режим доступа: http://www.risques.gouv.fr/menaces-terroristes/le-plan-vigipirate, свободный. – Загл. с экрана. – Яз. франц.

4) Национальное агентство безопасности информационных систем =L'Agence nationale de la sécurité des systèmes d'information: http://www.ssi.gouv.fr

5) Вижипират: задачи кибербезопасности = Vigipirate: objectifs de cybersécurité [Электронный ресурс]/ ANSSI. – Электр. дан. – Париж, 2014. – Режим доступа : http://www.risques.gouv.fr/sites/default/files/upload/objectifs_de_cybersecurite_document_ свободный. – Яз. франц.

Слова благодарности

Благодарю моего научного консультанта Милану Владимировну Захарову за помощь в работе над исследованием.