СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: РАЗРАБОТКА, ИДЕЯ, МИССИЯ

ЗАМЕСТИТЕЛЬ ГУБЕРНАТОРА ЧЕЛЯБИНСКОЙ ОБЛАСТИ, ЧЛЕН КОМИТЕТА СОВЕТА ФЕДЕРАЦИИ ПО НАУКЕ, ОБРАЗОВАНИЮ, КУЛЬТУРЕ И ИНФОРМАЦИОННОЙ ПОЛИТИКЕ (2010–2014 ГОДЫ)

Руслан Усманович Гаттаров

Особенностью нашего времени является постоянное и стремительное развитие информационных и телекоммуникационных технологий. С приходом в XXI век они дали человечеству практически незаменимые блага, которые окружают многих людей. Сегодня слово «интернет» основательно вошло в повседневную жизнь. При помощи Интернета мы легко и быстро можем получить интересующую нас информацию, заказать и оплатить нужный нам товар, пополнить денежными средствами устройство сотовой связи и т.д. Ресурсы и возможности Всемирной паутины задействованы на различных инфраструктурных объектах.

Безусловно, Интернет является неким катализатором различных общественных процессов. В этом плане он оказывает позитивное влияние на общество, ускоряет прогресс в различных сферах. Но всё ли так позитивно, как кажется на первый взгляд? Что скрывается за благами, которые дает нам информационно-телекоммуникационная сеть?

Недавние события, связанные с раскрытием Эдвардом Сноуденом информации о программе PRISM, включающей в себя массовую слежку за переговорами американцев и иностранных граждан посредством телефона и Интернета, информации о факте всеобъемлющего слежения в 60 странах за более чем 1 млрд человек, правительствами 35 стран, позволяют дать отрицательный ответ на первый вопрос.

Отвечая на второй вопрос, можно отметить, что всё большее количество объектов информационно-коммуникационной инфраструктуры – электронное правительство, платежные системы, онлайн-банкинг, интернет-трейдинг и т.д. – становится потенциальными объектами для угроз, транслируемых через сеть Интернет. Например, программные закладки в программном обеспечении компьютеров в посольстве могут отправлять секретные данные злоумышленникам. Кража баз данных банка может привести к массовому выводу денег со счетов населения. Аналогичным угрозам может подвергаться кто угодно – государство, организации, личность.

В недалеком будущем Интернет может стать основным инструментом ведения войны. Примечательна цитата из книги «Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств», одним из авторов которой является председатель совета директоров компании Google Эрик Шмидт: «Война всё больше напоминает обычный информационный конфликт с использованием инструментария кибервойн, «медиавирусов», дезинформации и сетевых атак, а если дело дойдет до применения оружия, то, скорее всего, воевать опять будут роботы»[1].

Интеграция различных сфер общественной жизни в Интернет, с одной стороны, активное использование гражданами возможностей Интернета в повседневной жизни, использование Интернета в бизнесе и в государственном управлении – с другой, делают воз-

[1] Шмидт Э., Коэн Д. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств. М.: Манн, Иванов и Фербер, 2013.

можные негативные последствия угроз, которые приносит Интернет, более значимыми и разрушительными.

Понимая актуальность этой проблемы, Временная комиссия Совета Федерации по развитию информационного общества выступила инициатором разработки стратегии кибербезопасности Российской Федерации. В данной инициативе, на наш взгляд, можно выделить несколько аспектов. Во-первых, кибербезопасность выводится в самостоятельную категорию. Во-вторых, в качестве формата будущего документа выбрана стратегия. В-третьих, при разработке стратегии кибербезопасности необходимо использовать такой формат работы, который обеспечил бы разнонаправленность, комплексность итогового документа.

На сегодняшний день в Российской Федерации действует ряд концептуальных документов, направленных на обеспечение безопасности в информационной сфере. В качестве данных документов можно обозначить Доктрину информационной безопасности Российской Федерации[2], Стратегию развития информационного общества в Российской Федерации[3], Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации[4], Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[5] и др.

В этой связи логичным является вопрос о соотношении информационной безопасности и кибербезопасности: есть ли разница в этих категориях? Надо полагать, что ответ на этот вопрос лежит не только и не столько в теоретической плоскости. От ответа на него зависит право стратегии кибербезопасности на существование как самостоятельного документа. Действительно, если механизмов регулирования, основанного только на одной категории «информационная безопасность», хватит для цели ликвидации интернет-угроз, то достаточно внести изменения в Доктрину информационной безопасности Российской Федерации, иные концептуальные документы, а также в законодательство, актуализировав их содержание.

Обратившись к международному опыту, а именно к стандарту ISO/IEC 27032:2012[6], можно прийти к выводу, что информационная безопасность и кибербезопасность близкие, но не идентичные понятия. Приведенный стандарт дает четкое понимание связи термина cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, интернет-безопасностью и безопасностью критичных информационных инфраструктур. Обобщенный анализ позволяет определять кибербезопасность как более узкое по смыслу понятие, чем информационная безопасность. Сущность кибербезопасности можно свести к условиям, при которых коммуникационные каналы Интернета и других телекоммуникационных сетей, технологическая инфраструктура в период их функционирования защищены от максимально возможного числа угроз и воздействий, имеющих нежелательные последствия.

Таким образом, можно сделать вывод о том, что существования только Доктрины информационной безопасности Российской Федерации недостаточно для некой комплексной идейной базы, на основе которой будет осуществляться законодательное регулирование аспекта безопасности в информационной сфере. Существующее регулирование не охватывает в необходимой мере систему отношений, возникающих в рамках киберпространства как элемента информационного пространства. На наш взгляд, лаконичным дополнением, своего рода «помощником» информационной безопасности будет кибербезопасность, а «помощником» Доктрины информационной безопасности Российской Федерации и иных концептуальных документов – стратегия кибербезопасности Российской Федерации.

По своей природе стратегия является документом политической направленности. Логично, что она утверждается Президентом Российской Федерации или Правительством Российской Федерации. Стратегия задает политике государства общий вектор, который обращен к представителям как законодательной, так и исполнительной власти.

Поскольку политика государства вообще и политика государства в области информационной безопасности и цифрового суверенитета в частности должна быть сбалансированной, отвечать интересам личности, общества и государства, в процесс разработки стратегии кибербезопасности должны быть вовлечены представители гражданского общества, бизнеса и государства. Это предопределило использование мультистейкхолдерного подхода в формате работы над концепцией стратегии кибербезопасности. Согласно данному подходу Временная комиссия Совета Федерации по развитию информационного общества обеспечила вовлечение всех заинтересованных стейкхолдеров в процесс разработки концепции стратегии кибербезопасности. Так, к разработке были привлечены специалисты в области информационной безопасности, представители бизнеса, гражданского общества и государства.

В итоге продолжительной работы мы получили комплексный документ, который получил название Концепция стратегии кибербезопасности Российской Федерации.

---

[2] Утверждена Президентом Российской Федерации 9 сентября 2000 года (№Пр-1895).

[3] Утверждена Президентом Российской Федерации 7 февраля 2008 года (№Пр-212).

[4] Утверждены Президентом Российской Федерации 3 февраля 2012 года (№803).

[5] Утверждены Президентом Российской Федерации 24 июля 2013 года (№Пр-1753).

[6] ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity (ИСО/МЭК 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководство по кибербезопасности»).

Основная идея и цель стратегии заключается в необходимости обеспечить кибербезопасность личности, общества, организаций и государства, определив систему приоритетов, принципов и мер в области внутренней и внешней политики. Идейной основой стратегии кибербезопасности являются следующие принципы:

– гарантированность конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;
– максимальная защищенность личности, организаций, в том числе обеспечивающих функционирование критической информационной инфраструктуры, и государственных органов в части функционирования информационных ресурсов, информационных систем и информационно-телекоммуникационных сетей в киберпространстве;
– конструктивное сотрудничество всех субъектов информационного общества – личности, организаций и государства – в области обеспечения кибербезопасности;
– баланс между установлением ответственности за несоблюдение требований кибербезопасности и введением избыточных ограничений;
– приоритизация рисков кибербезопасности в соответствии с вероятностями реализации киберугроз и размерами негативных последствий от инцидентов кибербезопасности;
– систематическая актуализация средств и методов обеспечения кибербезопасности в целях противостояния изменяющимся киберугрозам.

Политика в области кибербезопасности должна быть ориентирована на результат. Именно в этом случае можно ожидать, что цели стратегии будут достигнуты, а ее основная идея воплощена в жизнь. Достижение конкретных результатов в области обеспечения кибербезопасности является основной миссией стратегии. На этот счет в документе предлагается семь ключевых результатоориентированных направлений деятельности:

– принятие общесистемных мер по обеспечению кибербезопасности;
– совершенствование нормативно-правовой базы и правовых мер обеспечения кибербезопасности;
– проведение научных исследований в области кибербезопасности;
– создание условий для разработки, производства и применения средств обеспечения кибербезопасности;
– совершенствование кадрового обеспечения и организационных мер обеспечения кибербезопасности;
– организация внутреннего и международного взаимодействия действующих лиц по обеспечению кибербезопасности;
– формирование и развитие культуры безопасного поведения в киберпространстве и безопасного пользования его сервисами.

Миссией стратегии кибербезопасности также является распределение ответственности между государством, бизнесом и обществом. Так, сферой ответственности государства является правовое регулирование вопросов кибербезопасности и координация усилий стейкхолдеров, сферой ответственности бизнеса является обеспечение кибербезопасности критической информационной инфраструктуры, находящейся в частной собственности, внедрение и соблюдение стандартов кибербезопасности, сферой ответственности общества – повышение уровня цифровой грамотности и обеспечение обратной связи в ответ на усилия государства и бизнеса.

Следует отметить, что проявление мультистейкхолдерного подхода в работе над концепцией стратегии кибербезопасности не ограничилось приглашением на площадку Временной комиссии Совета Федерации по развитию информационного общества представителей экспертного сообщества, гражданского общества и бизнеса. Не ограничилось его проявление и проведением парламентских слушаний в верхней палате российского парламента, в которых могли принять участие заинтересованные лица. Речь идет о том, что в январе 2014 года, концепция стратегии кибербезопасности была размещена для общественного обсуждения на официальном сайте Совета Федерации[7]. На наш взгляд, применение технологии краудсорсинга и учет замечаний и предложений по итогам общественного обсуждения придадут этому документу комплексности и демократичности.

Подводя итог вышеизложенному, обозначим перспективы концепции стратегии кибербезопасности Российской Федерации. Планируется представить ее Председателю Совета Федерации Федерального Собрания Российской Федерации как члену Совета Безопасности Российской Федерации для последующего внесения документа на рассмотрение.

На основе концепции стратегии кибербезопасности может быть создана собственно стратегия кибербезопасности Российской Федерации. Мы полагаем, что она станет существенным вкладом в развитие информационного общества России.

[7] URL: http://www.council.gov.ru/press-center/discussions/38324.