

Концептуальные различия в понимании информационной безопасности в западной и российской традициях

Научный руководитель – Барина Екатерина Александровна

Тихонов Александр Эдуардович

Студент (бакалавр)

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Москва, Россия
E-mail: al_rednaxe@mail.ru

В современном мире информация является неотъемлемой частью нашей жизни. По мере роста её количества, растут и угрозы по отношению к ней. Особый интерес представляет сравнение понимания термина «информационная безопасность» в западной и российской традициях не только с теоретической точки зрения, но и к каким практическим последствиям приводят расхождения в его понимании. В качестве примера западного подхода к ИБ в данной работе взята Великобритания.

В декабре 2016 года указом Президента Российской Федерации была утверждена новая Доктрина информационной безопасности нашей страны. По сравнению с предыдущим аналогичным документом от 2000 года, новая Доктрина направлена на защиту россиян от опасности «информационно-психологического воздействия» [3]. Параллельно в 2016 году в Великобритании был принят новый стратегический документ по информационной безопасности Соединённого королевства - Национальная Стратегия Правительства по кибербезопасности (National Cyber Security Strategy 2016-2021).

Начать следует с общего принципа, который содержится в обоих документах: информационная безопасность понимается как одна из главных составляющих государственной безопасности в современном мире. В этом случае по отношению к данному термину можно применить некое универсальное определение, которое подходит под понимание как России, так и Великобритании: информационная безопасность - это невозможность нанесения вреда человеку, обществу и государству путём воздействия на информационную сферу жизни каждого из этих субъектов [2]. Однако стоит понимать, что в Великобритании, которая представляет западную традицию, используется термин «кибербезопасность», который в большей степени фокусируется на технологических аспектах информационной безопасности, то есть кибербезопасность является составной частью информационной безопасности. Стратегия Соединённого Королевства и доктрина Российской Федерации направлены на поддержание информационной безопасности, но основные цели, направления и методы её обеспечения у двух стран различаются.

Различий в понимании ИБ на Западе и в России довольно много, но стоит сконцентрироваться на некоторых из них. В основе расхождений лежит различное понимание источников угроз информационной безопасности двух стран: для Великобритании главную угрозу несут террористические и экстремистские организации [5], например, Исламское Государство (запрещена в РФ), однако в Доктрине информационной безопасности Российской Федерации угрозой также служат другие государства и иностранные СМИ, которые публикуют материалы, содержащие «предвзятую оценку государственной политики РФ» [1].

Следующим важным аспектом являются цели, которые перед собой поставили два государства. Согласно Доктрине информационная безопасность в нашей стране более детально сосредотачивается на военно-политической сфере, а также на противодействии

психологическому давлению на наших граждан со стороны террористических группировок и зарубежных СМИ [1]. Тогда как в британской Национальной Стратегии Правительства по кибербезопасности акцент сделан не столько на информационную безопасность в военной сфере, сколько на экономическую сферу и на общество в целом [5]. Это может свидетельствовать о том, что в Соединённом Королевстве уже достаточно хорошо развита кибербезопасность военно-промышленного комплекса, в отличие от нашей страны.

И последнее, на чём стоит остановиться - источник формирования политики в сфере информационной безопасности согласно двум документам. В России этим занимаются Совет Федерации ФС РФ, Государственная Дума ФС РФ, Центральный банк РФ, Совет Безопасности РФ и другие государственные органы [1]. В Великобритании ситуация совершенно другая: планируется создание отдельного института по исследованию вопросов информационной безопасности, а также открытие Инновационного фонда по кибербезопасности [5].

В соответствии с разными ценностными парадигмами западного и российского обществ происходит и расхождение в подходах к ключевым вопросам информационной безопасности, по которым мы должны договариваться с нашими коллегами из других стран. Россия, а вместе с ней и другие государства индустриальной волны с сильной государственноцентристской традицией, верит в контроль и государственное регулирование, тогда как запад - в ценности свободы и саморегулирования. Иллюстрацией данного тезиса могут служить переговоры 2011 года, когда постоянные представители России, Китая, Таджикистана и Узбекистана при ООН предложили утвердить проект «Правил поведения в области обеспечения международной информационной безопасности» в качестве официального документа 66 сессии ГА ООН. Согласно документу должен был быть выработан кодекс ответственного поведения государств в сфере международной информационной безопасности с учётом всех современных угроз. Но США и Великобритания подвергли сомнению российские инициативы, расценив их как попытку насаждения цензуры [4]. С этого момента расхождения между Россией и Западом в понимании ИБ только усилились.

Проанализировав два документа, Доктрину информационной безопасности РФ и Национальную Стратегию Правительства по кибербезопасности, можно сделать вывод, что существуют серьёзные расхождения в понимании информационной безопасности в западной и российской традициях. Есть всего лишь один общий пункт, согласно которому кибербезопасность - это то, о чём сейчас должны задумываться страны, так как информация стала играть ключевую роль в современной жизни. Однако различий намного больше: разные цели, разное видение угрозы и разная опора при выработке политики в этой области. Пока не будут урегулированы противоречия в области информационной безопасности между Россией и Западом, о развитии какого-либо сотрудничества в этой сфере можно забыть.

Источники и литература

- 1) Доктрина информационной безопасности Российской Федерации [Текст]: указ Президента РФ от 5 декабря 2016 г. №646.
- 2) Губанов В.М., Михайлов Л.А., Соломин В.П. Чрезвычайные ситуации социального характера и защита от них. М., 2007.
- 3) «Доктрина информационной безопасности РФ. Досье» [сайт]: <http://tass.ru/info/3845810>
- 4) «Понятие свободы не абсолютно» [сайт]: <https://www.gazeta.ru/business/2012/02/09/3994965.shtml>

5) National Cyber Security Strategy 2016-2021: 1 November 2016.