***Л.В.Николаева**, доцент*
Mikalayeva@bsuir.by
УО «БГУИР» (Минск)

ИНФОРМАЦИОННАЯ ВОЙНА КАК СОВРЕМЕННОЕ СРЕДСТВО ДОСТИЖЕНИЯ ПОЛИТИЧЕСКИХ ЦЕЛЕЙ

Одной из современных общемировых тенденций и реалий является переход от стадии индустриального общества к постиндустриальному, информационному обществу. Поступательное развитие Республики Беларусь как сильного и процветающего государства невозможно вне контекста данных процессов и явлений. В связи с чем информационная безопасность становится одним из важнейших направлений безопасности белорусского государства.

В пункте 2 Главы 1 «Мировое значение информационной сферы» «Концепции информационной безопасности Республики Беларусь», принятой в 2019 г., указывается, что «трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов» [4].

Одной из таких угроз и новых форм борьбы между государствами являются информационные войны, предстающие как система мер, которые осуществляется одними государствами с целью подрыва информационной безопасности других государств. Термин «информационная война» может быть определен как **«**деятельность, направленная на получение преимущества над конкурентом или противником, когда методом и механизмом выступают мобилизация своих собственных информационных ресурсов, либо отказ (препятствие) противнику в полной мере использовать свои информационные ресурсы. Целью такого рода войн является попытка манипуляции общественным сознанием для дестабилизации противника и привлечения сторонников как внутри государства, так и за его пределами» [3, с. 202]. В данной связи становится особенно очевидным, что развитие и внедрение в различные общественные сферы новых информационно-коммуникационных технологий (далее – ИКТ), как и любых других научно-технических достижений, способны не только приносить пользу, но и таят в себе опасность.

Исследователи выделяют два вида опасных информационных воздействий. Первый связан с потерей ценной информации, что может привести либо к снижению эффективности собственной деятельности, либо к повышению результативности деятельность противника, конкурента. Объектом такого воздействия могут быть либо сознание людей, либо технические системы. В первом случае это может привести к разглашению государственных тайн, вербовке агентов, сопряжено с применением специальных мер и средств для подслушивания, использованием детекторов лжи, медикаментозными, химическими и другими воздействиями на психику человека. Во втором случае

речь идет уже о технической разведке, или шпионаже (перехват телефонных разговоров, радиограмм, сигналов других систем коммуникации), проникновении в компьютерные сети, банки данных. «Безопасность от информационного воздействия данного вида обеспечивают органы цензуры, контрразведки и другие субъекты информационной безопасности» [2, с. 10].

Второй вид опасного информационного влияния связан с внедрением деструктивной информации, что может не только привести к принятию опасных ошибочных решений, но и заставить действовать во вред, даже поставить общество на грань катастрофы. «Информационную безопасность этого вида должны обеспечивать специальные структуры информационно-технической борьбы. Они нейтрализуют акции дезинформации, пресекают манипулирование общественным мнением, ликвидируют последствия компьютерных атак» [2, с. 10].

В данной связи можно выделить несколько групп опасностей, возникших в условиях активного внедрения ИКТ. Во-первых, бурное развитие информационного оружия, способного эффективно воздействовать на психику и сознание людей, а также на общественную информационно-техническую инфраструктуру. Такие информационно-психологические технологии могут использоваться в качестве специальных механизмов управления кризисами и провоцирования жестокости на территории противника.

Во-вторых, появление новой разновидности преступлений, связанных с использованием ИКТ (махинации с криптовалютой, компьютерное хулиганство и др.). Особенно актуальными становятся проблемы транснациональной трансграничной киберпреступности.

В-третьих, использование ИКТ в политических целях [2, с. 10–11]. Исследователи отмечают резкий рост массовых протестных выступлений в различных странах и регионах мира, которые отличаются активным использованием потенциала глобальной сети Интернет и социальных сетей [1, с. 47].

Данная тенденция была отмечена и в «Концепции информационной безопасности Республики Беларусь». Так, пункте 40 Главы 10 «Обусловленность мер по обеспечению безопасности в информационном пространстве» данного документа указывается, что «… механизмы деструктивного информационно-психологического воздействия на личность, общество и государство постоянно совершенствуются, а масштабное манипулирование массовым сознанием принимает такую же остроту, как борьба за территории, ресурсы и рынки. Через информационное пространство осуществляется преднамеренная дискредитация конституционных основ государств и их властных структур, размывание национального менталитета и самобытности, вовлечение людей в экстремистскую и террористическую деятельность, разжигание межнациональной и межконфессиональной вражды, формирование радикального и протестного потенциала. Информационный фактор играет все более значительную роль в межгосударственных конфликтах и неявных действиях, направленных на нарушение суверенитета,

территориальной целостности стран и снижение темпов их развития. В результате информационных воздействий существенно меняются социальные связи человека в обществе, стиль мышления, способы общения, восприятие действительности и самооценка.

Все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к фейковым сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных и иных подобных целях» [4].

В последнее время можно наблюдать активное использование в рамках информационных войн потенциала социальных сетей. После событий так называемой «арабской весны» 2011 года, когда по странам Северной Африки и Ближнего Востока прокатилась волна протестов граждан против политики властей, в лексикон политологов прочно вошло понятие «сетевая революция». Под данным термином следует понимать «активное использование современных компьютерных технологий, программного обеспечения, мессенджеров, коммуникационных возможностей Интернета в качестве катализатора протестных настроений, организатора и координатора проведения массовых уличных акций, ставящих своей целью получение от действующей власти уступок, выполнение определенных требований в социально-политической, экономической и других сферах либо смену власти, в том числе неконституционным путем» [1, с. 48]. В условиях широкого использования населением средств сетевой коммуникации «сетевые революции» становятся инструментом с большим потенциалом применения для смены политических режимов.

Таким образом, на современном этапе развития общества может быть классифицирован новый тип революций, которые обусловлены внедрением и эксплуатацией новейших сетевых технологий. Последние «позволяют в кратчайшие сроки мобилизовать для участия в протестных акциях огромное количество лично не знакомых и не связанных между собой людей. Целенаправленное манипулирование средствами сетевых коммуникаций позволяет согласовывать интересы, позиции и точки зрения огромного числа людей, разбросанных в пространстве, формировать у них чувство принадлежности к единому целому (группе, сообществу, территории и т. д.). Их использование позволяет аккумулировать протестный потенциал, осуществлять запуск социального протеста, переводить его в массовую форму и использовать для получения политических результатов» [1, с. 56].

Отдельные приемы политических технологий сетевого протеста были опробованы в Беларуси в ходе президентских выборов 2020 г. Анализ применения ИКТ и сетевых технологий в белорусском социуме позволяет утверждать наличие опасности применения деструктивных методов «сетевых революций» в будущем. В связи с данными обстоятельствами представляется

необходимым учесть подобные риски в рамках работы по обновлению «Концепции национальной безопасности Республики Беларусь».

Список источников:

1. Арчаков, В. К пониманию феномена современных «сетевых революций» в контексте обеспечения национальной безопасности Республики Беларусь / В. Арчаков, А. Баньковский, Ю. Александров // Беларуская Думка. – 2021. – № 12. – С. 47–57.

2. Мигун, Д. А. Информационный экстремизм и информационная безопасность / Д. А. Мигун. – Минск : РИВШ, 2020. – 64 с.

3. Политические институты и процессы в информационном обществе : учеб. пособие / И. В. Вашкевич [и др.] ; под ред. И. В. Вашкевич. – Минск : БГУИР, 2018. – 236 с.

4. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 года № 1 «О концепции информационной безопасности Республики Беларусь» // Национальный правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P219s0001&ysclid=la29rok0us664497979. – Дата доступа: 04.11.2022.