УДК 342.7

ПРАВО НА ЗАЩИТУ ОТ ДЕСТРУКТИВНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ КАК НЕОТЪЕМЛЕМЫЙ ЭЛЕМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Кузьменкова Татьяна Николаевна,
Могилёвский государственный университет имени А. А. Кулешова
(г. Могилев, Беларусь)

В работе отражена актуальность и проблематика правового сопровождения информационной безопасности личности. Акцент сделан на исследовании права личности на защиту от деструктивного информационного воздействия; предложены направления совершенствования организационно-правового механизма в рассматриваемой области общественных отношений.

Современные процессы эволюции общества в направлении тотального применения информационно-коммуникационных технологий обусловливают актуальность защиты личности от различного рода угроз в информационном пространстве.

Посягательство на интересы личности может вестись по нескольким направлениям:

– уязвимость персональных данных и информации о личной жизни, в том числе в глобальном информационном пространстве;

– воздействие кибератак, непосредственно направленных на технические средства, системы и технологии создания, преобразования, передачи, использования и хранения информации (например, использование вредоносных программ, организация ботнетов, несанкционированный доступ к компьютерной информации);

– распространение экстремистских материалов, вовлечение в преступную и антигосударственную деятельность;

– совершение правонарушений с использованием киберпространства (онлайн-грумминг, кибербуллинг, различные виды мошенничества);

– магистральным трендом информационного мира становится «…наполненность слухами и фейками, которые в силу неопределенности развития ситуации и встревоженности населения быстро распространяются в обществе… провоцируют риторику ненависти, повышают риск конфликтов, насилия и нарушений прав человека» [1, с. 68].

Подавляющее большинство существующих в информационном пространстве угроз можно охватить понятием «деструктивное информационное воздействие». К нему можно отнести как распространение явной ин-

формации вредоносного характера (например, пропаганда употребления наркотиков, призывы к самоубийству), так и использование приемов манипулятивного воздействия (то есть таких технологий, которые оказывают скрытое воздействие на подсознание и поведение целевых групп): «утаивание психологически важной информации или включение значимой информации в общий контекст информационного потока; намеренное упрощение и суггестия, выражающаяся в целенаправленном повторении; изменение смысла понятий…; намеренное включение широко известного образа – известных политических деятелей, представителей шоу-бизнеса…; ангажированность в освещении событий, акцентирование и поиск негатива в абсолютно любом явлении, происходящем в обществе; использование собственно «фейк-ньюс», создающих эмоциональную волну; вынесение абсурдной либо спорной мысли в заголовок в форме вопроса или предположения…» [2, с. 8], распространение оценочной информации.

В рамках развития исследуемой темы автором обосновывается необходимость теоретико-правовой формулировки права личности на безопасность в информационной сфере в качестве отдельной комплексной категории, включающей следующие элементы: право на кибербезопасность, право на защиту персональных данных и иной личной информации, право на защиту от деструктивного информационного воздействия. При этом последний элемент является ключевым в общей структуре информационной безопасности личности, однако ввиду отсутствия в законодательстве четких критериев определения деструктивного характера информационного воздействия, глобализации информационного пространства, а также недостаточного уровня развития технических средств защиты, его правовое сопровождение сталкивается с определенными трудностями.

Совершенствование национального организационно-правового механизма, обеспечения информационной безопасности личности в целом и права личности на защиту от деструктивного информационного воздействия, в частности, может вестись по нескольким направлениям:

– во первых, **создание целостной теоретической основы** (эффективность принимаемых мер напрямую будет зависеть от теоретико-правовой проработки категории), что предполагает: теоретическое обоснование информационной безопасности личности, определение ее места в структуре правового статуса, формулировка определения и составляющих информационной безопасности личности, фиксация ценностно-мировоззренческой основы правового регулирования.

– во-вторых, формирование организационной основы: определение конкретного перечня субъектов, вовлеченных в процесс обеспечения информационной безопасности личности (государственных органов, учреж-

дений, предприятий, субъектов гражданского общества), определение (корректировка) их функций и конкретных задач в общем механизме защиты.

– в-третьих, **совершенствование технических средств защиты либо установление административных барьеров в случае**, если уровень развития технических средств защиты не соответствует существующим угрозам. Ярким примером выступает опыт Австралии, где в 2024 году Парламент принял закон, запрещающий использование социальных сетей детьми младше 16 лет [3].

– в-четвертых, ключевым направлением совершенствования организационно-правового механизма обеспечения защиты личности от деструктивного информационного воздействия должна стать **эволюция нормативно-нравовой основы**: фиксация права личности на безопасность в информационной сфере и его составляющих в законодательстве как в общем, так и в отношении отдельных групп (например, несовершеннолетние, избиратели); определение компетенции государственных органов и иных субъектов, вовлеченных в процесс обеспечения информационной безопасности личности, нормативно-правовое сопровождение использования технических средств защиты и административных барьеров. При этом именно «нормативное закрепление определения информационной безопасности личности может стать той отправной точкой, от которой будет в дальнейшем происходить формирование соответствующей государственной политики» [4, с. 27].

Таким образом, оптимизация теоретической основы и законодательства в сфере обеспечения информационной безопасности личности должна осуществляться с учетом специфики информационного общества, когда, с одной стороны, обеспечивается право на получение информации, свобода слова и свобода самовыражения, с другой – информационная безопасность личности, общества и государства.

Синеок исиользованных источников

1. Пунченко, В. Н. Информационная безопасность: новые вызовы в условиях пандемии / В. Н.Пунченко, Е. В. Речиц // Беларуская думка. – № 6. – 2021. – С. 66–72.
2. Фейковизация как средство информационной войны в интернет-медиа : научно-практическое пособие. – Москва : Блок-Принт, 2023. – 144 с.
3. В Австралии запретили подросткам до 16 лет пользоваться соцсетями. – URL: https://www.rbc.ru/life/news/674987709a7947d5f68e9e45 (дата обращения: 29.11.2024).
4. Шаршун, В. А. О некоторых вопросах правового регулирования обеспечения информационной безопасности личности / В. А. Шаршун // Информацнонная безопасность личности и государства в современном международном праве : материалы круглого стола каф. гос. упр. юрид. фак. Белорус. гос. ун-та, Минск, 12 апр. 2022 г. / Белорус. гос. ун-т ; редкол.: В. С. Михайловский (гл. ред.), Е. Ф. Довгань, П. О. Мороз. – Минск : БГУ, 2022. – С. 23–30.