ВОПРОСЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ НОВЫХ ВЫЗОВОВ И УГРОЗ

А.К. Дубень

младший научный сотрудник Института государства и права
Российской академии наук

Доклад посвящен актуальным проблемам правового регулирования отношений в сфере информационной безопасности. Рассмотрена нормативная база в области обеспечения информационной безопасности в сфере обороны. Отмечается, что возрастающая роль информационных технологий ставит перед современным государством новые вызовы и угрозы как с внешней, так и с внутренней стороны. Актуальность данной темы обусловлена возрастающей активностью государств в мировом информационном пространстве, а также действиями государственных служб по обеспечению внутренней информационной безопасности и организации кибератак на информационную инфраструктуру. Проанализирована Стратегия национальной безопасности Российской Федерации в области информационной безопасности, которая определяет вектор развития и совершенствования информационного пространства. Сделан вывод, что технический прогресс, обусловленный созданием новейших технологических платформ и инновационных технологий, влечет за собой угрозы личной, коллективной и национальной безопасности.

В связи с развитием информационно-коммуникационных технологий и повышением вероятности возникновения угроз безопасности личности, общества и государства в целом приобретает актуальность проблема информационной безопасности в обеспечении национальной безопасности государства. В Стратегии национальной безопасности Российской Федерации вопросам информационной безопасности с учетом стратегических национальных приоритетов уделено особое внимание¹.

Президентом Российской Федерации В.В. Путиным на заседании Совета Безопасности (26 марта 2021 г.) отмечено: «Новые технологические решения порождают новые риски. Мы видим, что глобальное цифровое пространство нередко становит-

ся площадкой для жесткого информационного противоборства, для нечестной конкуренции и кибератак. ...Важно сохранить преемственность нашего стратегического курса на предотвращение конфликтов в информационном пространстве»².

Глава государства особое внимание обратил на то, что Российская Федерация открыта для диалога и конструктивного взаимодействия со всеми государствами мира, причем как в двустороннем формате, так и на площадках международных структур и форумов.

Установление на конституционном уровне гарантий обеспечения безопасности при применении информационных технологий обуславливает необходимость формулиро-

¹ Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 2 июля 2021 г. № 400.

² Заседание Совета Безопасности // Сайт Президента РФ. Новости, выступления и стенограммы. 26 марта 2021 г. (URL: <http://www.kremlin.ru/events/president/news/65231>) (дата обращения: 28.08.2021).

вания основных положений, определяющих подходы к новым вызовам и угрозам.

Министр иностранных дел Российской Федерации С.В. Лавров обратил внимание на отдельные вопросы по обеспечению информационной безопасности с учетом стратегических национальных приоритетов, о чем свидетельствуют отдельные положения его статьи: «Россия продолжит работать над наращиванием двустороннего и многостороннего сотрудничества по всему комплексу актуальных вопросов обеспечения международной информационной безопасностью, в том числе в интересах противодействия угрозам, возникающим в связи с масштабным использованием информационно-коммуникационных технологий в военно-политических целях»³.

Неслучайно вопросы обеспечения информационной безопасности в области обороны страны все более актуальны в системе национальной безопасности России, отечественный законодатель оперативно реагирует на вызовы и угрозы, возникающие в этой области. В соответствии со Стратегией национальной безопасности Российской Федерации одной из основных задач по обеспечению информационной безопасности является укрепление и совершенствование информационной инфраструктуры Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной техники⁴.

³ Статья Министра иностранных дел Российской Федерации С.В. Лаврова «Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью» для журнала «Внешнеэкономические связи» // Сайт МИД РФ, 28 сентября 2020 г. (URL: https://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuDIW/content/id/4350978) (дата обращения: 28.08.2021).

⁴ Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 2 июля 2021 г. № 400.

Состояние информационной безопасности в области обороны сопровождается увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях. Наметилась тенденция смещения военных опасностей и угроз в информационное пространство. Вместе с тем, несмотря на снижение вероятности развязывания крупномасштабных войн, на этом направлении военные опасности для нашей страны усиливаются.

Исходя из анализа документов стратегического планирования к внутренним угрозам информационной безопасности в сфере обороны отнесены: нарушение правил по сбору, обработке, хранению информации, находящейся в воинских формированиях и органах военного управления; ненадежное функционирование информационно-телекоммуникационных систем специального назначения; незащищенность персональных данных военнослужащих и лиц, проходящих военную службу; отсутствие надлежащей защиты интеллектуальной собственности предприятий оборонного комплекса. Вместе с тем, к внешним угрозам, представляющим наибольшую опасность для информационной безопасности военной организации, относятся: разведывательная деятельность иностранных государств на территории Российской Федерации; информационно-техническое воздействие, в том числе кибероружие; деятельность политических и экономических организаций, направленная против интересов Российской Федерации в сфере обороны. В связи с этим ведущие государства при решении проблем обеспечения собственной кибербезопасности в военной сфере все больше внимания уделяют развитию средств защиты национальных информационных ресурсов специального назначения, а также способам

беспрепятственного влияния на информационное пространство других стран.

Таким образом, к числу главных направлений совершенствования системы обеспечения информационной безопасности в области обороны отнесены:

- стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

- совершенствование системы обеспечения информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противооборота;

- прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам в информационной сфере⁵.

Вместе с тем, одними из основных негативных факторов информационной безопасности с развитием автономных систем вооружения являются: нарушение военно-стратегического баланса и формирование глобального военного превосходства отдельных стран; стимулирование гонки вооружений; недостаток транспарентности в этой области, рост подозрений и напряженности в международных отношениях; неоправданное и неконтролируемое распространение и использование автономных систем вооружения, в том числе террористическими организациями; нарастание угроз в области информационной безопасности; милитаризация научно-технических исследований; отсутствие единых правовых основ применения и игнорирование существующих норм международного права⁶.

⁵ Концептуальные взгляды на деятельность Вооруженных Сил в информационном пространстве. URL: <http://www.pravo.gov.ru> (дата обращения: 04.09.2021).

⁶ Военная доктрина Российской Федерации. Утверждена Президентом Российской Федерации 25 декабря 2014 г. № Пр-2976.

Указанные выше проблемы неизбежно требуют усиления позиций Российской Федерации на международной арене в условиях конкурентоспособной информационной борьбы как с уже существующими, так и с новыми центрами силы в области обороны, а также дальнейшего совершенствования международно-правовой регламентации средств и методов обеспечения информационной безопасности на основе применения передовых технологий.

При решении проблем обеспечения собственной безопасности в области обороны все больше внимания уделяется развитию средств защиты национальных информационных ресурсов, а также способам беспрепятственного влияния на информационное пространство других стран. С этой целью большинство влиятельных государств (таких как США, Великобритания, Китай, Индия и др.) либо создали, либо находятся в процессе формирования специализированных концепций (программ) использования информационного пространства в военных целях.

С учетом отсутствия согласованной системы международной информационной безопасности необходимо принять во внимание опыт зарубежных партнеров по защите информационной безопасности в военной организации государства. В частности, Военная стратегия Китая определяет следующие меры: увеличение возможностей наблюдения за состоянием безопасности; возможность обеспечения кибербезопасности; усиление возможности по предотвращению и контролю киберпреступных деяний; обеспечение защиты национальной сетевой и информационной безопасности⁷. Из анализа данного доку-

⁷ Военная стратегия Китая: Девятая «Белая книга» / пер. Н.Н. Шишкиной. Центр Сулакшина (Центр научной политической мысли и идеологии). URL: <https://rusrand.ru/events/>

мента следует сделать вывод о том, что в последнее время национальная политика этого государства предполагает применение специальных информационных систем в целях обеспечения его информационной безопасности на основе комплексного использования военных, политических и экономических мер.

На сегодняшний день информационная безопасность в российском законодательстве проявляется не только как самостоятельный вид безопасности, но и как аспект

voennaja-strategija-kitaja-devjataja-belaja-kniga (дата обращения: 06.09.2021).

военного обеспечения национальной безопасности страны. Рассматриваемые новые вызовы и угрозы возникают в результате увеличения количества центров мирового экономического и политического развития, укрепления позиций глобальных и региональных стран-лидеров. В связи с этим информационная безопасность страны способствует дальнейшему повышению внутренней стабильности, наращиванию экономического, политического и военного потенциала, необходимого для укрепления ее роли как одного из влиятельных центров современного мира.

ВОЕННО-УГОЛОВНОЕ ПРАВО КАК ПОДОТРАСЛЬ ВОЕННОГО ПРАВА: ПРАКТИЧЕСКИЕ ВОПРОСЫ РЕАЛИЗАЦИИ ПОДХОДА

Я.Н. Ермолович,

профессор кафедры уголовного права и криминологии ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации», доктор юридических наук, доцент

В докладе рассматриваются проблемные вопросы соотношения и взаимосвязи военного и уголовного законодательства, автором формулируется проблема институционализации военно-уголовного права, предлагается авторское видение вариантов разрешения данной проблемы.

В дореволюционной науке в широком смысле в понятие военно-уголовного закона включалось «всякое законодательное постановление, касающееся военно-уголовного правосудия». В узком смысле под военно-уголовным законом понимался законодательный запрет или приказ, нарушение или неисполнение которого гарантируется положенным в нем наказанием. Отмечалось, что не могут представлять особенностей ни учение о соотношении военно-уголовного закона и охраняемых им правовых норм, ни учение об элементах

военно-уголовного закона¹. Военно-уголовный закон охраняет от нарушения нормы военного закона, что является его единственной задачей. Поскольку нормы военного закона не охраняются общим уголовным законодательством, постольку в этих пределах имеет право на существование закон военно-уголовный. Соотношение общего и военно-уголовного законодательства должно выражаться идеей зависимости. Воинский устав есть закон специальный, применяемый лишь к лицам подлежащим

¹ Кузьмин-Караваев В.Д. Военно-уголовное право. Часть Общая. СПб., 1895. С. 105 – 107.