УДК 349

Саралиев Ш. И.., магистрант
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации
Россия, г. Москва

ТЕРМИНОЛОГИЯ КИБЕРБЕЗОПАСНОСТИ: АНАЛИЗ ЮРИДИЧЕСКИХ ПОДХОДОВ

Аннотация. *В статье рассматриваются вопросы правового определения кибербезопасности в нормах современного российского права. Автором рассматриваются определения кибербезопасности, существующие в нормативно-правовых актах РФ, а также контекст применения данного термина. Отдельно анализируются положения предлагаемого проекта Концепции стратегии национальной кибербезопасности, который находится в разработке Совета Федерации. По результатам проведенного анализа автором сделаны выводы об отсутствии единого правового толкования термина «кибербезопасность», что создает определенные сложности для единообразного правоприменения в отношении данной категории в российской законодательной системе.*

Abstract. *The article discusses the issues of the legal definition of cybersecurity in the norms of modern Russian law. The author examines the definitions of cybersecurity existing in the regulatory legal acts of the Russian Federation, as well as the context of the use of this term. The provisions of the proposed draft Concept of the National Cybersecurity Strategy, which is being developed by the Federation Council, are analyzed separately. Based on the results of the analysis, the author concludes that there is no uniform legal interpretation of the term "cybersecurity", which creates certain difficulties for uniform law enforcement in relation to this category in the Russian legislative system.*

Ключевые слова: *кибербезопасность, национальная безопасность, информационная безопасность, информационная защищенность, юридическая доктрина.*

Keywords: *cybersecurity, national security, information security, information security, legal doctrine.*

Информатизация современного общества требует сопутствующего развития правовой сферы, регулирующей возникающие социальные и экономические процессы. Одним из важнейших вопросов современного общества выступает вопрос безопасности данных и конфиденциальной информации, существующей в информационном виде. Основные аспекты информационной безопасности в российской правовой практике сформулированы в действующих положениях Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»[1]. Однако самого термина «кибербезопасность», которое распространено в научной литературе, нормы закона не содержат, что создает правовую неопределенность с точки зрения терминологии. Стоит отметить, что термин «кибербезопасность» характерен для зарубежных правовых систем, в то время как российские законодательные нормы оперируют определениями информационной безопасности.

Изучаемый вопрос требует углубленного изучения терминологии, представленной в российских правовых актах и научной литературе. В понимании О. А. Пучкова юридическая доктрина разграничивает понятия информационной безопасности и кибербезопасности[2]. Интересным представляется тот факт, что точного определения соотношения указанных

[1] Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 31.07.2006. - №31 (1 ч.). – Ст. 3448.

[2] Пучков О. А. Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике // Право и государство: теория и практика. – 2019. – №5 (173). – С. 66.

терминов в настоящее время не сформулировано, а вопрос тождественности является дискуссионным, поскольку в зависимости от контекста указанные определения могут использовать как синонимичные, либо как нетождественные. В частности, О. А. Пучков рассматриваемые понятия схожими не считает: информационная безопасность (либо InfoSec) есть «процесс цифрового противодействия несанкционированному доступу к информации (данным)», в то время как кибербезопасность имеет отношение непосредственно к технологическому процессу в части применения протоколов безопасности.

Обратимся к положениям нормативных документов. Содержание Доктрины информационной безопасности Российской Федерации трактует определение информационной безопасности следующим образом – «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Однако, представленное определение достаточно обширное и не поясняет правовой сущности рассматриваемого термина.

Исходя из смысла ст. 11.2 Федерального закона от 03.04.1995 №40-ФЗ «О федеральной службе безопасности» под информационной безопасностью понимается конкретная область деятельности указанной властной структуры, которая реализуется посредством использования криптографических и инженерно-технических методов безопасности, применяемая в отношении информационно-телекоммуникационных систем, а также сетей связи, которые используются для передачи

шифрованной информации как на территории РФ, так и в учреждениях федерации, расположенных за ее пределами[3].

Анализируя нормативно-правовые дефиниции, предложенные российским законодателем, можно отметить отсутствие детальной проработки терминологии с позиции технических тонкостей. Однако, более детальная проработка термина представлена в нормативно-правовых актах, имеющих меньшую юридическую силу.

В соответствии с положениями ГОСТ Р 56205-2014 кибербезопасность рассматривается в качестве синонима термина защищенности сети, либо термина киберзащиты[4]. В отличии от норм Доктрины информационной безопасности, которая рассматривает информационную безопасность как поддерживаемое состояние защищенности, в то время как нормы указанного ГОСТ трактуются как конкретные действия, которые осуществляются с целью предотвращения несанкционированного доступа к информации и иных негативных последствий такого доступа. Примечателен тот факт, что к последствиям, которые должны быть предотвращены посредством мер кибербезопасности, отнесены не только вопросы использования информации, но и потери прибыли, а также повреждения самих информационных объектов (либо критических систем). Исходя из представленного термина можно отметить, что область кибербезопасности охватывает не только вопросы защиты информации, но также и защиты физических объектов, обеспечивающих функционирование информационных систем от внешнего либо внутреннего воздействия, а также защиты предпринимательских интересов.

Согласно положениям выше указанного ГОСТ, к области действия кибербезопасности отнесены не только интересы в информационной сфере, но и непосредственные риски угрозы здоровья граждан, потери доверия

---

[3] Федеральный закон от 03.04.1995 №40-ФЗ (ред. от 01.07.2021) «О федеральной службе безопасности» // Собрание законодательства РФ. – 10.04.1995. - №15. – Ст. 1269.

[4] ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели // М.: Стандартинформ, 2020.

общественности либо риски несоответствия нормативам. Подобный подход расширяет границы термина «кибербезопасность», тем самым информационная деятельность в контексте употребляемого термина перестает быть исключительной сферой, к которой возможно применение действий киберзащиты.

Обратимся к положениям Дорожной карты развития «сквозной» цифровой технологии «Системы распределенного реестра», которые были разработаны Минцифры. Данный документ не содержит прямого определения термина кибербезопасности, однако определяет результаты, которые должны быть достигнуты за счет применения мер кибербезопасности. Основываясь на положениях документа можно отметить, что под кибербезопасностью понимаются действия, которые осуществляются с целью повышения уровня защищенности от кибератак в виде захвата ресурсов или вычислительных мощностей и направлены на снижение количества сбоев инфраструктуры (исходя из специфики Дорожной карты применяется термин финансовой инфраструктуры)[5].

В настоящий момент в Совете Федерации находится в разработке проект Концепции стратегии кибербезопасности РФ. Данный проект концептуально меняет понимание кибербезопасности и ее места в стратегии национальной безопасности. Согласно проектным положениям кибербезопасность является частью информационной безопасности, которая характеризуется как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями»[6]. Соответственно, приведенная трактовка охватывает непосредственно защиту коммуникационных каналов – сети интернет, иных телекоммуникационных сетей.

---

[5] Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций https://digital.gov.ru/, 14.10.2019.

[6] Концепция стратегии кибербезопасности Российской Федерации (проект) // Официальный сайт Совета Федерации Федерального собрания РФ http://council.gov.ru/

Таким образом, термин кибербезопасности не применяется в юридических актах высшей силы, однако, активно употребляется в нормативных документах министерств и ведомств, а также в общеполитическом дискурсе. Это позволяет сделать вывод о том, что термин «кибербезопасность» употребляется в официальных документах, но вместе с тем должной юридической трактовки не имеет, а единообразное толкование в настоящий момент не разработано. Сложившаяся ситуация не создает условий для единства правоприменения, что может негативно сказываться на состоянии национальной или локальной информационной безопасности в целом.

Использованные источники:

1. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 31.07.2006. - №31 (1 ч.). – Ст. 3448.
2. Федеральный закон от 03.04.1995 №40-ФЗ (ред. от 01.07.2021) «О федеральной службе безопасности» // Собрание законодательства РФ. – 10.04.1995. - №15. – Ст. 1269.
3. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели // М.: Стандартинформ, 2020.
4. Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций https://digital.gov.ru/, 14.10.2019.
5. Концепция стратегии кибербезопасности Российской Федерации (проект) // Официальный сайт Совета Федерации Федерального собрания РФ http://council.gov.ru/
6. Пучков О. А. Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике // Право и государство: теория и практика. – 2019. – №5 (173). – С. 66-69.