УДК 340

Д. Н. Лемтюгов (dlemtyugov@mail.ru),
ст. преподаватель
Белорусский торгово-экономический
университет потребительской кооперации
г. Гомель, Республика Беларусь

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ: СООТНОШЕНИЕ ПОНЯТИЙ И ЗАКРЕПЛЕНИЕ В ЗАКОНОДАТЕЛЬСТВЕ РЕСПУБЛИКИ БЕЛАРУСЬ

Статья посвящена рассмотрению соотношения понятий «информационная безопасность» и «кибербезопасность». Автор подчеркивает исключительную важность вопросов обеспечения информационной безопасности в эпоху повсеместной информатизации и цифровизации и возникающих на этом фоне новых правовых и технологических проблем. В статье сопоставляются мнения и взгляды на проблематику теоретиков и ученых в сфере права и технических наук, проводится анализ законодательства Республики Беларусь, регулирующего аспекты информационной безопасности и кибербезопасности.

This article examines the relationship between the concepts of “information security” and “cybersecurity.” The author emphasizes the critical importance of ensuring information security in the era of widespread computerization and digitalization, and the new legal and technological challenges that arise. The article compares the opinions and perspectives of legal and technical scholars and scientists, and analyzes Belarusian legislation regulating information security and cybersecurity.

Ключевые слова: информационная безопасность; информация; информационная инфраструктура; концепция; национальная безопасность; кибератака; кибербезопасность.

Key words: information security; information; information infrastructure; concept; national security; cyberattack; cybersecurity.

В современном мире понятие безопасности государства включает в себя все больше элементов: на первый план выходят аспекты комплексной правовой безопасности человека, его защищенности в многообразии изменяющихся под влиянием научно-технического прогресса общественных отношений. В новых условиях цифровой реальности государство должно гарантировать безопасность реализации прав и свобод человека и гражданина, стабильность и динамичное развитие при сохранении и укреплении национальных фундаментальных ценностей белорусского общества и государства. Сегодня наблюдается возрастающий объем информации любого вида во всех сферах жизни государства, и информация эта используется широко и распространяется в различных областях: от политики и экономики до культуры и бытовых социальных контактов. Во всех этих процессах основой становится повсеместное использование информационных и компьютерных технологий. В связи с этим особую значимость приобретают задачи укрепления и совершенствования системы защиты информационных ресурсов государства.

В настоящее время вопросы определения информационной безопасности и кибербезопасности являются для специалистов и ученых актуальными и дискуссионными. На сегодняшний день нет единых и общепризнанных определений данным элементам безопасных общественных отношений. Так, исследователь Ю. А. Баландин в концептуальном понимании национальной безопасности по «информационной безопасностью» подразумевает способность системы противостоять наносимым извне угрозам технологического и психологического характера, сочетанию данных типов воздействия и восстанавливаться после реализации таковых [1, с. 263–264].

Специалист Ж. О. Кулжабаева, проанализировав законодательство различных государств, предлагает трактовку информационной безопасности как общего термина для создания и обслуживания систем и политик для защиты любой информации – электронной или физической, при этом, данный термин может включать в себя состояние защищенности личности, общества и государства [2, с. 185].

Профессор Ю. К. Язов обращает внимание на то, что спектр угроз информационной безопасности значительно шире спектра угроз безопасности информации [3, с. 4]. Доктор юридических наук В. С. Овчинский в книге «Криминология цифрового мира» приводит следующее определение информационной безопасности – безопасность программно-аппаратных комплексов и сетей, а также размещенных в сетях виртуальных платформ поиска, распознавания, передачи, обработки и хранения сигналов и данных. Информационная безопасность предполагает исключение помех, нарушений или разрушения программно-аппаратных средств, сетей и виртуаль-

ных платформ в результате использования различного рода вредоносного и разрушительного программного кода, а также кражу или нарушение целостности баз данных сведений и знаний [4, с. 223].

В Республике Беларусь систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере представляет Концепция информационной безопасности Республики Беларусь, утвержденная Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1. Именно в тексте Концепции определен термин «информационная безопасность», которая представляет собой состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [5]. Кроме того, информационная безопасность является важнейшей составляющей информационного суверенитета Республики Беларусь – неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность [5].

Говоря о таких категориях общественной безопасности как информационная безопасность и кибербезопасность, нам представляется необходимым упомянуть, что предметом почти всех противоправных деяний в этом сегменте общественных отношений будет являться либо информация, либо компьютерная информация. В 2008 г. в Республике Беларусь был принят Закон «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З. В данном нормативно-правовом акте информация в целом определена как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Данным нормативно-правовым актом регулируются общественные отношения, возникающие при взаимодействии с информацией, информационными технологиями и обеспечением защиты информации. Целями защиты информации вышеназванный закон определяет:

– обеспечение национальной безопасности, суверенитета Республики Беларусь;

– сохранение и неразглашение информации о частной жизни физических лиц и персональных данных, содержащихся в информационных системах;

– обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

– недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий [6].

Анализируя цели защиты информации в целом, стоит обратить внимание на важный вопрос о соотносимости понятий «информационная безопасность» и «кибербезопасность». Среди ученых и теоретиков этот вопрос также является дискуссионным. Например, исследователь Ю. А. Баландин подчеркивает, что не представляется возможным выделить кибербезопасность как элемент системы информационной безопасности [1, с. 262]. Ученый считает, что кибербезопасность представляется комплексной категорией, сочетающей различные отрасли науки, и характеризующейся способностью системы противостоять угрозам, распространяющимся в цифровой среде [1, с. 266].

Кандидат технических наук А. Ю. Добродеев, проанализировав в своей статье различные подходы к определению данной категории общественной безопасности, утверждает, что кибербезопасность – это информационная безопасность компьютерной и инфо-телекоммуникационной инфо-сферы (в том числе в части процессов, контроллеров и «интернет вещей») в современных условиях информационного противоборства, реализующая дополнительно в системе защиты информации не только оборонительные функции, но и функции превентивного воздействия и подавления враждебных и опасных информационных сил и средств противника в угрожаемый период и в военное время [7, с. 67].

Специалист Ж. О. Кулжабаева считает, что необходимо выработать новый подход к законодательному разграничению понятий «кибербезопасность» и «информационная безопасность». Исследователь подчеркивает, что кибербезопасность направлена на защиту систем и содержащихся в них данных, хранящихся исключительно в электронном виде, в киберпространстве [2, с. 185].

Профессор Ю. К. Язов предлагает определение кибербезопасности как состояние защищенности цифровой информации и устройств ее обработки от киберугроз [3, с. 4].

Доктор юридических наук В. С. Овчинский считает, что в рамках цифровой безопасности кибербезопасность – это поддержание целостности и обеспечение бесперебойного функционирования телекоммуникационных сетей и программно-аппаратных средств или модулей управления физическими объектами любого типа, включая машины, механизмы, оборудование, инфраструктурные сети, робототехнику, системы вооружения, а также человека как биологического существа. Кибербезопасность в буквальном ее понимании означает безопасность управления [4, с. 223].

В Республике Беларусь кибербезопасность национального сегмента сети интернет обеспечивается главным образом за счет отражения основного объема кибератак на информационные системы и сети передачи данных путем блокирования вредоносных коммуникаций между субъектами и объектами воздействий. Концепцией информационной безопасности Республики Беларусь термин «кибербезопасность» определен как состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз. Для более полного понимания данного термина раскроем и значение понятия информационная инфраструктура, под которой в соответствии с Концепцией понимают совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации [5].

Важным достижением правового сегмента белорусского государства стало принятие и вступление в силу Указа Президента Республики Беларусь «О кибербезопасности» от 14 февраля 2023 г. № 40. Данным нормативно-правовым актом предусматривается создание в целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз национальной системы обеспечения кибербезопасности. Задачами национальной системы обеспечения кибербезопасности являются:

– достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

– постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети интернет;

– проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;

– оценка эффективности защищенности объектов информационной инфраструктуры от кибератак;

– прогнозирование ситуации в области обеспечения кибербезопасности [8].

Для более полного понимания задач национальной системы обеспечения кибербезопасности отметим, что в соответствующем Указе даны определения понятий «кибератака» и «киберинцидент». Так, под кибератакой понимается целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Киберинцидентом признается событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности [8].

Говоря о соотношении понятий «информационная безопасность» и «кибербезопасность», необходимо отметить, что понятие информационная безопасность – это всеобъемлющее понятие, включающее в себя по логике обеспечение безопасности всей существующей информации как ресурса, обеспечивающего соответствующие потребности личности, общества и в целом государства. Кибербезопасность – понятие, неразрывно связанное с цифровыми технологиями, созданием, обработкой, приемом и передачей информации в цифровой среде. Именно поэтому кибербезопасность можно рассматривать как компонент информационной безопасности. Говоря же исключительно о информационно-коммуникационных технологиях, нужно отметить, что и информационная безопасность и кибербезопасность в совокупности с поведенческой безопасностью являются элементами цифровой безопасности, под которой понимают безопасность использования информационно-коммуникационных технологий во всех аспектах человеческой деятельности на уровне государств, международного сообщества, организаций негосударственного характера, социальных сообществ, групп и отдельных людей.

Вместе с тем представленное в Концепции информационной безопасности Республики Беларусь определение информационной безопасности нам представляется несколько статич-

ным. В условиях быстроразвивающихся технологий и эволюционирующей преступности важным становится не только умение «защищать информацию», но и умение «быстро восстанавливаться и работать» даже под целенаправленной и спланированной атакой. Поэтому мы предлагаем дополнить существующее определение информационной безопасности и изложить его в следующей редакции: «Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере, включающее технологическую независимость, целостность и непрерывность функционирования информационных систем в условиях целенаправленного деструктивного воздействия».

Список использованной литературы

1. **Баландин, Ю. А.** Кибербезопасность и информационная безопасность. Демаркация правовых категорий / Ю. А. Баландин // Правовая политика и правовая жизнь. – 2023. – № 3. – С. 260–270.

2. **Кулжабаева, Ж. О.** Законодательное разграничение понятий «кибербезопасность» и «информационная безопасность» / Ж. О. Кулжабаева // Вестник института законодательства и правовой информации РК. – 2024. – № 4 (79). – С. 178–186.

3. **Язов, Ю. К.** Об определении понятия «кибербезопасность» и связанных с ним терминов / Ю. К. Язов // Вопросы кибербезопасности. – 2025. – № 1 (65). – С. 2–6.

4. **Овчинский, В. С.** Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. – М. : Норма : ИНФРАМ, 2018. – 352 с.

5. **О Концепции** информационной безопасности Республики Беларусь : Постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1 // Национальный центр законодательства и правовой информации Республики Беларусь / Национальный правовой Интернет-портал Республики Беларусь. – Мн., 2026.

6. **Об информации**, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З : в ред. от 12 окт. 2022 г. №209-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 05.04.2026).

7. **Добродеев, А. Ю.** Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века / А. Ю. Добродеев // Вопросы кибербезопасности. – 2021. – № 4 (44). – С. 61–72.

8. **О кибербезопасности** : Указ Президента Респ. Беларусь от 14 февр. 2023 г. № 40 // ЭТАЛОН : информ.-поисковая система (дата обращения: 05.04.2026).