УДК 340.1

ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ КИБЕРПРАВА КАК ОТРАСЛИ ПРАВА

К. В. ЛЕДАК
(Представлено: Я. А. Курто)

В статье исследуются понятие, предмет, объект, метод и принципы киберправа как формирующегося комплексного направления правового регулирования. Рассматривается соотношение киберправа с информационным, цифровым и интернет-правом, а также особенности применения императивного и диспозитивного методов. Обосновывается необходимость правового регулирования цифровых отношений в условиях роста киберпреступности и развития цифровых технологий.

Цифровизация существенно изменила способы осуществления общественных отношений, а именно: взаимодействие граждан и организаций посредством информационных систем, сети Интернет, иных цифровых технологий. Одновременно расширяются угрозы для прав личности, собственности, публичных интересов и национальной безопасности. Так в Беларуси значительная часть киберпреступлений связана с хищениями и мошенничеством. В 2024 году преступления, совершенные с использованием информационно-коммуникационных технологий, составили значительную долю зарегистрированных преступлений, причем более 90 процентов киберпреступлений были связаны с преступлениями против собственности [1]. Распространенными способами обмана являются “фишинг”, мошенничество под видом инвестиционной деятельности, фиктивная продажа товаров и услуг, предложения об аренде жилья [2]. Поэтому осознание того, что информационная сфера нуждается в специальном правовом регулировании, вызвало появление новых понятий и терминов. В результате стало выделяться такое направление, как киберправо, которое находится в процессе активного формирования.

Актуальность темы заключается в том, что киберправо пока не имеет общепризнанного места в системе права. Оно развивается на стыке информационного, уголовного, гражданского, международного, административного права.

Под киберправом стоит понимать область права, включающую в себя отдельные правовые отрасли и регулирующая цифровые отношения, задачей которой является регулирование цифровых отношений субъектов киберпространства, то есть физических и юридических лиц, компаний и государств [3].

Термин “киберправо” пока остается недостаточно четко определенным. Оно формируется как относительно новое направление, которое выделилось из информационного права. При этом до сих пор признается самостоятельной отраслью права не всеми учеными-правоведами. В научной литературе встречаются несколько подходов к понятию киберправа, а именно: его рассматривают как самостоятельную отрасль права, комплексную отрасль и подотрасль информационного права. И.В. Прокопьев отмечает, что отсутствие единого понимания связано с использованием близких терминов и невозможностью провести абсолютно четкую границу между соответствующими направлениями [4, с. 608–609].

К смежной терминологии относятся понятия “цифровое право”, “интернет-право” и “информационное право”. Информационное право регулирует более широкий круг отношений по поводу создания, поиска, получения, хранения, обработки, распространения и защиты информации [5]. Цифровое право обычно понимается как совокупность норм, регулирующих отношения, опосредованные цифровыми технологиями, цифровыми объектами и электронными способами взаимодействия [6]. Интернет-право акцентирует внимание на отношениях, складывающихся именно в сети Интернет, т.е. использование сайтов и платформ, распространение контента и реализация прав пользователей и т.д. Его необходимо рассматривать в рамках информационного права [7]. Киберправо же включает отношения в Интернете, но не ограничивается им, поскольку охватывает также информационные системы, цифровую инфраструктуру и кибербезопасность. Следовательно, эти все термины могут использоваться как близкие, однако полностью отождествлять их не следует [6].

Киберправо определяется автором как совокупность правовых норм, регулирующие общественные отношения, возникающие в цифровом пространстве, включая сеть Интернет, а также в процессе использования цифровых технологий и информационных систем. Оно направлено на упорядочение взаимодействий, складывающихся в условиях цифровизации, когда значительная часть общественных отношений переносится в электронную сферу. Предметом киберправа являются общественные отношения, возникшие в цифровом пространстве, в том числе в сети Интернет, в процессе использования информационно-коммуникационных технологий, информационных систем и иных цифровых технологий. Объектом киберправа являются цифровые блага, по поводу которых возникают общественные отношения, складывающиеся при использовании информационно-коммуникационных технологий, информационных систем и иных цифровых технологий.

Метод киберправа представляет совокупность способов юридического воздействия на отношения в цифровой среде. Он имеет комплексный характер и сочетает императивные и диспозитивные средства [8]. Императивный метод проявляется в установлении обязательных требований к защите информации, обработке персональных данных, расследованию киберпреступлений. Диспозитивный метод характерен для договора об оказании цифровых услуг, электронной торговли и определения условий использования цифровых платформ.

Важное значение имеют также разрешительный, запретительный и обязывающий способы регулирования. Право может разрешать субъекту совершать юридически значимые действия в электронной форме, запрещать неправомерный доступ к системе или распространение охраняемой информации, а также возлагать обязанность принимать организационные и технические меры защиты. В трансграничной цифровой среде метод дополняется международным сотрудничеством, поскольку данные и правонарушители могут находиться в разных государствах. Будапештская конвенция о киберпреступности рассматривается Советом Европы как первый международный договор о преступлениях, совершаемых через Интернет и компьютерные сети [9].

Киберправо основывается на общих правовых принципах, которые применяются с учетом особенностей цифровой среды. Их назначение – обеспечить правомерное использование информационных технологий, защитить права человека и данные, поддержать безопасность информационных систем и установить справедливые последствия за противоправные действия. Положения Конвенции ООН против киберпреступности (принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года) отражают часть этих подходов. В частности, в ней закреплены уважение прав человека, защита суверенитета государств и сотрудничество в предупреждении и расследовании преступлений [11].

Принцип законности означает, что деятельность в цифровой среде, полномочия государственных органов и меры ответственности должны осуществляться в соответствии с Конституцией, законами и иными нормативными правовыми актами. Принцип уважения и защиты прав человека заключается в обеспечении неприкосновенности частной жизни, свободы выражения мнения, права на информацию и судебную защиту.

Принцип безопасности информации предполагает защиту электронных данных и информационно-коммуникационных систем от неправомерного доступа, изменения, уничтожения, блокирования и иных вредоносных воздействий. Он имеет как техническую, так и правовую сторону, а именно: государственные органы должны принимать меры для предупреждения инцидентов и снижения их последствий, а законодательство – устанавливать ответственность за посягательства на данные и инфраструктуру.

Принцип ответственности за цифровые правонарушения означает, что использование цифровых технологий не освобождает лицо от ответственности за деяния, которые нарушают закон и причиняют вред охраняемым интересам. В Республике Беларусь предусмотрена ответственность за цифровые правонарушения, т.е. неотвратимость юридической ответственности при наличии состава преступления (ст. 212, 349, 350, 352, 354, 355 Уголовного кодекса Республики Беларусь от 9 июля 1999 г. № 275-З) [10].

Принцип соразмерности дополняет законность и защиту прав человека. Он предполагает, что вмешательство государства в цифровую сферу должно соответствовать законной цели и не выходить за пределы необходимого. Это особенно важно при получении электронных доказательств, ограничении доступа к информации, проведении обыска цифровых устройств и обработке персональных данных. Чем глубже мера затрагивает частную жизнь, тем существеннее должны быть ее правовое основание, обосновании необходимости и гарантии от злоупотреблений.

Принцип уважения государственного суверенитета имеет особое значение при трансграничных киберинцидентах. Цифровые данные и системы могут находится в разных странах, однако расследование не должно означать произвольное осуществление властных полномочий на территории другого государства. Конвенция ООН против киберпреступности требует действовать с соблюдением суверенного равенства, территориальной целостности и принципа невмешательства [11]. Она также не предоставляет государству права самостоятельно осуществлять на территории другого государства функции, отнесенные его внутренним правом к компетенции местных органов.

Заключение. Киберправо является формирующимся комплексным правовым образованием, регулирующим в общественные отношения в цифровом пространстве. Его понятийная неопределенность обусловлена новизной технологий и пересечением с информационным, цифровым и интернет-правом. Предмет киберправа составляют отношения по поводу цифровой информации, систем, сетей и технологий, а объектом выступают цифровые блага и связанные с ними права.

Метод киберправа составляют императивные и диспозитивные способы, а его принципы направлены на достижение баланса между развитием цифровых технологий, защитой личности, интересами общества и национальной безопасностью. В настоящее время киберправо целесообразно рассматривать не как окончательно обособленную отрасль, а как активно развивающееся комплексное направление правового регулирования, которое может приобрести большую самостоятельность по мере формирования устойчивой системы специальных норм и институтов.

ЛИТЕРАТУРА

1. Национальный Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025. – Режим доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2025/october/90714/. – Дата доступа: 18.09.2026.
2. Национальный Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2026. – Режим доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2026/april/93071/. – Дата доступа: 20.09.2026.
3. Фишинг, вишинг, смишинг, фарминг – в чем разница [Электронный ресурс]. – 2018. – Режим доступа: https://www.protectimus.com/blog/ru-phishing-vishing-smishing-pharming/. – Дата доступа: 25.09.2026.
4. Прокопьев, И. В. Киберправо и его роль в обеспечении национальной безопасности России / И. В. Прокопьев // Образование и право. – 2024. – № 3. – С. 607–611.
5. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З : в ред. от 10 октября 2022 г. № 209-З // ilex : информ. правовая система / ООО “ЮрСпектр”, Нац. центр правовой информ. Респ. Беларусь. – Минск, 2026.
6. Баймакишева, Р. Б. Подходы к пониманию правовой природы цифрового права и его соотношение с другими правовыми категориями / Р. Б. Баймакишева // Молодой ученый. – 2024. – № 17 (516). – С. 233–235. – Режим доступа: https://moluch.ru/archive/516/113308. – Дата доступа: 01.10.2026.
7. Рассолов, И. М. Право и Интернет: теоретические проблемы / И. М. Рассолов – М. : Норма, 2003. – 336 с.
8. Бачило, И. Л. Информационное право : учебник для вузов / И. Л. Бачило. – 5-е изд., перераб. и доп. – М. : Юрайт, 2022. – 419 с.
9. Конвенция о киберпреступности [Электронный ресурс] // WIPO Lex. – Режим доступа: https://www.wipo.int/wipolex/ru/treaties/details/952. – Дата доступа: 08.10.2026.
10. Уголовный кодекс Республики Беларусь : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : в ред. Закона Респ. Беларусь от 20 октября 2025 г. № 101-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2026.
11. Конвенция Организации Объединенных Наций против киберпреступности [Электронный ресурс]. – 2024. – Режим доступа: https://share.google/sKSoJDHnCGaQS3ycX. – Дата доступа: 08.10.2026.