

КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМАЯ ИНФОРМАЦИЯ ЦИФРОВОГО ПРОСТРАНСТВА КАК ИСТОЧНИК ДОКАЗАТЕЛЬСТВ В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Статья исследует криминалистически значимую информацию из цифрового пространства как ключевой источник доказательств при расследовании киберпреступлений, отмечая отсутствие единого понятия «киберпреступления» и его важность для национальной безопасности. Рассматриваются вопросы процессуального оформления и применения электронных доказательств, а также необходимость их законодательного закрепления в Республике Беларусь, включая предложения по изменению уголовно-процессуального кодекса и введению новой статьи об «Электронных доказательствах» для повышения эффективности уголовного судопроизводства.

This article examines forensically significant information from the digital space as a key source of evidence in cybercrime investigations, noting the lack of a unified definition of “cybercrime” and its importance for national security. It examines the procedural registration and use of electronic evidence, as well as the need for its legislative codification in the Republic of Belarus, including proposals to amend the Criminal Procedure Code and introduce a new article on “Electronic Evidence” to improve the efficiency of criminal proceedings.

Ключевые слова: киберпреступность; информационная безопасность; судебная практика; доказательства; кибербезопасность.

Key words: cybercrime; information security; judicial practice; evidence; cybersecurity.

В настоящее время борьба с киберпреступлениями для каждого государства имеет приоритетное значение, поскольку последствия этого негативного социального явления сказываются не только на внутренней стабильности общества, но и на безопасности страны в целом. Киберпреступность сегодня признана глобальной международной проблемой, а одним из решений этой проблемы является обеспечение кибербезопасности – состояния защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Борьба с киберпреступностью занимает особое место в государственной политике по укреплению национальной безопасности в цифровом пространстве.

На сегодняшний день нет единого подхода к определению такого явления, как киберпреступление. Специалисты и ученые предлагают различные трактовки понятия киберпреступность.

Исследователь С. И. Буз предлагает определение киберпреступности как любого преступления, совершенного с помощью информационных технологий, либо в информационном пространстве [1].

Специалисты В. Н. Цимбал и С. Г. Ключев под киберпреступлением понимают противоправное деяние в сфере информационных технологий, совершаемое при помощи таких технологий в глобальных и локальных распределенных вычислительных сетях [2].

Исследователь М. А. Алиасхаб предлагает определение киберпреступности как комплекса правонарушений, совершаемых в информационно-коммуникационном пространстве, вместе с поддержкой или при помощи компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству [3].

Гл. 31 Уголовного кодекса Республики Беларусь посвящена преступлениям против информационной безопасности. Данную группу преступлений можно определить как виновные, общественно опасные и запрещенные нормами гл. 31 деяния (действия или бездействие), которые посягают на безопасность компьютерной информации [4, с. 770].

Президиум Верховного Суда Республики Беларусь отмечает, что противодействие преступлениям против информационной безопасности является одним из приоритетных направлений государственной политики обеспечения национальной безопасности в информационной сфере. Изучение судебной практики показывает, что судами в основном обеспечивается пра-

вильное и своевременное рассмотрение уголовных дел указанной категории. При назначении наказаний соблюдаются принципы уголовного закона и уголовной ответственности [5].

Важно акцентировать внимание на том, что понятие киберпреступлений значительно шире, чем преступления против информационной безопасности. Преступления против информационной безопасности зачастую входят в совокупность с такими преступлениями, как мошенничество, оборот наркотических средств, изготовление и распространение порнографии, нарушение авторских прав и др.

С появлением новых форм преступлений, импульс которым придали информационно-коммуникационные технологии, важнейшим стал и вопрос процессуального оформления доказательств, получаемых из электронных носителей информации, и особенностям их применения в уголовном процессе.

Как отмечает специалист в области уголовного процесса и криминалистики Н. А. Иванов, корректное определение понятия доказательства – необходимое условие решения задач и достижения целей, встающих в уголовном судопроизводстве, которое должно повлиять на весь круг деятельности правоприменительных органов по поиску, сбору, фиксации и использованию доказательств в ходе досудебного и судебного производств по уголовному делу [6, с. 48].

В соответствии со ст. 88 Уголовно-процессуального кодекса Республики Беларусь (УПК) доказательствами являются любые фактические данные, полученные в предусмотренном законом порядке, на основе которых орган, ведущий уголовный процесс, устанавливает наличие или отсутствие общественно опасного деяния, предусмотренного уголовным законом, виновность лица, совершившего это деяние, либо его невиновность и иные обстоятельства, имеющие значение для правильного разрешения уголовного дела [7].

В настоящее время информатизация и цифровизация затронули все направления судопроизводства: уголовное, гражданское и экономическое, – все это обусловило возможность представления сведений, имеющих значение для дела в новых формах. Это могут быть аудио- и видеозаписи, сообщения в мессенджерах, скриншоты и другая информация, полученная в информационно-коммуникационном пространстве.

В своей статье заместитель начальника отдела прокуратуры Минской области, советник юстиции Ю. А. Никитин отмечает: «информационная работа в ходе расследования преступлений – это собирание, хранение, систематизация доказательственной и ориентирующей информации в целях ее дальнейшего анализа и принятия оптимальных для данной следственной ситуации уголовно-правовых, процессуальных и тактических решений, а также в целях обеспечения должного взаимодействия следственных, экспертных подразделений и органов дознания» [8]. «Криминалистически значимая информация, – подчеркивает специалист, – может быть представлена в виде электронного сообщения, электронной страницы в сети интернет, сайта, скриншота переписки в различных мессенджерах, что ставит вопрос о том, к какому виду доказательств такую информацию необходимо отнести» [8].

В ч. 2 ст. 88 УПК указано, что источниками доказательств являются среди прочих и иные документы и другие носители информации, полученные в порядке, предусмотренном настоящим Кодексом. К другим носителям информации относятся материалы фото- и киносъемки, звуко- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, предусмотренном ст. 103 УПК [7]. По мнению специалиста-практика Ю. А. Никитина, к ним можно отнести электронные документы, переписки в социальных сетях и мессенджерах. Кроме того, Ю. А. Никитин акцентирует внимание на том, что в ст. 224¹ УПК, которая регламентирует проведение допроса, очной ставки, предъявление для опознания с использованием систем видеоконференцсвязи, фигурирует дефиниция электронный носитель информации следственного действия, который наряду с протоколом соответствующего следственного действия относится к источникам доказательств и приобщается к материалам уголовного дела. Электронные документы, другие документы в электронном виде, файлы как непосредственные носители компьютерной информации, размещенные на том или ином материальном носителе, при определенных условиях могут признаваться вещественными доказательствами [8].

Отметим, что в параграфе 4 действующего Кодекса гражданского судопроизводства Республики Беларусь в ст. 199 дано определение электронных доказательств, применяемых в гражданском судопроизводстве. Так, электронными доказательствами являются сведения о фактах, имеющих значение для правильного рассмотрения и разрешения дела, содержащиеся на электронных носителях информации, в том числе электронные документы, текстовые, мульти-

медийные и голосовые сообщения, базы данных и другие данные в электронной (цифровой) форме, а также информация, размещенная в глобальной компьютерной сети интернет [9].

Для того, чтобы информация, размещенная в сети интернет, приобрела статус процессуального доказательства, она должна быть представлена в какой-либо объективированной форме.

Каждое доказательство подлежит оценке с точки зрения относимости, допустимости, достоверности, а все собранные доказательства в их совокупности – с точки зрения достаточности для окончания предварительного расследования и разрешения уголовного дела в судебном разбирательстве. Допустимыми признаются доказательства, полученные органом, ведущим уголовный процесс, в установленном УПК порядке и из предусмотренных законом источников [7].

Стало быть, для того, чтобы можно было с уверенностью говорить о допустимости криминалистически значимой информации, полученной из цифрового пространства, именно в качестве электронных доказательств в уголовном судопроизводстве следует внести дополнения в действующую ч. 2 ст. 88 УПК и изложить ее в следующей редакции: «Источниками доказательств являются показания подозреваемого, обвиняемого, потерпевшего, свидетеля, в том числе их звуко- и видеозапись; заключения эксперта; вещественные доказательства; протоколы следственных действий, звуко- или видеозаписи хода судебных заседаний, протоколы судебных заседаний, материалы оперативно-розыскной деятельности, электронные доказательства, иные документы и другие носители информации, полученные в порядке, предусмотренном настоящим Кодексом.»

Помимо этого, необходимо дополнить действующую редакцию УПК ст. 99¹ «Электронные доказательства» и изложить ее в следующей редакции: «электронным доказательством признается цифровая информация, содержащаяся на электронных носителях информации, в том числе при помощи облачных технологий, размещенная в глобальной компьютерной сети интернет, которая служила орудием или средством совершения преступления, или сохранила в себе цифровые следы преступления, или была объектом преступных действий, а также электронные деньги, цифровая валюта, добытые преступным путем, и любая другая цифровая информация, которая может служить средством по обнаружению преступления, установлению фактических обстоятельств уголовного дела, выявлению виновных либо опровержению обвинения или смягчению ответственности обвиняемого».

Список использованной литературы

1. Буз, С. И. Киберпреступления: понятие, сущность и общая характеристика. – URL: <https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-suschnost-i-obschaya-harakteristika/viewer> (дата обращения :23.03.2026).
2. Цимбал, В. Н. Понятие киберпреступления и его содержательная часть / В. Н. Цимбал, С. Г. Ключев // Вестник Московского университета МВД России. – 2021. – № 1. – С. 129–132.
3. Алиасхаб, М. А. Киберпреступность и доказывание в уголовном процессе России. – URL: <https://cyberleninka.ru/article/n/kiberprestupnost-i-dokazyvanie-v-ugolovnom-protsesse-rossii/viewer> (дата обращения: 24.03.2026).
4. Уголовный кодекс Республики Беларусь : науч.-практ. коммент. / под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. – Мн. : Нац. центр правовой информ., 2019. – 1000 с.
5. О практике рассмотрения судами уголовных дел о преступлениях против информационной безопасности (глава 31 УК) : Постановление Президиума Верхов. Суда Респ. Беларусь от 18 дек. 2019 г. № 4. – 2026. – URL: <https://etalonline.by/document/?regnum=s219p0176s> (дата обращения: 10.03.2026).
6. Иванов, Н. А. О понятии «доказательство» в уголовном процессе / Н. А. Иванов // Вестник Омского юридического института. – 2012. – № 1 (18). – С. 47–50.
7. Уголовно-процессуальный кодекс Республики Беларусь от 16 июля 1999 г. № 295-3 // ЭТАЛОН: информ.-поисковая система (дата обращения: 05.04.2026).
8. Никитин, Ю. А. Глобальная сеть интернет как источник информации, значимой для расследования уголовных дел. Часть 2 / Ю. А. Никитин // Национальный центр законодательства и правовой информации Республики Беларусь. – 2026. – URL: <https://etalonline.by/novosti/mnenie/istochnik-informatsii-dlya-rassledovaniya-ugolovnykh-del-2/> (дата обращения: 30.03.2026).
9. Кодекс гражданского судопроизводства Республики Беларусь от 11 марта 2024 г. № 359-3 // ЭТАЛОН : информ.-поисковая система (дата обращения: 05.04.2026).