

Органы предварительного следствия Республики Беларусь в противодействии киберпреступности

А.Э. НАБАТОВА, А.В. ЛЕГЧИЛКИН, С.А. КУЗЬМИЧЁВ

В статье представлены количественный и качественные показатели киберпреступности в Республике Беларусь и исследованы закономерности деятельности по выстраиванию системы специализированных следственных подразделений для расследования киберпреступлений, отражена организационная структура данных органов, исследован информационный и образовательный компоненты указанной деятельности.

Ключевые слова: органы предварительного следствия, киберпреступность, противодействие киберпреступности.

The article presents quantitative and qualitative indicators of cybercrime in the Republic of Belarus and examines the patterns of activity in building a system of specialized investigative units to investigate cybercrimes, reflects the organizational structure of these bodies, and examines the information and educational components of these activities.

Keywords: preliminary investigation bodies, cybercrime, countering cybercrime.

В последние годы мы являемся свидетелями глобальных изменений в динамике и структуре преступности, обусловленных научно-техническим прогрессом, бурным развитием цифровых технологий, трансформацией социальных и экономических отношений в цифровую форму. Технологии цифровой сферы весьма активно применяются в преступной среде и существенно трансформируют традиционное понимание таких криминалистических категорий как время, место, способ, орудия, средства совершения преступлений. Изначально на практике, а позже и в научном обороте появились новые категории «киберпреступность», «киберпреступления». Именно они являются драйвером научного переосмысления тактики и методики расследования преступлений в целом и правоприменительной практики в частности, существенно переформатировали организационно-методические подходы по раскрытию и расследованию преступлений в данной сфере.

С киберпреступностью мир сталкивается на протяжении последних десятилетий, Республика Беларусь не является исключением, о чем свидетельствуют статистические данные последних лет [1], [2]:

Таблица 1 – Количественные показатели преступности и киберпреступности в Республике Беларусь за период с 2010 по 2024 гг.

Год	2010	2015	2018	2019	2020	2021	2022	2023	2024
Количество зарегистрированных преступлений по республике	140 920	96 982	88 813	88 378	95 478	87 696	88 555	85 374	73 270
Количество зарегистрированных киберпреступлений	2 514	2 440	4 741	10 539	25 561	16 446	14 839	18 321	20 137

Из статистических данных и оценок специалистов можно констатировать, что настоящий всплеск киберпреступности случился в Беларуси в 2020 г., когда было зарегистрировано 25 561 преступление, что составило 26,7 % от общего числа зарегистрированных преступлений. В 2021 г. количество киберпреступлений снизилось до 16 446, что составило 18,7 % от общего количества зарегистрированных преступлений. В 2022 г. наблюдалось дальнейшее снижение количества киберпреступлений. Начиная с 2023 г. фиксируется увеличение их числа. В 2024 г. доля киберпреступлений в общей структуре преступности возросла до 27,5 %.

Как отмечают практики, большинство киберпреступлений совершаются с территории Украины и России. Подавляющее количество инцидентов связаны с хищениями путем мо-

дификации компьютерной информации, мошенничества (ст. ст. 209, 212 Уголовного кодекса Республики Беларусь). Характеризуя личность киберпреступника, прослеживаем следующие тенденции. Например, из числа оконченных производством в 2024 г. уголовных дел анализируемой категории 74,1 % обвиняемых – это мужчины, 25,9 % – женщины, 23,0 % – лица, ранее судимые за различные преступления, 17,3 % составляют несовершеннолетние.

В нашей стране ведущая роль в деле противодействия киберпреступности отводится Следственному комитету Республики Беларусь (далее – СК) – единой централизованной системе, включающей государственные правоохранительные органы, являющиеся органами предварительного следствия и осуществляющие полномочия в сфере досудебного уголовного производства. Следует отметить, что абсолютное большинство уголовных дел в республике расследуется сотрудниками СК. Так, в 2023 г. на рассмотрении в следственных подразделениях находилось более 145 000 заявлений о преступлениях. По результатам их рассмотрения возбуждено свыше 85 000 уголовных дел [3].

Как отметил Председатель СК Д.Ю. Гора на коллегии ведомства по подведению итогов служебной деятельности за 2023 г. «Наблюдается ежегодное снижение общего уровня преступности. По сравнению с 2022 г., в 2023 г. общий уровень преступности снизился на 3,5 %. Это связано с позитивными изменениями, которые происходят в нашем обществе, слаженной работой правоохранителей. При этом, наряду с общим уровнем преступности, мы отмечаем рост тяжких и особо тяжких преступлений. Но речь идет не о насильственных преступлениях. Этот рост мы отмечаем за счет повышения уровня киберпреступности» [3].

Как было определено в ходе коллегии СК, наиболее распространены хищения путем модификации компьютерной информации, мошенничества, осуществляемые через глобальную компьютерную сеть Интернет. Со стороны ведомства в 2023 г. проведены совместные с Министерством внутренних дел Республики Беларусь мероприятия по пресечению деятельности трех крупных скам-групп, участники которых в течение трех лет совершили более 20 000 хищений с банковских карт белорусов. Также пресечена деятельность крупнейшего криптообменника, годовой оборот которого составлял около 40 000 000 долларов [3].

В связи с изложенным можно правомерно утверждать, что СК и его подразделения находятся на «передовой» борьбы с киберпреступностью. Причем, данная деятельность носит системный характер, включая различные компоненты – от пресечения преступлений, реализации досудебного производства до профилактики киберпреступлений. Таким образом, определение организационных основ противодействия киберпреступности подразделениями СК является весьма актуальным и заслуживает освещения в рамках настоящего исследования.

Итак, в качестве *объекта* для рассмотрения целесообразно определить закономерности деятельности по выстраиванию системы специализированных подразделений СК для расследования киберпреступлений. *Цель* исследования – продемонстрировать: структуру специализированных подразделений СК по расследованию киберпреступлений; иные организационные компоненты деятельности СК по противодействию преступности. Для достижения поставленной цели необходимо решить следующие *задачи*: 1) продемонстрировать организационную структуру подразделений СК в рассматриваемой сфере; 2) определить информационный компонент деятельности указанных подразделений; 3) определить образовательный компонент деятельности по противодействию киберпреступности.

Для выстраивания организационной структуры подразделений СК по расследованию киберпреступлений возникли предпосылки прикладного и правового характера. Во-первых, с точки зрения правоприменительной практики сложились условия, при которых киберпреступления заняли одно из ведущих мест в динамике преступности и доля их весьма существенна, что потребовало адекватных мер реагирования и оптимизации следственной деятельности по расследованию данных преступлений.

Во-вторых, на протяжении последнего десятилетия в Республике Беларусь постоянно совершенствуется законодательство в сфере информатизации и цифровизации, были приняты и действуют законы, указы, программные документы. Одним из них является государственная программа «Цифровое развитие Беларуси» на 2021–2025 гг., утвержденная постанов-

лением Совета Министров Республики Беларусь от 02.02.2021 г. № 66. Ею предусматривается развитие электронного правительства, повышение эффективности реализации государственных функций посредством создания комплексной цифровой инфраструктуры для осуществления межведомственного информационного взаимодействия, формирования современной системы оказания государственных услуг [4].

Во исполнение указанной программы принят Указ Президента Республики Беларусь от 07.04.2022 г. № 136 «Об органе государственного управления в сфере цифрового развития и вопросах информатизации» (далее – Указ № 136), в соответствии с которым Министерство связи и информатизации Республики Беларусь наделено полномочиями в части управления процессами цифрового развития в государстве, цифровой трансформации системы государственного управления всех отраслей экономики [5]. Для реализации указанных целей создан Центр цифрового развития, оказывающий содействие государственным органам и организациям по цифровизации их деятельности. Также, в соответствии с Указом № 136 руководителям государственных органов и иных государственных организаций предписано определить «офисы цифровизации» по организационному и техническому обеспечению реализации мероприятий в сфере цифровизации.

Так, по согласованию с Главой государства в СК с 12 апреля 2023 г. создан «офис цифровизации» – главное управление цифрового развития предварительного следствия. Как отмечает А.Ф. Мотолько, одной из задач подразделений цифрового развития предварительного следствия СК является информатизация служебной деятельности, обеспечение реализации единой технической и технологической политики цифрового развития в ведомстве, организация и координация деятельности по разработке программного обеспечения и информационных систем [6, с. 252]. Помимо указанных целей главное управление цифрового развития предварительного следствия реализует координирующую и руководящую роль по противодействию киберпреступности в различных ее формах. В целях упорядочения деятельности в рассматриваемой сфере помимо указанного управления образованы специализированные подразделения СК на региональном уровне.

Подразделения, расследующие киберпреступления, выступают в качестве самостоятельной подсистемы в структуре СК, функционирующей на республиканском, областном и районном (межрайонном) уровнях.

I. Республиканский уровень:

Главное управление цифрового развития предварительного следствия в центральном аппарате СК (далее по тексту ГУЦРПС).

Ведомственный процессуальный контроль осуществляется сотрудниками главного управления процессуального контроля центрального аппарата СК.

II. Областной уровень управления СК по областям и г. Минску:

Отделы цифрового развития предварительного следствия по областям и г. Минску.

Отдел по расследованию преступлений против компьютерной безопасности и незаконного оборота наркотических средств следственного управления.

Ведомственный процессуальный контроль за осуществлением предварительного следствия осуществляется сотрудниками управлений процессуального контроля СК по областям и г. Минску.

III. Районный (межрайонный) уровень (городские отделы / районные отделы СК):

Специализированные группы по расследованию преступлений, совершенных с использованием информационно коммуникационных технологий. В небольших районных подразделениях предусмотрена специализация отдельных следователей.

Таким образом, есть все основания полагать, что на сегодняшний день в структуре СК Республики Беларусь функционирует система специализированных подразделений, отвечающих реалиям сегодняшнего дня. Деятельность по расследованию киберпреступлений и противодействию киберпреступности в структуре СК приобрела системный, целеустремленный и упорядоченный характер, продолжает совершенствоваться.

Среди приоритетных задач для ГУЦРПС и территориальных подразделений можно выделить следующие. Во-первых, установление и задержание организаторов киберпреступлений. Как правило, последние находятся за пределами страны. Тем не менее, данная работа ведется постоянно во взаимодействии с коллегами из других стран. При этом, наиболее эф-

фактивно она осуществляется с российскими коллегами. Во-вторых, выявление и устранение цифровых средств совершения преступлений – фишинговых ресурсов, скомпрометированных банковских карт, других инструментов преступлений. В СК функционирует эффективный алгоритм по оперативной блокировке фишинговых ресурсов – в течение суток с момента их выявления. Реализация данного алгоритма стала возможной благодаря принятию Указа Президента Республики Беларусь № 269 «О мерах по противодействию несанкционированным платежным операциям» (далее – Указ № 269).

Так, в соответствии с п. 1 Указа № 269 Национальный банк нашей страны организует информационное взаимодействие между правоохранительными органами и поставщиками платежных услуг по обмену информацией о несанкционированных платежных операциях и попытках их совершения (далее – инциденты). Причем, сбор, получение, систематизация, накопление, хранение, изменение, обезличивание, блокирование, использование, передача, предоставление, распространение, удаление, иная обработка информации об инцидентах, включающая сведения, составляющие банковскую тайну, и персональные данные, осуществляются посредством автоматизированной системы обработки инцидентов Национального банка (далее – АСОИ) с соблюдением требований законодательства об информации, информатизации и защите информации, в том числе о персональных данных.

Правоохранительные органы имеют право передавать информацию об инцидентах, установленных в ходе своей деятельности, посредством АСОИ в Национальный банк и поставщикам платежных услуг, а также получать информацию об инцидентах из АСОИ на безвозмездной основе.

В соответствии с п. 3 Указа № 269 правоохранительным органам предоставлено право на принятие решений о приостановлении на срок до 10 суток расходных операций по банковскому счету, счету по учету вкладов (депозитов), электронному кошельку пользователя платежных услуг, являющегося участником инцидента, в отношении которого имеется информация (подозрения), свидетельствующая об его участии в совершении противоправных деяний [7]. В практическом поле указанная норма применяется следующим образом. Оперативная информация о подозрительных операциях передается в Национальный банк. В дальнейшем осуществляется блокировка (приостановление) операций на срок до 10 суток. Следователь, в свою очередь, в указанный период при наличии оснований налагает арест на действовавшие в преступной схеме счета.

В-третьих, пресечение деятельности пособников на территории Беларуси – дропов, дроповодов, которые за деньги на системной основе снабжают организованные группы киберпреступников банковскими картами, сим-картами для использования при совершении преступлений на территории нашей республики. Так, за 2023 г. СК выявлена и пресечена деятельность нескольких групп пособников (дропов) численностью от 100 и более лиц, действующих на территории разных областей страны. В-четвертых, расследование уголовных дел о киберпреступлениях. В-пятых, обобщение следственной практики, изучение материалов уголовных дел, находящихся в производстве, изучение способов совершения киберпреступлений, занесение сведений о них в информационные базы, распространение среди следователей передового опыта расследования и предупреждения киберпреступлений.

Для решения указанных задач в СК успешно функционируют компьютеризированные системы статистических и аналитических учетов – Единая автоматизированная система СК (далее – ЕАИС), система «Аналитика», автоматизированная информационная система «След» [8, с. 227]. Последняя, весьма активно, в ежедневном формате, наполняется следователями по всей республике цифровыми следами, что в дальнейшем позволяет выявлять признаки многоэпизодности киберпреступлений, индивидуальные особенности в действиях организованных групп и т. д. Накопленную информацию используют следователи при расследовании уголовных дел о киберпреступлениях (например, для выдвижения версий, анализа действий преступников, выявления общих черт с ранее расследуемыми преступлениями, установления личности организаторов, соучастников, пособников). Также следователям СК обеспечен доступ к базам данных иных государственных органов посредством ЕАИС.

Противодействие киберпреступлениям невозможно без образовательного компонента. На сегодняшний день выстроена четкая система подготовки кадров по направлению расследования киберпреступлений. В учреждении образования «Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь» функционирует кафедра обеспечения цифрового развития предварительного следствия, где с привлечением сотрудников ГУЦРПС проводится обучение следователей, расследующих киберпреступления. Кроме того, практикуется участие сотрудников в программах повышения квалификации по направлению расследования преступлений, совершенных с применением информационно-коммуникационных технологий, организованных на базе учреждений образования Российской Федерации в рамках двустороннего сотрудничества государств в научно-образовательной сфере.

Таким образом, можно констатировать, что в Республике Беларусь посредством образования специализированных подразделений в СК создана эффективная система по реализации досудебного производства по уголовным делам о киберпреступлениях. Как представляется, предпосылками для функционирования данной системы послужили изменения в структуре и динамике преступности, связанные с цифровой трансформацией последней; принятие нормативных правовых актов, обязывающих государственные органы на учреждение «цифровых офисов»; необходимость в структуризации и объединении под единым управлением различных следственных подразделений по противодействию киберпреступности в целях придания данной деятельности целеустремленности и наибольшей эффективности.

Литература

1. Количество совершенных преступлений // Национальный статистический комитет [Электронный ресурс]. – Режим доступа : <http://dataportal.belstat.gov.by/Indicators/Search?code=1063066>. – Дата доступа : 27.05.2025.
2. Киберпреступность в Беларуси [Электронный ресурс]. – Режим доступа : <https://www.belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/>. – Дата доступа : 27.05.2025.
3. Следственным комитетом на заседании коллегии подведены итоги работы за прошлый год [Электронный ресурс]. – Режим доступа : <https://sk.gov.by/ru/news-ru/view/snizhenie-prestupnosti-i-rost-effektivnosti-itogi-raboty-sledstvennogo-komiteta-za-proshlyj-god-14575/>. – Дата доступа : 27.05.2025.
4. Государственная программа «Цифровое развитие Беларуси» на 2021–2025 гг. [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 2 февраля 2021 г., № 66 : в ред. постановления Респ. Беларусь от 25.02.2025, № 119 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.
5. Об органе государственного управления в сфере цифрового развития и вопросах информатизации [Электронный ресурс] : Указ Президента Республики Беларусь от 7 апреля 2022 г., № 136 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.
6. Мотолько, А. Ф. Цифровизация подразделений Следственного комитета Республики Беларусь в условиях развития информационного общества / А. Ф. Мотолько // Следственная деятельность : наука, образование, практика : тез. докл. III Междунар. науч.-практ. конф., Минск, 9 июня 2023 г. ; редкол.: С. Я. Аземша (предс.) [и др.]. – Минск : СтройМедиаПроект, 2023. – С. 250–253.
7. О мерах по противодействию несанкционированным платежным операциям [Электронный ресурс] : Указ Президента Республики Беларусь от 30 августа 2023 г., № 269 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.
8. Елётнов, В. И. Принятие управленческих решений в условиях цифровизации, Системы поддержки принятия решений / В. И. Елётнов // Следственная деятельность : наука, образование, практика : тез. докл. III Междунар. науч.-практ. конф., Минск, 9 июня 2023 г. ; редкол.: С. Я. Аземша (предс.) [и др.]. – Минск : СтройМедиаПроект, 2023. – С. 226–229.