

ОБЪЕКТИВНЫЕ И СУБЪЕКТИВНЫЕ ВИКТИМОГЕННЫЕ ФАКТОРЫ КИБЕРМОШЕННИЧЕСТВ

Пожарная О.В.,

*старший преподаватель кафедры теории и истории государства и права
учреждения образования «Брестский государственный университет
имени А.С. Пушкина»*

Стремительная цифровизация белорусского общества влечет за собой активное внедрение цифровых технологий во все сферы жизнедеятельности человека. Однако такая трансформация обуславливает не только позитивные изменения (упрощение коммуникации, развитие гибких форм работы и образования, расширение сферы услуг), но и ряд негативных аспектов, одним из которых является появление и последующий лавинообразный рост киберпреступности, под которой традиционно понимается совокупность деяний, совершенных с использованием информационно-коммуникационных технологий или направленных на объекты информационной инфраструктуры.

Первое киберпреступление в Республике Беларусь было зафиксировано в 2002 году. И если в 2006 году таких преступлений было 334, то в 2016 году их число возросло до 2471, а в 2019 г. – до 10539. Наибольшее количество киберпреступлений в Республике Беларусь было зафиксировано в 2020 г. – 25560 случаев, что составляло более четверти от всех зарегистрированных уголовно наказуемых деяний. В последующие годы наблюдалось определенное сокращение числа совершаемых киберпреступлений, однако их доля в общей структуре преступности по-прежнему высока, что не может не вызывать тревоги [1].

Если опираться на данные статистики, то можно отметить, что около 90% всех киберпреступлений составляют кибермошенничества, которые обычно квалифицируются по статьям 209 и 212 Уголовного Кодекса Республики Беларусь (мошенничество и хищение имущества путем модификации компьютерной информации). Эта разновидность киберпреступлений была распространена всегда и в настоящее время остается серьезной угрозой кибербезопасности граждан. Так, только за первый квартал 2026 года сотрудники правоохранительных органов зарегистрировали более 2,5 тыс. фактов кибермошенничества [2].

Представляется, что такой высокий процент кибермошенничеств в структуре виртуальных преступлений обусловлен рядом виктимогенных факторов, под которыми в научной литературе понимается совокупность обстоятельств, повышающих вероятность того, что индивид станет жертвой преступления. Эти факторы могут быть как объективными (характеризовать явления внешней среды), так и субъективными (касаться социально-психологических особенностей личности).

К объективным виктимогенными факторам кибермошенничеств стоит отнести следующие:

- интенсификация эксплуатации информационных технологий, проявляющаяся как в увеличении числа их пользователей (абонентов сотовой связи и сети Интернет, держателей банковских платежных карт и пр.), так и в повсеместном внедрении различных цифровых продуктов, рынок которых динамично развивается;

- рост популярности социальных сетей, мессенджеров, сервисов по определению геолокации, предполагающих размещение в открытом доступе информации личного характера и сведений о местонахождении пользователей;

- быстрая адаптация преступников к технологическим, социальным и экономическим изменениям, которая обуславливает постоянное появление новых уникальных схем кибермошенничеств, для борьбы с которыми еще не разработаны защитные механизмы. Один из примеров такого быстрого реагирования – использование кибермошенниками инструментов социальной инженерии, а также возможностей искусственного интеллекта для создания реалистичных изображений, голоса и видео с целью подделки личности.

К субъективным виктимогенными факторам кибермошенничеств можно отнести:

- интеллектуальные особенности жертв, которые во многом обуславливают низкий уровень цифровой грамотности и цифровой гигиены таких пользователей. С этой точки зрения в особую зону риска попадают как люди преклонных лет, которые не могут или не хотят вникать в тонкости эксплуатации цифрового пространства, так и подростки ввиду присущей им чрезмерной уверенности в собственных знаниях. Кроме того, представители обеих этих категорий в силу своего возраста характеризуются слабым критическим мышлением и способностью прогнозировать последствия (у пожилых людей эти навыки уже ослаблены, а у детей еще до конца не сформированы);

- эмоциональные особенности жертв. Излишняя доверчивость, тревожность, слабая стрессоустойчивость, импульсивность, чувство одиночества, азартность – эти и другие подобные характеристики индивидов дают кибермошенникам (которые зачастую обладают полученной из сети Интернет информацией о своей потенциальной жертве) широкие возможности для манипулирования;

- поведенческие особенности жертвы, связанные со спецификой ее образа жизни (работа, хобби), ценностными ориентациями, жизненными устремлениями и т.д. Так, ожидаемо повышен уровень виктимности у лиц, которые увлечены онлайн-играми и виртуальными тотализаторами, активно ведут соцсети с размещением в них личной информации, участвуют в сомнительных онлайн-схемах заработка, заказывают товары и услуги

по подозрительно низким ценам, из любопытства переходят по «кликабельным» ссылкам и пр.

Таким образом, мы можем констатировать, что виктимогенные факторы кибермошенничеств достаточно разнообразны и во многом обусловлены спецификой посягательств в сфере информационно-коммуникационных технологий. Их комплексное и систематическое изучение необходимо для разработки и последующей реализации эффективных мер как общей, так и индивидуальной виктимологической профилактики, призванной обеспечить информационную безопасность пользователей.

Список использованных источников:

1. Современная киберпреступность // Управление по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома. – URL: <https://www.beshenkovichi.vitebsk-region.gov.by/upload/files/30-07-25-5.pdf> (дата обращения: 18.04.2026)
2. Более 2500 кибермошенничеств выявлено в Беларуси за три месяца: МВД раскрыло новые схемы // Белновости. – URL: <https://www.belnovosti.by/proisshestiya/bolee-2500-kibermoshennichestv-vuyavleno-v-belarusi-za-tri-mesyaca-mvd-raskrylo> (дата обращения: 18.04.2026)

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В РЕСПУБЛИКЕ БЕЛАРУСЬ И РОССИЙСКОЙ ФЕДЕРАЦИИ

Путова Н.В.,

*старший преподаватель кафедры уголовного права
и уголовного процесса учреждения образования*

«Витебский государственный университет имени П.М. Машерова»

Ловинская У.И.,

студентка юридического факультета учреждения образования

«Витебский государственный университет имени П.М. Машерова»

Осмотр места происшествия является одним из наиболее сложных и ответственных следственных действий, от качества проведения которого во многом зависит успех всего дальнейшего расследования. Как справедливо отмечают исследователи, информация, полученная при производстве тщательного и правильного осмотра, в дальнейшем является поводом для выдвижения следователем версий совершенного преступления и определяет направление расследования.

В уголовно-процессуальном законодательстве Республики Беларусь осмотру места происшествия посвящены статьи 203 – 204 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК) [1]. Нормы права закрепляют основания, порядок проведения и процессуальное