

ним интимной информации и тем самым уменьшить возможность повторного возникновения психотравмирующей ситуации. Для признания результатов данного опроса в качестве доказательства практикой выработан специальный алгоритм, предусматривающий видеозапись опроса, просмотр данной видеозаписи, допрос психолога в качестве свидетеля, последующее назначение психиатрических экспертиз несовершеннолетнего (например, судебно-психиатрической, судебно-психологической). Легализация опроса несовершеннолетнего в дружественной комнате с использованием представленного алгоритма была положительно воспринята судебной практикой.

Вместе с тем проведение опроса в дружественной комнате не избавляло несовершеннолетнего от необходимости участия в проведении обычного допроса, что часто негативно сказывалось на психике ребенка. Новелла УПК относительно допроса несовершеннолетнего потерпевшего, свидетеля, не достигших 16-летнего возраста, по уголовным делам о преступлениях против личной свободы, чести и достоинства, жизни и здоровья, половой неприкосновенности или половой свободы в условиях дружественной детской комнаты, несомненно, направлена на преодоление обозначенной проблемы. Однако реализация данной нормы на практике имеет ряд трудностей, что, на наш взгляд, связано с недостаточной правовой регламентацией процессуального порядка проведения такого допроса.

Так, по общему правилу допрос проводится лично следователем. Педагог (психолог) в соответствии с ч. 1 ст. 62 УПК участвует в допросе в качестве специалиста. Вместе с тем при проведении допроса пусть и в условиях дружественной комнаты, но с участием и допрашивающего, и психолога теряется изначальный смысл данного следственного действия – создание благоприятных психологических условий для получения максимально полных и достоверных показаний несовершеннолетнего потерпевшего (свидетеля). Присутствие следователя в ходе допроса в дружественной комнате может не позволить ребенку раскрыться в полной мере, обострить чувство стыда и повысить вероятность повторного травмирования психики ребенка.

Идеальной моделью представляется присутствие в дружественной комнате для допроса только психолога. Однако говорить о том, что психолог единолично проводит допрос нельзя, так как психолог не наделен достаточными процессуальными полномочиями и не обладает достаточными специальными компетенциями для проведения полноценного допроса. В данном случае речь идет о проведении следственного действия следователем, но без его непосредственного присутствия, посредством участвующего специалиста. В уголовно-процессуальном законодательстве примером этого может служить проведение освидетельствования врачом в отсутствие следователя (ч. 4 ст. 206 УПК). Следователь организует данное следственное действие, руководит им, инструктирует врача, составляет протокол от своего имени, но лично не присутствует. Гарантией объективности получаемой информации от врача выступают понятия.

На наш взгляд, при проведении допроса несовершеннолетнего потерпевшего (свидетеля) в условиях дружественной комнаты аналогичный подход уместен:

следователь в ходе подготовки к проведению допроса консультирует психолога относительно обстоятельств, подлежащих выяснению в ходе допроса, составляет список вопросов;

непосредственно в ходе допроса с ребенком общается психолог, следователь воспринимает все происходящее по видеосвязи и с помощью связи с психологом посредством мессенджера при необходимости корректирует предмет допроса; по окончании допроса следователь составляет протокол, который подписывается им и психологом.

Гарантией объективности получаемой информации будет служить обязательная звуко- и видеозапись допроса.

Реализация данного подхода, несомненно, требует соответствующей правовой регламентации. В связи с этим предлагаем дополнить ч. 2¹ ст. 221 УПК предложением следующего содержания: «В этом случае допрос проводится психологом без присутствия следователя с обязательным применением звуко- и видеозаписи».

УДК 343.985.7

Ю.М. Юбко

ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Для принятия решения о возбуждении уголовного дела по поступившей информации о совершенном преступлении, предусмотренном гл. 31 УК Республики Беларусь, необходимо наличие поводов и оснований (ст. 166, 167 УПК). По уголовным делам данной категории наиболее распространенными поводами являются:

заявления граждан (физических лиц), являющихся обладателями, пользователями компьютерной информации, пользователями информационной системы и (или) информационной сети;

сообщения должностных лиц государственных органов, иных организаций (юридических лиц), являющихся собственниками, владельцами программно-технических средств, информационных ресурсов, информационных систем и информационных сетей;

непосредственное обнаружение органом уголовного преследования сведений, указывающих на признаки преступления против компьютерной безопасности (как подразделениями главного управления по противодействию киберпреступности МВД Республики Беларусь, так и органами уголовного преследования иностранных государств).

При принятии решения о возбуждении уголовного дела должны быть установлены признаки преступления, совершенного против компьютерной безопасности. Оценочное толкование некоторых из них не всегда позволяет принять данное решение в практической деятельности.

Так, анализ конструкций норм гл. 31 УК свидетельствует об использовании законодателем признака «существенный вред», что представляет определенные сложности при его установлении и доказывании. Современная практика свидетельствует о том, что участники не всегда объективно оценивают содержание данного признака в рамках конкретной следственной ситуации. В частности, физическое лицо (представитель юридического лица), обратившееся в орган уголовного преследования, в процессе дачи объяснений не может мотивировать мнение о сущности причиненного вреда и, как свидетельствует практика, занимает позицию, что причиненный вред является для него несущественным. Вместе с тем сотрудник, доказывая данный признак в процессе проверки, занимает противоположную позицию и приходит к мнению, что причиненный вред по своему содержанию является существенным. В частности, по мнению сотрудников органов уголовного преследования, при анализе и оценке имеющейся информации следует считать, что причиненный вред является существенным, когда:

в результате преступных действий страдает производственно-хозяйственная деятельность юридического лица (например, в ситуациях, связанных с несанкционированным доступом, умышленным уничтожением, приведением в непригодное состояние финансовой, производственно-хозяйственной и прочей информации);

в результате преступных действий страдает деловая репутация юридического лица в одних случаях, а в других – репутация физического лица. Так, завладев подлинными данными юридического (физического) лица, подозреваемый использует их, в одних случаях выступая от имени конкретного юридического лица, совершая «мнимые сделки», а в других – с их помощью от имени физического лица приобретает наркотические средства или иные предметы, запрещенные к обороту, с целью скомпрометировать последнего. Имеют место и ситуации, когда с целью скомпрометировать конкретное лицо осуществляется несанкционированный доступ к компьютерной информации и производится ее модификация (например, размещение на персональной странице лица информации об оказании им интимных услуг и т. д.);

когда в процессе проверки по материалам о преступлениях рассматриваемой категории устанавливается совокупность (система) эпизодов и в сферу данной преступной деятельности вовлечено большое количество пострадавших лиц.

Приведенный перечень имеющих место в практике ситуаций не является исчерпывающим, перечислить их все невозможно, поэтому решение вопроса об отнесении причиненного вреда к существенному необходимо принимать в каждом конкретном случае, с учетом всех индивидуальных обстоятельств.

Решая вопрос об оценке вреда, следует иметь в виду, что он может носить как материальный, так и нематериальный характер. В случае его материального характера ущерб будет оцениваться на сумму, в 40 и более раз превышающую размер базовой величины. В случае нематериального характера существенным вредом охватываются нарушения конституционных прав граждан, значительное ущемление прав и законных интересов организаций и учреждений.

Наряду с понятием «существенный вред» в ч. 2 ст. 349, ч. 3 ст. 350, ч. 3 ст. 352, ч. 3 ст. 354, ч. 2 ст. 355 УК законодатель оперирует термином «иные тяжкие последствия». Уясняя и доказывая его содержание, следует абстрагироваться от трактовки данного определения, сформулированной в научных публикациях. Под «иными тяжкими последствиями» следует понимать причинение ущерба в особо крупном размере; уничтожение информации особой ценности; нарушение графиков движения транспортных средств, подачи электроэнергии; создание политической напряженности в обществе; искажение результатов голосования на референдумах, выборах Президента, депутатов Национального собрания; осложнения в международных отношениях; военные или политические инциденты и т. д.

Необходимо учитывать, что в некоторых нормативных правовых актах сформулированы критерии, относящие отдельные виды информационных ресурсов к категории особо ценных, что также свидетельствует о значимости наступивших последствий.

Принимая во внимание, что преступления, предусмотренные ч. 1 ст. 349, ч. 1 ст. 350, ч. 1 ст. 352 УК, совершенные в отношении лиц, пострадавших от преступления, их близкими, отнесены законодателем к делам частного обвинения, необходимо исследовать отмеченное обстоятельство, так как уголовное преследование данной категории лиц осуществляется только по заявлению лица, пострадавшего от преступления.

По большинству составов субъектом рассматриваемых деяний выступает вменяемое физическое лицо, достигшее 16-летнего возраста, однако в ст. 355 УК речь идет о специальном субъекте, т. е. лице, имеющем доступ к компьютерной системе или сети. В связи с чем необходимо доказать статус данного субъекта как законного пользователя, имеющего право в соответствии с установленными правилами эксплуатации компьютерной системы или сети, изложенными в нормативных правовых актах, осуществлять правомерный доступ к компьютерной информации, однако нарушающего эти предписания ввиду легкомыслия или небрежности.

В ходе проверки должны быть установлены и отдельные элементы криминалистической характеристики: следовая картина; способ совершения преступления; предмет преступного посягательства; место совершения преступления против компьютерной безопасности. Так, в ситуациях, связанных с разработкой, использованием, распространением либо сбытом вредоносных компьютерных программ либо специальных программных или аппаратных средств, необходимо установить их функции (свойства), позволяющие дать юридическую оценку им как вредоносным.

Выполняя требования п. 1 ст. 167 УПК, при организации проверки следует выяснить, имели ли место обстоятельства, исключающие производство по уголовному делу. Применительно к рассматриваемым преступлениям таковыми могут быть действия персонала организации при производстве профилактических работ, техническом обслуживании компьютерной системы или сети и подробные ситуации, исчерпывающий перечень которых привести фактически невозможно в связи с отдельными особенностями их функционирования.

Установление в ходе проверки рассмотренных признаков позволит принять законное и обоснованное решение о возбуждении уголовного дела.