

НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И РАЗГРАНИЧЕНИЯ СО СМЕЖНЫМИ СОСТАВАМИ

Жартун С.Д.

Республика Беларусь, г. Минск

Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники»,
курсант военного факультета

Научный руководитель

Игнатенко А.С.

Республика Беларусь, г. Минск

Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники»,
преподаватель - начальник юридической службы,
кандидат юридических наук

Стремительное развитие информационных технологий, наряду с позитивными эффектами, сопровождается ростом числа преступлений в сфере компьютерной информации. В связи с этим особую актуальность приобретает уголовно-правовая охрана информационной безопасности, одним из ключевых элементов которой является норма, предусмотренная ст. 349 Уголовного кодекса Республики Беларусь (далее – УК), устанавливающая ответственность за несанкционированный доступ к компьютерной информации. Несмотря на ряд законодательных новелл, принятых в последние годы, правоприменительная практика до сих пор сталкивается с трудностями при толковании признаков данного состава, а также при его отграничении от смежных уголовно-правовых запретов. Целью настоящего доклада является выявление этих проблем и выработка рекомендаций по их разрешению.

Объективная сторона преступления, предусмотренного ст. 349 УК, выражается в действии — несанкционированном доступе к информации, хранящейся в компьютерной системе, сети или на машинных носителях. Обязательным условием является то, что такой доступ должен сопровождаться нарушением системы защиты. Ключевым признаком, вызывающим дискуссии в доктрине, является понятие «несанкционированность». В.В. Лосев определяет несанкционированный доступ как неправомерное получение возможности ознакомиться с информацией или распорядиться ею по своему усмотрению, совершаемое без согласия собственника или иного уполномоченного лица [1, с. 26–27]. Однако, как обоснованно отмечает Н.А. Швед, проблемной остается ситуация, когда доступ осуществляет лицо, имеющее легальный доступ к системе, но действующее вопреки установленным правилам (например, системный администратор, просматривающий личную переписку сотрудников). В своём исследовании она приходит к выводу, что такие действия также должны признаваться несанкционированными, так как выход за пределы предоставленных полномочий нарушает установленный режим защиты информации [2, с. 10–13]. Более того, подход, согласно которому несанкционированным признается доступ как постороннего лица, так и лица, имеющего легальный доступ, но действующего

за его пределами, представляется наиболее логичным и практически значимым [3, с. 32–34].

Конструкция состава преступления, предусмотренного ст. 349 УК, является сложной. Часть 1 данной статьи сформулирована как материальный состав, где обязательным признаком является наступление последствий в виде изменения, уничтожения, блокирования информации или вывода из строя компьютерного оборудования либо причинения иного существенного вреда по неосторожности. В то же время ч. 2 этой же статьи устанавливает ответственность за несанкционированный доступ, совершенный из корыстной или иной личной заинтересованности. Данный состав, как отмечает В.В. Лосев, является формальным, считающимся оконченным с момента совершения самого действия [3, с. 25–26]. Данная особенность порождает на практике проблему конкуренции частей одной статьи и требует от уполномоченного органа точного установления мотива и цели преступника. Анализ судебной практики, проведенный Д.В. Деминим, показывает, что в подавляющем большинстве случаев несанкционированный доступ совершается лицами с использованием своего служебного положения, которое даёт им непосредственный доступ к носителям информации [4, с. 3].

Наиболее сложной в правоприменительной практике является проблема разграничения ст. 349 УК со смежными составами преступлений. В первую очередь, это касается соотношения со ст. 350 УК (модификация компьютерной информации). Ключевым критерием разграничения здесь выступает направленность умысла. Как обоснованно указывает М.А. Дубко, при квалификации по ст. 349 УК умысел лица направлен на получение доступа к охраняемой информации, а последующие действия по её изменению, уничтожению или блокированию охватываются неосторожной формой вины. Если же лицо, осуществляя несанкционированный доступ, сразу же ставит целью модификацию информации, содеянное требует дополнительной квалификации по ст. 350 УК [5, с. 2].

Особого внимания заслуживает также разграничение ст. 349 УК с хищением, совершенным с использованием компьютерной техники (ст. 212 УК). Анализируя данную проблему, М.А. Дубко приходит к выводу, что если несанкционированный доступ является лишь способом завладения чужим имуществом или приобретения права на него, то содеянное в целом охватывается составом ст. 212 УК и дополнительной квалификации по ст. 349 УК не требует. Однако, если преступник, осуществив доступ, копирует информацию, которая сама по себе представляет материальную ценность (например, базы данных, программное обеспечение), то в такой ситуации имеет место идеальная совокупность преступлений, поскольку нарушается и информационная безопасность, и отношения собственности [5, с. 3].

Проведенный анализ позволяет сформулировать ряд выводов и предложений по совершенствованию правоприменительной практики. Во-первых, необходимо разъяснить, что несанкционированным следует признавать доступ к компьютерной информации, осуществленный как посторонним лицом, так и лицом, имеющим доступ к системе, но действующим за пределами предоставленных ему полномочий. Во-вторых, уполномоченным органам следует руководствоваться правилом, что при конкуренции ч. 1 и ч. 2 ст. 349 УК приоритет имеет специальная норма — ч. 2, устанавливающая ответственность за деяние, совершенное из корыстной или иной личной заинтересованности. В-третьих, в целях обеспечения единообразия судебной практики необходимо рекомендовать квалифицировать по совокупности ст. 349 и ст. 350 (352) УК в тех случаях, когда умыслом лица охватывалось не только получение доступа, но и последующее незаконное изменение (копирование) информации.

В заключение сформулируем следующие выводы и предложения.

1. Уголовно-правовые нормы нуждаются в совершенствовании – целесообразно дополнить ч. 1 ст. 349 УК указанием на возможность привлечения к ответственности за сам факт несанкционированного ознакомления с компьютерной информацией, если такое ознакомление создавало реальную угрозу наступления тяжких последствий, а также исключить из диспозиции ч. 2 ст. 349 УК признак «существенный вред», сделав состав формальным для случаев корыстного или иного личного доступа.

2. Понятие «несанкционированный доступ» в диспозиции ст. 349 УК следует толковать более точно: к нему должны относиться не только действия посторонних лиц, но и действия субъектов, наделённых правом доступа к информационной системе, однако вышедших за пределы предоставленных им полномочий (например, системных администраторов, изучающих личные данные сотрудников без служебной необходимости).

3. Разграничение ст. 349 и ст. 350 УК должно проводиться по направленности умысла: если изменение, блокирование или уничтожение информации охватывалось первоначальным умыслом лица, содеянное подлежит квалификации по совокупности преступлений. При использовании несанкционированного доступа исключительно как способа хищения чужого имущества дополнительная квалификация по ст. 349 УК не требуется.

Список цитированных источников

1. Лосев, В. В. Преступления против информационной безопасности: метод. рекомендации / В. В. Лосев. – Брест: БрГУ, 2000. – 45 с.

2. Швед, Н. А. Уголовная ответственность за несанкционированный доступ к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Н. А. Швед. – Минск, 2010. – 166 с.

3. Лосев, В. В. Преступления против информационной безопасности: учеб.-метод. пособие / В. В. Лосев. – Брест: БрГУ, 2002. – 120 с.

4. Демин, Д. В. Проблемы квалификации неправомерного доступа к компьютерной информации / Д. В. Демин // E-Scio. – 2020. – № 6. – С. 1–5.

5. Дубко, М. А. Особенности квалификации неправомерного завладения компьютерной информацией и отграничения от иных преступлений против информационной безопасности / М. А. Дубко // Вестник Полоцкого государственного университета. Серия D, Экономические и юридические науки. – 2015. – № 13. – С. 180–185.