# Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации" (утв. Генпрокуратурой России от 14.04.2014)

## Введение

Повсеместное развитие и совершенствование компьютерных технологий, расширение производства технических устройств и сферы их применения, широкая доступность компьютерной техники, кроме упрощения различных технологических и бытовых процессов, способствуют появлению новых видов преступных посягательств, объектами которых являются информация, информационно-телекоммуникационные ресурсы, а также денежные средства, находящиеся в обращении глобальных и локальных компьютерных сетей.

В настоящее время преступления в сфере компьютерной информации хотя и имеют незначительный удельный вес в общей структуре преступности (в сравнении с другими преступлениями), однако проявляют стойкую тенденцию к ежегодному росту.

Количество преступлений экономической направленности, совершенных с использованием электронных средств, возрастает, а их способы становятся все более изощренными.

Любые действия над компьютерной информацией, составляющей государственную тайну или содержащейся в компьютерных сетях, управляющих системами военного, жизнеобеспечивающего или крупного производственного назначения, могут повлечь за собой самые непредсказуемые по характеру и размеру негативные последствия.

Жертвами преступлений этой категории могут стать и обычные граждане, в отношении которых возможны угрозы нарушения неприкосновенности частной жизни, тайны сообщений, нарушения авторских и смежных, изобретательских и патентных прав, мошенничества, незаконного получения и разглашения сведений, составляющих коммерческую и банковскую тайну, сокрытия информации об обстоятельствах, создающих опасность для жизни или здоровья, и другие не менее значимые нарушения их прав.

Если раньше специфика преступлений в сфере компьютерной информации была обусловлена использованием при их совершении высоких технологий и новейших достижений науки и техники, необходимостью обладания определенным уровнем специальных познаний, то в настоящее время в глобальной сети Интернет в практически свободном доступе находятся как программы, предназначенные для совершения несанкционированных действий с компьютерной информацией, так и инструкции по их применению.

При этом следует констатировать низкую эффективность расследования преступлений в сфере компьютерной информации и судебного рассмотрения таких дел.

В подобной ситуации нельзя недооценивать роль прокурорского надзора за расследованием преступлений в сфере компьютерной информации, поскольку своевременное выявление нарушений уголовно-процессуального и уголовного законодательства и использование мер прокурорского реагирования позволяют избежать признания большинства собранных по уголовному делу доказательств недопустимыми и необоснованного привлечения лица к уголовной ответственности.

## 1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации

Уголовная ответственность за преступления в сфере компьютерной информации предусмотрена главой 28 УК РФ, содержащей три статьи.

Так, статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Впервые в уголовном законодательстве Российской Федерации Федеральным законом от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» в примечании к ст. 272 УК РФ дано понятие компьютерной информации, как предмета преступления, к которому теперь относятся сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Общим объектом преступления, предусмотренного ст. 272 УК РФ, выступают общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями. В ч. 3 ст. 272 УК РФ указан дополнительный объект преступления - общественные отношения, обеспечивающие интересы службы.

Диспозиция ч. 1 ст. 272 УК РФ в предыдущей редакции от 07.03.2011 была изложена следующим образом: «Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование

информации, нарушение работы ЭВМ, системы ЭВМ или их сети». В действующей редакции от 07.12.2011 ч. 1 ст. 272 УК РФ изложена следующим образом: «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации».

Несомненно, законодатель внес данные изменения, чтобы решить ряд проблем, возникающих в правоприменительной практике. Например, при рассмотрении дел указанной категории суды зачастую сталкивались с трудностями, когда неправомерный доступ осуществлялся к устройству, не подпадающему под определение ЭВМ, но по своим свойствам и функциям фактически не уступающему ЭВМ по возможности хранения и обработки информации (мобильные телефоны, смартфоны, карманные персональные компьютеры).

Объективная сторона состава преступления включает в себя: действие, состоящее в неправомерном доступе к охраняемой законом компьютерной информации (информации ограниченного доступа); последствие (альтернативно) в виде уничтожения, блокирования, модификации, копирования компьютерной информации, и причинно-следственную связь между указанным действием и любым из названных последствий.

Законодателем не уточнено понятие доступа к информации. Указанное понятие содержится в п. 6 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: «доступ к информации - возможность получения информации и ее использования».

Под охраняемой законом понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.).

Неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты.

Другими словами, неправомерный доступ к компьютерной информации - это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее).

Состав данного преступления носит материальный характер и предполагает обязательное наступление одного из последствий:

а) уничтожение информации - это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени;

б) блокирование информации - результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

в) модификация информации - внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

г) копирование информации - создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме - от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

Однако, по нашему мнению, если в силу настроек компьютерной программы при работе с ней, пусть даже и в результате неправомерного доступа, автоматически создается резервная копия компьютерной информации, то данное действие не будет иметь уголовно-правовых последствий, поскольку оно осуществляется независимо от волеизъявления лица и, соответственно, в прямой причинной связи с его действиями не состоит.

Преступление окончено с момента наступления любого из указанных последствий. Устанавливая причинную связь между несанкционированным доступом и наступлением вредных последствий следует иметь в виду, что в компьютерных системах возможны уничтожение, блокирование и модификация компьютерной информации в результате технических неисправностей или ошибок при функционировании операционной среды или иных программ. В этих случаях лицо, совершившее неправомерный доступ к компьютерной информации, не подлежит ответственности по данной статье ввиду отсутствия причинной связи между его действиями и наступившими последствиями.

Субъективная сторона рассматриваемого преступления характеризуется виной в форме умысла (прямого или косвенного) или неосторожности.

Субъект преступления общий - вменяемое лицо, достигшее шестнадцати лет. Вместе с тем ч. 3 ст. 272 УК РФ предусматривает наличие специального субъекта, совершившего данное преступление с использованием своего служебного положения.

Под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается использование

возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и прочие).

Статья 273 УК РФ предусматривает уголовную ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Компьютерная программа - это объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютерного устройства с целью получения определенного результата.

Очевидно, что под компьютерными программами по смыслу данной статьи УК РФ, в основном понимаются программы, известные, как компьютерные вирусы (черви, троянские кони, кейлоггеры, руткиты и др.).

Основной объект преступления - общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Предмет преступления по содержанию совпадает с предметом преступления, предусмотренного ст. 272 УК РФ.

Объективная сторона преступления включает альтернативные действия, состоящие: а) в создании программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты; б) в распространении таких программ или машинных носителей с такими программами; в) в использовании таких программ или машинных носителей с ними.

Создание программ представляет собой деятельность, направленную на разработку, подготовку программ, способных по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Под распространением таких программ понимается предоставление доступа к ним любому постороннему лицу любым из возможных способов, включая продажу, прокат, бесплатную рассылку по электронной сети, то есть любые действия по предоставлению доступа к программе сетевым или иным способом.

Использование программы - это работа с программой, применение ее по назначению и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме. Под использованием вредоносных программ понимается их применение (любым лицом), при котором активизируются их вредные свойства.

Рассматриваемое преступление будет окончено с момента создания, использования или распространения таких программ или информации, создающих угрозу наступления указанных в законе последствий, вне зависимости от того, наступили реально эти последствия или нет. Состав преступления формальный.

Субъективная сторона состава преступления, предусмотренного ч. 1 ст. 273 УК РФ, характеризуется виной в виде прямого умысла. При этом виновный должен осознавать, что создаваемые или используемые им программы заведомо приведут к указанным в законе общественно опасным последствиям. Мотив и цель не влияют на квалификацию преступления.

Субъект преступления общий - вменяемое лицо, достигшее шестнадцати лет.

В ч. 3 ст. 273 УК РФ предусмотрен квалифицирующий признак рассматриваемого состава преступления - наступление тяжких последствий или создание угрозы их наступления. Следует учитывать, что в случае наступления тяжких последствий данный квалифицированный состав преступления является материальным, то есть деяние окончено с момента наступления общественно опасных последствий, а если создана угроза их наступления, то состав является усеченным.

При этом тяжесть последствий должна определяться с учетом всей совокупности обстоятельств дела (причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, наступление аварий и катастроф, причинение тяжкого и средней тяжести вреда здоровью людей или смерти, уничтожение, блокирование, модификация или копирование привилегированной информации особой ценности, реальность созданной угрозы и др.).

Субъективная сторона указанного квалифицированного состава преступления характеризуется двумя формами вины - умыслом по отношению к самому деянию и неосторожностью по отношению к последствиям. В случае если преступник умышленно относился к наступлению тяжких последствий или созданию угрозы их наступления, то в зависимости от качественной и количественной оценки наступивших тяжких последствий его действия подлежат дополнительной квалификации по совокупности преступлений, предусмотренных соответствующими статьями УК РФ.

Следует иметь в виду, что ст. 273 УК РФ устанавливает ответственность за незаконные действия с компьютерными программами, записанными не только на машинных, но и на иных носителях, в том числе на бумаге. Это обусловлено тем, что процесс создания компьютерной программы зачастую начинается с написания ее текста с последующим введением его в компьютер или без такового. С учетом этого наличие исходных текстов вредоносных компьютерных программ уже является основанием для привлечения к ответственности по ст. 273 УК РФ. Однако использование вредоносной компьютерной программы для личных нужд (например, для уничтожения собственной компьютерной информации) ненаказуемо. В случае если действие вредоносной программы было условием совершения другого преступления, содеянное подлежит квалификации по совокупности преступлений вне зависимости от степени тяжести другого преступления.

Диспозиция части 1 статьи 273 УК РФ ранее была изложена следующим образом: «Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами» (в ред. от 08.12.2003). В действующей редакции от 07.12.2011 диспозиция ч. 1 ст. 273 УК РФ предусматривает ответственность за «создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации».

Гражданский кодекс Российской Федерации определяет программу для ЭВМ как «представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения».

Следует отметить, что законодательного определения средств защиты компьютерной информации не существует. Сходные определения содержатся в Законе Российской Федерации от 21.07.1993 № 5485-1 (ред. от 08.11.2011) «О государственной тайне» («...средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации...»), в Соглашении между Правительством Российской Федерации и Правительством Украины о сотрудничестве в области технической защиты информации от 14.06.1996 («...Средства технической защиты информации» - технические средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации...») и в ряде ведомственных нормативных актов.

В соответствии со ст. 274 УК РФ уголовная ответственность наступает за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Диспозиция ч. 1 ст. 274 УК РФ ранее предусматривала ответственность за «нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред». В редакции Федерального закона от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» она изложена следующим образом: «Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб».

Основной объект преступления - общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Дополнительный объект преступления, повлекшего причинение существенного вреда, - общественные отношения, обеспечивающие в зависимости от характера последних, иные значимые социальные ценности (жизнь человека, здоровье многих людей, собственную безопасность и т.п.).

Предметом данного преступления являются средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование.

Данная норма является бланкетной и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети Интернет не существует.

Объективная сторона преступления состоит в нарушении правил хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, если такое нарушение повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь, а также доказано, что наступившие последствия являются результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными ст. 272 и 273 УК РФ.

Правила, о которых идет речь в ст. 274 УК РФ, должны быть направлены только на обеспечение информационной безопасности. В ней говорится о нарушении правил, которое может повлечь уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, то есть такие же последствия, что и при неправомерном доступе к компьютерной информации, создании, использовании и распространении вредоносных программ для ЭВМ.

Правила доступа и эксплуатации, относящиеся к обработке информации, содержатся в различных положениях, инструкциях, уставах, приказах, ГОСТах, проектной документации на соответствующую автоматизированную информационную систему, договорах, соглашениях и иных официальных документах.

Субъективная сторона состава данного преступления характеризуется двумя формами вины. Нарушение правил эксплуатации и доступа, предусмотренное ч. 1 ст. 274 УК РФ, может совершаться как умышленно (при этом умысел должен быть направлен на нарушение правил эксплуатации и доступа), так и по неосторожности (например, программист, работающий в больнице, поставил полученную им по сетям программу без предварительной проверки ее на наличие в ней компьютерного вируса, в результате чего

произошел отказ в работе систем жизнеобеспечения реанимационного отделения больницы).

Частью 2 статьи 274 УК РФ предусмотрен один квалифицирующий признак - тяжкие последствия или создание угрозы их наступления, характеристика которых рассматривалась нами ранее.

Если раньше применение статьи не вызывало вопросов в отношении субъекта преступления, которым выступало специальное лицо, обязанное в силу занимаемой должности соблюдать установленные правила эксплуатации ЭВМ, системы ЭВМ или их сети, то в новой редакции возникает вопрос о личности субъекта данного преступления, особенно в части нарушения правил доступа к информационно-телекоммуникационным сетям, которые определены Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» как «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники». Под данное определение попадает фактически любая компьютерная сеть, включая Интернет и локальные сети, как правило, создаваемые поставщиками услуг доступа в Интернет по территориальному принципу. Следует отметить, что каждый провайдер, предоставляющий доступ в Интернет, заключает с физическими и юридическими лицами договор оказания услуг, в котором прописаны определенные правила доступа к информационно-телекоммуникационным сетям. Таким образом, можно сделать вывод, что законодатель предусмотрел ответственность по данной статье и для общего субъекта преступления.

## 2. Прокурорский надзор на стадии возбуждения уголовного дела о преступлениях в сфере компьютерной информации

В последние годы, наиболее часто, возбуждение уголовных дел этой категории происходит по поводу, предусмотренному п. 3 ч. 1 ст. 140 УПК РФ, а именно по материалам, содержащим результаты оперативно-розыскных мероприятий специализированных подразделений МВД России и ФСБ России. В частности, для выявления преступлений в сфере так называемых высоких технологий (к которым относятся и преступления в сфере компьютерной информации), а также для установления лиц и преступных группировок, занимающихся преступной деятельностью в этой области, создано Управление «К» МВД России.

Вместе с тем, прокурору необходимо тщательно проверять законность возбуждения уголовных дел и оценивать представленные материалы.

Учитывая стремительное развитие компьютерных технологий, изобретательность и высокую квалификацию лиц, совершающих компьютерные преступления, охватить многообразие всех существующих способов совершения преступлений в сфере компьютерной информации, не представляется возможным. Тем не менее, в данной работе следует указать наиболее распространенные из них.

Способы совершения преступления, предусмотренного ст. 272 УК РФ, можно разделить на две группы. К первой относятся способы непосредственного воздействия лица на компьютерную информацию, когда проникновение осуществляется путем введения различных команд в компьютерную систему. В этом случае следы совершения преступления останутся только на носителе компьютерной информации, задействованном при совершении преступного посягательства. Такой доступ может осуществляться как лицами, имеющими право на него, так и лицами, специально проникающими в зоны с ограничениями по допуску.

Вторая группа - это способы удаленного (опосредованного) воздействия на компьютерную информацию, например: проникновение в чужие информационные сети путем соединения с тем или иным компьютером; проникновение в компьютерную систему с использованием чужих идентификационных данных; подключение к линии связи легитимного пользователя с получением доступа к его системе; использование вредоносных программ для удаленного доступа к информации и т.п.

Способы совершения преступлений предусмотренных ст. 273 и 274 УК РФ, в достаточной степени описаны в главе первой настоящих рекомендаций при рассмотрении объективной стороны указанных составов преступлений.

Как правило, на стадии возбуждения уголовного дела складываются следующие типичные ситуации:

заявители (администрация организации, владелец компьютерной информации) сами выявили факт преступления или признаки совершенного преступления, но не смогли установить конкретных лиц, в связи с чем обратились в правоохранительные органы;

заявители (администрация организации, потерпевший) не только обнаружили преступление, его признаки, но и выявили установочные данные подозреваемого лица (чаще всего это номер телефона, сообщенный провайдером услуг сети Интернет, или IP адрес, если подсоединение к компьютерной сети произведено с использованием Интернета).

Изучая представленные материалы, прокурор должен убедиться, что объективно подтверждаются факты, изложенные в заявлениях, материалах ведомственной и иной проверки о нарушении целостности (конфиденциальности) информации в компьютерной системе, сети; о наличии причинной связи между неправомерными действиями и наступившими последствиями, предусмотренными диспозицией ст. 272 и 274 УК РФ, в виде копирования, уничтожения, модификации, блокирования информации, (для возбуждения уголовного дела по ст. 273 УК РФ наступление таких последствий не обязательно); о предварительном размере ущерба, причиненного в результате преступных действий.

Следует отметить, что копирование, уничтожение, модификация информации могут быть вызваны не только преднамеренными неправомерными действиями, но и ошибками, неумышленным неправильным поведением персонала потерпевшей организации при профилактике, техническом обслуживании либо ремонте компьютера, компьютерной системы или сети; случайных неумышленных повреждениях аппаратуры, обрывах соединительных кабелей при нестандартном поведении в помещении, где расположены компьютеры, подключенные к ним устройства, компьютерная система или сеть; ошибочных действиях оператора в

процессе работы, приведших к разрушению информационных данных; и неумышленном неправильном обращении с машинными носителями информации в ходе их использования и хранения и т.д.

Важной составляющей при возбуждении уголовного дела являются объяснения сотрудников (персонала) потерпевшей организации - администраторов сети, инженеров-программистов, разработавших программное обеспечение и осуществляющих его сопровождение (т.е. отладку и обслуживание), операторов, специалистов, занимающихся эксплуатацией и ремонтом компьютерной техники; системных программистов, инженеров по средствам связи и телекоммуникационному оборудованию, специалистов, обеспечивающих информационную безопасность, работников службы безопасности и других.

Из данных объяснений можно выяснить обстоятельства обнаружения факта преступления (признаков его совершения, способов и средств, наступивших негативных последствий), наличие и функционирование информационной защиты, ее недостатки, иные причины и условия, которые могли быть использованы для совершения противоправных действий.

Решение о возбуждении уголовного дела принимается не только на основании материалов предварительных проверок заявлений потерпевших, организаций и должностных лиц, но и, как указывалось выше, по материалам органов, осуществляющих оперативно-розыскную деятельность при реализации оперативных разработок, результатов оперативно-розыскных действий по выявлению преступлений в сфере компьютерной информации и лиц, их совершивших.

В соответствии со ст. 11 Федерального закона от 12.08.1995 № 144-ФЗ (ред. от 02.11.2013) «Об оперативно-розыскной деятельности» ее результаты могут служить поводом и основанием для возбуждения уголовного дела и использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств.

Надзирающему прокурору необходимо проверить полноту материалов, легитимность их получения и последующего предоставления в орган расследования.

С учетом специфики компьютерных преступлений в направляемых для возбуждения уголовного дела материалах должны содержаться:

сопроводительное письмо руководителя органа дознания (оперативной службы);

рапорт сотрудника, проводившего оперативно-розыскные и иные мероприятия;

документы, фиксирующие этапы проведения оперативно-розыскных мероприятий (за исключением сведений, составляющих государственную тайну);

протоколы наблюдений и контрольных закупок (при продаже, распространении компакт-дисков с вредоносными компьютерными программами);

протоколы и стенограммы прослушивания телефонных переговоров и иных сообщений (радиообмена, пейджинговых, модемных, иных), перехвата информации с иных каналов связи, свидетельствующие о неправомерной деятельности подозреваемых лиц (необходимо иметь в виду, что согласно действующему законодательству указанные оперативно-розыскные мероприятия могут проводиться только на основании судебного решения и только в отношении преступлений особо тяжких, тяжких и средней тяжести);

протоколы перехвата и регистрации информации электронной почты лиц, причастных к преступлению;

протоколы оперативного наблюдения с приобщенными фото- и видео- кадрами;

материалы оперативных экспериментов;

протоколы изъятия образцов для сравнительного исследования с участием специалистов;

протоколы (акты) изъятия компьютерной техники (машинных носителей) либо отражение такого изъятия непосредственно в протоколах оперативно-розыскных мероприятий (следует обратить внимание на тот факт, что доказательства, изъятые в ходе проведения оперативно-розыскных мероприятий, в соответствии со ст. 89 УПК РФ должны отвечать требованиям, предъявляемым к доказательствам, указанным Кодексом (разъяснение соответствующих прав лицам, присутствующим при изъятии, присутствие общественных наблюдателей и т.п.). В противном случае доказательства, полученные таким образом не будут легитимными и не могут быть положены в основу приговора. Соответственно, теряется какая-либо целесообразность проведения судебных экспертиз по изъятым объектам);

бумажные распечатки информации с изъятых машинных носителей информации и информации, находившейся на жестком диске переносного компьютера подозреваемого (при негласном снятии информации или при добровольной выдаче компьютерного оборудования);

материалы лабораторных исследований содержимого системных блоков и машинных носителей, изъятых у подозреваемого;

протоколы изъятия и осмотров финансовых документов, кассовых чеков, свидетельствующих о внесенных изменениях в базы данных компьютеров, некоторых видов кассовых аппаратов, являющихся разновидностью компьютеров;

протоколы использования специальных химических средств (химловушек) при фиксации использования компьютерного оборудования в целях неправомерного доступа, краж машинных носителей информации;

объяснения должностных и иных лиц;

инструкции, справки, другие документы и материалы.

Если представленных материалов для возбуждения уголовного дела, по мнению прокурора, недостаточно, постановление о возбуждении уголовного дела должно быть отменено в течение 24 часов с момента получения материалов, послуживших основанием для возбуждения уголовного дела.

## 3. Прокурорский надзор за расследованием преступлений в сфере компьютерной информации

При осуществлении прокурорского надзора за расследованием преступлений в сфере компьютерной информации прокурору необходимо руководствоваться не только положениями уголовно-процессуального законодательства, но и требованиями приказа Генерального прокурора Российской Федерации от 02.06.2011 № 162 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия».

Учитывая сложность расследования преступлений в сфере компьютерной информации, уже отмечавшуюся низкую квалификацию следственных работников, необходимость применения при расследовании специальных знаний, прокурорский надзор за расследованием данных преступлений должен осуществляться на протяжении всего периода расследования.

С целью предотвращения нарушений и затягивания сроков следствия прокурору необходимо осуществлять постоянное взаимодействие с руководителем следственного органа, привлекая прокурора, который в последующем будет поддерживать государственное обвинение в судебном заседании.

Организовать такое взаимодействие возможно в виде совместных оперативных совещаний по обсуждению хода следствия при прокуроре, проводимых как при принятии важных процессуальных решений по уголовному делу, например, при оценке достаточности доказательств для предъявления обвинения, при назначении экспертиз и обсуждении их выводов для последующего планирования расследования, при окончании предварительного следствия, при рассмотрении поступающих к прокурору жалоб и заявлений.

Более того, во многих субъектах Российской Федерации изданы межведомственные приказы и иные нормативные документы, регулирующие порядок взаимодействия при расследовании уголовных дел между следственными органами и прокурорами. Это позволяет избежать многих нарушений и недостатков предварительного расследования, которые, в свою очередь, могут повлечь за собой возвращение уголовного дела прокурором для дополнительного расследования или судом прокурору в порядке ст. 237 УПК РФ.

Учитывая особенности рассматриваемой категории преступлений, прокурору следует тщательно изучать собранные в ходе предварительного расследования доказательства, которые должны в полной мере устанавливать все обстоятельства, предусмотренные ст. 73 УПК РФ. При этом, как отмечалось ранее, по составам преступлений, предусмотренных главой 28 УК РФ, помимо основных признаков преступления определяется причинно-следственная связь между деянием и наступившими последствиями.

Специфика преступлений в сфере компьютерной информации обуславливает необходимость проведения по уголовным делам данной категории ряда специальных судебных экспертиз. В связи с этим важно осуществлять прокурорский надзор уже на первоначальном этапе расследования. Изучая в процессе расследования уголовное дело, прокурор должен установить, в полной ли мере данные экспертные заключения отвечают на поставленные следователем вопросы, все ли необходимые вопросы поставлены перед экспертом и достаточно ли в конечном итоге информации, содержащейся в заключении эксперта, для подтверждения обстоятельств совершения преступления. Несомненно, надзирающий прокурор должен обладать специальными знаниями о видах судебных экспертиз, проводимых по уголовным делам данной категории, давать руководителю следственного органа соответствующие рекомендации.

Так, при расследовании преступлений данной категории помимо традиционных видов экспертиз (криминалистической, дактилоскопической и т.д.) должны проводиться специальные судебные экспертизы - информационно-технологическая и информационно-техническая. Объединяет эти виды судебных экспертиз компьютерная информация, исследуемая, однако, с разных сторон - технологической либо технической. Различаются они и по непосредственным объектам исследования.

Проведение указанных судебных экспертиз необходимо для исследования собственно информационно-технологических процессов сбора (накопления, хранения, поиска, актуализации, распространения) информации и представления ее потребителю в условиях функционирования автоматизированных информационных систем и сетей и отдельно взятых технических и иных средств обеспечения этих процессов.

К подобным техническим средствам относятся компьютерные устройства, включающие в себя системный блок, устройство внешней памяти, устройства ввода и вывода информации, периферийные устройства, а также средства связи и телекоммуникации. К иным средствам следует отнести программы для компьютеров. Эти средства, обеспечивающие обработку информации, и составляют основу информационно-компьютерной технологии.

Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

Непосредственными предметами информационно-технологической экспертизы могут быть:

проектная документация на разработку и эксплуатацию компьютерных систем и сетей, отражающая процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

документированная информация (документ), то есть зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (отдельные документы и массивы документов в информационных системах), в том числе конфиденциальная информация;

материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов;

приказы и распоряжения администрации, инструкции, протоколы, договоры, положения, уставы и методики по эксплуатации компьютерных систем и сетей, отражающие порядок формирования информационных массивов и доступа к ним (важнейшими из этих предметов исследования могут быть должностные инструкции сотрудников соответствующих информационных подразделений);

схемы движения информации от источников к потребителю с указанием пунктов ее сбора, контроля, накопления, обработки и использования;

табель распределения выходных данных (перечень пользователей с указанием периодичности, объема и сроков поступления информации), а также другие документы, позволяющие наиболее полно раскрыть сущность информационной технологии данной компьютерной системы или сети (они обычно прилагаются к техническому заданию на их разработку);

входные и выходные документы, установленные для данной автоматизированной информационной системы;

словари, тезаурусы и классификаторы;

иные эксплуатационные и сопроводительные документы (особое значение для расследования компьютерных преступлений имеют журналы и другие виды учета работы операторов, регистрации сбойных ситуаций и обращений в компьютерную систему или сеть).

Несомненно, что все указанные документы должны быть изъяты своевременно и с соблюдением установленных законом норм. На необходимость этого прокурор должен обращать внимание следователя (в том числе на межведомственных оперативных совещаниях при обсуждении хода расследования уголовного дела), ориентируя последнего на соблюдение разумных сроков уголовного судопроизводства, установленных ст. 61 УПК РФ.

Информационно-технологическая экспертиза назначается в тех случаях, когда для возникающих в ходе расследования вопросов требуются специальные познания в технологии информационных процессов.

Возможности этой экспертизы достаточно широки. С ее помощью можно определить:

соответствие существующего технологического процесса компьютерной обработки информации проектной и эксплуатационной документации на конкретную информационную систему либо сеть;

конкретные отклонения от установленной информационной технологии, а также непосредственных исполнителей, допустивших нарушение установленной информационной технологии;

надежность организационно-технологических мер защиты компьютерной информации;

вредные последствия, наступившие из-за неправомерного нарушения установленной технологии компьютерной обработки информации;

обстоятельства, способствовавшие преступному нарушению технологии электронной обработки информации.

Изучая заключение информационно-технологической экспертизы, прокурору следует обратить внимание на то, выяснено ли следователем:

соответствие процессов сбора, обработки, накопления, хранения, поиска и распространения информации установленной проектной и эксплуатационной документации информационной технологии в данной компьютерной системе или сети;

какие конкретно отклонения от нее допущены;

кем нарушены технологические требования в процессе эксплуатации данной компьютерной системы или сети;

кто из должностных лиц должен был обеспечить соблюдение установленной технологии электронной обработки данных;

какие организационно-технологические меры защиты компьютерной системы, предусмотренные эксплуатационной документацией, были приняты;

какие вредные последствия связаны с нарушением установленной технологии электронной обработки информации;

является ли указанное отклонение от технологии обработки данных причиной наступивших последствий;

каковы причины нарушения установленной обработки компьютерной информации;

какие меры необходимо принять для их устранения.

Объектом информационно-технической экспертизы является техническое обеспечение информационной безопасности компьютерных систем и сетей.

Предметы информационно-технической экспертизы очень разнообразны. Иными словами, это инструменты, с помощью которых осуществляется доступ к информационным технологиям.

Условно их можно разделить на три основные группы:

1) технические средства обработки информации;

2) машинные носители информации и машинограммы, создаваемые средствами вычислительной техники;

3) программные средства и базы данных.

К первой группе относятся: компьютеры, отдельные узлы, устройства ввода и вывода информации; печатающие устройства (принтеры); периферийные устройства; устройства для связи между пользователями (модемы и факс-модемы); технические устройства и приспособления, специально разработанные для обхода средств защиты компьютерных систем и сетей от несанкционированного доступа; технические средства защиты информации и другие устройства.

Ко второй группе относятся: накопители на жестких дисках («винчестеры»); накопители на гибких магнитных дисках (дискеты); устройства для быстрого сохранения всей информации, находящейся на жестком диске (стримеры); оптические диски; пластиковые карты; аудио- и видеокассеты и другие носители информации, обрабатываемые компьютерами.

К третьей группе относятся программы для электронных вычислительных машин и базы данных.

Следует отметить, что исходя из анализа предметов указанных двух экспертиз, каждая из них имеет свои характерные особенности.

Информационно-техническая экспертиза назначается в том случае, когда в ходе следствия возникает необходимость в специальных исследованиях непосредственно технической части (отдельных узлов, блоков, периферийных устройств, оборудования, составляющих компьютерные системы или сети, пластиковых карт, дисков, дискет, других носителей информации, обрабатываемых компьютерами, а также программных средств).

К ее основным задачам относятся:

определение технического состояния компьютерного оборудования и пригодности его для решения задач, предусмотренных проектной и эксплуатационной документацией на данную автоматизированную систему;

техническое исполнение конкретных технологических информационных процессов и отдельных операций, ставших предметом предварительного следствия, установление конкретного терминала, с которого совершен несанкционированный доступ в данную компьютерную систему или сеть;

восстановление содержания поврежденных информационных массивов, отдельных файлов на магнитных носителях;

выявление технических причин сбойных ситуаций в работе компьютера;

установление подлинности информации, записанной на машинных носителях (дисках, дискетах, пластиковых картах), и внесенных в них изменений;

выявление в компьютерной программе разного рода неправомерных изменений, дополнений, вставок преступного характера;

установление вида компьютерного вируса, источника его проникновения в исследуемую систему и причиненных им вредных последствий;

установление соответствия средств защиты информации от несанкционированного доступа и проникновения компьютерного вируса сертификационным требованиям.

Изучая заключение информационно-технической экспертизы, прокурору необходимо выяснить, установлено ли:

техническое состояние компьютерного оборудования и его пригодность для решения в полном объеме задач, предусмотренных проектной и эксплуатационной документацией на данную компьютерную систему или сеть;

с какого терминала и по каким средствам связи и телекоммуникации мог быть совершен несанкционированный доступ в компьютерную систему или сеть;

возможность восстановления записанной прежде информации на частично поврежденном машинном носителе и ее содержание;

причина выявленных в ходе следствия сбоев данного компьютерного оборудования и наличие возможности их предотвращения с помощью технических средств;

перечень действий, предусмотренных соответствующими правилами для предотвращения сбоя, несанкционированного доступа, уничтожения файла, неправомерного копирования компьютерной информации, и не выполненных ответственным лицом;

признаки несанкционированных изменений информации, записанной на сменные диски (дискеты) и их содержание;

возможность использования в данной компьютерной системе посторонних программ без автоматической регистрации ее использования;

наличие в программе преднамеренной «закладки» (зарезервированного места в программе на случай необходимости последующей вставки дополнительных команд), ее назначение и автор;

средства защиты от вредоносных программ, предусмотренные в данной системе, их надежность, наличие сертификата и соответствие средств его требованиям;

процедура заражения данной системы компьютерным вирусом;

класс (тип) вируса, заразившего данную компьютерную систему и источник его происхождения;

размер и характер вреда, причиненного компьютерным вирусом.

Разумеется, круг вопросов по двум указанным видам экспертиз предлагаемыми перечнями не исчерпывается. С учетом характера каждого конкретного преступления могут быть поставлены и другие вопросы, объем которых определяется следователем в зависимости от расследуемого события и выяснения обстоятельств информационно-технологического или информационно-технического характера.

Так, по делам о неправомерном доступе к охраняемой законом компьютерной информации перед информационно-технологической экспертизой могут быть поставлены более частные вопросы, относящиеся к режиму ее обработки и охраны, главным образом к организационно-административным мерам защиты этой информации.

В настоящее время встречаются и другие виды экспертиз компьютерно-технической информации, что обусловлено динамичным развитием сферы высоких технологий, например, экспертиза электронно-цифровой подписи; экспертиза процесса разработки и использования программного обеспечения; компьютерно-сетевая экспертиза, экспертиза обстоятельств создания и использования файлов и баз данных и др. Все они отличаются, как правило, предметом, целью исследования и вопросами, которые могут быть поставлены перед экспертом.

В процессе расследования преступлений в сфере компьютерной информации может возникнуть необходимость производства и других видов экспертиз.

Например, идентификационная задача может быть решена с помощью комплексной компьютерно-технической и судебно-авторoведческой экспертизы, позволяющей проверить, не написана ли данная компьютерная программа конкретным лицом.

Для проведения носящих комплексный характер экспертных исследований в сфере компьютерной информации приглашаются высококвалифицированные специалисты в области информатики, вычислительной техники и программирования, а также традиционных видов криминалистической экспертизы, экономической, финансовой, бухгалтерской и товароведческой экспертиз.

В ходе комплексной судебно-бухгалтерской экспертизы и экспертизы программного обеспечения, устанавливают:

возможность несанкционированного скрытого доступа к программному обеспечению с целью внесения изменений, влияющих на результаты расчетов и отчетность, механизм совершения таких изменений, их характер и последствия;

кто из работников учреждения, обслуживающих и эксплуатирующих эти средства, имеет указанные выше возможности;

размер причиненного материального ущерба;

какие нарушения правил, регламентирующих ведение бухгалтерского учета и отчетности, могли способствовать образованию ущерба;

какая операционная система использована в конкретном компьютере;

не вносились ли в программу данного системного продукта какие-либо коррективы, изменяющие выполнение операций (какие именно);

возможно ли получение доступа к конфиденциальной финансовой информации, имеющейся в данной сети, и каким образом может быть осуществлен этот доступ.

Поскольку подлинная информация на машинных носителях при производстве экспертиз может быть безвозвратно уничтожена, следует убедиться в ее наличии в уголовном деле в качестве вещественного доказательства и направлении для проведения экспертного исследования ее копия.

В случае, если прокурор установит, что какие-либо вопросы в заключении эксперта раскрыты не полностью или невозможно сделать однозначный вывод об исследуемых обстоятельствах на основании данного заключения, целесообразно ориентировать следователя провести допрос эксперта с целью устранения указанных недостатков. Учитывая, что необходимо осуществлять надзор также и за соблюдением разумных сроков уголовного судопроизводства, нарушение которого ущемляет права

потерпевших, назначать дополнительную судебную экспертизу следует только в том случае, если возникшие вопросы нельзя выяснить в ходе допроса эксперта. Невыяснение всех необходимых вопросов в ходе экспертного исследования может впоследствии негативно сказаться на сроках судебного рассмотрения уголовного дела.

Если же прокурор выявляет уже допущенное в ходе предварительного расследования нарушение, то он должен использовать предоставленные ему Уголовно-процессуальным кодексом Российской Федерации полномочия и внести требование об устранении нарушений, допущенных в ходе предварительного следствия.

Как известно, предварительное следствие оканчивается ознакомлением обвиняемого и его защитника с материалами дела, составлением и подписанием следователем обвинительного заключения и передачей уголовного дела прокурору для решения вопроса о его направлении в суд.

Процессуальный порядок реализации полномочий прокурора по уголовному делу, поступившему с обвинительным заключением, регламентирован ст. 221, 222 УПК РФ.

В соответствии со ст. 221 УПК РФ прокурор или его заместитель обязаны рассмотреть поступившее уголовное дело в срок, не превышающий десяти суток, и принять одно из следующих решений:

об утверждении обвинительного заключения и о направлении уголовного дела в суд;

о возвращении уголовного дела следователю для производства дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения и устранения выявленных недостатков со своими письменными указаниями;

о направлении уголовного дела вышестоящему прокурору для утверждения обвинительного заключения, если оно подсудно вышестоящему суду.

Признав, что имеются основания для направления дела в суд, прокурор на первой странице обвинительного заключения ставит свою подпись об утверждении обвинительного заключения. Для принятия такого решения прокурором по материалам уголовного дела должны быть установлены следующие обстоятельства:

достаточность доказательств для рассмотрения дела в суде;

возможность поддержания с имеющимися доказательствами государственного обвинения;

относимость и допустимость собранных по делу доказательств;

соответствие предъявленного обвинения собранным доказательствам;

отсутствие обстоятельств, влекущих прекращение уголовного дела или уголовного преследования;

отсутствие процессуальных нарушений, исключающих возможность рассмотрения дела в суде;

соответствие обвинительного заключения требованиям закона.

Особое внимание, прокурору при изучении дел о преступлениях в сфере компьютерной информации, поступивших для утверждения обвинительного заключения, следует обращать на предъявленное обвинение, которое должно полностью подтверждаться имеющимися в уголовном деле доказательствами, и содержать текст идентичный тексту постановления о привлечении в качестве обвиняемого.

Прокурор согласно п. 2 ч. 1 ст. 221 УПК РФ вправе возвратить уголовное дело следователю для производства дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения и устранения выявленных недостатков со своими письменными указаниями. В настоящее время суд не имеет такого права, однако он может вернуть уголовное дело прокурору, при наличии оснований, предусмотренных ст. 237 УПК РФ, что, как правило, свидетельствует о ненадлежащем прокурорском надзоре за ходом предварительного следствия.

Хотя уголовно-процессуальным законом и предусмотрена возможность восполнения государственным обвинителем неполноты следствия, в том числе и путем предоставления суду новых доказательств, изначально отталкиваться от такой возможности при наличии нарушений, допущенных следователем и выявленных на стадии утверждения обвинительного заключения, нецелесообразно, поскольку направлять в суд с утвержденным обвинительным заключением уголовное дело, имеющее заведомые недостатки, прокурор не имеет права.

Поэтому при выявлении прокурором обстоятельств, препятствующих рассмотрению уголовного дела судом, в том числе и неустановлении обстоятельств, подлежащих доказыванию, он обязан своим мотивированным постановлением возвратить уголовное дело следователю для дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемого или составления нового обвинительного заключения и устранения выявленных недостатков.

Таким образом, в условиях увеличения числа преступлений в сфере компьютерной информации возрастает и роль прокурорского надзора за исполнением законов при расследовании преступлений указанной категории. Надлежащая организация прокурорского надзора позволяет обеспечить защиту прав и законных интересов лиц и организаций, потерпевших от преступлений, и личности от незаконного и необоснованного обвинения, осуждения, ограничения ее прав и свобод, восстановить уже нарушенные права и предотвратить совершение новых преступлений.

государственная тайна, служебная тайна, коммерческая тайна, персональные данные

From:
https://sps-ib.ru:80/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
**https://sps-ib.ru:80/npa:prok_14.04.2014**

Last update: **2018/09/28 17:51**