УДК 343.534(476)(043.3)

Н.А. Швед

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ТЕРМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ

В юридической литературе неоднократно указывалось на тот факт, что одним из существенных недостатков гл. 31 Уголовного кодекса Республики Беларусь является перегруженность ее узкоспециальными техническими терминами, которые законодатель не раскрывает в УК. Уяснение терминов, использованных при конструировании ст. 349–354 УК, требует от правоприменителя познаний в области не только уголовного права, но и компьютерной техники. В противном случае это может повлечь неоднозначное применение указанных норм на практике. В частности, хотелось бы остановиться более подробно на ст. 349 УК, устанавливающей ответственность за несанкционированный доступ к компьютерной информации.

В этой связи необходимо выяснить, что представляет собой несанкционированный доступ вообще и в каких случаях он признается преступлением, а также в чем заключается различие между несанкционированным и неправомерным доступом. Для начала проанализируем понятие «доступ к информации», являющееся составной частью рассматриваемого термина.

Закон Республики Беларусь «Об информации, информатизации и защите информации» раскрывает содержание понятия доступа к информации в ст. 1 как возможность получения информации и пользования ею. Практически идентичное определение содержится и в Федеральном законе «Об информации, информационных технологиях и о защите информации». Е.А. Миндрова, критикуя законодательное определение, считает, что понятие необоснованно расширено, так как к доступу относится правомочие использования полученной информации, т. е. в понятии «доступ к информации» смешаны возможности получения и распространения.

В научной литературе определения понятия доступа в основном, по сути, схожи с нормативными. Например, И.А. Клепицкий понимает под доступом к компьютерной информации приобретение и использование лицом возможности получать, вводить, изменять или уничтожать информацию либо влиять на процесс обработки. Однако есть и иные. Так, В.Г. Степанов-Егиянц считает, что под доступом к компьютерной информации следует понимать получение возможности обращения к компьютерной информации, в результате которого лицо получает правомочия обладателя информации.

На основании анализа нормативных и литературных источников можно выделить две существующие позиции относительно содержания понятия «доступ к информации»: 1) только полномочие на ознакомление с информацией; 2) полномочие на ознакомление и использование информации. При этом толкование содержания данных полномочий позволяет говорить о том, что ознакомление заключается в получении сведений, а использование – в извлечении из этих сведений пользы, применение их.

Представляется, что доступ к информации – это комплексное понятие, включающее в себя оба правомочия, поскольку они взаимосвязаны. Ознакомление, как правило, предполагает возможность дальнейшего использования информации, соответственно, прежде чем воспользоваться информацией, нужно сначала с ней ознакомиться. Возможность ознакомления с информацией без использования ее не представляет общественной опасности – информация должна быть воспринята.

Если обратиться к УК государств – участников СНГ, то можно заметить, что в России, Туркменистане, Азербайджане, Казахстане и Таджикистане такой доступ к информации именуется неправомерным, а в Беларуси, Узбекистане и Армении – несанкционированным. Н.Ф. Ахраменка считает предпочтительным использование прилагательного «неправомерный», которое характеризует сущностный, а не организационный признак доступа. М.Ю. Демьянович полагает, что доступ к компьютерной информации возможен только при наличии определенных законных полномочий, т. е. правового основания, поэтому правильно называть его неправомерным. В то же время некоторые российские авторы определяют неправомерный доступ как несанкционированное собственником информации ознакомление лица с данными (подобное используется в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации).

Заслуживающую внимания точку зрения высказывает Д.А. Овсюков, рассматривая такое условие как неправомерность. В частности, он отмечает, что при проведении DdoS-атаки доступ к сайту/серверу является именно правомерным. Такое право дает сам владелец сайта в соответствии с п. 1 ч. 3 ст. 6 Федерального закона «Об информации, информационных технологиях и о защите информации», разрешив доступ к информации на своем сайте/сервере для любого пользователя интернета (неограниченного круга лиц). Единственным различием между обычным доступом и DdoS-атакой является количество и частота подключений к серверу для получения информации. Таким об-

разом, сам доступ является правомерным, преступник при DdoS-атаке злоупотребляет предоставленным правом на доступ к сайту-жертве. В этой связи автор предлагает для надлежащей уголовно-правовой защиты от данного вида кибератак внести изменения в ст. 272 УК Российской Федерации, убрав из объективной стороны такое обстоятельство, как неправомерность доступа, заменив его признаками несанкционированности и умышленности в отношении последствий.

Т.Л. Тропина считает, что понятие неправомерного доступа является оценочным. Неправомерность может означать как несоответствие нормам права, так и совершение действия при отсутствии прав на его совершение. Автор также предлагает заменить термин «неправомерный» термином «несанкционированный».

В Положении о технической и криптографической защите информации в Республике Беларусь, утвержденном Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, несанкционированный доступ к информации определяется как доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа. В п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» разъясняется, что несанкционированным при хищении с использованием компьютерной техники считается доступ к компьютерной информации лица, не имеющего права на доступ к этой информации либо имеющего такое право, но осуществляющего его помимо установленного порядка. Кроме того, в технической литературе употребляется именно термин «несанкционированный доступ». Также прилагательное «несанкционированный» по отношению к доступу используется и в государственных стандартах.

На наш взгляд, несанкционированное ознакомление означает, что у лица нет ни прав на ознакомление с информацией, ни разрешения (санкции) владельца информации. Ведь ситуацию, когда у лица имеется право на доступ к информации, но такой доступ осуществлен помимо установленного порядка, относят к несанкционированному доступу. Поэтому считаем традиционное использование прилагательного «несанкционированный» более приемлемым.

Таким образом, несанкционированный доступ к компьютерной информации состоит из представленных в единстве получения и реализации возможности – ознакомления и использования указанной информации, сопряженных с нарушением системы ее защиты. При этом действие осуществляется лицом, не имеющим права на ознакомление с информацией либо имеющим такое право, но осуществляющим его с

нарушением установленного порядка. В предметно-содержательном аспекте несанкционированный доступ состоит из ознакомления с полученной информацией и из возможного затем ее использования, независимо от фактической реализации этой возможности. В организационно-управленческом аспекте несанкционированный доступ – это нарушение установленных правил и порядка доступа, связанных с системой защиты.

УДК 504.75.05

С.Л. Яблочников, И.О. Яблочникова, М.С. Яблочникова

АЛЬТЕРНАТИВНЫЙ ВЗГЛЯД НА ПРОБЛЕМЫ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Как правило, научные публикации в сфере обеспечения информационной безопасности в первую очередь касаются вопросов разработки методов и средств защиты информации от несанкционированного доступа к ней, ее искажения, уничтожения, модификации или же создания условий гарантированного доступа для определенного круга пользователей. Мероприятия, связанные с защитой информации, реализуются при ее приеме, передаче, хранении, обработке, визуализации и т. д. Таким образом, в качестве объектов, на защиту которых направлены соответствующие действия в рамках выработанной политики безопасности, рассматриваются либо некоторые информационные ресурсы, либо совокупность информационных процессов, осуществляемых в сложных технических системах. Также речь идет об обеспечении бесперебойного функционирования программно-технических комплексов, непосредственно реализующих указанные выше защищаемые информационные процессы.

Упомянутые сложные технические системы, существующие для обеспечения информационных процессов, в большинстве случаев являются человеко-машинными. Конечная цель функционирования таких систем – информационная поддержка производственной, экономической, технологической, социальной и иной деятельности отдельных личностей, определенных групп людей или же социума в целом. При этом общая логика совокупности действий в рамках обеспечения информационной безопасности такова: необходимо защитить информационные ресурсы или информационные процессы, которые человек (общество), в конечном счете, использует себе во благо.

Фактически мало кто из исследователей задумывается о том факте, что кроме негативных, несанкционированных воздействий (внешних и