УГОЛОВНОЕ ПРАВО И ПРОЦЕСС

УДК 343:004.056

В.В. Воробьёв

V. Vorobyov

К ВОПРОСУ О ПОНЯТИИ «НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» И МОМЕНТЕ ЕГО ОКОНЧАНИЯ

TO THE QUESTION OF THE CONCEPT «ILLEGAL ACCESS TO THE COMPUTER INFORMATION» AND THE MOMENT OF ITS TERMINATION

В статье проанализировано содержащееся в диспозиции ч.1 ст.272 Уголовного кодекса РФ понятие «неправомерный доступ к компьютерной информации». Рассмотрены различные точки зрения учёных на определение этого понятия, изучены международные правовые акты, касающиеся этих преступлений. Дана авторская редакция исследуемого понятия. Также представлена схема различных видов доступа к компьютерной информации и их влияние на момент окончания данного преступления.

In the article the concept «Illegal access to the information», that is included in the disposition p.1, Art.272 of the criminal code of the Russian Federation , is analyzed. Various points of view of scientists on definition of this concept are considered, the international legal acts concerning these crimes are studied. Author's edition of studied concept is given. The scheme of different types of access to computer information and their influence on the moment of the termination of this crime is also submitted.

Ключевые слова: компьютерные преступления, неправомерный доступ к компьютерной информации, состав преступления, объективная сторона преступления, момент окончания преступления, расследование компьютерных преступлений, уголовная ответственность за компьютерные преступления.

Keywords: computer crimes, illegal access to computer information, crime structure, objective party of a crime, moment of the termination of a crime, investigation of computer crimes, criminal liability for computer crimes.

Уголовная ответственность за неправомерный доступ к компьютерной информации предусмотрена ст.272 Уголовного кодекса РФ [1]. Объективная сторона состава ст.272 заключается в неправомерном доступе к охраняемой законом компьютерной информации, если это деяние повлекло за собой её уничтожение, блокирование, модификацию либо копирование.

Исходя из содержания диспозиции ст.272 Уголовного кодекса РФ, можно выделить следующие **обязательные признаки объективной стороны** этого **состава преступления**:

1) общественно опасное деяние, которое заключается в неправомерном доступе к охраняемой законом компьютерной информации;

2) общественно опасные последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации;

3) наличие причинной связи между совершённым деянием и наступившими последствиями.

Отсутствие одного из перечисленных признаков исключает уголовную ответственность за оконченное преступление.

Общественно опасное деяние в данном преступлении всегда проявляется в активной форме поведения виновного. Неправомерный доступ к компьютерной информации совершается только путём действия.

Понятие «неправомерный доступ к охраняемой законом компьютерной информации»* в законодательстве, науке и на практике трактуется по-разному, что вызывает необходимость формулирования унифицированного определения этого понятия.

Согласно п.6 ст.2 Федерального закона «Об информации, информационных технологиях и о защите информации» доступ к информации – это

* Термины «неправомерный доступ к охраняемой законом компьютерной информации», «неправомерный доступ к компьютерной информации» и «неправомерный доступ» автор использует как равнозначные.

возможность получения информации и её использования [2].

Закон Российской Федерации «О государственной тайне» доступ к сведениям, составляющим государственную тайну, трактует как санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну (ст.2) [3].

Федеральный закон «О коммерческой тайне» доступ к информации, составляющей коммерческую тайну, определяет как ознакомление определённых лиц с информацией, составляющей коммерческую тайну, с согласия её обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации (п.5 ст.3) [4].

В Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Соглашение вступило в силу для России 17.10.2008) неправомерный доступ определяется как несанкционированное обращение к компьютерной информации [5].

Так, например, С.А. Пашин предложил понимать под неправомерным доступом такие случаи, когда лицо проникает к информации, хотя не имеет права на доступ; лицо имеет право на доступ к информации, однако осуществляет его с нарушением правил [6]. Аналогичной позиции придерживается и И.А. Клепицкий [7]. По мнению В.П. Числина, под доступом к информации следует понимать ознакомление с охраняемой законом информацией и/или получение возможности совершать операции с данной информацией, в частности, её копирование, блокирование, модификацию и уничтожение. При этом, по его мнению, не имеет значения, осуществляется доступ к самой информации или к её носителям [8]. В.В. Крылов, М.В. Богомолов, А.В. Сизов полагают, что под неправомерным доступом к компьютерной информации следует понимать не санкционированное собственником или владельцем информации ознакомление лица с данными, содержащимися на машинных носителях или в электронных вычислительных машинах (далее – ЭВМ) [9]. С данной позицией не соглашается А.Л. Осипенко, который факт ознакомления с информацией считает не соответствующим закону и в связи с этим предлагает дополнить диспозицию ст.272 Уголовного кодекса РФ таким последствием, как «не санкционированное обладателем ознакомление лица с информацией ограниченного доступа» [10].

Таким образом, наблюдаются расхождения в определении понятия доступа к информации как в нормативном, так и научном толковании.

Применительно к составу ст.272 Уголовного кодекса РФ представление неправомерного доступа к компьютерной информации в виде несанкционированного ознакомления с информацией существенно сузит применение данной нормы. Если предположить, что лицо, имея целью уничтожить всю хранящуюся в компьютере информацию, отформатирует* жёсткий диск компьютера без «раскрытия» (просмотра) файлов, то указанное лицо не совершит неправомерного доступа к компьютерной информации, повлёкшего за собой её уничтожение, т.к. это лицо, исходя из логики определения, не ознакомилось с информацией, содержащейся на этом носителе [11].

Заслуживает внимания точка зрения, высказанная Е.И. Панфиловой и А.С. Поповым, которые неправомерный доступ к компьютерной информации понимают как незаконное получение возможности манипулировать информацией, т.е. воспринимать её, собирать, обрабатывать, накапливать, анализировать, хранить, искать, распространять и совершать с ней иные действия, при отсутствии на это у виновного действительного или предполагаемого права [12]. Однако это определение также не является безупречным.

Ранее автор в своих работах предлагал под неправомерным доступом к компьютерной информации понимать такое не санкционированное собственником или иным законным владельцем компьютерной информации проникновение к ней, в том числе с возможностью ознакомления, которое позволяет распоряжаться этой информацией (уничтожать, блокировать, модифицировать, копировать) и создаёт опасность как для самой информации, так и для интересов собственника [13]. Однако в 2006 г. был принят Федеральный закон «Об информации, информационных технологиях и о защите информации», а в 2008 г. Россия ратифицировала Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, которые, как отмечалось ранее, имеют нормы, определяющие понятие «доступ к информации».

С учётом положений данных нормативных актов под неправомерным доступом к компьютерной информации предлагается понимать несанкционированное обращение к компьютерной информа-

---

* **Форматирование диска** – способ разбиения поверхности носителя (например, магнитного диска) на адресуемые элементы (дорожки и сектора). Данная операция приводит к полному уничтожению информации, хранящейся на жёстком диске (винчестере) либо дискете (см., напр.: *Воройский Ф.С.* Систематизированный толковый словарь по информатике. – М.: Либерия, 1998. – С.47; *Синклер А.* Большой толковый словарь компьютерных терминов. – М.: Вече, АСТ, 1998. – С.326).

ции, дающее возможность получить (ознакомиться) и/или использовать эту информацию. Однако принятие данного определения за основу требует внесения изменений в диспозицию ст.272 Уголовного кодекса РФ. Так, к числу альтернативных последствий необходимо добавить и «ознакомление».

Также необходимо отметить, что уничтожение или модификация компьютерной информации путём внешнего воздействия на машинные носители теплом, магнитными волнами, механическими ударами и т.п. не является неправомерным доступом к компьютерной информации. Это связано с тем, что данные приёмы воздействия на информацию не соответствуют особенностям доступа к информации, определённым нами в приведённом выше определении. При уничтожении информации указанными способами отсутствует какое-либо обращение к компьютерной информации, которое могло бы рассматриваться как доступ.

Существует точка зрения о том, что для признания доступа неправомерным необходимо, чтобы информация была защищена от произвольного копирования. По нашему мнению, защищённость информации не может являться обязательным признаком состава преступления, предусмотренного ст.272 Уголовного кодекса РФ, потому что это неоправданно сужало бы действие данной статьи. Достаточно и того, что информация является чужой (ею кто-либо владеет, пользуется, распоряжается) и что она защищена законом.

В вопросе о моменте окончания неправомерного доступа автор солидарен с мнением таких учёных-правоведов, как М.М. Карелина [14], А.Н. Попов [15], А.А. Витвицкий [16], Н.И. Ветров [17], В.П. Малков [18], В.В. Крылов [19], А.Ю. Чупрова [20] и т.д. Их позиция заключается в том, что рассматриваемое преступление окончено с момента наступления в результате неправомерного доступа одного либо нескольких из указанных в статье последствий, т.е. несанкционированный просмотр информации, хранящейся в ЭВМ, преступления не образует. Для наличия состава преступления необходимо наступление хотя бы одного из перечисленных в диспозиции ст.272 последствий.

Моментом окончания доступа к компьютерной информации Ю.И. Ляпунов считает «момент отсылки пользователем компьютеру последней интерфейсной команды (голосовой, нажатием клавиши и т.п.) вызова хранящейся информации, независимо от наступления дальнейших последствий». Однако, по его мнению, преступлением это деяние станет только при наступлении указанных в диспозиции последствий. Все действия, выполненные до подачи последней команды, будут образовывать состав неоконченного преступления [21].

По мнению С.А. Пашина, преступление может быть окончено и после нейтрализации интеллектуальных средств защиты компьютерной информации. Если же при этом не наступили последствия в виде её уничтожения, блокирования, модификации или копирования, а также нарушения работы ЭВМ, системы ЭВМ или их сети, то такие действия (нейтрализация интеллектуальных средств защиты) должны рассматриваться как покушение на неправомерный доступ к компьютерной информации [22].

Можно выделить 3 основных вида доступа к компьютерной информации (см. *рис.*).

В первом виде доступа, если он осуществляется неправомерно, присутствует нейтрализация программных средств защиты информации. Нейтрализация достигается путём блокирования, модификации или уничтожения программы, ограничивающей доступ к информационным ресурсам. А эта программа в свою очередь является компьютерной информацией. Теперь предположим, что программные средства защиты компьютерной информации нейтрализованы, и осуществлён неправомерный доступ к охраняемой законом информации. Но виновное лицо, совершая доступ к информации, ничего неправомерного с ней не делает, а лишь просматривает её. В данной ситуации можно ошибочно предположить наличие оконченного преступления, предусмотренного ст.272 Уголовного кодекса РФ, т.к. программное средство защиты информации является компьютерной информацией, подвергшейся блокированию, модификации или уничтожению.

Однако программные средства защиты информации как продукт интеллектуальной деятельности являются объектом авторского права, а как товар – чьей-либо собственностью. Следовательно, нейтрализация этих программ не может рассматриваться как оконченное преступление, ответственность за которое предусмотрена ст.272 Уголовного кодекса РФ.

В подобных случаях ответственность может наступать только за нарушение авторских или смежных прав либо за умышленное уничтожение или повреждение имущества (ст.167 Уголовного кодекса РФ).

Таким образом, можно сделать вывод о том, что в ситуациях, когда программные средства защиты информации преодолены и виновное лицо получает доступ к охраняемой информации, но не совершает с ней никаких манипуляций, а лишь просматривает её, следует говорить об отсутствии состава преступления, предусмотренного ст.272 Уголовного кодекса РФ. Аналогичной точки зрения придерживаются Н.Г. Шурухнов, А.В. Пушкин, Е.А. Соцков и Ю.В. Гаврилин [23].

В данном случае можно вести речь о приготовлении, т.к. умышленно создаются условия для совершения преступления, но согласно ст.30 Уго-

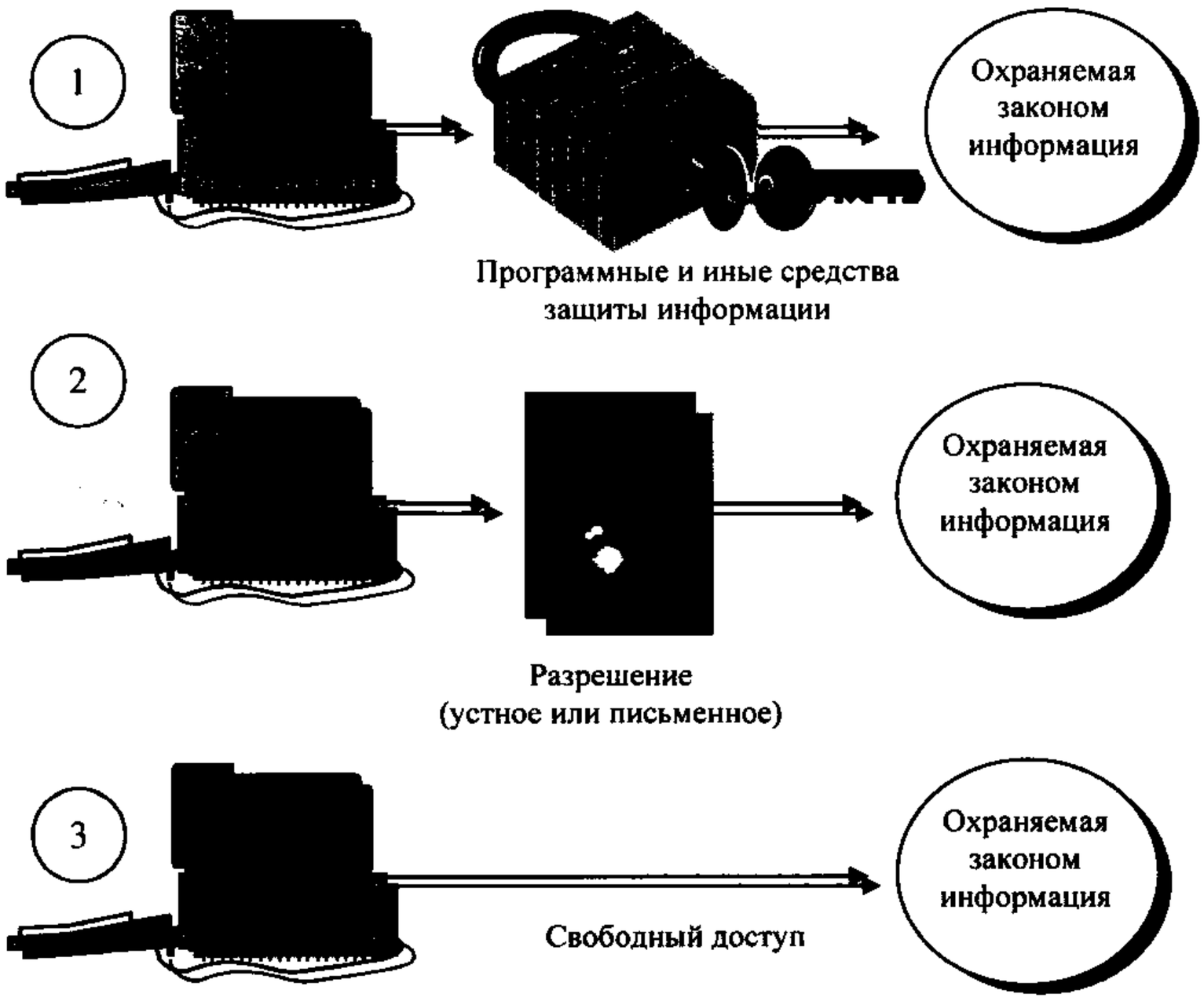

Рис. Виды доступа к компьютерной информации

ловного кодекса РФ уголовная ответственность за приготовление наступает только за тяжкие и особо тяжкие преступления, а к таковым преступление, предусмотренное ст.272, не относится.

Во втором виде доступа отсутствует нейтрализация средств ограничения доступа к информации. То есть лицо превышает свои полномочия и без разрешения уполномоченного лица осуществляет доступ к охраняемой законом информации. Однако, как и в первом случае, предполагаем, что виновный только знакомится с информацией.

При данном виде доступа к информационным ресурсам, если не наступило ни одно из указанных в диспозиции ст.272 Уголовного кодекса РФ последствий и лицом не была предпринята попытка к достижению этих последствий, состав неправомерного доступа также отсутствует.

Третий вид доступа полностью исключает неправомерность обращения к информации, т.к. доступ к информации ничем не ограничен. Исключением здесь может быть ситуация, когда имеет место правомерное ограничение прав пользователей по манипулированию информацией. В качестве примера могут послужить блоки информации с пометкой «только для чтения». Информация, имеющая такую пометку, запрещена к копированию, удалению, модификации и может только *просматриваться*. Если в нарушение условий работы с такой информацией лицо осуществляет её копирование, удаление или модификацию, то в его деянии присутствуют признаки неправомерного доступа к компьютерной информации.

Таким образом, моментом окончания неправомерного доступа к компьютерной информации (ст.272 Уголовного кодекса РФ) следует считать уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации [24].

* * *

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собр. законодательства РФ. – 1996. – № 25. – Ст.2954.

2. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2013) // Рос. газета. – 2006. – 29 июля.

3. О государственной тайне: закон РФ от 21.07.1993 № 5485-1 (ред. от 21.12.2013) // Рос. газета. – 1993. – 21 сент.

4. О коммерческой тайне: федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) // Рос. газета. – 2004. – 5 авг.

5. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001, вступило в силу для России 17.10.2008) // Собр. законодательства РФ. – 2009. – № 13. – Ст.1460.

6. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть / под общ. ред. Ю.И. Скуратова, В.М. Лебедева. – М.: ИНФРА-М; Норма, 1996. – С.412.

7. Комментарий к Уголовному кодексу Российской Федерации / под ред. А.В. Наумова. – М.: Юристъ, 1996. – С.664.

8. *Числин В.П.* Уголовно-правовые меры защиты информации от неправомерного доступа: автореф. … канд. юрид. наук. – М., 2004. – С.13–14.

9. *Крылов В.В.* Криминалистические проблемы оценки преступлений в сфере компьютерной информации // Уголовное право. – 1998. – № 3. – С.84; *Богомолов М.В.* Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. – Красноярск, 2002. – С.68; *Сизов А.В.* Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. – 2009. – № 1. – С.32–35.

10. *Осипенко А.* Уголовная ответственность за неправомерный доступ к конфиденциальной компьютерной информации // Уголовное право. – 2007. – № 3. – С.43–47.

11. *Воробьёв В.В.* Уголовно-правовая охрана компьютерной информации: учеб. пособие. – Сыктывкар: СыктГУ, 2003. – С.63.

12. См.: *Панфилова Е.И., Попов А.С.* Компьютерные преступления. Серия «Современные стандарты в уголовном праве и уголовном процессе» / под ред. Б.В. Волженкина. – СПб., 1998. – С.28.

13. *Воробьёв В.В.* Преступления в сфере компьютерной информации: юридическая характеристика составов и квалификация: дис. … канд. юрид. наук. – Н. Новгород, 2000. – С.18.

14. См.: Уголовный кодекс Российской Федерации. Научно-практический комментарий / под ред. В.М. Лебедева. – М.: Юридическая литература, 1998. – С.585.

15. См.: Комментарий к Уголовному кодексу Российской Федерации / отв. ред. В.И. Радченко, науч. ред. А.С. Михлин. – М.: СПАРК, 2000. – С.650.

16. См.: Уголовное право. Особенная часть: учебник / под ред. В.Н. Петрашаева. – М.: Приор, 1999. – С.431.

17. См.: *Ветров Н.И.* Уголовное право. Особенная часть: учеб. для вузов. – М.: ЮНИТИ-ДАНА, Закон и право, 2000. – С.367.

18. См.: Уголовное право России. Часть Особенная: учеб. для вузов / отв. ред. Л.Л. Кругликов. – М.: БЭК, 1999. – С.604.

19. См.: Уголовное право. Часть Общая. Часть Особенная: учебник / под ред. Л.Д. Гаухмана, Л.М. Колодкина, С.В. Максимова. – М.: Юриспруденция, 1999. – С.655.

20. См.: Научно-практический комментарий к уголовному кодексу Российской Федерации: в 2 т. / под ред. П.Н. Панченко. – Н. Новгород, 1996. – Т.2. – С.236.

21. См.: *Ляпунов Ю.И.* Ответственность за компьютерные преступления // Законность. – 1997. – № 1. – С.11.

22. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть / под общ. ред. Ю.И. Скуратова, В.М. Лебедева... – С.414.

23. См.: Расследование неправомерного доступа к компьютерной информации / под общ. ред. Н.Г. Шурухнова. – М.: Щит-М, 1999. – С.70.

24. *Воробьёв В.В.* Уголовно-правовая охрана компьютерной информации: учеб. пособие... – С.71–72.