

# 03, март 2016

УДК 343.791

**Неправомерный доступ к компьютерной информации как преступление,  
представляющее повышенную опасность охраняемым правам и интере-  
сам физических и юридических лиц**

*Шувалова Е.В., студент*

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,  
кафедра «Юриспруденция, интеллектуальная собственность и судебная экспертиза»*

*Научный руководитель: Кадников Б.Н., к.ю.н.*

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана  
кафедра «Юриспруденция, интеллектуальная собственность и судебная экспертиза»*

[\*bauman@bmstu.ru\*](mailto:bauman@bmstu.ru)

На протяжении последних нескольких десятилетий в мире активно поддерживалось и пропагандировалось мнение о том, что с развитием и усовершенствованием компьютерных и иных технологий жизнь человека, общества, государства становится значительно удобнее и легче. В результате последовательных действий, направленных на повсеместное внедрение соответствующих технологий практически во все сферы жизни, в современном мире большинство информации различного рода хранится в памяти всевозможных информационных системах (персональные данные граждан, сведения, касающиеся их материальных благ, трудовой деятельности др.).

На данный момент практически вся подобная информация о лице (физическом или юридическом) хранится в т.н. электронных базах данных. Следует признать, что в отличие, например, от формата хранения на бумажных носителях, этот способ во многом более практичен и удобен для хранения информации. Это значительно ускоряет поиск нужного документа, информации, а также позволяет использовать меньше пространства для подобных целей.

Как представляется автору, на современном этапе многие уже не в состоянии представить жизнь без электронных (компьютерных) технологий. Во многом это объясняется тем, что эти технические средства в значительной степени облегчают жизнь, делают ее более комфортной. Например, телефон (в большей степени, разумеется, имеется в виду мобильный телефон) позволяет практически в любой момент и в любой ситуации связать-

ся с нужным абонентом; воспользовавшись «электронными» деньгами можно оплатить практически любую покупку и т.д.

Кроме того, с помощью информационных технологий становится возможным принятие экономически значимых и важных решений и непосредственное участие в процессе эффективного и качественного управления деятельностью.

Не менее значимы компьютерные технологии и в области политической деятельности, например, в деятельности парламента. В качестве примеров можно указать такие случаи как регистрация депутатов, электронное голосование, доступ к мировым библиотечным центрам и справочным базам данных при разработке, экспертизе, принятии законов, иных важных решений, контроль за выполнением таких решений, получение с помощью факс-модемов электронных версий книг, газет, документов, электронная почта и многое другое.

Таким образом, со временем информационные технологии стали неотъемлемой частью практически всех сфер жизни. Однако наряду со всеми положительными моментами, перечисленными выше, становится очевидным, что указанная сфера порой является очень уязвимой и привлекательной для совершения определенными субъектами преступлений в области информационных технологий.

Неправомерный доступ к компьютерной информации как один из видов преступления закреплён в ст. 272 «Уголовного кодекса Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 30.03.2015, с изм. от 07.04.2015) (далее - УК РФ). К сожалению, наряду с развитием указанных технологий данный вид преступления набирает все большую популярность, становится весьма распространенным деянием, затрагивающим права и интересы физических и юридических лиц, а в некоторых случаях создает опасность и для государства как весьма важного участника различных правоотношений. Количество рассматриваемых преступлений постоянно увеличивается. Преступления в области компьютерной информации впервые были включены в УК РФ в 1996 году. В соответствии с ч.1 ст. 272 УК РФ (в действующей редакции) в качестве наказания за данное преступление предусмотрены штраф, исправительные работы, ограничение свободы, принудительные работы либо лишение свободы на срок до двух лет. Как следует из данной статьи, последствиями совершения указанного преступления (неправомерный доступ к охраняемой законом компьютерной информации) являются уничтожение, блокирование, модификация либо копирование компьютерной информации.

К сожалению, в настоящее время далеко не все понимают высокую степень общественной опасности данного вида преступления, хотя специалисты в области информаци-

онных технологий на протяжении уже достаточно длительного периода времени «бьют тревогу», поскольку вред, ущерб, причиненный в результате такого рода действий, может быть настолько серьезным, что порой его трудно представить. Однако существует уже достаточно много примеров, заставляющих обратить особое внимание на данную проблему. Например, одним из весьма «ярких» примеров является т.н. «ограбление века» о котором стало известно в феврале 2015 года. В результате осуществления лицами, явно обладающими соответствующими знаниями в сфере компьютерных технологий, определенных действий, из банков было похищено около одного миллиарда долларов. «Хакерам» удалось заразить вирусами информационные системы около ста финансовых организаций.

Следует наиболее подробно рассмотреть элементы и признаки состава рассматриваемого преступления.

Объектом преступления являются права на информацию ее владельца и третьих лиц, а также безопасность компьютерной информации.

Предмет посягательства - информация в компьютерных файлах, программах или базах данных, причем не любая, а только охраняемая законом, т.е. доступ к которой (возможность ознакомления, копирования, изменения, уничтожения) ограничен. Данная информация должна содержаться исключительно на электронных носителях.

Относительно объективной стороны данного преступления автор считает необходимым сообщить следующее.

Бездействие лица, даже в случае если оно повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, под действие ст. 272 УК РФ не подпадает. Такое бездействие может быть признано преступлением, например, по статье 274 УК РФ («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»).

Само понятие «доступ» в УК РФ не раскрывается. Однако из содержания ст. 8 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации» (далее - Закона «Об информации») следует, что под «доступом» необходимо понимать поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законом.

Одним из элементов, определяющих «неправомерность» доступа является наличие юридических (правовых) методов, которые призваны обеспечить защиту информации. Например: защита от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев,

установку сигнализации. Также среди обязательных элементов, определяющих неправомерность доступа к компьютерной информации следует выделить нахождение данной информации под охраной российского законодательства (например, норм Закона «Об информации»).

Поправки к ст. 272 УК РФ, внесенные Федеральным законом от 07.12.2011 №420-ФЗ (ред. от 28.12.2013) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», установили, что под «компьютерной информацией» в уголовно-правовом аспекте понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

На основании положений данного закона к охраняемой информации относятся сведения ограниченного доступа, которыми являются:

- сведения, составляющие государственную тайну,
- информация конфиденциального характера,
- коммерческая, служебная или иная тайна.

Перечень сведений, составляющих государственную тайну, определяется Законом РФ от 21.07.1993 № 5485-1 (ред. от 21.12.2013) «О государственной тайне». К государственной конфиденциальной информации относятся, в частности, служебная тайна, государственная тайна, данные предварительного расследования, сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса, сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа. За нарушения данных видов тайн и раскрытие соответствующей информации предусмотрена уголовная ответственность (в частности, по ст. 310 и 311 УК РФ, а также ст. 320 УК РФ).

Субъектом преступления, как правило, является физическое вменяемое лицо, достигшее к моменту его совершения 16-летнего возраста. В некоторых случаях субъект наделен дополнительным признаком. Однако необходимо обратить внимание, что лицо также может являться участником группы лиц, действующих по предварительному сговору, участником организованной группы, либо может использовать для совершения преступления свое служебное положение.

Субъективная сторона преступления характеризуется умышленной формой вины в виде прямого или косвенного умысла.

Мотивы совершения преступления могут быть различными. Например, это т.н. «спортивный интерес», проверка своего уровня квалификации, любопытство, совершение другого преступления, корыстная заинтересованность и пр.

Чтобы представить возможные масштабы совершения рассматриваемого преступного деяния, необходимо указать, что посредством неправомерного доступа к компьютерной информации возможно совершение таких преступлений, как, например, нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (см. ст. 138 УК РФ), авторских/смежных прав (см. ст. 146 УК РФ), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ).

Автор считает целесообразным привести практические примеры по рассматриваемой в настоящей статье теме, которые достаточно точно отражают ее суть и содержание.

**14.08.2014**

**Сотрудниками Управления «К» МВД России пресечена деятельность лиц, подозреваемых в неправомерном доступе к компьютерной информации**

Два гражданина решили оказывать услуги, связанные со взломом электронных ящиков почтовых сервисов, а также страниц граждан и организаций в социальных сетях.

В целях рекламы данными гражданами публиковались объявления на различных ресурсах сети Интернет с предложениями указанных услуг.

Денежные средства (от трех до десяти тысяч руб.) для выполнения данной деятельности должны были переводиться исключительно путем использования электронных платежных систем.

Заказчиками выступали как физические, так и юридические лица. Как правило, цель составляло получение конфиденциальной информации относительно частной жизни граждан, а также коммерческой тайны юридических лиц.

В результате оперативно-розыскных мероприятий были установлены личности злоумышленников, вследствие чего были обнаружены и изъяты компьютеры, различные носители информации. Возбуждено уголовное дело по ст. 272 УК РФ <sup>1</sup>

**21.03.2015**

**Возбуждено уголовное дело по факту неправомерного доступа к компьютерной информации**

---

<sup>1</sup> <https://mvd.ru/news/item/2455036>

Правоохранительными органами было установлено, что в начале февраля гражданин, действовавший в целях блокирования доступа к компьютерной информации сайта одного из городских информационных агентств, совершил неправомерный доступ к соответствующей компьютерной информации, в результате чего доступ к сайту был заблокирован в течение нескольких часов.

Возбуждено уголовное дело по ч. 1 ст. 272 УК РФ<sup>2</sup>.

На основании вышеизложенного можно сделать вывод о том, что неправомерный доступ к компьютерной информации, как преступление, предусмотренное статьей 272 УК РФ, является весьма опасным деянием. Кроме того, принимая во внимание скорость развития и внедрения различных компьютерных технологий на современном этапе, следует ожидать увеличения количества данных преступлений, а также подобного рода правонарушений в целом.

Вместе с тем следует указать, что ст. 272 УК нуждается в дальнейших изменениях и дополнениях, в частности, для учета в наиболее полном объеме аспектов «неправомерного доступа». Также можно утверждать, что одновременно с внедрением компьютерных технологий во все сферы жизни общества и государства, увеличивается потребность в усилении защиты компьютерной информации.

### Список литературы

- [1]. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).
- [2]. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.03.2015, с изм. от 07.04.2015).
- [3]. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М.: БЕК, 2007. 215 с.
- [4]. Алескеров В.И. Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации: монография. Домодедово: ВИПК МВД России, 2014. 110 с.
- [5]. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М.: Новый юрист, 2008. 256 с.

---

<sup>2</sup> <http://vtk-24.ru/index.php/categories/proisshestiya/18703>

- [6]. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации».
- [7]. Федеральный закон от 07.12.2011 № 420-ФЗ (ред. от 28.12.2013) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».
- [8]. Закон РФ от 21.07.1993 № 5485-1 (ред. от 21.12.2013) «О государственной тайне».
- [9]. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных».