Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет»
(Национальный исследовательский университет)
Юридический институт
Кафедра «Уголовное и уголовно-исполнительное право, криминология»

ДОПУСТИТЬ К ЗАЩИТЕ
Руководитель магистерской программы,
д.ю.н., профессор, профессор кафедры
_____Ю.А. Воронин
_____ 2017 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.04.01.2017.244.М

Направление: «Юриспруденция»
Магистерская программа: «Уголовное право, криминология и уголовно-исполнительное право»

Руководитель магистерской диссертации
Горбатова Марина Анатольевна
к.ю.н., доцент _____
_____2017 г.

Автор магистерской диссертации
магистрант группы Юм – 244
Климков Станислав Дмитриевич___
_____2017 г.

Нормоконтролер
Бирюкова Дарья Вячеславовна
Преподаватель _____
_____2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы обусловлена тем, что современное существование и развитие любого государства основано на широком использовании информационных технологий, телекоммуникационных инфраструктур.

Информатизация внедрилась в государственную и общественную жизнь, телекоммуникационные системы охватывают практически все сферы жизнедеятельности человека. При этом все ценные сведения, в том числе и личные данные, уже давно обрабатываются и используются в электронной форме.

Вместе с тем любые достижения научно-технического прогресса провоцируют и появление новых форм криминальной деятельности. Поэтому в обязанности государства входит защита интересов личности, общества и государства от преступных посягательств мерами, адекватными существующей криминальной обстановке. На появление преступлений в сфере компьютерной информации законодатель отреагировал установлением уголовной ответственности за некоторые виды общественно опасных посягательств (глава 28 УК РФ), в том числе и за неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Однако данные уголовно-правовые нормы достаточно быстро «устарели», поскольку законодательство не успевало за развитием информационных технологий.

И, несмотря на внесение изменений в 2011 г. в составы компьютерных преступлений, которые должны были ликвидировать отставание законодательства от криминальных реалий, уголовно-правовое противодействие неправомерному доступу к охраняемой законом компьютерной информации на данный момент является недостаточно эффективным.

Правоприменительная практика по определенным причинам все еще не адаптировалась к новой редакции состава неправомерного доступа к

компьютерной информации.

В настоящее время имеются существенные противоречия в толковании такого признака состава как предмет преступления. Законодательная конструкция объективной стороны усложняет решение важных вопросов квалификации, связанных с установлением причинной связи, вины, квалифицирующих признаков. Нередко возникают трудности с отграничением неправомерного доступа от смежных составов преступлений. Недостатки просматриваются и в соразмерности санкций, предусмотренных в рассматриваемой статье. Все это создает некие препятствия для эффективного противодействия неправомерному доступу к компьютерной информации уголовно-правовыми средствами, в связи с этим обращение к данной проблематике представляется весьма своевременным.

Объектом диссертационной работы являются общественные отношения, возникающие в связи с совершением неправомерного доступа к охраняемой законом компьютерной информации.

Предмет диссертационной работы – нормы отечественного уголовного законодательства, регламентирующие ответственность за неправомерный доступ к компьютерной информации; нормы информационного права, регулирующие отношения в сфере охраны компьютерной информации; материалы судебной практики по уголовным делам о неправомерном доступе к компьютерной информации.

Цель диссертационной работы – комплексное изучение проблем уголовной ответственности за неправомерный доступ к компьютерной информации, определение путей совершенствования уголовного законодательства и практики его применения.

Задачи диссертационной работы:

– исследовать уголовно-правовую характеристику состава неправомерного доступа к компьютерной информации;

– провести юридический анализ квалифицирующих признаков;

– выявить проблемы квалификации неправомерного доступа к компьютерной информации;

– разработать предложения по совершенствованию законодательства и правоприменительной практики в сфере противодействия неправомерному доступу к компьютерной информации.

Результаты диссертационной работы имеют практическую значимость, содержат выводы и предложения по совершенствованию нормы уголовного закона, регламентирующей ответственность за неправомерный доступ к компьютерной информации, а также практики применения данной нормы.

Изложенные в работе выводы, определение ряда актуальных понятий и результаты изучения проблемных вопросов квалификации неправомерного доступа к компьютерной информации могут быть полезными в деятельности правоохранительных органов по противодействию данным посягательствам. Кроме того, они могут использоваться для дальнейших исследований проблем уголовной ответственности за совершение преступлений данной категории, будут способствовать обогащению и развитию знаний в области противодействия преступлениям в сфере компьютерной информации.

1 УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Согласно ст. 272 УК РФ преступлением является неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации.

1.1 Объект и предмет неправомерного доступа к компьютерной информации

В науке уголовного права существует много подходов к определению объекта преступления. «Традиционная теория объекта как общественного отношения»[1] – справедлива во многих случаях: например, при признании отношений собственности в качестве объекта преступлений, предусмотренных главой 21 УК РФ. В то же время, «представление об объекте преступления как правовом благе, охраняемом уголовным законом от преступных посягательств»[2], продолжает традиции российской уголовно-правовой науки и соответствует современным взглядам на сущность, социальную ценность права. Поэтому необходимо признать тот факт, что обе теории в настоящее время имеют полное право на существование. Мы же в своей работе будем придерживаться концепции объекта как правового блага.

Исходя из того, что главу 28 УК РФ «Преступления в сфере компьютерной информации» законодатель включил в раздел IX «Преступления против общественной безопасности и общественного

[1] Трайнин А.Н. Учение о составе преступления. – М., 1946. – С. 72 – 73; Никифоров Б.С. Об объекте преступления // Советское государство и право. – 1948. – № 9. – С. 48; Рарог А.И. Уголовное право России. Общая часть: учебник /– М., 2009. – С. 70; Здравомыслов Б.В.Уголовное право РФ. Общая часть / – М., 1999. – С. 111.

[2] Сергиевский И.Д. Русское уголовное право. Общая часть: пособие к лекциям. – СПб., 1908. – С. 56; Познышев С.В. Учебник уголовного права: Общая часть. Очерк основных начал общей и особенной части уголовного права. Т. 1 / – М., 1923. – С. 53; Наумов А.В. Уголовное право. Общая часть: курс лекций. – М., 1996. – С. 147.

порядка», родовым объектом неправомерного доступа, как и всех преступлений в сфере компьютерной безопасности, следует признать общественную безопасность и общественный порядок.

Концепция общественной безопасности в РФ рассматривает «общественную безопасность как часть национальной безопасности Российской Федерации»[1]. Понятие национальной безопасности определено в Стратегии национальной безопасности РФ до 2020 г. как «состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства»[2].

Учитывая структуру раздела IX УК РФ, общественную безопасность в теории уголовного права рассматривают в широком и узком значениях.

В широком значении она является составной частью родового объекта преступлений, предусмотренных данным разделом, а в узком – видовым объектом посягательств, предусмотренных главой 24 УК РФ «Преступления против общественной безопасности». При этом, как справедливо отметила И.А. Сало, «преступления в сфере компьютерной информации посягают не на всю общественную безопасность в целом, а лишь на часть, связанную с безопасным производством, хранением, использованием и распространением компьютерной информации»[3].

Видовой объект преступлений в сфере компьютерной информации в теории уголовного права определяется неоднозначно. Заметим, что перечисленные ниже позиции сформированы учеными еще до внесения

---

[1] Концепция общественной безопасности в Российской Федерации: утв. Президентом РФ. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/19653.

[2] Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации до 2020 г.» от 12 мая 2009 г. № 537 // Российская газета. – 2009. – № 88.

[3] Сало И.А. Преступные действия с компьютерной информацией ограниченного доступа: дисс. … канд. юрид. наук. – М., 2001. – С. 50.

изменений в главу 28 УК РФ Федеральным законом от 07 декабря 2011 г. № 420 – ФЗ[1], поэтому в некоторых из них упоминаются ЭВМ, системы ЭВМ или сети ЭВМ. В качестве видового объекта специалисты называют:

– «права и интересы личности, общества и государства, выступающих в качестве собственника или владельца, и возникающие отношения по поводу безопасности использования ЭВМ, системы ЭВМ или сети ЭВМ»[2];

– «порядок создания, ведения, пользования, хранения, защиты и распространения компьютерной информации»[3];

– «общественные отношения, обеспечивающие безопасное использование компьютерных систем и сетей, т. е. такое их использование, которое исключает причинение вреда личности, обществу и государству»[4];

– «отношения по производству, хранению, использованию, распространению или защите компьютерной информации»[5];

– «отношения по нормальному, безопасному использованию компьютерной информации»[6];

– «отношения в сфере безопасности компьютерной информации и нормальной работы ЭВМ»[7];

– «компьютерная безопасность, понимаемая как состояние защищенности информации, обращаемой в ЭВМ, компьютерной системе и сетях, ее технических и программных средств, обеспечивающая минимальную

---

[1] Федеральный закон РФ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 07 декабря 2011 г. № 420 – ФЗ // Российская газета. – 2011. – № 278.

[2] Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания. – Тамбов: Издательство ТГУ, 2003. – С. 40.

[3] Постатейный комментарий к Уголовному кодексу РФ / под ред. А.И. Чучаева. – М.: ИНФРА-М: КОНТРАКТ, 2004. – С. 623.

[4] Здравомыслов Б.В. Уголовное право Российской Федерации. Особенная часть: учебник / Изд. 2-е, перераб. и доп. – М.: Юристъ, 2000. – С. 352.

[5] Колобов В.А. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решения. – Нижний Новгород: Финансовый факультет ННГУ, 2001. – С. 37.

[6] Максимов В.Ю. Компьютерные преступления (вирусный аспект). – Ставрополь: Кн. изд-во, 1999. – С. 23.

[7] Ветров Н.И. Уголовное право: учебник / 4-е изд. испр. и доп. – М.: ИД «Юриспруденция», 2007. – С. 630.

вероятность причинения им вреда»[1];

– «информационная безопасность»[2].

Именно последняя позиция представляется нам соответствующей современным отношениям в сфере компьютерной информации. На сегодняшний день законодательное определение термина «информационная безопасность» отсутствует, данное понятие определено лишь в одноименной Доктрине[3], где под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В юридической науке отсутствует единый взгляд на данное понятие.

Одни ученые рассматривают информационную безопасность как «невозможность причинения ущерба объекту – с одной стороны, и как свойство самого объекта не наносить ущерба другому объекту в информационной сфере – с другой»[4].

Другие авторы, опираясь на Доктрину информационной безопасности РФ, рассматривают ее как состояние защищенности. В то же время, если информационную безопасность определять через интересы личности, общества и государства в информационной сфере, то нам будет сложно отграничить преступления главы 28 УК РФ от других посягательств, связанных с информацией (например, нарушение авторских, смежных,

---

[1] Ахраменка Н.Ф. Родовой объект компьютерных преступлений // Проблемы развития юридической науки и совершенствования правоприменительной практики: сб. науч. тр. – Минск: БГУ, 2005. – С. 309 – 314; Батурин Ю.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие // Советское государство и право. – 1990. – № 12. – С. 89.

[2] Попов А.Н. О предмете преступления, предусмотренного ст. 272 УК РФ // Криминалистъ. – 2008. – № 1. – С. 5; Дворецкий М.Ю. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации: монография. – Тамбов: Изд- во ТГУ им. Г.Р. Державина, 2006. – С. 63.

[3] Доктрина информационной безопасности РФ: утв. Президентом РФ 09.09.2000 г. № Пр-1895 // Российская газета. – 2000. – № 187.

[4] Юсупов Р.М. Научно-методологические основы информатизации. – СПб.: Наука, 2000. - – С. 345.

изобретательских и патентных прав, государственная измена, шпионаж и др.).

Согласно третьей позиции, информационная безопасность определяется через общественные отношения.

В частности, под ней понимают: «специальную группу общественных отношений, содержание которых составляют права и интересы различных субъектов в области обеспечения безопасности использования информации и информационных ресурсов, необходимых для нормальной жизнедеятельности социума»[1]; «совокупность общественных отношений, складывающихся в процессе защиты информационных ресурсов и охраны прав субъектов информатизации, а также обеспечения безопасности пользователей и пользования компьютерными системами и сетями»[2].

По нашему мнению, видовым объектом преступлений в сфере компьютерной информации следует признавать информационную безопасность в сфере использования компьютерной техники, понимаемую как состояние защищенности производства, хранения, передачи, использования, обработки компьютерной информации и нормального функционирования компьютерной техники от различных посягательств. Данное определение видового объекта позволит нам отграничивать преступления, объединенные в гл. 28 УК РФ, от иных преступлений против информационной безопасности.

Непосредственный объект неправомерного доступа к охраняемой компьютерной информации в теории уголовного права тоже определяется неоднозначно.

Одни авторы, не разделяя по объекту преступления в сфере компьютерной информации, называют общий для них непосредственный

---

[1] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореферат дис. … канд. юрид. наук. – М., 1998. – С. 12.

[2] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2002. – С. 40.

объект в виде состояния защищенности компьютерной информации (для составов ст.ст. 272 и 273 УК РФ) и ЭВМ, системы ЭВМ и их сети (для ст. 274 УК РФ)[1].

Другие ученые, выделяя самостоятельный непосредственный объект неправомерного доступа к охраняемой законам компьютерной информации, определяют его по-разному:

– «конкретные права и интересы, охраняемые уголовным законом, подвергающиеся посягательству в результате совершения общественно опасного деяния, предусмотренного одной из статей главы 28 УК»[2];

– «общественные отношения по соблюдению и обеспечению безопасности законного получения, обработки и использования компьютерной информации, а также нормального функционирования компьютерной техники»[3];

– «право владельца системы на неприкосновенность информации, содержащейся в системе, интерес относительно правильной эксплуатации системы»[4];

– «общественные отношения, обеспечивающие информационную безопасность»[5].

Судебная практика, например, объектом преступления признает «общественные отношения, связанные с использованием компьютерной информации»[6].

Мы полагаем, что непосредственным объектом неправомерного доступа является безопасность компьютерной информации, т. е. состояние

---

[1] Уголовное право России. Часть Особенная: учебник для ВУЗов / отв. ред. Л.Л. Кругликов. – М., 2005. – С. 630, 633 – 634.

[2] Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания. – Тамбов: Издательство ТГУ, 2003. – С. 40.

[3] Буз С.А. Уголовно-правовые средства борьбы с преступлениями в сфере компьютерной информации. – Краснодар, 2002. – С. 35.

[4] Клепицкий И.А. Указ. соч. – С. 352.

[5] Мазуров В.А. Указ. соч. – С. 26.

[6] Дело № 10-11502 … из архива Московского городского суда за 2013 г. [Электронный ресурс]. – Режим доступа: http://www.mos-gorsud.ru.

защищенности производства, хранения, передачи, использования и обработки компьютерной информации от различных посягательств.

Весьма актуальным для квалификации рассматриваемого преступления считается вопрос о его предмете, т. к. предмет является конструктивным признаком состава, необходимым для установления основания уголовной ответственности за неправомерный доступ к охраняемой законом компьютерной информации.

Преобладающей позицией в теории уголовного права является признание вещной формы предмета преступления, исходя из чего под предметом понимаются: «овеществленный элемент материального мира»[1]; «материальный субстрат»[2]; «предметы внешнего мира»[3], «материальные феномены»[4]. Однако при таком подходе охраняемую законом компьютерную информацию нельзя признать предметом преступления, т. к. она ни предметом, ни вещью не является.

В связи с этим, учитывая тенденции современного информационного общества, предлагается включить в понятие предмета преступления «нематериальные блага»[5]; «интеллектуальные ценности, энергию»[6]; «информацию»[7].

Как верно отмечает М.П. Бикмурзин, «вещь – далеко не единственная форма существования материи. Любые предметы материального мира, в том

---

[1] Бикмурзин М.П. К вопросу о правовой природе и понятии предмета преступления // Соискатель. – 2004. – № 1. – С. 12; Пашковская А.В. Указ. соч. – С. 210; Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Харьков, 1988. – С. 47.

[2] Иманалиева А.Ж. Проблемы криминалистического учения о предмете преступления: автореферат дис. ... канд. юрид. наук. – М., 2004. – С. 11.

[3] Наумов А.В. Указ. соч. – С. 153 – 154.

[4] Игнатова А.Н. Уголовное право России. Учебник для ВУЗов. Т. 1. Общая часть / под ред. – М.: Изд-во НОРМА, 2000. – С. 111.

[5] Козаченко И.Я. Уголовное право. Общая часть. Учебник для ВУЗов / отв. ред.– М.: Изд-во НОРМА, 1999. – С. 133 – 134.

[6] Спиридонова О.Е. Символ как предмет преступления: автореферат дис. ... канд. юрид. наук. – Казань, 2002. – С. 11.

[7] Букалерова Л.А. Некоторые вопросы квалификации преступлений с использованием информации как предмета преступлений и предмета совершения корыстных преступлений // Научные труды РАЮН. – Вып.2. – Т.1. – М., 2002. – С. 411.

числе невещественной природы, могут быть подвергнуты воздействию, учтены и зафиксированы»[1].

В уголовном законодательстве информация как признак состава преступления прямо указывается в ряде диспозиций, в том числе и в ст. 272. Определенные действия виновного в отношении информации имеют такое же значение, как и воздействие на указанные в законе вещи материального мира. Кроме того, «теория информации уже давно способна обеспечить количественный учет информации, единицей измерения которой является бит»[2].

Поэтому полагаем, что информация уже вполне может признаваться предметом преступления. А значит, информацию можно признать и предметом незаконного доступа.

Специалисты называют три основных свойства информации, ради охраны которых создана рассматриваемая уголовно-правовая норма: «конфиденциальность, целостность и доступность»[3].

Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем. Для некоторых типов информации конфиденциальность является одним из наиболее важных элементов (например, сведения медицинских учреждений о состоянии здоровья пациентов). Понятие конфиденциальности будет рассмотрено ниже.

Целостность информации подразумевает, что только уполномоченные лица могут вносить в эту информацию изменения.

Показателен пример, когда злоумышленник вторгся в компьютерную систему исследовательской лаборатории ядерной физики в Швейцарии и изменил один знак в значении числа "пи", в результате чего из-за ошибок в

---

[1] Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: дис. ... канд. юрид. наук. – Уфа, 2005. – С. 55.
[2] Бикмурзин М.П. Указ. соч. – С. 57.
[3] Амелин Р.В. О возможном решении проблемы неполноты главы 28 УК РФ // Уголовно-исполнительная система: право, экономика, управление. – 2009. – № 5. – С. 5 – 6.

расчетах был сорван важный эксперимент, а организация понесла миллионные убытки[1].

Целостность особенно важна для данных, связанных с функционированием объектов критических инфраструктур (например, управления воздушным движением, энергоснабжения и т. д.), финансовых данных.

Доступность информации означает наличие своевременного беспрепятственного доступа к информации для субъектов, обладающих соответствующими полномочиями.

В этой связи следует заметить, что Конвенция «о преступности в сфере компьютерной информации»[2], выделяя пять групп киберпреступлений, первую из них именует «Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем» (незаконный доступ, незаконный перехват, воздействие на компьютерные данные или системы, а также деяния, связанные с противозаконным использованием специальных технических устройств).

В связи с тем, что термины, используемые при конструировании составов компьютерных преступлений, имеют технический характер, данные понятия определяются в специальных нормативных актах. Базовым при этом является Федеральный закон от 27 июля 2006 г. № 149 – ФЗ «Об информации, информационных технологиях и о защите информации»[3] (далее Закон «Об информации»), в котором информация определяется как сведения (сообщения, данные) независимо от формы их предоставления.

До внесения изменений в составы компьютерных преступлений

---

[1] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография. – М.: Норма, 2004. – С. 21.

[2] Конвенция о преступности в сфере компьютерной информации (вступила в силу 01.07.2004). Россия в настоящей Конвенции не участвует.

[3] Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // Российская газета. – 2006. – № 165.

Федеральным законом от 07 декабря 2011 г. № 420 – ФЗ[1] понятие компьютерной информации определяли путем толкования диспозиции ст. 272 УК РФ – как информацию на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Приведем лишь некоторые точки зрения на компьютерную информацию:

– «это организационно упорядоченная совокупность сведений, представляющих ценность для личности, общества и государства, зафиксированных в ЭВМ или на машинных носителях с реквизитами, позволяющими их идентифицировать, имеющих собственника, устанавливающего правила пользования ими, реализующего свои полномочия на них»[2];

– «это информация, зафиксированная на машинном носителе и передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ»[3];

– «это сведения о лицах, предметах, фактах, событиях, явлениях и процессах, подлежащих вводу в ЭВМ, хранимые в памяти, обрабатываемые на ЭВМ и выдаваемые пользователям»[4].

Такое понимание компьютерной информации способствовало постоянной дискуссии, связанной с решением вопроса о том, что такое машинный носитель, ЭВМ, система ЭВМ и пр. Правоприменительная практика тоже не отличалась единообразием: «одни и те же устройства (контрольно-кассовые машины с электронной памятью) в одних случаях признавались ЭВМ, а в других – нет»[5].

---

[1] Федеральный закон РФ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 07 декабря 2011 г. № 420 – ФЗ // Российская газета. – 2011. – № 278.

[2] Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания. – Тамбов: Издательство ТГУ, 2003. – С. 52 – 53.

[3] Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. Ю.И. Скуратова, В.М. Лебедева. – М, 1996. – С. 412.

[4] Уголовное право. Особенная часть: Учебник / под ред. Н.И. Ветрова и Ю.И. Ляпунова. – М.: Новый Юрист, 1998. – С. 544.

[5] Ткачев А.В. Исследование компьютерной информации в криминалистике // Эксперт-

Примером признания контрольно-кассовой машины специализированной ЭВМ может служить уголовное дело в отношении Т. и К. по обвинению в уничтожении информации о финансовых операциях в памяти контрольно-кассовых аппаратов АМС 100-Ф[1].

Законодатель, по всей видимости, учел данный опыт и постарался исправить положение. Теперь понятие «компьютерная информация» закреплено в примечании 1 к ст. 272 УК РФ: под ней понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Таким образом, предмет преступления теперь понимается гораздо шире – это сведения в любом техническом средстве, способном обрабатывать их в форме электрических сигналов.

Согласно теории информации и связи, сигнал – это материальный носитель информации, используемый для передачи сообщений в системе связи. Сигналы генерируются, и если они принимаются, то становятся сообщениями. Любую систему передачи информации можно считать состоящей из трех частей: источника сообщений, канала связи и приемного устройства. Между отправителем сообщения и каналом связи могут находиться устройства, преобразующие сообщение в форму, удобную для передачи по каналу связи.

По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими, оптическими и т. д. Вся информация, обрабатываемая компьютером, должна быть представлена двоичным кодом с помощью цифр 0 и 1. В связи с этим в ЭВМ организовано два процесса: кодирование (преобразование входной информации в форму, воспринимаемую компьютером, т. е. двоичный код) и декодирование (преобразование данных из двоичного кода в форму, понятную человеку). В вычислительных машинах коды нуля и единицы представляются

криминалист. – 2012. – № 4. – С. 7.

[1] Сало И.А. Указ. соч. – С. 76.

электрическими сигналами.

Вполне вероятно, что именно этим и руководствовался законодатель при включении термина «электрический сигнал» в понятие компьютерной информации. Теперь компьютерная информация не привязана лишь к машинному носителю, ЭВМ, системе ЭВМ или их сети. Таким образом, под защиту уголовного закона попала и та информация, которая еще не зафиксирована на каком-либо носителе или устройстве, а находится в процессе передачи.

Однако данное определение компьютерной информации имеет ряд недостатков. Во-первых, термин «компьютерная» определяет принадлежность только к компьютеру, что в условиях сегодняшнего технологического прогресса является некорректным, поскольку современные объекты обращения электронной информации (цифровая видеокамера, мобильный телефон, телевизор и т. д.) могут подключаться к Интернету и способны выполнять многие из тех функций, которые ранее было возможно осуществить только при помощи компьютера[1].

Во-вторых, помимо электрических сигналов, компьютерная информация может передаваться и иными способами: с помощью электромагнитных сигналов (Wi-Fi) или распространённого сегодня оптоволокна, информация по которому передаётся в виде световых сигналов. Такая информация не будет являться объектом уголовно-правовой охраны, т. к. она не подпадает под определение электрических сигналов при трактовке этого термина с точки зрения физики. В связи с этим использование такого термина, как «электрический сигнал», лишь вводит в заблуждение и поэтому нуждается в дальнейшем разъяснении или замене более подходящим термином.

Сходной позиции придерживается и Верховный Суд Российской Федерации, который отмечал, что «предложенный в примечании к ст. 272 УК РФ термин «электрический сигнал» не вносит достаточной ясности в

[1] Гостева М.Б. Преступления в сфере компьютерной информации: преимущества и недостатки новой редакции // Проблемы права. – 2012. – № 5 (36). – С. 180.

определение понятия и требует дополнительного пояснения»[1].

Данная позиция получила развитие в заключении Комитета Государственной Думы по информационной политике, информационным технологиям и связи от 05 июля 2011 г., где указывается, «что понятие компьютерной информации отсутствует в федеральных законах, а в предлагаемой дефиниции неясен смысл термина «электрические сигналы». Представляется необходимым уточнить данную формулировку.

Понятие компьютерной информации дается в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (от 1 июня 2001 г.). Согласно п. "б" ст. 1 названного Соглашения компьютерная информация – это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи»[2].

Предложения о заимствовании понятия компьютерной информации из этого Соглашения высказывались и ранее[3]. Ввиду недостаточной ясности термина «электрический сигнал», который используется в настоящее время в определении компьютерной информации в примечании к ст. 272 УК РФ, вышеназванное предложение о заимствовании этого определения из Соглашения вновь может стать предметом научной дискуссии.

В прежней редакции норм главы 28 УК РФ компьютерная информация, как уже отмечалось, находилась в неразрывной связи с машинным

---

[1] Официальный отзыв от 07 апреля 2011 г. № 1/общ-1583 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» // Доступ из СПС Консультант плюс

[2] Заключение Комитета Государственной Думы по информационной политике, информационным технологиям и связи от 05 июля 2011 г. «На проект Федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» (к первому чтению)» // Доступ из СПС Консультант плюс

[3] Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: автореферат дис. ... канд. юрид. наук. – М., 2005. – С. 8.

носителем, в электронно-вычислительной машиной (ЭВМ), системой ЭВМ или их сетью и именно поэтому она получила такое название. До изменений УК РФ в 2011 г. именно понятие «компьютер» или «ЭВМ» являлось базовым для определения других понятий. При этом само понятие «ЭВМ» учеными определялось по-разному: «электронное устройство, производящее заданные управляющей программой операции по хранению и обработке информации и управлению периферийными устройствами»[1]; «совокупность аппаратно-технических средств и средств программирования, позволяющая производить операции над символьной и образной информацией»[2].

Высказывалось мнение и о том, что крайне важно дать легальное определение понятия «ЭВМ» (компьютера), которое, как и каждое определение, в перспективе может уточняться.

При этом в основе определения нельзя использовать ни размеры, ни какие-либо внешние признаки, ни описание набора необходимых компонентов или решаемых задач: «эти подходы себя исчерпали, поскольку компьютеры непрерывно совершенствуются как по внешнему виду, так и по своим функциональным задачам»[3].

Так, например, «в УК штата Аризона компьютер означает электронное устройство, которое осуществляет логическую, арифметическую или запоминающую функцию посредством манипулирования электронными или магнитными импульсами и включает в себя все средства ввода, вывода, обработки, хранения компьютерных данных, компьютерного программного обеспечения или все средства связи, которые подключаются к такому устройству и соотносятся с таким устройством в системе или сети»[4].

---

[1] Гаврилин Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание / Книжный мир. – М. – 2003. – С. 18.

[2]Ушаков С.Ю. Преступления в сфере компьютерной информации (теория, законодательство, практика): дис. ... канд. юрид. наук. – Ростов н/Д, 2000. – С. 51.

[3]Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. канд. ... юрид. наук. – Ижевск, 2002. – С. 70.

[4] Казаков С.Э. Компьютерные преступления в законодательстве США и Канады: учебное пособие. – Нижний Новгород: Право, 2003. – С. 44.

Однако, как мы видим, законодатель пошел по иному пути, что представляется нам верным, так как термин «компьютер» является техническим. Использование технических терминов в Особенной части УК РФ может привести правоприменителя к затруднениям. В переводе с английского «computer» означает вычислитель. Первоначально в английском языке это слово обозначало человека, производящего арифметические вычисления. Затем этот термин стал использоваться для обозначения автоматических устройств для проведения вычислений, сбора, хранения и передачи информации. Усовершенствование и появление новой техники, которая используется для передачи, хранения и обработки информации – процесс динамичный.

В настоящее время компьютерная информация может обращаться и в таких устройствах, которые собственно компьютерами и не являются, но имеют некоторые схожие с ними свойства либо сам компьютер руководит работой такого устройства[1].

Правоприменительная практика пошла по такому пути, когда компьютерами стали признаваться мобильные телефоны, игровые приставки, игровые автоматы и даже банкоматы. В наши дни мобильный телефон является многофункциональным устройством: он оборудован микропроцессором, имеет как оперативную, так и постоянную память, с его помощью можно получить доступ в Интернет, получать и отправлять почту, принимать телевизионные сигналы и многое другое.

Например, «С. используя принадлежащий ему мобильный телефон «Нокиа», а также активную СИМ-карту подключенную к сети оператора мобильной связи «Билайн», действуя умышленно, из корыстных побуждений, воспользовался услугой «Мобильный банк», которая была подключена к указанному номеру, находившемуся ранее в пользовании гражданина П. при оформлении им банковской карты ОАО «Сбербанка

[1] Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. – 2012. – № 7. – С. 52.

России» для проведения комплекса операций, осуществляемых посредством мобильной связи». «Имея преступный умысел, направленный на незаконное копирование информации, представленной в виде электрического сигнала, в систему информационной сети ЭВМ ОАО «Сбербанка России», с последующей модификацией информации о состоянии счета, предоставленной услугой «Мобильный банк», что согласно ст. 26 Федерального закона № 395-1 от 02 декабря 1990 г. «О банках и банковской деятельности», а также Закона «Об информации» является охраняемой законом компьютерной информацией, осуществил тем самым неправомерный доступ к компьютерной информации, позволяющей распоряжаться денежными средствами, находящимися на лицевом счете банковской карты ОАО «Сбербанка России», оформленной на имя П.»[1].

В другом примере «Б., осознавая, что правообладателем оригинальной игровой приставки Microsoft Xbox 360 является корпорация Microsoft, используя специальные познания, внес несанкционированные производителем изменения в программное обеспечение игровой приставки посредством специализированного программного обеспечения «JangleFlasher» и персонального компьютера, с целью получения возможности использования на данной приставке нелицензионных игровых приложений, а именно нейтрализовал программно-технические средства защиты информации, примененные производителем для защиты от использования нелицензионных копий программных продуктов, тем самым блокировал, модифицировал и уничтожил средства защиты информации и нарушил штатную работу игровой приставки. Таким образом, Б. совершил неправомерный доступ к охраняемой законом компьютерной информации, который повлек уничтожение, блокирование и модификацию информации»[2].

[1] Дело № 1-213/2012 … из архива Белгородского районного суда Белгородской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://belgorodsky.blg.sudrf.ru/

[2] Дело № 1-642/2012 … из архива Калужского районного суда Калужской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://kaluga.klg.sudrf.ru/

Представляется, что такое широкое понимание компьютера не соответствует существующим законодательным формулировкам. Но, с другой стороны, эти устройства также используются при совершении преступлений, предусмотренных главой 28 УК РФ. Они выступают предметом или средством совершения указанных преступлений, однако в настоящее время выпадают за пределы действия ст.ст. 272 – 274 УК РФ. Еще и поэтому использование термина «компьютерная» выглядит не совсем логичным и корректным. В связи с изложенным полагаем, что понятие «компьютерная информация» целесообразно заменить на более широкое понятие «электронная информация».

Учитывая сказанное, а также недостаточную ясность термина «электрический сигнал», представляется возможным изложить примечание к ст. 272 УК РФ в следующем виде: «Под электронной информацией понимаются сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи».

Для квалификации незаконного доступа к информации по ст. 272 УК РФ необходимо также установить, что данная информация была охраняемой законом.

Вопрос о содержании указанного признака также является дискуссионным. По мнению одних авторов, «неохраняемой информации не бывает вообще, и поэтому указание в законе на этот признак представляется излишним»[1].

Другие авторы полагают, что «охраняемая законом компьютерная информация должна обязательно находиться в чьей-либо интеллектуальной собственности»[2]. По мнению третьих авторов, «информация является

[1] Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. – № 10. – С. 24 – 25.

[2] Айсанов Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореферат дис. ... канд. юрид. наук. – М., 2006. – С. 15.

охраняемой только в том случае, если это непосредственно установлено каким-либо нормативным актом»[1] (например, «О государственной тайне). И, наконец, четвертые авторы считают, что «охраняемая информация должна быть ограничена в доступе»[2].

В соответствии со ст. 5 Закона «Об информации» информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

В п. 4 ст. 8 названного Закона установлен перечень сведений, доступ к которым не может быть ограничен:

1) нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информация о состоянии окружающей среды;

3) информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информация, накапливаемая в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

---

[1] Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 44 – 45; Комментарий к Уголовному кодексу РФ / отв. ред. В.М. Лебедев. 2-е изд., доп. и испр. – М., 2003. – С. 579.

[2] Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореферат дис. ... канд. юрид. наук. – М., 2007. – С. 18.

Сведения ограниченного доступа, согласно Закону, подлежат защите, а степень защиты определяет их обладатель. Ответственность за выполнение мер по защите информации возлагается именно на обладателя информации.

Информация с ограниченным доступом, в свою очередь, подразделяется на сведения, составляющие государственную тайну, и конфиденциальную информацию (ст. 9 Закона).

Так, ст. 2 Закона устанавливает, что конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Конфиденциальной является информация, доступ к которой ограничивается также в соответствии с законодательством. Ст. 16 Закона устанавливает, что «защита информации представляет собой принятие правовых, организационных и технических мер, направленных на соблюдение конфиденциальности информации ограниченного доступа».

Указом Президента Российской Федерации от 6 марта 1997 г. № 188[1] утвержден Перечень сведений конфиденциального характера, в котором частично упорядочен состав конфиденциальной информации. В названный перечень входят:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к

[1] Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06 марта 1997 г. № 188 // Российская газета. – 1997. – № 51.

которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК Российской Федерации и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

Таким образом, можно сделать вывод о том, что доступ к информации может быть ограничен не только посредством соответствующего указания в федеральных законах, но и путем установления обладателем информации специального режима ее получения и использования.

В связи с этим, предметом незаконного доступа к компьютерной информации является электронная информация, ограниченная в обороте законом либо обладателем данной информации на основании предоставленных ему прав. Под электронной информацией следует понимать сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи.

1.2 Объективная сторона неправомерного доступа к компьютерной информации

Согласно диспозиции ст. 272 УК РФ, объективная сторона неправомерного доступа к компьютерной информации, включает в себя три обязательных признака: общественно опасное деяние в виде неправомерного доступа к охраняемой законом компьютерной информации; общественно опасные последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации; причинную связь между

совершенным деянием и наступившими последствиями.

Несмотря на отсутствие уточнения в диспозиции, полагаем, что общественно опасное деяние, связанное с неправомерным доступом к охраняемой законом компьютерной информации, может быть выполнено только в активной форме (действии). Бездействие лица, даже если оно повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, состава данного преступления не образует. Оно может влечь уголовную ответственность, например, за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Само понятие «доступ» в УК РФ не раскрывается. Легальное определение доступа к информации закреплено в ст. 2 Закона «Об информации» – это возможность получения информации и ее использование.

В специальной технической литературе под доступом понимают:

1) процедуру установления связи с запоминающим устройством и размещенными на нем файлами (или отдельным файлом) для записи или чтения данных;

2) процедуры считывания и записи данных. При этом, как правило, подразумеваются разрешенные типы доступа к устройствам памяти определенной системы, например, «только для считывания» или для «считывания и записи»;

3) в вычислительных сетях: «процедуру установления связи со средой передачи данных и терминалами сети для реализации предоставляемых ею услуг или функций обслуживания»[1].

В юридической литературе также существует несколько точек зрения на данное определение. Под доступом к компьютерной информации понимается:

[1] Сало, И.А. Указ. соч. – С. 90.

– «ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации, совершенное путем использования программно-технических средств ЭВМ»[1];

– «любая форма проникновения в источник информации с использованием ЭВМ, позволяющая производить манипуляции с полученной компьютерной информацией, то есть получение виновным возможности распоряжаться этой информацией (копировать, модифицировать, блокировать либо уничтожать ее)»[2];

– «санкционированное и упорядоченное собственником (владельцем) информационной системы взаимодействие лица с устройствами ЭВМ»[3].

Необходимым условием уголовной ответственности за доступ к компьютерной информации является его неправомерность, однако и это понятие в УК РФ в настоящее время не определено, что, естественно, порождает дискуссию среди ученых. Неправомерный доступ они рассматривают как:

1) «несанкционированное (неразрешенное) полномочным лицом ознакомление конкретного лица со сведениями, содержащимися на машинных носителях или в ЭВМ»[4];

2) «способы получения либо просмотра информации, которые совершаются в обход установленного порядка обращения с охраняемой информацией, а также вопреки воле собственника или законного владельца»[5];

---

[1] Комментарий к Уголовному кодексу РФ / под ред. В.И. Радченко, А.С. Михлина. – СПб.: Питер, 2007. – С. 564.

[2] Абов А.И., Велиев Э.Э., Ткаченко С.Н. Экономическая безопасность и компьютерные преступления. – М.: «Прима-Пресс», 2003. – С. 13; Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. – 2002. – № 9. – С. 38; Ястребов Д.А. Указ. соч. – С. 19 – 20.

[3] Крылов В.В. Указ. соч. – С. 40.

[4] Кузнецов А.П. Ответственность за преступления в сфере компьютерной информации: учеб.-практ. пособие. – Нижний Новгород: Нижегородская правовая академия, 2007. – С. 32.

[5] Борзенкова Г.Н. Курс уголовного права. Особенная часть. Том 4. Учебник для ВУЗов / –

3) «незаконное получение возможности сбора, обработки, накопления, хранения, поиска и распространения информации, на которую у лица нет ни действительного, ни предполагаемого права»[1];

4) «несанкционированное собственником информации ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ, то есть нарушение установленного и зафиксированного собственником информации порядка»[2];

5) «совершение доступа без согласия собственника этой информации либо иного лица, обладающего ею по закону»[3];

6) «доступ, противоречащий действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации»[4];

7) «несанкционированное собственником или владельцем информации ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ, и имеющих уровень защиты в соответствии с законодательством РФ»[5];

8) «доступ в закрытую информационную систему лица, не являющегося законным пользователем либо не имеющего разрешения для работы с данной информацией[6]»;

9) «доступ к защищенной компьютерной информации лица, не обладающего правами на получение и работу с данной информацией, либо

М., 2002. – С. 646.

[1] Пособие для следователя. Расследование преступлений повышенной опасности / под ред. Н.А. Селиванова и А.И. Дворкина. – М., 1998. – С. 339.

[2] Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания. – Тамбов: Издательство ТГУ, 2003. – С. 73.

[3] Уголовный кодекс РФ: Постатейный комментарий. – М., 1997. – С. 582.

[4] Гульбин Ю. Указ. соч. – С. 24.

[5] Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // Красноярск, 2002. – С. 68.

[6] Уголовное право. Особенная часть: учебник для ВУЗов / отв. ред. И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов. – М: Издательская группа НОРМА-ИНФРА-М, 1998. – С. 557.

компьютерной системой»[1];

10) «способ проникновения к компьютерной информации, который применяется в обход легально установленного порядка обращения к ней, а также без официального разрешения со стороны собственника этой информации или его законного представителя на такой доступ»[2].

Как мы видим, несмотря на разнообразие приведенных позиций, большинство ученых связывает неправомерность доступа, во-первых, с отсутствием у субъекта разрешения со стороны обладателя информации (юридический аспект), во-вторых, с преодолением установленной системы защиты информации (технический аспект).

Например, «Нестеров, имея умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, хранящейся в электронном почтовом ящике, с целью неправомерного просмотра личной информации пользователя А., заведомо зная, что к сведениям о логине, исходном коде и пароле отсутствует свободный доступ, без разрешения владельца А. внес сведения о них на электронный сайт, что повлекло копирование информации»[3].

Таким образом, неправомерным признается доступ к компьютерной информации лица, не обладающего правами на обращение к данной информации, в отношении которой приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

Несмотря на то, что ст. 272 называется «Неправомерный доступ к компьютерной информации», ответственность наступает не за сам факт совершения доступа, а лишь только, если этот доступ повлек указанные в диспозиции последствия. В связи с этим М.А. Зубова и У.В. Зинина

---

[1] Наумов В.Б. Отечественное законодательство в борьбе с компьютерными преступлениями / [Электронный ресурс]. – Режим доступа: http://www.russianlaw.net/law/computer_crime/a01.

[2] Айсанов Р.М. Указ. соч. – С. 16.

[3] Дело № 1-351/2011 … из архива Миасского городского суда Челябинской области за 2011 г. [Электронный ресурс]. – Режим доступа: http://miass.chel.sudrf.ru.

предлагают изменить конструкцию рассматриваемого состава преступления таким образом, чтобы он стал формальным: «установить уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации»[1].

Полагаем, что с данным предложением трудно согласиться, т. к. неправомерный доступ к компьютерной информации, не приведший к копированию, блокированию, модификации или уничтожению информации, на наш взгляд, не обладает достаточной общественной опасностью, чтобы признавать его преступлением.

Так как при описании состава законодатель использовал конструкцию «если это деяние повлекло», состав неправомерного доступа к компьютерной информации является материальным. В качестве последствий в диспозиции ч. 1 ст. 272 УК РФ названы: уничтожение, блокирование, модификация либо копирование информации.

В связи с тем, что названные термины могут означать не только процесс, но результат преступных действий, С.А. Буз и С.Г. Спирина предположили, «перечисленные в ч. 1 ст. 272 УК РФ последствия представляют собой не конечный результат преступных действий (причиненный вред), а самостоятельные действия, и предложили эти действия (операции, производимые с применением информации) предусмотреть в уголовном законе в качестве самостоятельных составов преступления»[2].

Наибольшее распространение получило мнение о том, что «для наступления уголовной ответственности неправомерный доступ к охраняемой законом компьютерной информации должен повлечь одно из указанных в диспозиции последствий»[3].

---

[1] Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: автореферат дис. ... канд. юрид. наук. – Казань, 2008. – С. 13; Зинина У.В. Указ. соч. – С. 72.

[2] Буз С.А. Указ. соч. – С. 47.

[3] Кудрявцев В.Н. Уголовное право. Особенная часть: учебник / 2-е изд. – М., 2000. – С. 350.

В настоящий момент правовые определения понятий «уничтожение», «блокирование», «модификация» и «копирование» встречаются в различных нормативных РФ, и их содержание не всегда носит тождественный характер.

Нет единства в толковании признака «уничтожение информации» и в юридической литературе, под ним понимают:

1) «удаление с физических носителей»[1];

2) «несанкционированное изменение составляющих ее данных, кардинально меняющее ее содержание (например, внесение ложной информации, добавление, изменение, удаление записей)»[2];

3) «утрату информации при невозможности ее восстановления»[3];

4) «стирание информации в памяти ЭВМ»[4];

5) «приведение информации либо полностью, либо в существенной части в непригодное для использования по назначению состояние»[5];

6) «полную физическую ликвидацию информации или ликвидацию таких ее элементов, которые влияют на изменение существенных идентифицирующих информацию признаков»[6].

Специалисты отмечают, что «все методы уничтожения информации в зависимости от способа воздействия на носитель можно разделить на программные и аппаратные (посредством механического, теплового или иного воздействия, например с помощью электромагнитного импульса)»[7].

---

[1] Андреев Б.В. Расследование преступлений в сфере компьютерной информации // Юрлитинформ, – М. – 2001. – С. 38.

[2] Научно-практический комментарий к Уголовному кодексу Российской Федерации в двух томах. Том 2. – Нижний Новгород: Изд. НОМОС, 1996. – С. 235.

[3] Комментарий к Уголовному кодексу РФ / отв. ред. А.В. Наумов. – М .: Юристъ, 1997. – С. 664.

[4] Комментарий к Уголовному кодексу Российской Федерации / под ред. Ю. И. Скуратова и В. М. Лебедева. – М.: ИНФРА-М-НОРМА, 2001. – С. 699.

[5] Уголовный кодекс Российской Федерации: постатейный комментарий. – М.: ЗЕРЦАЛО, ТЕИС, 1997. – С. 583.

[6] Крылов В.В. Информационные компьютерные преступления // ИНФРА-М-НОРМА. – М.: – 1997. – С. 47.

[7] Демидов А.А. Сравнительный анализ известных методов уничтожения информации с энергонезависимых носителей. [Электронный ресурс]. – Режим доступа: http://www.ci.ru/inform03_07/bezop.htm.

Необратимое уничтожение хранящейся на носителе информации может быть вызвано его физическим повреждением. Однако, по нашему мнению, такое уничтожение информации не образует объективную сторону исследуемого преступления, так как в этом случае неправомерный доступ к компьютерной информации отсутствует. Поэтому из двух названных специалистами методов к составу преступления, предусмотренному ст. 272 УК РФ, имеет отношение только программный метод. Это наиболее простая и часто применяемая форма уничтожения информации, основанная на использовании операций удаления и перезаписи с помощью компьютерных программ, не требующая дополнительных аппаратных устройств.

В то же время при таком методе уничтожения, по мнению М.В. Богомолова, говорить о полной физической ликвидации информации чаще всего некорректно, поскольку операционные системы обычно не удаляют информацию, а лишь изменяют имя файла и переносят в скрытый список. И только по прошествии времени, если информация осталась невостребованной, она действительно уничтожается, а на ее место записывается другая информация. Даже при форматировании машинного носителя информация не уничтожается полностью, ее можно восстановить с помощью специализированных утилит. Таким образом, считает автор, «пользователь при удалении информации, считает ее удаленной и не имеет возможности ее использовать, однако специалист может восстановить информацию, часто без искажения»[1].

Поэтому в литературе высказывается мнение о том, что «необходимо разграничивать понятия «уничтожение» и «удаление/стирание» информации – при уничтожении восстановление информации невозможно, а при стирании имеются возможности для восстановления таковой при помощи специальных программ»[2].

---

[1] Богомолов М.В. Указ. соч. – С. 82.

[2] Комментарий к Уголовному кодексу РФ / под ред. В.И. Радченко, А.С. Михлина. – СПб.: Питер, 2007. – С. 566.

Например, «Центральный районный суд г. Челябинска усмотрел уничтожение компьютерной информации в действиях Ивасько, который, являясь заместителем начальника отдела технического обслуживания ООО, в связи со служебной необходимостью получил доступ к имени пользователя и паролю почтового сервера ООО». «В связи со сложившимися неприязненными отношениями с руководством фирмы, Ивасько уволился из ООО, после чего, используя имя пользователя и пароль почтового сервера ООО, в нарушение ст. 16 Закона «Об информации», умышленно, не имея права доступа к охраняемой законом информации, используя принадлежащую ему электронно-вычислительную машину, через открытую телекоммуникационную сеть «Интернет», осуществил неправомерный доступ к охраняемой законом информации, а именно к адресам электронной почты ООО». «Затем Ивасько, умышлено, введя команду …, из чувства мести за увольнение из ООО, удалил компьютерную информацию – адреса электронной почты ООО»[1].

Легальное определение уничтожения информации, применительно к персональным данным, дано в п. 7 ст. 3 Федерального закона «О персональных данных»: «уничтожение персональных данных – это действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных»[2].

Таким образом, возможность восстановления данных исключает их уничтожение.

В связи с этим полагаем, что под уничтожением информации в ст. 272 УК РФ, законодатель все-таки имел в виду не просто удаление, а разрушение информации, в результате чего происходит ее утрата.

---

[1] Дело № 1-356/2010 … из архива Центрального районного суда г. Челябинска за 2010 г. [Электронный ресурс]. – Режим доступа: http://centr.chel.sudrf.ru/

[2] Федеральный закон РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // Российская газета. – 2006. – № 165.

Таким образом, уничтожение информации – это утрата информации без возможности ее восстановления, когда законный обладатель информации не может использовать ее по назначению.

Если лицо намеревалось удалить информацию, но она была восстановлена потерпевшим, его действия по неправомерному доступу к компьютерной информации следует квалифицировать как покушение на уничтожение.

Неоднозначно подходят ученые и к определению следующего последствия, указанного в диспозиции рассматриваемой нормы – блокирование информации. Под блокированием компьютерной информации понимают:

1) «невозможность ее использования при сохранности такой информации»[1];

2) «искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением»[2].

3) «создание условий (в том числе и с помощью специальных программ), исключающих использование компьютерной информацией ее законным владельцем»[3].

Иногда выделяют аппаратную или программную блокировку ЭВМ, что влечет невозможность использования информации[4].

Следует согласиться с И.С. Сало, по мнению которой, «блокирование информации должно характеризоваться двумя признаками: а) она становится недоступной для получения и использования по прямому назначению, б) она не подвергается уничтожению, то есть при условии полной сохранности

---

[1] Комментарий к Уголовному кодексу РФ / отв. ред. А.В. Наумов. – М .: Юристъ, 1997. – С. 664.

[2] Комментарий к Уголовному кодексу Российской Федерации / под ред. Ю. И. Скуратова и В. М. Лебедева. – М.: ИНФРА-М-НОРМА, 2001. – С. 698.

[3] Научно-практический комментарий к Уголовному кодексу Российской Федерации в двух томах. Том 2. – Нижний Новгород: Изд. НОМОС, 1996. – С. 236.

[4] Крылов В.В. Информационные компьютерные преступления // ИНФРА-М-НОРМА. – М.: 1997. – С. 51.

такой информации ее законный обладатель не может ей воспользоваться»[1].

Например, «Зубков, используя свой личный ноутбук, заведомо зная о порядке и правилах осуществления выхода во внутреннюю сеть и в сеть Интернет и об отсутствии у него права на доступ к учетно-регистрационным данным других пользователей Интернет, обладая достаточными знаниями в области информационных технологий, навыками пользования компьютерной техникой, опытом работы в сети Интернет и во внутренней сети провайдера, посягая на права собственника информационных ресурсов на нормальное функционирование и безопасность его информационной системы, умышленно изменяя IP-адрес, присвоенный его ноутбуку ЗАО «Озерск Телеком» на IP-адреса, присвоенные другим пользователям, осуществлял неправомерный доступ к охраняемой законом компьютерной информации, находящейся на машинном носителе в сети ЭВМ провайдера ЗАО «Озерск Телеком». Действия Зубкова привели к блокированию информации, выразившемуся в невозможности доступа правомерным пользователям к внутренним ресурсам ЗАО «Озерск Телеком» и невозможности получения информации из сети Интернет»[2].

Таким образом, под блокированием компьютерной информации понимается временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией при ее сохранности.

Исходя из смысла закона, длительность блокирования информации значения для квалификации не имеет. Однако полагаем, что в случае непродолжительного ограничения доступа пользователя к компьютерной информации (например, в течение несколько минут), если это не причинило существенного вреда пользователю, деяние можно признать малозначительным на основании ч. 2 ст. 14 УК РФ.

Что касается модификации информации, то определение данного понятия

---

[1] Сало И.А. Указ. соч. – С. 107.

[2] Дело № 1- 77/2011 … из архива Озерского городского суда Челябинской области за 2011 г. [Электронный ресурс]. – Режим доступа: http://ozersk.chel.sudrf.ru.

осложнено тем, что этот же термин используется законодателем и в ГК РФ в отношении программ для ЭВМ как объектов авторского права, и в главе 28 УК РФ применительно к компьютерной информации.

Согласно ч. 9 ст. 1270 ГК РФ под переработкой (модификацией) программы для ЭВМ или базы данных понимаются любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой язык, за исключением адаптации, то есть внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Полагаем, что использовать данное понятие применительно к модификации компьютерной информации нецелесообразно. В юридической литературе под модификацией компьютерной информации понимают:

1) «любые изменения компьютерной информации»[1];

2) «изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя»[2];

3) «такое вмешательство, переработка или иное действие по отношению к информации, которые могут заключаться в несанкционированном ее изменении»[3].

По мнению В.М. Быкова и В.Н. Черкасова, «от несанкционированной модификации компьютерной информации следует отличать внесение таких изменений, которые направлены исключительно на адаптацию информации, т.е. на приспособление этой информации к функционированию с

---

[1] Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 44 – 45; Комментарий к Уголовному кодексу РФ (постатейный) / отв. ред. Л.Л. Кругликов. – М., 2005. – С. 831.

[2] Комментарий к Уголовному кодексу Российской Федерации / отв. ред. А.В. Наумов. – М.: Юрист, 1996. – С. 664.

[3] Королев А.Н., Плешакова О.В. Комментарий к ФЗ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» (постатейный). – М.: ЗАО Юстицинформ, 2007. – С. 106.

использованием конкретных технических средств пользователя»[1].

Гражданским законодательством РФ разрешены следующие виды легальной модификации программ, баз данных лицами, правомерно владеющими этой информацией:

а) исправление явных ошибок;

б) внесение изменений в программы, базы данных для их функционирования на технических средствах пользователя;

в) частичная декомпиляция программы для достижения способности к взаимодействию с другими программами при соблюдении следующих условий:

1) информация, необходимая для достижения способности к взаимодействию, которая ранее не была доступна этому лицу из других источников;

2) указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

3) информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

Модификация будет признаваться незаконной, если информация изменяется без необходимости, что, в свою очередь, затруднит возможность

[1] Быков В.М. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. – 2012. – № 5. – С. 16.

ее применения обладателем информации.

Например, «Нестеров осуществил неправомерный доступ к охраняемой законом компьютерной информации, а именно к электронным сообщениям, переданным и полученным А., хранившимся в электронном почтовом ящике, блокировав доступ к указанному ящику законного владельца и пользователя, а также модифицировал информацию, изменив при этом пароль доступа, регистрационные данные, ответ на секретный вопрос к электронному почтовому ящику законного владельца»[1].

При квалификации данного преступления может возникнуть вопрос о наличии в действиях виновного признаков модификации в том случае, если в результате незаконного доступа им были произведены несущественные для обладателя изменения информации (например, изменен формат текста или он переведен на другой язык и т. д.). Полагаем, что, если эти действия не изменили содержание документа и не создали препятствий для его использования по назначению, состав преступления, предусмотренного ст. 272 УК РФ, отсутствует.

Таким образом, модификация компьютерной информации представляет собой любое изменение ее первоначального состояния, осуществляемое без разрешения законного обладателя информации и ущемляющее его интересы.

В качестве последнего последствия незаконного доступа к компьютерной информации в диспозиции ст. 272 УК РФ названо ее копирование.

С технической точки зрения копирование представляет собой перенос информации или ее части с одного физического носителя на другой. В уголовно-правовой литературе данное понятие авторы наделяют различным содержанием: «при копировании повторение информации является несанкционированным»[2], «то есть вопреки либо помимо воли обладателя

[1] Дело № 1-351/2011 … из архива Миасского городского суда Челябинской области за 2011 г. [Электронный ресурс]. – Режим доступа: http://miass.chel.sudrf.ru/

[2] Борчева Н.А. Компьютерные преступления в России (комментарии к Уголовному кодексу РФ). – М.: «Прима-Пресс», 2001. – С. 8.

информации; с сохранением оригинала информации»[1], когда возможно ее дальнейшее использование по назначению.

Некоторые авторы отождествляют копирование информации с ее «распространением и разглашением»[2]. По мнению других, «копирование информации имеет место при ее воспроизведении в любой материальной форме, даже при переписывании с дисплея»[3]; «при перенесении информации на любой другой носитель в электронном виде (в память другого компьютера, на внешний накопитель компьютерной информации, иные электронные устройства), создание печатной версии (с помощью принтера), а равно размещение в электронных каналах связи (например, в Интернете)»[4]. «То есть неправомерное изготовление копий содержания соответствующей информации в любой материальной форме»[5].

Поскольку в диспозиции рассматриваемой нормы способы копирования не конкретизируются, то высказывается мнение о том, что «копирование компьютерной информации – это воспроизведение информации в любой материальной форме», и такие способы копирования как фотографирование информации с экрана монитора, распечатка и пр. должны влечь ответственность по ст. 272 УК РФ[6].

Однако в данном случае, как правильно заметил С.Ю. Бытко, «широкое толкование неоправданно увеличивает сферу действия преступлений,

---

[1] Уголовный кодекс РФ. Постатейный комментарий. – М, 1997. – С. 583; Российское уголовное право. Особенная часть / под ред. В.Н. Кудрявцева, А.В. Наумова. – М.: Юристъ, 1997. – С. 349.

[2] Кочои С. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 44 – 45.

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.В. Бриллиантова. – М.: Проспект, 2010. – С. 1040.

[4] Комментарии к УК РФ / отв. ред. В.И. Радченко, науч. ред. А.С. Михлин. – М.: ТК Велби, Издательство Проспект, 2008. – С. 515.

[5] Ивановский П.С. Уголовно-правовая борьба с компьютерными преступлениями. – М.: ПОЛТЕКС, 2007 – с. 17; Наумов А.В. Российское уголовное право. Курс лекций: в 3 т. Т. 3. Особенная часть (главы XI—XXI) / – М.: Волтерс Клувер, 2007. – С. 283 и др.

[6] Ястребов Д.А. Указ. соч. – С. 74 – 79.

предусмотренных главой 28 УК РФ»[1]. Поэтому следует согласиться с узким пониманием копирования информации как «изготовления копии объекта информации, то есть копии файла, информации, представленной в электронном виде»[2].

Например, «Горбачев, незаконно приобрел путем скачивания на компьютер из сети «Интернет» и последующей записи на внешний жесткий магнитный диск и оптический носитель, нелицензионные версии программных продуктов «Microsoft Windows XP Professional Edition» и «Microsoft Office 2010 Professional Plus», правообладателем которых является корпорация «Microsoft». После этого он, действуя умышленно, из корыстной заинтересованности подключил внешний жесткий магнитный диск к ноутбуку «Lenovo» и загрузил в него оптический носитель, содержащий ранее незаконно приобретенные им нелицензионные версии программных продуктов, после чего произвел копирование с указанных носителей на жесткий диск ноутбука указанных нелицензионных версий программных продуктов»[3].

Уголовно-наказуемое копирование информации следует отличать от действий, не связанных с волеизъявлением лица, осуществляющего неправомерный доступ. По нашему мнению, не может быть признано копированием сохранение на ЭВМ пользователя информации в виде cache, cookie и других технических данных. Сохранение подобной служебной информации не находится в прямой причинной связи с волеизъявлением пользователя (его командами), а является неотъемлемой частью функционирования используемого им программного обеспечения.

---

[1] Бытко С.Ю. Преступления в сфере компьютерной информации: учеб. пособие для студентов юрид. специальностей. – Саратов: изд-во Сарат. гос. ун-та, 2004. – С. 31.

[2] Комментарий к Уголовному кодексу РФ / под ред. В.И. Радченко, А.С. Михлина. – СПб.: Питер, 2008. – С. 567.

[3] Дело № 1- 100/2012 ... из архива Егорьевского городского суда Московской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://egorievsk.mo.sudrf.ru.

С данным утверждением категорически не согласен В.В. Крылов[1].

Однако солидарен с нами Д.А. Ястребов[2], который также указывает на отсутствие в данном случае состава преступления, ссылаясь на ст. 13 Директивы ЕС «Об электронной коммерции» 2000/31/ЕС, содержащей положение о том, что лицо должно быть освобождено от уголовной ответственности за осуществление копирования, если оно делается автоматически, имеет «промежуточный» или временный характер, и его единственной целью является обеспечение более эффективной обработки информации.

Ответственность за ознакомление с информацией в диспозиции ст. 272 УК РФ прямо не предусмотрена, что некоторыми авторами расценивается как «пробел в уголовном законодательстве»[3], восполнить который предлагается путем квалификации таких действий как «копирование информации»[4].

Полагаем, что данное суждение является ошибочным и противоречащим логике уголовного закона. В подобных ситуациях ответственность может наступать за иные информационные преступления (например, нарушение неприкосновенности частной жизни, незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну и т. д.).

Таким образом, копирование компьютерной информации – это повторение информации в электронном виде при сохранении ее неизменности.

---

[1] Крылов В.В. Основы криминалистической теории расследования преступлений в сфере информации: дис. ...докт. юрид. наук. – М., 1998. – С. 103.

[2] Ястребов Д.А. Неправомерный доступ *к* компьютерной информации: вопросы последствий // Проблемы управления безопасностью сложных систем. Труды XIV Международной конференции. В 2-х т. Т. 1. – М.: ИЦ РГГУ, 2006. – С. 74 – 79.

[3] Гостева М.Б. Указ. соч. – С. 181; Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. – М.: Норма,2004. – С. 213.

[4] Быков В.М. Указ. соч. – С. 16.

Изменениями, внесенными в ст. 272 УК РФ Федеральным законом от 07 декабря 2011 г. № 420 – ФЗ[1], из объективной стороны состава исключено такое последствие, как «нарушение работы ЭВМ, системы ЭВМ или их сети», что, по мнению М.Б. Гостевой, «является необоснованным, поскольку неоправданно исключает из действия уголовного закона большой объем неправомерных действий»[2].

В подтверждение своей позиции автор приводит пример незаконного использования чужих логинов и паролей для соединения с глобальной компьютерной сетью Интернет. Данное действие обычно приводит к блокированию и нарушению работы сети ЭВМ, выразившемуся в невозможности собственника логина и пароля выходить в Интернет во время использования этих же данных доступа преступником.

До последних изменений подобные посягательства на компьютерную информацию, получившие значительное распространение, успешно квалифицировались судом по ч. 1 ст. 272 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло нарушение работы сети ЭВМ. В соответствии же с действующей редакцией данной нормы такое поведение не является преступным, т. к. в результате неправомерного доступа происходит не блокирование информации, а временное блокирование доступа законного пользователя, поскольку сеть распознает его уже присутствующим.

Таким образом, значительная часть деяний, связанных с неправомерным доступом к компьютерной информации оказалась декриминализована.

Высказывается мнение, что по той же причине теперь невозможно привлечь к уголовной ответственности лиц, осуществляющих DDoS-атаки на

---

[1] Федеральный закон РФ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 07 декабря 2011 г. № 420 – ФЗ // Российская газета. – № 278. – № 278.

[2] Гостева М.Б. Указ. соч. – С. 180 – 181.

сайты, поскольку и в этом случае блокируется не компьютерная информация, а доступ к сайтам.

В то же время судебная практика доказывает обратное. Летом 2010 г. на сервер платежной системы «Ассист» была осуществлена DDoS-атака, из-за которой в течение недели невозможно было купить электронные билеты на сайте ее основного клиента – компании «Аэрофлот».

По данному делу П. Врублевский, И. Артимович, Д. Артимович признаны виновными в том, что совершили неправомерный доступ к охраняемой законом компьютерной информации, то есть информации в системе ЭВМ и их сети, повлекшей блокирование и нарушение работы системы ЭВМ и их сети, группой лиц по предварительному сговору (ч. 2 ст. 272 УК РФ в редакции ФЗ № 26 от 7 марта 2011 г.).

П. Врублевский, являясь генеральным директором ЗАО «Хронопэй», в начале июля 2010 г. с целью создания условий для разрыва деловых отношений, установленных между ОАО «Аэрофлот» и ООО «Ассист» по оказанию обществом услуг по продаже электронных авиабилетов ОАО «Аэрофлот», и устранения конкурента своей фирмы в данной сфере, принял решение дискредитировать ООО «Ассист» как надежную фирму. Для этого П. Врублевский, вступив с подчиненным ему ведущим специалистом службы информационной безопасности ЗАО «Хронопэй» М. Пермяковым, а также И. Артимовичем и Д. Артимовичем, занимавшимися оказанием «хакерских услуг», в предварительный сговор, и действуя согласно единого преступного плана и отведенных каждому участнику группы ролей, в период с 15 июля 2010 г. по 24 июля 2010 г., осуществили, имея в своем пользовании созданную Артимовичами с использованием вредоносных программ сеть зараженных компьютеров (бот-сеть), компьютерную DDoS-атаку (типа «отказ в обслуживании») на информационные ресурсы ООО «Ассист», которая заключалась в одномоментном обращении множества компьютеров, входящих в бот-сеть, с запросом на обслуживание. В результате

неправомерного доступа работы системы ЭВМ ООО «Ассист», объединенная в единую платежную сеть, была блокирована, в связи с чем, ее пользователям было отказано в возможности приобретения электронных билетов на сайте ОАО «Аэрофлот». Осуществление данной компьютерной атаки привело к блокированию работы системы оплаты и приобретения электронных билетов на сайте ОАО «Аэрофлот» на весь период атаки.

Летом 2013 г. в апелляционной жалобе осужденный П. Врублевский указал, что действия, за которые он осужден, в настоящее время преступлением не являются, поскольку такое последствие как блокирование работы системы ЭВМ и их сети (а не компьютерной информации) никогда уголовным законом не признавалось последствием, влекущим уголовную ответственность за неправомерный доступ к компьютерной информации, а такое последствие, как нарушение работы ЭВМ и их сети, тоже не упомянуто в действующем законе, то есть он осужден за действия, повлекшие последствия, не предусмотренные ныне действующей редакцией ст. 272 УК РФ.

Однако, по мнению суда апелляционной инстанции, новая редакция ст. 272 УК РФ, равно как и ее прежняя редакция, устанавливает, что объектом преступления являются общественные отношения, связанные с использованием компьютерной информации.

В прежней редакции ч. 1 ст. 272 УК РФ указывалось, что компьютерная информация – это информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, в новой редакции же редакции законодатель отказался от того, чтобы конкретно указывать и перечислять все технические средства, на которых может находиться охраняемая законом компьютерная информация, при этом объективная сторона состава преступления, предусмотренного ст. 272 УК РФ в новой редакции, как и в прежней редакции, заключается в неправомерном доступе лица к охраняемой законом компьютерной информации, если это деяние

повлекло за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации, что не декриминализует действия осужденных.

В соответствии с требованиями ст. 2 Закона «Об информации» доступ к информации понимается как возможность ее получения и использования. Поскольку в результате проведенной осужденными DDos-атаки, повлекшей блокирование (то есть невозможность законного доступа к сведениям при их сохранности) работы системы ЭВМ ООО «Ассист», осужденными была получена возможность неправомерного, несанкционированного доступа к защищенной законом компьютерной информации ООО «Ассист», нормальный ход работы ООО «Ассист» был нарушен, а система ЭВМ блокирована, то есть, блокированы информационные ресурсы и система ЭВМ, объединенные в единую платежную систему. Поэтому судом совершенное деяние правильно квалифицировано как неправомерный доступ к компьютерной информации.

В апелляционной жалобе указывалось также, что материалами дела не установлен факт доступа именно к охраняемой законом информации. Однако в соответствии со ст. 16 ч. 4 Закона «Об информации» обладатель информации обязан обеспечить недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование, то есть по смыслу закона в качестве охраняемой законом информации следует рассматривать любую информацию в чужом компьютере, если она защищена собственником. В ходе судебного разбирательства судом исследовалось свидетельство об официальной регистрации программы для ЭВМ и договор о полной передаче исключительного права на программу для ЭВМ ООО «Ассист», что указывает на то, что ООО «Ассист» является законным обладателем информации и принимал меры по её охране.

В итоге, оценив собранные доказательства в их совокупности, апелляционный суд пришел к выводу, что судом первой инстанции действия осужденных обоснованно квалифицированы по ч. 2 ст.272 УК РФ (в редакции ФЗ № 26 от 7 марта 2011 г.) как совершение неправомерного доступа к охраняемой законом компьютерной информации, то есть информации в системе ЭВМ и их сети, повлекшее блокирование и нарушение работы системы ЭВМ и их сети, группой лиц по предварительному сговору[1].

При этом заметим, что положение об обратной силе уголовного закона суд так и не применил, а значит, по его мнению, новый закон не устраняет преступность совершенного осужденными деяния.

В отношении рассмотренного дела представляет интерес предложение И.Г. Чекунова ввести уголовную ответственность за неправомерное воздействие на функционирование системы. Цель предлагаемой нормы – защита от Dos/DDos-атак. Состав сформулирован как «неправомерное деяние, направленное на отказ в обслуживании компьютера, компьютерных систем или их сети, осуществляемое с использованием протоколов межсетевого взаимодействия, с целью прекращения или создания задержек обработки сетевых запросов»[2].

Названные в диспозиции последствия должны находиться в причинной связи с неправомерным доступом к охраняемой законом компьютерной информацией.

Исследуя вопрос об установлении причинной связи по делам данной категории, некоторые авторы используют теорию необходимого причинения, согласно которой для наличия причинной связи нужно, чтобы деяние *с* внутренней необходимостью вызывало наступление последствия, чтобы оно

---

[1] Дело № 10-11502 … из архива Московского городского суда за 2013 г. [Электронный ресурс]. – Режим доступа: http://www.mos-gorsud.ru.

[2] Чекунов И.Г. Криминологические и уголовно-правовые аспекты предупреждения киберпреступлений // Российский следователь. – 2013. – № 3. – С. 42.

было главным, решающим условием, с неизбежностью породившим данное последствие.

По мнению Д.А. Ястребова и С.В. Григоренко, «ответственность по ст. 272 УК РФ наступает только в том случае, если преступные последствия, альтернативно отраженные в ее диспозиции, явились именно необходимым следствием, закономерно вызванным неправомерным доступом лица к охраняемой законом компьютерной информации»[1].

Другие авторы придерживаются теории непосредственной (ближайшей) причины, согласно которой последнее, непосредственное и ближайшее к последствию деяние должно признаваться причиной наступления результата. По мнению сторонников данной теории, «деяние должно быть непосредственной причиной общественно опасного последствия»[2], то есть не отделено от последствия никакими звеньями.

Согласно эквивалентной теории, именуемой также теорией необходимого условия (conditio sine gua non), деяние должно быть одним из необходимых условий наступления результата. Недостаток этой концепции заключается в ее неспособности разграничить причины и условия, необходимые для наступления последствия.

И.С. Сало наиболее приемлемой для установления причинной связи по делам о преступлениях, предусмотренных ст. 272 УК РФ, признает концепцию реальной возможности, согласно которой главным критерием причинной связи выступает реальная возможность деяния причинить вред или превращение этой возможности в действительность. По мнению данного автора, «алгоритм установления причинной связи по делам рассматриваемой категории может быть следующим»[3]:

1) необходимо установление факта наступления хотя бы одного из

---

[1] Ястребов Д.А. Правовые вопросы обеспечения информационной безопасности (уголовная ответственность за преступления в сфере компьютерной информации в Российской Федерации) // – М.: Издательство «Прима-Пресс», 2007. – С. 30.
[2] Здравомыслова Б.В. Уголовное право России. Общая часть / – М., 1999. – С. 150.
[3] Сало, И.С. Указ. соч. – С. 126 – 130.

перечисленных в диспозиции ст. 272 УК РФ последствий в виде уничтожения, блокирования, модификация либо копирования информации;

2) неправомерный доступ к охраняемой законом компьютерной информации по времени должен предшествовать наступлению данных последствий. При этом следует иметь в виду, что уничтожение, блокирование, модификация, копирование информации в компьютерных системах возможны и в результате технических неисправностей или ошибок при функционировании аппаратно-программных средств. В связи с этим, в каждом конкретном случае необходимо выяснять, что имело место: «сбой, отказ в работе, ошибка персонала или преднамеренные преступные действия»[1]. Кроме того, к первоначальным действиям субъекта могут присоединяться и действия третьих лиц, влияющие на преступный результат;

3) противоправное поведение лица лишь в том случае может быть признано причиной общественно опасного результата, если оно было необходимым условием его наступления, то есть условием, при отсутствии которого данные последствия вообще могли не наступить;

4) деяние должно создавать реальную возможность наступления общественно опасного результата или превратить эту возможность в действительность, т. о. необходимо установить, что неправомерный доступ к компьютерной информации содержал возможность уничтожения, блокирования, модификации или копирования информации. Данная возможность должна иметь конкретное, реальное содержание, а не быть абстрактной.

По нашему мнению установлению причинной связи по делам рассматриваемой категории мешают проблемы регламентации объективной стороны неправомерного доступа к компьютерной информации.

Перечисленные в диспозиции последствия, по сути, представляют собой самостоятельные активные действия, производимые с компьютерной

[1] Иванов А. Предварительная проверка сообщений о неправомерном доступе к компьютерной информации // Уголовное право. – 2003. – № 4. – С. 117.

информацией, которые совершаются виновным после осуществления доступа, то есть после получения возможности манипуляции компьютерной информацией.

В связи с этим, по мнению Н.В. Богомолова, «процесс установления причинной связи приводит правоприменителя в замешательство. Ввиду того, что неправомерный доступ является условием для осуществления непосредственно второго действия (например, копирования), то их сложно связать с помощью причинной связи. Поэтому в обвинительных заключениях встречаются некорректные, с технической точки зрения, формулировки о причинной связи между неправомерным доступом и последствиями, но чаще следователи не устанавливают ее, а упоминают о ней, указывая лишь на общую последовательность отдельных действий. Есть даже примеры, где следователи, пытаясь показать причинную связь, «нагромождают» лишними, выходящими за рамки статьи 272, последствиями»[1].

Полагаем, что совершенствование объективной стороны рассматриваемого преступления позволило бы снять хотя бы часть из выявленных в ходе исследования проблем квалификации неправомерного доступа к компьютерной информации.

Например, Р.В. Амелин, полагает, что «при криминализации преступлений в сфере компьютерной информации разумнее было бы использовать подход, устанавливающий уголовную ответственность независимо от способа совершения преступления, за нарушение конфиденциальности, целостности и доступности информации (с учетом равной значимости всех трех свойств ответственность могла бы быть единой)»[2]. Именно названные три свойства охраняются ст. 272 УК РФ.

Так, копирование компьютерной информации является нарушением конфиденциальности, модификация – нарушением целостности, а

[1] Богомолов М.В. Указ. соч. – С. 87.
[2] Амелин Р.В. О возможном решении проблемы неполноты главы 28 УК РФ // Уголовно-исполнительная система: право, экономика, управление. – 2009. – № 5. – С. 5 – 6.

блокирование и уничтожение – нарушением доступности.

Мы все же солидарны с Г.П. Новоселовым, который считает, что «правильнее было бы рассматривать основанием уголовной ответственности за неправомерный доступ к компьютерной информации случаи, когда неправомерный доступ сопряжен с уничтожением, блокированием и т. д. (т. е. такому доступу следовало бы придать значение не только причины, но и необходимого условия)»[1].

Думаем, что в этом случае состав преступления следует сформулировать как формальный: «Неправомерный доступ к охраняемой законом компьютерной информации, сопряженный с ее уничтожением, блокированием, модификацией или копированием».

1.3 Субъективные признаки неправомерного доступа к компьютерной информации

Характеристика субъективной стороны неправомерного доступа к компьютерной информации так же, как и остальные элементы состава данного преступления, является поводом для дискуссии. Анализ юридической литературы демонстрирует отсутствие единого подхода в решении данного вопроса, причем имеют место диаметральные суждения как о форме вины, так и о видах умысла и неосторожности.

Обостряет спор и то, что одни авторы определяют вину в отношении преступления в целом, другие анализируют ее содержание отдельно в отношении деяния и последствий, третьи устанавливают вину и в отношении каждого последствия.

Полагаем, что такой разноплановый подход к исследованию субъективной стороны обусловлен как отсутствием указаний в диспозиции рассматриваемой уголовно-правовой нормы на признаки данного элемента

[1] Козаченко И.Я. Уголовное право. Особенная часть: учебник для ВУЗов / Издательская группа НОРМА-ИНФРА-М, – М. – 1998. – С. 556.

состава, так и выявленными нами проблемами регламентации объективной стороны.

Преобладающим в теории является мнение о том, что «неправомерный доступ к компьютерной информации может быть совершен только умышленно»[1]. В качестве аргумента авторы приводят суждение о том, что в соответствии с действующим законодательством при создании информационных систем их собственники обязаны предусмотреть такие меры безопасности, которые бы обеспечили лишь правомерный и упорядоченный доступ к информационным ресурсам. Преодоление этих мер защиты всегда связано с определенным профессионализмом лица, осуществляющего доступ к компьютерной информации, что свидетельствует об умышленном воздействии на нее.

В то же время по поводу возможных видов умысла при совершении данного преступления мнения ученых расходятся.

Часть из них стоит на позиции, что «умысел может быть только прямым»[2]. Однако, все же большинство ученых не исключает «совершение данного преступления и с косвенным умыслом»[3].

С. Кочои, Д. Савельев также придерживаются мнения, что преступление

---

[1] Например: Крылов В.В. Указ. соч. – С. 85; Мазуров В.А. Указ. соч. – С. 113; Дворецкий М.Ю. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации: монография. – Тамбов: Изд- во ТГУ им. Г.Р. Державина, 2006. – С. 130; Иногамова-Хегай Л.В. Уголовное право РФ: в 2 т. Т. *2*. Особенная часть / – М., 2002. – С. 317 и др.

[2] Абов А.И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации. – М.: Прима-Пресс, 2002. – С. 16; Бытко С.Ю. Преступления в сфере компьютерной информации: учеб. пособие для студентов юридических специальностей. – Саратов: Изд-во Сарат. ун-та, 2004. – С. 32; Борчева Н.А. Указ. соч. – С. 10; Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дисс. ... канд. юрид. наук. – М.:, 2002. – С. 95; Григоренко С.В. Преступления в сфере компьютерной информации. – М.: Полтекс, 2003. – С. 11.

[3] Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания. – Тамбов: Издательство ТГУ, 2003. – С. 116; Пантелеев И.А. Криминологические и уголовно-правовые вопросы борьбы с компьютерной преступностью: учеб. пособие. – Екатеринбург, 2004. – С. 33; Кругликов Л.Л. Уголовное право России. Часть Особенная: учебник для ВУЗов / – М., 2005. – С. 632 и др.

совершается умышленно. «Человек, пытающийся получить доступ к информации, должен сознавать, что свободный доступ к информации ограничен, он не имеет прав на доступ к этой информации. Об умысле будут свидетельствовать меры защиты информации от доступа посторонних (коды, пароли и т. п.), которые приходится преодолеть, чтобы получить доступ к информации, вывод на экран дисплея компьютера предупреждающих сообщений, устные уведомления о запрете доступа к информации и т. д.»[1] Но по отношению к последствиям, уточняют авторы, вина может быть, как умышленной, так и неосторожной. Аналогичной позиции придерживается К.Н. Евдокимов[2].

Интересен взгляд А.Г. Волеводза, который считает, что «субъективная сторона данного преступления характеризуется виной в форме прямого умысла. Косвенный умысел и неосторожная форма вины могут иметь место по отношению к наступлению вредных последствий неправомерного доступа»[3].

Высказываются и иные позиции по поводу определения субъективной стороны рассматриваемого преступления, которые предполагают неосторожность в отношении самого неправомерного доступа к компьютерной информации. Так, по мнению С.А. Пашина, «преступление, предусмотренное ст. 272 УК РФ, может совершаться как с умыслом, так и по неосторожности. Причем неосторожность автор допускает даже в отношении деяния: «неосторожная форма вины может проявляться при оценке лицом правомерности своего доступа к компьютерной информации, а также в отношении неблагоприятных последствий доступа, предусмотренных

[1] Кочои С. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 44 – 45.
[2] Евдокимов К.Н. Субъективная сторона неправомерного доступа // Вестник Академии Генеральной Прокуратуры РФ. – 2009. – № 12. – С. 42 – 46.
[3] Волеводз А.Г. Противодействие к компьютерным преступлениям: правовые основы международного сотрудничества. – М., 2002. – С. 71.

диспозицией нормы уголовного закона», – указывает автор»[1]. Такого же мнения придерживаются С.Н. Золотухин и А.З. Хун, характеризуя ситуацию с неосторожной формой вины при оценке лицом правомерности своего доступа к компьютерной информации как своеобразную «юридическую ошибку»[2].

С.В. Озерский, Ю.Н. Лазарев и А.Ю. Лавров также считают, что «преступление совершается с прямым или косвенным умыслом, однако «неосторожная форма вины может проявляться при неверной оценке лицом правомерности своего доступа к компьютерной информации, а также в отношении неблагоприятных последствий доступа, предусмотренных диспозицией данной нормы уголовного закона»[3]. А.Е. Шарков излагает свою позицию следующим образом: «субъект, осуществляющий неправомерный доступ по неосторожности, либо сознает опасность своих действий, но действует легкомысленно, либо не предвидит возможных опасных последствий, хотя мог и должен предвидеть»[4].

Некоторые ученые углубляются еще больше, выясняя вину в отношении каждого из последствий.

По мнению И.А. Сало, исходя из того, что «форма вины определяется отношением лица к общественно опасным последствиям, предусмотренным в уголовно-правовой норме, форму вины необходимо устанавливать применительно к каждому последствию, перечисленному в диспозиции данной статьи»[5]. Оценивая содержание вины с этих позиций, автор приходит

---

[1] Комментарий к УК РФ / под общ. ред. Ю.И. Скуратова, В.М, Лебедева. – М., 1997. – С. 640.

[2] Золотухин С.Н. Уголовно-правовые и криминологические аспекты преступлений в сфере компьютерной информации: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2008. – С. 72.

[3] Озерский С.В. Компьютерные преступления: методы противодействия и защиты информации // учебное пособие. – Саратов: Саратовский юридический институт МВД России, 2004. – С. 24.

[4] Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дисс. …канд. юрид. наук. – Ставрополь, 2004. – С. 149.

[5] Сало И.А. Указ. соч. – С. 142.

к выводу, что, «если последствием незаконного доступа является уничтожение, блокирование или копирование компьютерной информации, то вина может быть как умышленная, так и неосторожная. Если же незаконный доступ повлек за собой модификацию информации, то по отношению к данному последствию необходимо устанавливать прямой умысел субъекта»[1].

Применяя тот же подход к анализу субъективной стороны, В.С. Карпов, в свою очередь, полагает, что «с прямым умыслом может быть совершено только копирование информации, а ее уничтожение, модификация и блокирование могут быть совершены, как умышленно, так и по неосторожности»[2]. Обосновывает свою позицию автор тем, что копирование информации направлено именно на достижение поставленного результата, а уничтожение, модификация, блокирование информации могут быть совершены как умышленно, так и по неосторожности.

Мы полагаем, что тщательное исследование субъективной стороны рассматриваемого преступления должно проводиться с учетом положений, закрепленных в главе 5 УК РФ.

В соответствии с ч. 2 ст. 24 УК РФ, деяние, совершенное только по неосторожности, признается преступлением лишь в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК РФ. Но в связи с тем, что в ст. 272 УК РФ указание на форму вины отсутствует, то теоретически неправомерный доступ к компьютерной информации может быть совершен как умышленно, так и по неосторожности. На это положение опираются многие авторы в своих рассуждениях.

Что касаемо установления умышленной формы вины в отношении действия (неправомерного доступа к компьютерной информации) и неосторожной в отношении последствий (уничтожение, блокирование,

---

[1] Сало И.А. Указ. соч. – С. 143 – 145.

[2] Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дисс. …канд. юрид. наук. – Красноярск, 2002. – С. 134.

модификация или копирование информации), то, продолжая рассуждения ученых, мы должны признать, что посягательство, предусмотренное ст. 272 УК РФ, следует рассматривать как преступление с двумя формами вины.

Однако к таким преступлениям относятся лишь квалифицированные составы ввиду того, что согласно ст. 27 УК РФ в результате совершения умышленного преступления должны быть причинены тяжкие последствия, за которые установлено более строгое наказание. В нашем же случае уголовная ответственность за неправомерный доступ к компьютерной информации, не повлекший указанные в диспозиции последствия, не предусмотрена. А потому констатация двух форм вины – умысла в отношении действия и неосторожности в отношении последствий – не основана на законе.

По нашему мнению, неправомерный доступ к компьютерной информации может совершаться только умышленно, поскольку на это указывает понятие «неправомерность» в диспозиции рассматриваемой нормы. Значит, субъект должен осознавать фактический характер и общественную значимость своего действия, в том числе и отсутствие соответствующего допуска к компьютерной информации. Кроме того, на то, что неправомерный доступ совершается умышленно, указывается и в некоторых источниках информационного права.

Так, например, согласно ст. 3 Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, подписанного в Минске 1 июня 2001 г., «Стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния, если они совершены умышленно: а) осуществление неправомерного доступа к компьютерной информации…»[1].

[1] Федеральный закон РФ «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01 октября 2008 г. № 164-ФЗ // Российская газета. – 2008. – № 208.

Мы считаем, что в данном случае нельзя ставить форму вины в зависимость от вида последствий: если лицо осознает неправомерность доступа, оно уже действует умышленно.

При этом рассматриваемое преступление может быть совершено как с прямым, так и с косвенным умыслом.

Осуществляя неправомерный доступ к охраняемой законом компьютерной информации, виновный осознает общественную опасность своих действий, в частности тот факт, что у него нет допуска к данной информации, предвидит неизбежность или реальную возможность наступления хотя бы одного из перечисленных в ст. 272 УК РФ последствий (уничтожение, блокирование, копирование или модификацию компьютерной информации) и либо желает их наступления (стремится к ним), либо не желает, но сознательно допускает наступление данных последствий или относится к ним безразлично.

Анализ судебной практики по делам о неправомерном доступе к компьютерной информации показал, что суды в одних случаях устанавливают умысел только на неправомерный доступ к охраняемой законом компьютерной информации, а в других – и на достижение указанных в диспозиции последствий.

Например, «Златоустовский городской суд установил, что М., имея умысел на неправомерный доступ к охраняемой законом компьютерной информации, действуя из корыстной заинтересованности, осуществил неправомерный доступ к охраняемой законом компьютерной информации – неправомерно приобрел с целью сбыта с помощью ЭВМ, через сеть «Интернет» путем копирования контрафактные экземпляры программных продуктов, незаконно скопировав их на машинные носители информации»[1].

В другом деле «З., умышленно изменяя IP-адреса, осуществлял неправомерный доступ к охраняемой законом компьютерной информации,

[1] Дело № 1-348/2012 … из архива Златоустовского городского суда Челябинской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://zlatoust.chel.sudrf.ru.

находящейся на машинном носителе в сети ЭВМ организации-провайдера, повлекший блокирование, модификацию информации»[1]. В ходе судебного разбирательства Озерский городской суд установил, что З. действовал из корыстных побуждений, имел цель осуществить неправомерный доступ к внутренней сети провайдера и сети Интернет и, в тоже время, допускал возможность блокирования компьютерной информации. Как мы видим, в этом примере вина подсудимого устанавливалась и в отношении неправомерного доступа (указание на цель), и в отношении последствий в виде модификации информации (умышленно изменял адреса) и блокирования информации (допускал ее возможность).

В третьем случае «Центральный районный суд г. Челябинска установил, что И. умышленно, не имея на то права, осуществил неправомерный доступ к охраняемой законом информации, после чего умышленно удалил компьютерную информацию, что привело к уничтожению, блокированию и модификации охраняемой законом компьютерной информации»[2].

Белгородский районный суд Белгородской области установил, что «С., имея преступный умысел, направленный на незаконное копирование информации, представленной в виде электрического сигнала, осуществил неправомерный доступ к компьютерной информации, позволяющей распоряжаться денежными средствами, находящимися на лицевом счете банковской карты ОАО «Сбербанка России», оформленной на имя П.»[3].

Приведенные примеры отражают основную позицию судов – неправомерный доступ к охраняемой законом информации преступник осуществляет с прямым или косвенным умыслом.

В то же время полагаем, что указание в диспозиции рассматриваемой

---

[1] Дело № 1-77/2011… из архива Озерского городского суда Челябинской области за 2011 г. [Электронный ресурс]. – Режим доступа: http://ozersk.chel.sudrf.ru/

[2] Дело № 1-356/2010 … из архива Центрального районного суда г. Челябинска за 2010 г. [Электронный ресурс]. – Режим доступа: http://centr.chel.sudrf.ru/

[3] Дело № 1-213/2012 … из архива Белгородского районного суда Белгородской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://belgorodsky.blg.sudrf.ru

нормы на последствия в виде действий второго порядка приводит суды к необходимости устанавливать вину и к самому неправомерному доступу к компьютерной информации, и, например, к ее модификации, хотя нередко эти действия совершаются одномоментно, и даже сам преступник их не разграничивает.

Представляется, что совершенствование объективной стороны состава неправомерного доступа к компьютерной информации, о необходимости которого говорилось ранее, позволило бы решить часть проблем, возникающих при установлении вины субъекта в отношении данного состава преступления.

Мотивы и цели неправомерного доступа к компьютерной информации не являются обязательными признаками состава преступления. Однако их установление позволяет выявить причины преступления, индивидуализировать ответственность, назначить справедливое наказание. Мотивом преступления является причина, побудившая лицо совершить преступление, а целью – результат к которому это лицо стремится. Корысть, зависть, хулиганство, желание испортить репутацию, месть являются основными мотивами к совершению преступления. В некоторых случаях установление мотивов и целей могут существенным образом повлиять на квалификацию преступления.

Так, совершение данного преступления из корыстной заинтересованности образует квалифицированный состав и влечет уголовную ответственность по ч. 2 ст. 272 УК РФ.

Ряд ученых считает, что «отсутствие в уголовном законе прямого указания на обязательность анализа мотивов и целей совершения компьютерных преступлений можно рассматривать как пробел в законодательстве»[1].

По нашему мнению, не включение законодателем мотива и цели в

[1] Кочои, С.М. Ответственность за корыстные преступления против собственности // М.,1998. – С. 132.

диспозицию ч. 1 ст. 272 УК РФ свидетельствует о следующем: с какими бы мотивом и целью не совершался неправомерный доступ к охраняемой законом компьютерной информации, виновное лицо подлежит уголовной ответственности. Однако некоторые мотивы и цели, безусловно, повышают степень общественной опасности преступления. В связи с этим, по мнению В.Г. Степанова-Егиянца, «ст. 272 УК РФ следует дополнить квалифицирующим признаком, учитывающим цель скрыть другое преступление или облегчить его совершение»[1]. Представляется, что неправомерный доступ к компьютерной информации, совершенный с указанной целью, обладает большей общественной опасностью.

Согласно нормам главы 4 УК РФ, субъектом неправомерного доступа к компьютерной информации является вменяемое физическое лицо, достигшее 16-ти летнего возраста. Анализ ч. 1 ст. 272 УК РФ свидетельствует о том, что субъект данного преступления является общим, т. к. он не наделен никакими дополнительными признаками.

В юридической литературе периодически обсуждается вопрос «о социальной обусловленности возраста, с которого установлена ответственность за компьютерные преступления вообще и неправомерный доступ к компьютерной информации в частности»[2].

По мнению Д.Г. Малышенко, «минимальный возраст уголовной ответственности за данное преступление необходимо понизить до 14 лет с учетом того, что и в более раннем возрасте подростки уже могут осознавать общественную опасность неправомерного доступа и предвидеть последствия своих действий»[3]. А.Ж. Кабанова в качестве обоснования такого предложения указывает на «большую доступность технических средств хранения, обработки и передачи информации большинству населения,

---

[1] Степанов-Егиянц В.Г. Субъективная сторона компьютерных преступлений // Бизнес в законе. – 2013. – № 2. – С. 74.
[2] Айсанов Р.М. Указ. соч. – С. 105.
[3] Малышенко Д.Г. Указ. соч. – С. 95 – 96.

повышение уровня образованности в сфере использования высоких технологий, в том числе и среди несовершеннолетних»[1].

Криминологические исследования свидетельствуют, что среди лиц, совершающих преступления в сфере компьютерной информации, значительна доля подростков. В ходе работы первой международной конференции Интерпола по компьютерной преступности были выявлены три основные возрастные группы компьютерных преступников: 11 – 15, 17 – 25, 30 – 45 лет.

По данным исследователей, молодежь интересующей нас первой группы в основном совершает кражи с помощью кредитных карт и телефонных номеров, взламывая пароли и коды чаще по мотиву самоутверждения или из любознательности[2]. Именно в отношении этой возрастной группы и ведутся споры о снижении возрастной границы уголовной ответственности.

По нашему мнению, данная проблема требует глубокого и всестороннего изучения. Расширение перечня преступлений, уголовная ответственность за совершение которых наступает с 14 лет, должно осуществляться не только на основе анализа результатов криминологических исследований, но и с учетом достижений педагогики, психологии, психиатрии и др. наук.

Учитывая, что одним из направлений современной уголовно-правовой политики является все-таки «постепенное повышение возраста начала уголовной ответственности»[3], полагаем, что предложение установить нижний возрастной предел уголовной ответственности за неправомерный доступ к компьютерной информации в 14 лет, является не вполне обоснованным.

---

[1] Кабанова А.Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты): автореферат дис. ... канд. юрид. наук. – Ростов-н/Д, 2004. – С. 4.

[2] Айсанов Р.М. Указ. соч. – С. 103 – 104.

[3] Волошин В.М. Уголовно-правовая политика России в отношении несовершеннолетних правонарушителей и роль ответственности в ее реализации: автореферат дис. ... докт. юрид. наук. – Екатеринбург, 2008. – С. 5.

1.4 Юридический анализ квалифицирующих признаков

Часть 2 ст. 272 УК РФ устанавливает повышенную уголовную ответственность при наличии таких отягчающих обстоятельств как причинение крупного ущерба и наличие корыстной заинтересованности.

Согласно примечанию 2 к ст. 272 УК РФ крупным ущербом признается ущерб, сумма которого превышает один миллион рублей.

Обращает на себя внимание конструкция квалифицированного состава по признаку причинения крупного ущерба. Как было рассмотрено ранее, законодатель сформулировал основной состав неправомерного доступа к компьютерной информации по типу материального. В качестве деяния указан неправомерный доступ, а в качестве последствия данного деяния названы уничтожение, блокирование, модификация или копирование компьютерной информации.

Если толковать часть вторую рассматриваемой статьи буквально, то причинение крупного ущерба должно наступить в результате совершения только деяния, указанного в части 1, т. е. неправомерного доступа. И в этом случае для квалификации не имеет значения, повлек данный доступ уничтожение, блокирование и т. д. информации или нет. Если же законодатель все-таки имел в виду причинение крупного ущерба в результате наступления любого из указанных в части 1 последствий, то ему надо было формулировать состав именно таким образом, чтобы не допускать двусмысленное толкование нормы.

Кстати, с позиции правоприменительной практики первый вариант существенно бы облегчил квалификацию преступления, т. к. во втором случае суду придется устанавливать причинную связь, во-первых, между неправомерным доступом и последствиями, указанными в первой части статьи, и, во-вторых, между данными последствиями и причинением крупного ущерба.

А так как мы убедились, что вопрос установления причинной связи по делам данной категории не из легких, и связано это с законодательной конструкцией объективной стороны основного состава, то полагаем, что предложенная нами конструкция не усложнила бы процесс квалификации неправомерного доступа к компьютерной информации, причинившего крупный ущерб.

Вторым квалифицирующим признаком в ч. 2 ст. 272 назван мотив – корыстная заинтересованность лица. Обычно этот признак законодатель использует в тех составах, где, помимо корыстной, предусмотрена еще и иная личная заинтересованность. В остальных случаях указывается на корыстные побуждения.

Обращает на себя внимание тот факт, что законодатель при конструировании составов преступлений использует различную терминологию, в целом охватываемую понятием корыстного мотива преступления: корыстные побуждения, корыстная цель, корыстная заинтересованность.

Одной из причин неверного применения закона и, как следствие, ошибок в квалификации на практике являются разночтения в определении корыстного мотива преступления, когда происходит смешение понятий мотива и цели преступления.

При установлении корыстного мотива в деянии лица следует ориентироваться на то, что основным содержанием корыстных побуждений является направленность устремлений виновного на извлечение материальной выгоды, незаконное обогащение. Корыстная заинтересованность, будучи по своей сути осознаваемым мотивом, изначально включает в себя корыстную цель, которая может быть достигнута путем совершения противоправного деяния.

Таким образом, для вменения лицу, совершившему неправомерный доступ к компьютерной информации, данного отягчающего обстоятельства

необходимо установить, что его действия были направлены на получение материальной выгоды. В судебной практике наличие корыстной заинтересованности без труда подтверждается установлением корыстной цели при совершении неправомерного доступа ради использования контрафактной продукции.

Так, например, «у Зайцева возник преступный умысел, направленный на совершение неправомерного доступа к охраняемой законом компьютерной информации, а именно к программе «MicrosoftWindowsXPServicePack 3» и программе «MicrosoftOffice – профессиональный выпуск версии 2003», с корыстной целью, путем их установки и незаконной активации с находящегося в этот момент у него с собой личного, нелицензионного компакт-диска, содержащего дистрибутивы данных программ и ключи активации, не имеющего надлежащей упаковки установленного образца и наклейки «ProofofLicense» (Подтверждение лицензии), которая отличает подлинное программное обеспечение корпорации «Microsoft» и доказывает наличие у пользователя лицензионной копии программы, ранее приобретенного им у неустановленных следствием лиц. Реализуя свой преступный умысел, Зайцев предложил С. установить вышеуказанные программы, правообладателем которых является корпорация «Microsoft», на жесткий диск ноутбука за денежное вознаграждение ему лично, на что С. согласился»[1].

В случае причинения крупного ущерба из корыстных побуждений, виновному должны вменяться оба предусмотренных частью второй квалифицирующих обстоятельства.

В части 3 данной статьи в качестве квалифицирующих признаков законодатель предусмотрел совершение преступления группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.

[1] Дело № 1-139/2012 … из архива Советского районного суда Рязанской области. [Электронный ресурс]. – Режим доступа: http://sovetsky.riz.sudrf.ru.

Согласно ч. 2 ст. 35 УК РФ, преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления. Несмотря на отсутствие в данной норме прямого указания на то, что в преступлении должны участвовать соисполнители, судебная практика рассматривает данную форму соучастия именно в таком субъектном составе.

Таким образом, для вменения данного признака необходимо, чтобы объективную сторону преступления полностью или частично выполнили два или более исполнителей, причем сговор на совершение неправомерного доступа должен состояться до начала выполнения объективной стороны.

Полагаем, что группа лиц по предварительному сговору будет как в случае, когда два субъекта параллельно осуществляют неправомерный доступ к охраняемой законом компьютерной информации, а также копируют, уничтожают, блокируют или модифицируют информацию, так и в случае, когда, например, один из них обеспечил неправомерный доступ к информации, а другой блокировал ее.

При этом действия всех соисполнителей должны квалифицироваться по ч. 3 ст. 272 УК РФ.

В приведенном ранее примере с DDos-атакой на сервер платежной системы «Ассист», «Врублевский, вступил с братьями Артимовичами, занимавшимися оказанием «хакерских услуг», в предварительный сговор. Зная, что в распоряжении Артимовичей имеется созданная ими ранее с использованием вредоносных программ сеть зараженных компьютеров (бот-сеть), Врублевский поставил перед ними задачу произвести атаку на информационные ресурсы ООО «Ассист». В целях финансирования указанной деятельности Врублевский дал указание выделить им денежные средства в любом размере, необходимом для осуществления задуманного. Действуя согласно единого преступного плана и отведенных каждому участнику группы ролей, они осуществили компьютерную DDoS-атаку на

информационные ресурсы ООО «Ассист». Ход атаки Врублевский несколько раз контролировал лично путем входа на сайт ОАО «Ассист» и последующего заказа билетов, убеждаясь, что работа данного ресурса блокирована.

Таким образом, суд усмотрел наличие признака группы лиц по предварительному сговору в действиях виновных. Указанный вывод суда основан на том, что подсудимые действовали согласованно, предварительно распределив между собой роли, заранее подготовившись к совершению преступления, каждый соучастник знал и выполнял свою роль при совершении преступления, действия каждого подсудимого были направлены на достижения единого преступного результата, о чем свидетельствуют показания осужденных»[1].

Согласно ч. 3 ст. 35 УК РФ преступление признается совершенным организованной группой, если оно совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Несмотря на то, что участники организованной группы, согласно разработанному плану, могут выполнять разные роли соучастников в процессе совершения преступления, судебная практика идет по пути квалификации действий каждого из них по соответствующей статье Особенной части без ссылки на ст. 33 УК РФ, т. е. признает их соисполнителями. И хотя это не в полной мере соответствует положениям уголовного закона, регламентирующим ответственность соучастников, данная практика считается устоявшейся, в основном по той причине, что она учитывает высокую степень общественной опасности преступлений, совершенных организованными группами, которые, как правило, отличаются профессионализмом в сфере криминальной деятельности.

В полной мере это относится и к совершению неправомерного доступа к

[1] Дело № 10-11502 … из архива Московского городского суда за 2013 г. [Электронный ресурс]. – Режим доступа: http://www.mos-gorsud.ru/

компьютерной информации, совершенному организованной группой. Для квалификации преступления с учетом данного квалифицирующего обстоятельства необходимо, в первую очередь, доказать, что преступная группа является устойчивой – она существует длительное время (как показывает практика, не менее 2 - 3 месяцев), характеризуется стабильным составом, тесной связью между соучастниками (возможно, только виртуальной), постоянством методов преступной деятельности и т. д.

Как отмечает Т.М. Лопатина, «в последние годы появилась тенденция совершения преступлений в рассматриваемой сфере организованными группами со свойственной им иерархией и распределением ролей и обязанностей»[1].

Предусмотрев в ч. 3 ст. 272 два квалифицирующих признака, связанных с соучастием, законодатель, тем самым, не учел влияние формы соучастия на дифференциацию уголовной ответственности с точки зрения общественной опасности деяния. Очевидно, что совершение преступления организованной группой обладает гораздо большей опасностью. Поэтому полагаем, что признак «то же деяние, совершенное организованной группой» необходимо перенести в ч. 4 ст. 272 УК РФ.

В части 3 рассматриваемой статьи предусмотрен еще один квалифицирующий признак, характеризующий субъекта преступления, - использование лицом своего служебного положения.

Вопрос о том, что следует понимать под «использованием своего служебного положения» является актуальным как в теории, так и в практике. Проблемы квалификации обусловлены отсутствием законодательной регламентации данного признака, а также разъяснений высшей судебной инстанции применительно к составу неправомерного доступа к компьютерной информации.

Некоторые авторы рассматривают признак использования служебного

[1] Лопатина Т.М. Указ. соч. – С. 41.

положения узко, в связи с чем «субъектами данного преступления признают только лиц, перечень которых содержится в примечаниях к ст. 285 УК РФ и к ст. 201 УК РФ»[1].

Другие ученые, и их большинство, относят к «специальному субъекту преступления не только должностных лиц, государственных служащих и служащих органов местного самоуправления, не являющихся должностными лицами, лиц, выполняющих управленческие функции в коммерческой или иной организации, но и иных служащих, в том числе коммерческих и некоммерческих организаций, не наделенных управленческими функциями»[2].

Так как признак «использование лицом своего служебного положения» используется также при дифференциации уголовной ответственности за мошенничество, присвоение и растрату, имеет смысл обратиться к рекомендациям, которые дает высшая судебная инстанция для квалификации преступлений данной категории.

К лицам, использующим свое служебное положение, Пленум Верховного Суда РФ относит: «должностных лиц, обладающих признаками, предусмотренными примечанием 1 к статье 285 УК РФ; государственных или муниципальных служащих, не являющихся должностными лицами; иных лиц, отвечающих требованиям, предусмотренным примечанием 1 к статье 201 УК РФ (например, лиц, которые используют для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные

---

[1] Методические рекомендации по расследованию преступлений в сфере компьютерной информации. – М.: КМУ Следственный комитет при МВД России. – 1997. – С. 23.

[2] Например, Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания // Издательство ТГУ. – Тамбов. – 2003. – С. 142; Ястребов Д.А. Неправомерный доступ к компьютерной информации // под общ. ред. А.А. Тер-Акопова и Г.И. Загорского. 3-е изд. перераб. и доп. – М.: Издательство «Прима-Пресс». – 2006. – С. 61; Бородин А.В. Феномен компьютерных вирусов: элементы теории и экономика существования // учеб. пособие. – Йошкар-Ола: МарГТУ. – 2004. – С. 111 – 112 и др.

обязанности в коммерческой организации)»[1].

Таким образом, Пленум не рекомендует признавать специальными субъектами служащих коммерческих или иных организаций, не наделенных управленческими функциями. Тогда неправомерный доступ к компьютерной информации, совершенный лицами, наделенными служебными, но не управленческими, полномочиями и использующими свое служебное положение для совершения преступления, должен быть квалифицирован по ч. 1, а не ч. 3 ст. 272 УК РФ.

Однако в судебной практике встречаются и противоположные решения.

«Киселев работал ведущим специалистом отдела по работе с ключевыми клиентами. В его обязанности входило обслуживание, развитие и сохранение корпоративных клиентов; организация улучшения качества связи с использованием служебной компьютерной техники, служебных сим-карт и доступа к Автоматизированной Системе Расчетов, с помощью которой можно произвести замену сим-карт. У Киселева, исполняющего служебные обязанности, в целях извлечения для себя материальной выгоды возник преступный умысел на неправомерную замену (модификацию) двух служебных сим-карт, с целью последующего их использования в личных корыстных целях. Реализуя задуманное, Киселев осуществил регистрацию на сервере доступа и статистики оператора связи под своими учетными (регистрационными) данными, после чего осуществил без согласия собственника несанкционированный доступ к Автоматизированной Системе Расчетов, используя свое служебное положение, путем введения логина и пароля, выданных ему для служебного использования и доверенных ему по работе. Киселев произвел модификацию информации – несанкционированную замену учетной записи двух служебных сим-карт, осуществив несанкционированную регистрацию, модификацию

[1] Постановление Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» от 27 декабря 2007 г. № 51 // Российская газета. – 2008. – № 4.

компьютерной информации на сервере доступа оператора связи, что привело к блокированию абонентских номеров и модификации сим-карт с указанными номерами»[1].

Полагаем, что для единообразного понимания рассматриваемого признака в правоприменительной практике законодателю следовало бы конкретизировать его содержание либо непосредственно в уголовно-правовой норме, либо в примечании к ст. 272 УК РФ.

При квалификации неправомерного доступа к компьютерной информации с использованием лицом своего служебного положения по ч. 3 ст. 272 УК РФ дополнительной квалификации по статьям, предусматривающим ответственность за злоупотребление полномочиями, не требуется.

В ч. 4 ст. 272 УК РФ устанавливается ответственность за совершение деяний, предусмотренных частями первой, второй или третьей рассматриваемой статьи, если они повлекли тяжкие последствия или создали угрозу их наступления.

Закон не раскрывает конкретно, о каких тяжких последствиях идет речь, это понятие является оценочным.

На наш взгляд, тяжкими последствиями следует признавать гибель хотя бы одного человека, аварии на производстве или на транспорте, причинившие крупный материальный ущерб и ранения или гибель людей, возникновение больших пожаров, причинивших крупный ущерб и гибель людей, химическое и бактериологическое заражение местности, людей и животных, отравление воды в крупных водоемах и т. д.

Полагаем, что форма вины в отношении данных последствий может быть только неосторожная, иначе в действиях лица должны усматриваться составы умышленных преступлений против личности, собственности, общественной безопасности и т. д.

---

[1] Дело № 1-157/2011 … из архива Октябрьского районного суда города Ижевска Удмуртской Республики за 2011 г. [Электронный ресурс]. – Режим доступа: http://oktyabrskiy.udm.sudrf.ru.

2 ПРОБЛЕМЫ КВАЛИФИКАЦИИ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В судебно-следственной практике при квалификации неправомерного доступа к компьютерной информации нередко возникают вопросы о соотношении данного посягательства с иными преступлениями, по содержанию и юридическим признакам весьма близкими к нему. При этом практический интерес представляет как разграничение смежных составов, так и возможность квалификации неправомерного доступа по совокупности с другими преступлениями.

Наиболее актуальными, по нашему мнению, являются вопросы соотношения неправомерного доступа с иными компьютерными преступлениями (ст.ст. 273, 274 УК РФ); нарушением авторских и смежных прав (ст. 146 УК РФ); нарушением неприкосновенности частной жизни (ст. 137 УК РФ); незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ); мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ).

2.1 Отграничение неправомерного доступа к компьютерной информации от иных преступлений в сфере компьютерной информации

Учитывая, что изменения в 2011 г. подверглись все статьи главы 28 УК РФ, в первую очередь, необходимо рассмотреть соотношение неправомерного доступа к компьютерной информации с преступлением, предусмотренным ст. 273 УК РФ – 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.

Сложность разграничения рассматриваемых составов состоит в том, что создание и использование вредоносных программ, заведомо предназначенных для указанных выше последствий, могут сочетаться с неправомерным доступом к компьютерной информации.

Полагаем, что критериями разграничения рассматриваемых составов являются предмет преступления, а также признаки, характеризующие объективную и субъективную стороны преступления.

Предметом преступления, предусмотренного ст. 272 УК РФ, является охраняемая законом компьютерная (в нашем понимании электронная) информация. В то же время анализ названия и диспозиции ст. 273 приводит нас к выводу о том, что предметом преступления, предусмотренного данной нормой, являются вредоносные компьютерные программы, т. е. компьютерные программы или иная компьютерная информация, предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

Компьютерная программа, согласно ст. 1261 Гражданского кодекса РФ, понимается как представленная 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.

Иная вредоносная компьютерная информация не образует самостоятельную программу, но, взаимодействуя с полезными кодами, способна негативно влиять на их работу. Обязательным признаком вредоносной компьютерной программы или иной вредоносной компьютерной информации является их предназначение – для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты

компьютерной информации.

Наиболее значимым является разграничение рассматриваемых преступлений по объективной стороне. Диспозиция ст. 273 УК РФ, говоря о создании, распространении или использовании вредоносных компьютерных программ, не охватывает факт неправомерного доступа к компьютерной информации.

Для привлечения к ответственности по ст. 273 УК РФ достаточно только самого факта создания, использования и распространения вредоносной компьютерной программы. При этом наступление общественно опасных последствий в виде несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации не является обязательным - достаточно установить, что компьютерная программа или иная компьютерная информация были созданы с целью достижения хотя бы одного из таких последствий.

Состав же преступления, предусмотренного ст. 272 УК РФ, является материальным, то есть для привлечения лица к ответственности по указанной статье, должно наступить одно из последствий, выраженных в диспозиции статьи уничтожение, блокирование, модификация или копирования компьютерной информации.

Сравниваемые преступления отличаются и по субъективной стороне. В отличие от ст. 272 УК РФ, которая допускает как прямой, так и косвенный умысел, субъективная сторона преступления, предусмотренного ч. 1 ст. 273 УК РФ, характеризуется, по нашему мнению, только прямым умыслом, на что указывает признак «заведомость». Виновный должен достоверно знать, что компьютерная программа или иная информация предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

В судебной практике достаточно часто встречается квалификация преступлений, предусмотренных ст.ст. 272 и 273 УК РФ, по совокупности.

Так, «М. с целью распространения среди пользователей ресурсов глобальной сети Интернет вредоносной программы создал программу-вирус «Win95.Vlades 29696», являющуюся вирусом-трояном, который считывает с зараженного компьютера телефон провайдера, логин (имя) и пароль доступа пользователя к сети Интернет, А когда последний соединяется с сетью Интернет, отправляет полученную конфиденциальную информацию пользователя на его (М.) почтовый ящик.

Данную программу-вирус он разместил на принадлежащей ему страничке сети Интернет, которая доступна любому пользователю этой сети. Кроме того, он же с целью получения логина (имя) клиента, его пароля выхода в сеть Интернет и телефон провайдера, посредством копирования таких конфиденциальных данных клиентов через компьютер путем модемной связи осуществил веерную рассылку клиентам файла с созданным им вирусом. Не подозревая о наличии в компьютере вируса, указанные лица в своих целях соединялись с сетью Интернет, и в этот момент программа-вирус отправляла на принадлежащий М. почтовый ящик конфиденциальную информацию в закодированном виде о логинах и паролях названных пользователей.

Перекопировав эту информацию с почтового ящика на свой компьютер, он получил возможность неправомерного доступа к защищенной информации о логинах и паролях потерпевших.

Кроме того, он же с помощью созданной и распространенной им по сети среди клиентов программы-вируса, неправомерно получил на свой электронный почтовый ящик охраняемую законом закодированную информацию о паролях и логинах предприятий»[1].

Таким образом, действия М. верно квалифицированы по совокупности преступлений, предусмотренных ст. ст. 272 и 273 УК РФ, поскольку М,

[1] Сало И.А. Указ. соч. – С. 173 – 174.

создал и распространил вредоносную программу, которая заведомо предназначалась для несанкционирования копирования информации пользователей, а также совершил неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование. То есть злоумышленник сначала запустил в систему вредоносную программу, которая дает возможность скопировать информацию, а затем осуществил неправомерный доступ.

Однако в другом случае суд исключил из обвинения ст. 272 УК РФ как излишне вмененную: «Глухих установил на 3 компьютера гр-на А. программы, правообладателем которой является ЗАО. Установка этих программ осуществлялась им с помощью принадлежащих ему оптических дисков и флэш-носителя, на которые он заранее скачал из сети «Интернет» контрафактные экземпляры этих программ. При установке программного обеспечения Глухих была использована компьютерная информация, которая заведомо для него предназначена для нейтрализации средств защиты указанного программного обеспечения. При запуске этого файла часть оригинальных файлов программного продукта были модифицированы, что позволило использовать этот программный продукт без электронного ключа защиты. Была осуществлена нейтрализация средств защиты компьютерной информации, получен неправомерный доступ к указанному программному обеспечению.

Действия Глухих В.Б. подлежат квалификации по ч.1 ст. 273 УК РФ – использование компьютерной информации, заведомо предназначенной для нейтрализации средств защиты компьютерной информации. Осуществление неправомерного доступа к указанной компьютерной информации в данном случае охватывается этим составом преступления и дополнительной квалификации по ч.1 ст.272 УК РФ не требует, это квалификация подлежит исключению из обвинения»[1].

[1] Дело № 1-79/2012 … из архива Снежинского городского суда Челябинской области за

Ответственность по ст. 274 УК РФ наступает в случае нарушения 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.

Предметом данного преступления является оборудование, позволяющее работать с компьютерной - это средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование.

К средствам хранения, обработки или передачи компьютерной информации относятся средства электронно-вычислительной техники, обеспечивающие реализацию информационных технологий (в частности, компьютер, серверное оборудование и т. д.).

При этом структурно средства электронно-вычислительной техники состоят из совокупности двух взаимодействующих компонентов - системы аппаратных средств (в частности, процессора, карты памяти, видеокарты и т. д.) и системы программного обеспечения (операционной системы, сервисных и иных программ).

Информационно-телекоммуникационная сеть - это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (п. 4 ст. 2 Закона «Об информации»).

Оконечное оборудование означает электронное устройство, используемое для связи пользовательского оборудования (компьютера, мультимедийного терминала и т. д.) с информационно-телекоммуникационной сетью (кабельный модем, сетевая карта).

2012 г. [Электронный ресурс]. – Режим доступа: http://snez.chel.sudrf.ru.

Объективная сторона характеризуется двумя альтернативными деяниями. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации или информационно-телекоммуникационных сетей и оконечного оборудования представляет собой совершение действий (бездействия), связанных либо с нарушением правил эксплуатации аппаратного оборудования, либо с нарушением правил эксплуатации программного обеспечения (например, использование несертифицированного оборудования, нелицензионных программ и т. п.).

Нарушение правил доступа к информационно-телекоммуникационным сетям заключается в совершении действий (бездействия), которые связаны с несоблюдением правил пользования услугами по передаче данных в информационно-телекоммуникационных сетях (например, несогласованная с оператором сети рассылка электронных писем рекламного, коммерческого или агитационного характера, фальсификация пользователем своего *IP*-адреса, получение несанкционированного привилегированного доступа к ресурсам сети и т. п.).

Основным критерием разграничения составов, предусмотренных ст.ст. 272 и 274 УК РФ, является объект преступления. В последнем преступлении непосредственным объектом является внутренняя безопасность информационных систем с точки зрения целостности и конфиденциальности содержащейся в них информации.

С точки зрения объективной стороны разграничение рассматриваемых преступлений осложняется тем, что в качестве последствий в обеих статьях названы уничтожение, блокирование, модификация охраняемой законом компьютерной информации. Однако в ч. 1 ст. 274 указано на обязательное причинение крупного ущерба, в то время как для неправомерного доступа к компьютерной информации данный признак является квалифицирующим.

Основное же отличие составов преступления, предусмотренных ст. 272 и ст. 274 УК РФ, состоит в том, что в первом случае последствия,

перечисленные в диспозиции, наступают в результате неправомерного доступа, а не как результат нарушения 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.

Таким образом, в УК РФ, кроме неправомерного доступа к компьютерной информации, установлена уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 273) и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274). Критериями отграничения данных составов от неправомерного доступа к компьютерной информации являются предмет преступления, характеристика объективной стороны, а также содержание субъективной стороны.

2.2 Соотношение неправомерного доступа к компьютерной информации со смежными преступлениями, предусмотренными иными главами УК РФ

Внедрение информационных технологий в управленческую и производственную деятельность способствует совершению и иных преступлений, в том числе нарушение неприкосновенности частной жизни, нарушение тайны сообщений, нарушение авторских и смежных прав, нарушение изобретательских и патентных прав, мошенничество, незаконное получение кредита, незаконное получение и разглашение сведений, составляющих коммерческую и банковскую тайну, уклонение от уплаты налогов с организаций, сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей и другие.

Рассмотрим лишь разграничение неправомерного доступа к

компьютерной информации с самыми распространенными из перечисленных смежных преступлений.

Нарушение авторских и смежных прав (ст. 146 УК РФ)

В судебной практике нередко возникают вопросы отграничения неправомерного доступа к компьютерной информации от нарушения авторских и смежных прав (ст. 146 УК).

В ряде случаев виновный получает доступ к компьютерной программе, являющейся объектом авторского права, и использует ее в своих интересах. Между тем указанные составы преступлений имеют ряд существенных отличий.

Так как законодатель поместил нормы, предусматривающие ответственность за рассматриваемые преступления, в различных главах Особенной части УК РФ, данные преступления посягают на разные объекты. Видовым объектом нарушения авторских и смежных прав являются конституционные права и свободы человека и гражданина. Непосредственным объектом этого преступления является интеллектуальная собственность. В то время как преступление, предусмотренное ст. 272, посягает на безопасность компьютерной информации.

Существенные различия имеются в предмете рассматриваемых преступлений. Предметом неправомерного доступа является компьютерная информация, охраняемая законом. Предметом нарушения авторских и смежных прав - только объекты авторского права.

При этом следует отметить, что к предметам преступления, предусмотренного ст. 146 УК РФ, в частности, относятся программы для ЭВМ (ст. 1259 ГК РФ). В свою очередь в качестве предмета преступления, предусмотренного ст. 272 УК РФ, может выступать компьютерная программа.

В то же время в Законе «Об информации» закреплено, что положения данного закона «не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации» (ч. 2 ст. 1). Следовательно, определяемый этим законом термин «информация» не может применяться к отношениям с интеллектуальной собственностью.

Для разграничения отношений в сфере авторского и информационного права законодатель использует в указанных актах различную терминологию: в Законе «Об информации» – это «информация» и «обладатель информации», в ГК РФ – «произведение» и «правообладатель».

В связи с этим при квалификации данных преступлений возникают проблемы, так как программа для ЭВМ, являясь произведением, является еще и компьютерной информацией.

Потерпевшим по ст. 146 УК РФ может выступать только автор (правообладатель), в то время как потерпевшим по ст. 272 УК РФ может быть признано любое вменяемое физическое лицо, достигшее 16-ти летнего возраста.

Объективная сторона нарушения авторских и смежных прав в качестве необходимого признака включает наступление общественно опасных последствий в виде причинения крупного ущерба автору объекта авторского права в форме упущенной выгоды или морального вреда. Указанный признак не является обязательным для привлечения виновного к уголовной ответственности по ст. 272 УК РФ. Нарушение авторских и смежных прав связано либо с присвоением авторства, либо с незаконным использованием объектов авторского права.

При неправомерном доступе к компьютерной информации ее дальнейшее использование виновным не обязательно. В то же время возможны ситуации, когда виновный, желая присвоить права автора, копирует компьютерную программу и воспроизведенные копии незаконно использует в своих

преступных целях. В этом случае содеянное виновным подлежит квалификации по совокупности ст. ст. 146 УК и 272, если автору программы был причинен крупный ущерб.

«Менщиков, обладая специальными знаниями по копированию контрафактных программных обеспечений с сети «Интернет», а также по копированию (установке) контрафактных программных обеспечений на электронно-вычислительные машины (далее ЭВМ), с целью получения прибыли за копирование (установку) на принадлежащих заказчикам ЭВМ, контрафактных программных обеспечений, необходимых заказчикам, действуя умышленно, из корыстных побуждений, имея умысел, направленный на незаконное, вопреки воле правообладателя использование объектов авторского права, с целью сбыта, неправомерно приобрел с помощью ЭВМ через сеть «Интернет» контрафактные экземпляры программных продуктов - «Microsoft Office 2007», незаконно скопировав их на машинные носители информации, и с момента приобретения он стал хранить при себе с целью сбыта вышеперечисленные контрафактные экземпляры программных обеспечений, намереваясь сбыть контрафактную продукцию, посредством публичной оферты.

Продолжая свои преступные действия Менщиков, умышленно собственноручно, используя машинные носители информации - съемный жесткий диск емкостью и 20 оптических дисков различных форматов, осуществил копирование (установку) программных обеспечений «Microsoft Office 2007» на жесткий диск электронно-вычислительной машины заказчика, за что получил от него вознаграждение. Подобные действия Менщиков совершал неоднократно, тем самым, нарушил авторские права правообладателя - корпорации «Microsoft» причинив ему ущерб в крупном размере.

Таким образом, Менщиков совершил незаконное приобретение, хранение контрафактных экземпляров произведений в целях сбыта, в крупном размере,

а также неправомерный доступ к охраняемой законом компьютерной информации, повлекшем копирование такой информации из корыстной заинтересованности»[1].

Изучение диспозиций ст. ст. 146 и 272 УК РФ позволило сделать вывод, что данные составы являются смежными, поскольку имеют совпадающий признак – предметом преступления выступает информация. В судебной практике в связи с этим разграничение этих смежных составов нередко представляет определенные трудности. Проблема разграничения таких смежных составов как неправомерный доступ к компьютерной информации и нарушение авторских и смежных прав решается путем установления разграничительных признаков, рассмотренных в настоящем параграфе.

Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ)

В определенных случаях содержание компьютерной информации, к которой осуществляется неправомерный доступ, могут составлять сведения, являющиеся коммерческой, налоговой или банковской тайной. В этом случае интерес представляют вопросы соотношения составов преступлений, предусмотренных ст.ст. 183 и 272 УК РФ.

За нарушение коммерческой, налоговой или банковской тайны уголовная ответственность наступает при собирании сведений, составляющих коммерческую, налоговую или банковскую тайну, а также за незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Предметом преступного посягательства, предусмотренного ст. 183 УК РФ, может являться компьютерная информация, в которой тайна находит

[1] Дело № 1-348/2012 … из архива Златоустовского городского суда Челябинской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://zlatoust.chel.sudrf.ru.

свое отражение в виде символов, образов, сигналов, технических решений, процессов и т. д. Так как тайна в любом случае является охраняемой законом информацией, значит, в отношении нее может быть осуществлен неправомерный доступ. Таким образом, предмет этих двух преступлений может совпадать.

Разграничить рассматриваемые преступления можно по объекту посягательства.

«Непосредственным объектом, преступления, предусмотренного ст. 183 УК РФ, являются общественные отношения, возникающие между уполномоченными субъектами по поводу создания, распространения, преобразования и потребления информации, составляющей коммерческую, налоговую или банковскую тайну[1]».

Коммерческая тайна – это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. К информации, составляющей коммерческую тайну, относятся сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании, и в отношении которых обладателем таких сведений введен режим коммерческой тайны, направленные на получение максимальной прибыли при произведенных затратах, например объем выпускаемой продукции и цена ее поставки (ст. 3

[1] Клебанов Л.Р. Уголовно-правовая охрана коммерческой, налоговой и банковской тайны. – М., 2006. – С. 90.

ФЗ «О коммерческой тайне»)[1]. Утечка информации, составляющей коммерческую тайну, как правило, оборачивается для организации убытками.

Содержание банковской тайны определено в ст. 857 ГК РФ. Банковскую тайну составляют сведения о банковском счете и банковском вкладе, операциях по счету и сведения о клиенте.

Вместе с тем, существует перечень сведений, которые не могут составлять коммерческую тайну, который, в соответствии с п. 1 ст. 139 ГК РФ, определяется законом и иными правовыми актами (например, ст. 5 Закона «О коммерческой тайне»). Это может быть информация об учредительных документах, регистрационном удостоверении, лицензии, патенте, о платежеспособности, об уплате налогов и обязательных платежей и пр.

Понятие налоговой тайны содержится в ст. 102 Налогового кодекса РФ. В секрете должны оставаться любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: разглашенных налогоплательщиком самостоятельно или с его согласия; об идентификационном номере налогоплательщика; о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых, является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам); предоставляемых избирательным комиссиям в соответствии с законодательством о выборах по результатам проверок налоговым органом сведений о размере и об источниках доходов кандидата и его супруга, а также об имуществе, принадлежащем кандидату и

[1] Федеральный закон РФ «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ // Российская газета. – 2006. – № 166.

его супругу на праве собственности.

При неправомерном доступе к компьютерной информации, представляющей собой коммерческую, налоговую или банковскую тайну, необходимо применять по совокупности ст. 183 и ст. 272 УК РФ, поскольку законодательством об охране тайны никаких особых условий для компьютерной информации не предусмотрено, и поэтому незаконное получение сведений, ее составляющих, должно наказываться отдельно, а неправомерный доступ к информации – отдельно.

Копирование лицом компьютерной информации, составляющей коммерческую (банковскую или налоговую) тайну иного лица, приведшее к ее разглашению, квалифицируется по ст. 183 УК РФ и по ст. 272 УК РФ. Если копирования компьютерной информации не произошло, то квалифицироваться деяние должно по совокупности преступлений, предусмотренных ч. 1 ст. 183 и ст.ст. 30 и 272 УК РФ.

Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ)

Ответственность за мошенничество в сфере компьютерной информации введена Федеральным законом от 29 ноября 2012 № 207-ФЗ.

Мошенничество в сфере компьютерной информации – специальный состав мошенничества. Совершение данного преступного деяния возможно исключительно посредством использования современных компьютерных технологий.

Согласно ст. 6 Закона «Об информации» информационные ресурсы находятся в собственности юридических и физических лиц, включаются в состав их имущества, на них распространяется действие гражданского законодательства. Преступления в сфере информационных технологий включают взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов (фишинг). Наиболее опасными и распространенными

преступлениями, совершаемыми с использованием сети Интернет, является мошенничество. В частности, инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода мошеннические схемы. Другой пример мошенничества - интернет-аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные с имущественным ущербом.

Объект компьютерного мошенничества полностью совпадает с объектом хищения – это отношения собственности. Как и мошенничество вообще, мошенничество в сфере компьютерных технологий - всегда хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При этом форма объективной стороны содеянного строго ограничена законодателем – это хищение чужого имущества, равно приобретение права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Преступное деяние считается законченным с момента получения виновным суммы денег (чужого имущества), а равно приобретения им

юридического права на распоряжение такими деньгами (имуществом).

Сам по себе факт ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей в зависимости от обстоятельств дела может содержать признаки приготовления к мошенничеству в сфере компьютерной информации или покушения на совершение такого преступления.

В связи с некоторой схожестью объективной стороны деяний возникают вопросы по поводу отграничения ст. 159.6 УК РФ и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности.

Во-первых, разграничение следует проводить по объекту: при мошенничестве вред причиняется отношениям собственности, при неправомерном доступе – безопасности компьютерной информации. В то же время безопасность компьютерной информации может выступать дополнительным объектом мошенничества, а отношения собственности – дополнительным объектом неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности. Предмет данных преступлений также различен. Мошенничество совершается по поводу чужого имущества, неправомерный доступ - по поводу охраняемой законом компьютерной информации.

Объективная сторона рассматриваемых составов на первый взгляд схожа. Но, если при мошенничестве ввод, удаление, блокирование, модификация, либо иное вмешательство являются способами преступления, то, по смыслу диспозиции ст. 272 УК РФ, уничтожение, блокирование, модификация либо копирование информации выступают скорее обязательными последствиями.

С субъективной стороны мошенничество в сфере компьютерной информации и неправомерный доступ отличаются по направленности

умысла.

При мошенничестве умысел направлен на хищение имущества или завладение правом на имущество, при неправомерном доступе из корыстной заинтересованности – на получение определенных сведений, владение которыми будет способствовать получению выгоды имущественного характера, не связанной с незаконным безвозмездным обращением имущества в свою пользу или пользу других лиц, поскольку именно получение такой выгоды понимается под корыстной заинтересованностью в уголовном законе РФ.

Исходя из приведенных отличий рассматриваемых составов, можно сделать вывод о том, что хищение имущества, совершенное путем неправомерного доступа к компьютерной информации, следует квалифицировать по совокупности ст. ст. 159.6 и 272 УК РФ. Но вменяя два состава, в каждом из которых предусмотрен неправомерный доступ, мы действуем по принципу двойного вменения, что недопустимо. Следовательно, содеянное необходимо квалифицировать только по ст. 159.6 УК РФ.

Можно возразить, что включение статьи 159.6 в Уголовный кодекс не обосновано, поскольку хищение имущества или приобретение права на имущество, совершенное путем неправомерного доступа к компьютерной информации, согласно постановлению Пленума Верховного Суда «О судебной практике по делам о мошенничестве, присвоении и растрате», следует квалифицировать по совокупности ст. ст. 159 и 272 УК РФ и подобное положение не вызывало критики.

За неправомерный доступ к компьютерной информации предусмотрено более строгое наказание (ч. 1 ст. 272 – до двух лет лишения свободы, ч.2 – до 6 месяцев лишения свободы). Тогда как за мошенничество в сфере компьютерной информации предусмотрено самое строгое реально применяемое наказание – ограничение свободы на срок до 2 лет. В то же

время при мошенничестве осуществляется еще и завладение имуществом.

Таким образом, учитывая особенности объекта посягательства, способ совершения преступления, вид и размер наказания, мы приходим к выводу о нецелесообразности выделения ст. 159.6 УК РФ как отдельного состава, а хищение имущества или приобретение права на имущество, совершенное путем неправомерного доступа к компьютерной информации, следует квалифицировать по совокупности ст. ст. 159 и 272 УК РФ.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования особенностей уголовной ответственности за неправомерный доступ к компьютерной информации нами были сделаны вывод и сформулирован ряд предложений по совершенствованию уголовно-правовой нормы, закрепленной в ст. 272 УК РФ и практики ее применения.

Непосредственным объектом неправомерного доступа является безопасность компьютерной информации, т. е. состояние защищенности производства, хранения, передачи, использования и обработки компьютерной информации от различных посягательств.

Предметом данного преступления, согласно ст. 272 УК РФ, является охраняемая законом компьютерная информация, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Однако данное определение не лишено недостатков. Во-первых, термин «компьютерная» определяет принадлежность только к компьютеру, что в условиях сегодняшнего технологического прогресса является некорректным, поскольку современные объекты обращения электронной информации (игровая приставка, цифровая видеокамера, мобильный телефон, телевизор и т. д.) способны выполнять многие из тех функций, которые ранее было возможно осуществить только при помощи компьютера.

Во-вторых, помимо электрических сигналов, компьютерная информация может передаваться и иными способами: с помощью электромагнитных сигналов (Wi-Fi) или оптоволокна, информация по которому передаётся в виде световых сигналов.

Поэтому предлагаем понятие «компьютерная информация» заменить на более широкое понятие «электронная информация», а примечание к ст. 272 УК РФ изложить в следующем виде: «Под электронной информацией

понимаются сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи».

Согласно диспозиции ст. 272 УК РФ, объективная сторона неправомерного доступа к компьютерной информации, включает в себя три обязательных признака: деяние в виде неправомерного доступа к охраняемой законом компьютерной информации; последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации; причинную связь между совершенным деянием и наступившими последствиями.

Неправомерным признается доступ к компьютерной информации лица, не обладающего правами на обращение к данной информации, в отношении которой приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

Уничтожение информации – это утрата информации без возможности ее восстановления, когда законный обладатель информации не может использовать ее по назначению. Блокирование компьютерной информации – временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией при ее сохранности. Модификация компьютерной информации представляет собой любое изменение ее первоначального состояния, осуществляемое без разрешения законного обладателя информации и ущемляющее его интересы. Копирование компьютерной информации – это повторение информации в электронном виде при сохранении ее неизменности.

Полагаем, что перечисленные в диспозиции последствия, по сути, представляют собой самостоятельные активные действия, производимые с компьютерной информацией, которые совершаются виновным во время или после осуществления доступа, то есть при получении возможности манипуляции компьютерной информацией.

Поэтому считаем, что правильнее было бы состав рассматриваемого преступления сформулировать как формальный: «Неправомерный доступ к охраняемой законом компьютерной информации, сопряженный с ее уничтожением, блокированием, модификацией или копированием». Это позволило бы снять многие проблемы квалификации, связанные, в частности, с установлением причинной связи, вины, квалифицирующих обстоятельств и т. д.

По нашему мнению, неправомерный доступ к компьютерной информации может совершаться только умышленно, причем, умысел может быть как прямым, так и косвенным. Установление субъективной стороны данного преступления вызывает существенные сложности у правоприменителя, что связано с законодательной регламентацией объективной стороны. Суды в одних случаях устанавливают умысел только на неправомерный доступ к охраняемой законом компьютерной информации, а в других – и на уничтожение, копирование, модификацию или блокирование информации, что неверно в принципе.

Субъект неправомерного доступа к компьютерной информации – общий, это вменяемое физическое лицо, достигшее 16-ти летнего возраста.

Анализ квалифицированных составов неправомерного доступа выявил ряд проблем, возникающих с установлением отягчающих обстоятельств.

В частности, в ч. 2 ст. 272 установлена ответственность за то же деяние, причинившее крупный ущерб. Если толковать это положение буквально, то причинение крупного ущерба должно наступить в результате совершения только деяния, указанного в части 1, т. е. неправомерного доступа. И в этом случае для квалификации не имеет значения, повлек данный доступ уничтожение, блокирование и т. д. информации или нет. Если же законодатель все-таки имел в виду причинение крупного ущерба в результате наступления любого из указанных в части 1 последствий, то ему надо было формулировать состав именно таким образом, чтобы не допускать

двусмысленное толкование нормы.

С практической точки зрения первый вариант существенно бы облегчил квалификацию преступления, т. к. во втором случае суду придется устанавливать причинную связь, во-первых, между неправомерным доступом и последствиями, указанными в первой части статьи, и, во-вторых, между данными последствиями и причинением крупного ущерба.

Вторым квалифицирующим признаком в ч. 2 ст. 272 назван мотив – корыстная заинтересованность лица. Установление этого признака особых проблем у правоприменителя не вызывает. Однако следует отметить непоследовательность законодателя – обычно этот признак используется в тех составах, где, помимо корыстной, предусмотрена еще и иная личная заинтересованность (например, злоупотребление полномочиями). В остальных случаях указывается на корыстные побуждения.

Предусмотрев в ч. 3 ст. 272 два квалифицирующих признака, связанных с соучастием (группа лиц по предварительному сговору и организованная группа), законодатель, тем самым, не учел влияние формы соучастия на дифференциацию уголовной ответственности с точки зрения общественной опасности деяния. Очевидно, что совершение преступления организованной группой обладает гораздо большей опасностью. Поэтому полагаем, что признак «то же деяние, совершенное организованной группой» необходимо перенести в ч. 4 ст. 272 УК РФ.

И в теории, и в практике отсутствует единое понимание признака «использование лицом своего служебного положения»: либо рассматривать его узко, признавая специальным субъектом только лиц, перечень которых содержится в примечаниях к ст. 285 УК РФ и к ст. 201 УК РФ; либо относить к нему также иных служащих, в том числе коммерческих и некоммерческих организаций, не наделенных управленческими функциями.

Полагаем, что для решения данной проблемы законодателю следовало бы конкретизировать содержание данного признака либо непосредственно в

уголовно-правовой норме, либо в примечании к ст. 272 УК РФ.

Что касается тяжких последствий, предусмотренных в ч. 4 ст. 272 УК РФ, то полагаем, что под ними следует понимать аварии на производстве или на транспорте, причинившие особо крупный материальный ущерб или ранения, гибель людей; нарушение функционирования информационных систем, обеспечивающих государственную или общественную безопасность, если это причинило особо крупный материальный ущерб и т. д.

По нашему мнению, форма вины в отношении данных последствий может быть только неосторожная, иначе в действиях лица должны усматриваться составы умышленных преступлений против личности, собственности, безопасности государства, общественной безопасности и т. д.

В УК РФ, кроме неправомерного доступа к компьютерной информации, установлена уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 273) и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274). Критериями отграничения данных составов от неправомерного доступа к компьютерной информации являются предмет преступления, характеристика объективной стороны, а также содержание субъективной стороны.

Изучение диспозиций ст. ст. 146 и 272 УК РФ позволило сделать вывод, что данные составы являются смежными, поскольку имеют совпадающий признак – предметом преступления выступает информация. В судебной практике в связи с этим разграничение этих смежных составов нередко представляет определенные трудности. Проблема разграничения таких смежных составов как неправомерный доступ к компьютерной информации и нарушение авторских и смежных прав решается путем установления разграничительных признаков.

Сравнительный анализ норм, предусмотренных ст.ст. 272 и 183 УК РФ

привел нас к выводу о том, что копирование лицом компьютерной информации, составляющей коммерческую (банковскую или налоговую) тайну иного лица, приведшее к ее разглашению, должно квалифицироваться по ст. 183 УК РФ и по ст. 272 УК РФ. Если копирования компьютерной информации не произошло, то квалифицироваться деяние должно по совокупности преступлений, предусмотренных ч. 1 ст. 183 и ст.ст. 30 и 272 УК РФ.

Больше всего сложностей может вызвать разграничение неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности, и нового мошенничества в сфере компьютерной информации.

Во-первых, разграничение следует проводить по объекту: при мошенничестве вред причиняется отношениям собственности, при неправомерном доступе – безопасности компьютерной информации. В то же время безопасность компьютерной информации может выступать дополнительным объектом мошенничества, а отношения собственности – дополнительным объектом неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности. Предмет данных преступлений также различен. Мошенничество совершается по поводу чужого имущества, неправомерный доступ - по поводу охраняемой законом компьютерной информации.

Объективная сторона рассматриваемых составов на первый взгляд схожа. Но, если при мошенничестве ввод, удаление, блокирование, модификация, либо иное вмешательство являются способами преступления, то, по смыслу диспозиции ст. 272 УК РФ, уничтожение, блокирование, модификация либо копирование информации выступают скорее обязательными последствиями.

С субъективной стороны мошенничество в сфере компьютерной информации и неправомерный доступ отличаются по направленности умысла.

При мошенничестве умысел направлен на хищение имущества или завладение правом на имущество, при неправомерном доступе из корыстной заинтересованности – на получение определенных сведений, владение которыми будет способствовать получению выгоды имущественного характера, не связанной с незаконным безвозмездным обращением имущества в свою пользу или пользу других лиц, поскольку именно получение такой выгоды понимается под корыстной заинтересованностью в уголовном законе РФ.

Исходя из приведенных отличий рассматриваемых составов, можно сделать вывод о том, что хищение имущества, совершенное путем неправомерного доступа к компьютерной информации, следует квалифицировать по совокупности ст. ст. 159.6 и 272 УК РФ. Но вменяя два состава, в каждом из которых предусмотрен неправомерный доступ, мы действуем по принципу двойного вменения, что недопустимо. Следовательно, содеянное необходимо квалифицировать только по ст. 159.6 УК РФ.

Учитывая особенности объекта посягательства, способ совершения преступления, вид и размер наказания, мы приходим к выводу о нецелесообразности выделения ст. 159.6 УК РФ как отдельного состава, а хищение имущества или приобретение права на имущество, совершенное путем неправомерного доступа к компьютерной информации, следует квалифицировать по совокупности ст. ст. 159 и 272 УК РФ.

Полагаем, что решение названных и иных выявленных в ходе проведенного исследования проблем позволит повысить эффективность противодействия неправомерному доступу к компьютерной информации уголовно-правовыми средствами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Раздел 1 Нормативные правовые акты и иные официальные акты

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. // Российская газета. – 1993. – 25 декабря.
2. Гражданский кодекс Российской Федерации (с измен. и доп.) // Собрание законодательства РФ. – 1994 . – № 32. – Ст. 3301.
3. Уголовный Кодекс Российской Федерации (с измен. и доп.) // Собрание законодательства РФ. – от 17 июня 1996 г. – № 25. – Ст. 2347.
4. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 07 декабря 2011 г. № 420 – ФЗ // Российская газета. – 2011. – № 278.
5. Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ // Российская газета. – 2006. – № 166.
6. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // Российская газета. – 2006. – № 165.
7. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // Российская газета. – 2006. – № 165.
8. Федеральный закон «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01 октября 2008 г. № 164-ФЗ // Российская газета. – 2008.– № 208.
9. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06 марта 1997 г. № 188 // Российская газета. – 1997. – № 51.

10. Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации до 2020 года» от 12 мая 2009 г. № 537 // Российская газета. – 2009.– № 88.
11. Доктрина информационной безопасности РФ: утв. Президентом РФ от 09 сентября 2000 г. № Пр-1895 // Российская газета. – 2000.– № 187.
12. Концепция общественной безопасности в Российской Федерации: утв. Президентом РФ. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/19653.
13. Официальный отзыв от 07.04.2011 г. № 1/общ-1583 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации»». – http://base.consultant.ru
14. Заключение Комитета Государственной Думы по информационной политике, информационным технологиям и связи от 05.07.2011 г. «На проект Федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» (к первому чтению)» // Доступ из СПС «Консультант плюс»

Раздел 2 Использованная литература

1. Алешкин, А.И. Понятие субъекта малого предпринимательства и законодательство, регулирующее правоотношения в данной сфере / А.И. Алешкин // Предпринимательское право. – 2010. – № 7. – С. 23–27.
2. Абов, А.И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации / А.И. Абов. – М.: Прима-Пресс, 2002. – 25 с.

3. Абов, А.И. Экономическая безопасность и компьютерные преступления / А.И. Абов, Э.Э. Велиев, С.Н. Ткаченко. – М.: «Прима-Пресс», 2003. – 24 с.
4. Амелин, Р.В. О возможном решении проблемы неполноты главы 28 УК РФ / Р.В. Амелин // Уголовно-исполнительная система: право, экономика, управление. – 2009. – № 5. – с. 5 – 6.
5. Андреев, Б.В. Расследование преступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. – М.: Юрлитинформ, 2001. – 152 с.
6. Ахраменка, Н.Ф. Родовой объект компьютерных преступлений / Н.Ф. Ахраменка // Проблемы развития юридической науки и совершенствования правоприменительной практики: сб. науч. тр. – Минск: БГУ, 2005. – с. 309 – 314.
7. Батурин, Ю.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие / Ю.М. Батурин, А.М. Жодзишский // Советское государство и право. – 1990. – № 12. – с. 86 – 94.
8. Бикмурзин, М.П. К вопросу о правовой природе и понятии предмета преступления / М.П. Бикмурзин // Соискатель. – 2004. – № 1. – с. 12 – 15.
9. Богомолов, М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации / М.В. Богомолов. – Красноярск, 2002. – 91 с.
10. Борзенков, Г.Н. Курс уголовного права. Особенная часть. Том 4. Учебник для ВУЗов / под ред. Г.Н. Борзенкова, В.С. Комиссарова. – М., 2002. – 672 с.
11. Бородин, А.В. Феномен компьютерных вирусов: элементы теории и экономика существования: учеб. пособие / А.В. Бородин. - Йошкар-Ола: МарГТУ, 2004. – 144 с.

12. Борчева, Н.А. Компьютерные преступления в России (комментарии к Уголовному кодексу РФ) / Н.А. Борчева. – М.: «Прима-Пресс», 2001. – 22 с.
13. Бриллиантов, А.В. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.В. Бриллиантова. – М.: Проспект, 2010. – 1392 с.
14. Буз, С.А. Уголовно-правовые средства борьбы с преступлениями в сфере компьютерной информации / С.А. Буз, С.Г. Спирина. – Краснодар, 2002. – 135 с.
15. Букалерова, Л.А. Некоторые вопросы квалификации преступлений с использованием информации как предмета преступлений и предмета совершения корыстных преступлений / Л.А. Букалерова, А.В. Остроушко // Научные труды РАЮН. – Вып.2. – Т.1. – М., 2002. – с. 405 – 412.
16. Быков, В.М. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ / В.М. Быков, В.Н. Черкасов // Российский судья. – 2012. – № 5. – с. 14 – 19.
17. Бытко, С.Ю. Преступления в сфере компьютерной информации: учеб. пособие для студентов юрид. специальностей / С.Ю. Бытко. – Саратов: изд-во Сарат. гос. ун-та, 2004. – 49 с.
18. Ветров, Н.И. Уголовное право: учебник / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. 4-е изд. испр. и доп. – М.: ИД «Юриспруденция», 2007. – 912 с.
19. Ветров, Н.И. Уголовное право. Особенная часть: Учебник / под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М.: Новый Юрист, 1998. – 768 с.
20. Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: Юрлитинформ, 2002. – 496 с.

21. Волеводз, А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации / А.Г. Волеводз // Российский судья. – 2002. – № 9. – с. 34 – 41.
22. Гаврилин, Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание / под ред. Ю.В. Гаврилина. – М.: Книжный мир, 2003. – 245 с.
23. Гостева, М.Б. Преступления в сфере компьютерной информации: преимущества и недостатки новой редакции / М.Б. Гостева // Проблемы права. – 2012. – № 5 (36) – с. 180 – 181.
24. Григоренко, С.В. Преступления в сфере компьютерной информации / С.В. Григоренко, С.Н. Ткаченко, А.А. Каспаров. – М.: Полтекс, 2003. – 39 с.
25. Гульбин, Ю. Преступления в сфере компьютерной информации / Ю. Гульбин // Российская юстиция. – 1997. – № 10. – с. 24 – 25.
26. Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания / М.Ю. Дворецкий. – Тамбов: Издательство ТГУ. – 2003. – 197 с.
27. Дворецкий, М.Ю. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации: монография / М.Ю. Дворецкий, А.Н. Копырюлин. – Тамбов: Изд- во ТГУ им. Г.Р. Державина, 2006. – 212 с.
28. Демидов, А.А. Сравнительный анализ известных методов уничтожения информации с энергонезависимых носителей / А.А. Демидов. [Электронный ресурс]. – Режим доступа: http://www.ci.ru/inform03_07/bezop.htm.
29. Евдокимов, К.Н. Субъективная сторона неправомерного доступа / К.Н. Евдокимов // Вестник Академии Генеральной Прокуратуры РФ. – 2009. – № 12. – с. 42 – 46.

30. Ефремов, М.А. К вопросу о понятии компьютерной информации / М.А. Ефремова // Российская юстиция. – 2012. – № 7. – с. 50 – 52.
31. Здравомыслов, Б.В. Уголовное право Российской Федерации. Особенная часть: учебник / под ред. Б.В. Здравомыслова. Изд. 2-е, перераб. и доп. – М.: Юристъ, 2000. – 552 с.
32. Золотухин, С.Н. Уголовно-правовые и криминологические аспекты преступлений в сфере компьютерной информации: учебное пособие / С.Н. Золотухин, А.З. Хун. – Краснодар: Краснодарский университет МВД России, 2008. – 137 с.
33. Иванов, А. Предварительная проверка сообщений о неправомерном доступе к компьютерной информации / А. Иванов, Д. Силантьев // Уголовное право. – 2003. – № 4. – с. 117 – 119.
34. Ивановский, П.С. Уголовно-правовая борьба с компьютерными преступлениями / П.С. Ивановский, С.А. Чернышов, А.А. Попков. – М.: ПОЛТЕКС, 2007 – 119 с.
35. Игнатов, А.Н. Уголовное право России. Учебник для ВУЗов. Т. 1. Общая часть / под ред. А.Н. Игнатова, Ю.А. Красикова. – М.: Изд-во НОРМА, 2000. – 639 с.
36. Иногамова-Хегай, Л.В. Уголовное право РФ: в 2 т. Т. 2. Особенная часть / под ред. Л.В. Иногамовой-Хегай. – М., 2002. – 462 с.
37. Казаков, С.Э. Компьютерные преступления в законодательстве США и Канады: учебное пособие / С.Э. Казаков. – Нижний Новгород: Право, 2003. – 264 с.
38. Козаченко, И.Я Уголовное право. Общая часть. Учебник для ВУЗов / отв. ред. И.Я. Козаченко, З.А. Незнамова. – М.: Изд-во НОРМА, 1999. – 516 с.
39. Козаченко, И.Я. Уголовное право. Особенная часть: учебник для ВУЗов / отв. ред. И.Я. Козаченко, З.А. Незнамова, Г.П. Новоселов. – М: Издательская группа НОРМА-ИНФРА-М, 1998. – 768 с.

40. Колобов, В.А. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решения / В.А. Колобов. – Нижний Новгород: Финансовый факультет ННГУ, 2001. – 375 с.
41. Королев, А.Н. Комментарий к ФЗ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» (постатейный) / А.Н. Королев, О.В. Плешакова. – М.: ЗАО Юстицинформ, 2007. – 128 с.
42. Кочои, С. Ответственность за неправомерный доступ к компьютерной информации / С. Кочои, Д. Савельев // Российская юстиция. – 1999. – № 1. – с. 44 – 45.
43. Кочои, С.М. Ответственность за корыстные преступления против собственности / С.М. Кочои. – М.,1998. – 181 с.
44. Кругликов, Л.Л. Уголовное право России. Часть Особенная: учебник для ВУЗов / отв. ред. Л.Л. Кругликов. – М., 2005. – 839 с.
45. Кругликов, Л.Л Комментарий к Уголовному кодексу РФ (постатейный) / отв. ред. Л.Л. Кругликов. – М., 2005. – 1104 с.
46. Крылов, В.В. Информационные компьютерные преступления / В.В. Крылов. – М.: ИНФРА-М-НОРМА, 1997. – 285 с.
47. Кудрявцев, В.Н. Российское уголовное право. Особенная часть / под ред. В.Н. Кудрявцева, А.В. Наумова. – М.: Юристъ, 1997. – 496 с.
48. Кудрявцев, В.Н. Уголовное право. Особенная часть: учебник / под ред. В.Н. Кудрявцева, А.В. Наумова. 2-е изд. – М., 2000. – 493 с.
49. Кузнецов, А.П. Ответственность за преступления в сфере компьютерной информации: учеб.-практ. пособие / А.П. Кузнецов. – Нижний Новгород: Нижегородская правовая академия, 2007. – 127 с.
50. Максимов, В.Ю. Компьютерные преступления (вирусный аспект) / В.Ю. Максимов. – Ставрополь: Кн. изд-во, 1999. – 112 с.

51. Методические рекомендации по расследованию преступлений в сфере компьютерной информации. – М.: КМУ Следственный комитет при МВД России, 1997. – 30 с.
52. Наумов, А.В. Российское уголовное право. Курс лекций: в 3 т. Т. 3. Особенная часть (главы XI—XXI) / А.В. Наумов. – М.: Волтерс Клувер, 2007. – 656 с.
53. Наумов, А.В. Уголовное право. Общая часть: курс лекций / А.В. Наумов. – М., 1996. – 560 с.
54. Наумов, В.Б. Отечественное законодательство в борьбе с компьютерными преступлениями / В.Б. Наумов. – http://www.russianlaw.net/law/computer_crime/a01.
55. Наумов, А.В. Комментарий к Уголовному кодексу Российской Федерации / отв. ред. А.В. Наумов. – М.: Юрист, 1996. – 824 с.
56. Научно-практический комментарий к Уголовному кодексу Российской Федерации в двух томах. Том 2. – Нижний Новгород: Изд. НОМОС, 1996. – 608 с.
57. Никифоров, Б.С. Об объекте преступления / Б.С. Никифоров // Советское государство и право. – 1948. – № 9. – с. 46 – 50.
58. Озерский, С.В. Компьютерные преступления: методы противодействия и защиты информации: учебное пособие / С.В. Озерский, Ю.Н. Лазарев, А.Ю. Лавров. – Саратов: Саратовский юридический институт МВД России, 2004. – 114 с.
59. Пантелеев, И.А. Криминологические и уголовно-правовые вопросы борьбы с компьютерной преступностью: учеб. пособие / И.А. Пантелеев, Г.Г. Смирнов. – Екатеринбург, 2004. – 94 с.
60. Познышев, С.В. Учебник уголовного права: Общая часть. Очерк основных начал общей и особенной части уголовного права. Т. 1 / С.В. Познышев. – М., 1923. – 300 с.

61. Попов, А.Н. О предмете преступления, предусмотренного ст. 272 УК РФ / А.Н. Попов // Криминалистъ. – 2008. – № 1. – с. 5 – 10.
62. Радченко, В.И Комментарии к УК РФ / отв. ред. В.И. Радченко, науч. ред. А.С. Михлин. – М.: ТК Велби, Издательство Проспект, 2008. – 704 с.
63. Рарог, А.И. Уголовное право России. Общая часть: учебник / под ред. А.И. Рарога. – М., 2009. – 496 с.
64. Селиванов, Н.А. Пособие для следователя. Расследование преступлений повышенной опасности / под ред. Н.А. Селиванова и А.И. Дворкина. – М., 1998. – 444 с.
65. Сергиевский, И.Д. Русское уголовное право. Общая часть: пособие к лекциям / И.Д. Сергиевский. – СПб., 1908. – 452 с.
66. Скуратов, Ю.И. Комментарий к Уголовному кодексу Российской Федерации / под ред. Ю. И. Скуратова и В. М. Лебедева. – М.: ИНФРА-М-НОРМА, 2001. – 832 с.
67. Степанов-Егиянц, В.Г. Субъективная сторона компьютерных преступлений / В.Г. Степанов-Егиянц // Бизнес в законе. – 2013. – № 2. – с. 72 – 74.
68. Таций, В.Я. Объект и предмет преступления в советском уголовном праве / Т.Я Таций. – Харьков, 1988. – 198 с.
69. Ткачев, А.В. Исследование компьютерной информации в криминалистике / А.В. Ткачев // Эксперт-криминалист. – 2012. – № 4. – с. 5 – 8.
70. Трайнин, А.Н. Учение о составе преступления / А.Н. Трайнин. – М., 1946. – 185 с.
71. Чекунов, И.Г. Криминологические и уголовно-правовые аспекты предупреждения киберпреступлений / И.Г. Чекунов // Российский следователь. – 2013. – № 3. – с. 36 – 43.

72. Чучаев, А.И. Постатейный комментарий к Уголовному кодексу РФ / под ред. А.И. Чучаева. – М.: ИНФРА-М: КОНТРАКТ, 2004. – 819 с.
73. Юсупов, Р.М. Научно-методологические основы информатизации / Р.М. Юсупов. – СПб.: Наука, 2000. – 455 с.
74. Ястребов Д.А. Неправомерный доступ к компьютерной информации: вопросы последствий / Д.А. Ястребов // Проблемы управления безопасностью сложных систем. Труды XIV Международной конференции. В 2-х т. Т. 1. – М.: ИЦ РГГУ, 2006. – с. 74 – 79.
75. Ястребов Д.А. Правовые вопросы обеспечения информационной безопасности (уголовная ответственность за преступления в сфере компьютерной информации в Российской Федерации) / Д.А. Ястребов, С.В. Григоренко; под общ. ред. В.Е. Шаркова. – М.: Издательство «Прима-Пресс», 2007. – 76 с.
76. Ястребов, Д.А. Неправомерный доступ к компьютерной информации / Д.А. Ястребов; под общ. ред. А.А. Тер-Акопова и Г.И. Загорского. 3-е изд. перераб. и доп. - М.: Издательство «Прима-Пресс», 2006. – 200 с.

Раздел 3 Диссертации и авторефераты на соискание ученой степени

1. Айсанов, Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореферат дис. ... канд. юрид. наук / Р.М. Айсанов. – М., 2006. – 29 с.
2. Бикмурзин, М.П. Предмет преступления: теоретико-правовой анализ: дис. ... канд. юрид. наук / М.П. Бикмурзин. – Уфа, 2005. – 196 с.
3. Бражник, С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. канд. ... юрид. наук / С.Д. Бражник. – Ижевск, 2002. – 189 с.

4. Волошин, В.М. Уголовно-правовая политика России в отношении несовершеннолетних правонарушителей и роль ответственности в ее реализации: автореферат дис. ... докт. юрид. наук / В.М. Волошин. – Екатеринбург, 2008. – 363 с.
5. Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореферат дис. ... канд. юрид. наук / У.В. Зинина. – М., 2007. – 33 с.
6. Зубова, М.А. Компьютерная информация как объект уголовно-правовой охраны: автореферат дис. ... канд. юрид. наук / М.А. Зубова. – Казань, 2008. – 26 с.
7. Иманалиева, А.Ж. Проблемы криминалистического учения о предмете преступления: автореферат дис. ... канд. юрид. наук / А.Ж. Иманалиева. – М., 2004. – 28 с.
8. Кабанова, А.Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты): автореферат дис. ... канд. юрид. наук / А.Ж. Кабанова. – Ростов-н/Д, 2004. – 28 с.
9. Карпов, В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дисс. …канд. юрид. наук / В.С. Карпов. – Красноярск, 2002. – 202 с.
10. Крылов, В.В. Основы криминалистической теории расследования преступлений в сфере информации: дис. ...докт. юрид. наук / В.В. Крылов. – М., 1998. – 334 с.
11. Малышенко, Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дисс. ... канд. юрид. наук / Д.Г. Малышенко. – М.:, 2002. – 166 с.
12. Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография / А.Л. Осипенко. – М.: Норма, 2004. – 432 с.

13. Сало, И.А. Преступные действия с компьютерной информацией ограниченного доступа: дисс. … канд. юрид. наук / И.А. Сало. – М., 2001. – 285 с.
14. Смирнова, Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореферат дис. … канд. юрид. наук / Т.Г. Смирнова. – М., 1998. – 26 с.
15. Спиридонова, О.Е. Символ как предмет преступления: автореферат дис. ... канд. юрид. наук / О.Е. Спиридонова. – Казань, 2002. – 20 с.
16. Степанов-Егиянц, В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: автореферат дис. ... канд. юрид. наук / В.Г. Степанов-Егиянц. – М., 2005. – 25 с.
17. Ушаков, С.Ю. Преступления в сфере компьютерной информации (теория, законодательство, практика): дис. ... канд. юрид. наук / С.Ю. Ушаков. – Ростов н/Д, 2000. – 176 с.
18. Шарков, А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дисс. …канд. юрид. наук / А.Е. Шарков. – Ставрополь, 2004. – 174 с.

Раздел 4 Постановления высших судебных инстанций и материалы судебной практики

1. Постановление Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» № 51 от 27 декабря 2007 г. // Российская газета. – 2008. – № 4.
2. Дело № 1-356/2010 … из архива Центрального районного суда г. Челябинска за 2010 г. [Электронный ресурс]. – Режим доступа: http://centr.chel.sudrf.ru.

3. Дело № 1-157/2011 … из архива Октябрьского районного суда города Ижевска Удмуртской Республики за 2011 г. [Электронный ресурс]. – Режим доступа: http://oktyabrskiy.udm.sudrf.ru.
4. Дело № 1-351/2011 … из архива Миасского городского суда Челябинской области за 2011 г. [Электронный ресурс]. – Режим доступа: http://miass.chel.sudrf.ru.
5. Дело № 1-77/2011… из архива Озерского городского суда Челябинской области за 2011 г. [Электронный ресурс]. – Режим доступа: http://ozersk.chel.sudrf.ru.
6. Дело № 1-213/2012 … из архива Белгородского районного суда Белгородской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://belgorodsky.blg.sudrf.ru.
7. Дело № 1-642/2012 … из архива Калужского районного суда Калужской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://kaluga.klg.sudrf.ru.
8. Дело № 1- 100/2012 ... из архива Егорьевского городского суда Московской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://egorievsk.mo.sudrf.ru.
9. Дело № 1-348/2012 … из архива Златоустовского городского суда Челябинской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://zlatoust.chel.sudrf.ru.
10. Дело № 1-139/2012 … из архива Советского районного суда Рязанской области. [Электронный ресурс]. – Режим доступа: http://sovetsky.riz.sudrf.ru.
11. Дело № 1-79/2012 … из архива Снежинского городского суда Челябинской области за 2012 г. [Электронный ресурс]. – Режим доступа: http://snez.chel.sudrf.ru.

12. Дело № 10-11502/2013 … из архива Московского городского суда за 2013 г. [Электронный ресурс]. – Режим доступа: http://www.mos-gorsud.ru.