Введение

В связи с интенсивным развитием информационного общества актуальной задачей юридической науки и практики является совершенствование правового регулирования общественных отношений в сфере обеспечения информационной безопасности.

Практически вся современная человеческая деятельность в той или иной степени связана с компьютерами. Информационные технологии вошли в различные сферы жизни (в оборону, экономику, промышленность, транспорт, образование, культуру, медицину и пр.). Развитая информационная инфраструктура способствует социально-экономическому прогрессу, созданию и распространению научно-технической информации. Объединение компьютеров в сети дает возможность быстрого обмена информацией между пользователями в любом месте земного шара.

В настоящее время в мире насчитывается 3,2 млрд пользователей Интернета (все население Земли составляет 7,2 млрд человек), из них 2 млрд проживают в развивающихся странах. В период с 2000 по 2015 г. удельный вес пользователей сети «Интернет» увеличился почти в семь раз – с 6,5 до 43 % мирового населения[1]. За последние годы Интернет прочно вошел в повседневную и деловую жизнь страны. Россия не отстает и не остается в стороне от глобальных трендов. Российская аудитория Интернета — крупнейшая в Европе, превышает 80 млн пользователей, из них 62 млн человек выходят в онлайн ежедневно[2].

Компьютеризация жизни имеет не только положительные, но и отрицательные стороны. Председатель Правительства РФ Д.А. Медведев точно отметил, что «современные информационно-коммуникаци-

[1] Данные МСЭ по ИКТ за 2015 г. [Электронный ресурс]. – Режим доступа: http://www.itu.int/net/pressoffice/press_releases/2015/pdf/17-ru.pdf. Дата обращения: 10.12.2015.

[2] Российская интернет-аудитория является крупнейшей в Европе [Электронный ресурс]. – Режим доступа: http://www.gazeta.ru/tech/news/2015/12/22/n_8043815.shtml. Дата обращения: 10.12.2015.

онные технологии стали все чаще использоваться для военно-политического противоборства. Кроме того, интернет-технологии взяли на вооружение террористы и преступники. Со всеми этими проблемами многие страны сталкиваются уже постоянно. Эти угрозы нельзя игнорировать».

Конституция РФ в ст. 1 провозгласила Россию правовым государством, главной задачей которого является установление законности и правопорядка в обществе, в том числе путем борьбы с преступностью. Уголовное законодательство, обеспечивающее охрану общественных отношений в сфере высоких технологий, и эффективное использование системы уголовно-правовых мер защиты от преступных посягательств являются залогом успешной борьбы с общественно опасными деяниями в сфере компьютерной информации. Ответственность за совершение компьютерных преступлений впервые была введена в отечественное законодательство с принятием нового Уголовного кодекса РФ (далее – УК РФ). В настоящее время гл. 28 УК РФ именуется «Преступления в сфере компьютерной информации» и содержит три состава – ст. 272 (Неправомерный доступ к компьютерной информации), ст. 273 (Создание, использование и распространение вредоносных компьютерных программ), ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей).

По данным Министерства внутренних дел РФ, в 2006 г. было зарегистрировано 8889 преступлений в сфере компьютерной информации (7337 – ст. 272 УК РФ, 1549 – ст. 273 УК РФ и 3 – ст. 274 УК РФ); в 2007 г. – 7236; в 2008 г. – 9010; в 2009 г. – 11 636; в 2010 г. – 7398; в 2011 г. – 2698; в 2012 г. – 2820; в 2013 г. – 2563; в 2014 г. – 1739; в 2015 г. – 2382 (1396 – ст. 272 УК РФ, 974 – ст. 273 УК РФ, 12 – ст. 274 УК РФ)[1].

В современный период информационная безопасность общества стала неотъемлемой частью национальной безопасности. В Стратегии национальной безопасности России, утвержденной Указом Президента от 31 декабря 2015 г. № 683 г., в п. 22 отмечается появление новых форм противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Одной из угроз военной безопасности РФ является развитие информацион-

[1] Министерство внутренних дел [Электронный ресурс]. – Режим доступа: https://mvd.ru/folder/101762.html. Дата обращения: 19.10.2015.

ных средств ведения войны. Совет Безопасности РФ 5 октября 2015 г. представил проект новой Доктрины информационной безопасности России, в котором указывается, что использование информационного пространства для решения военно-политических задач, а также в террористических и иных целях может нанести серьезный ущерб интересам РФ в информационной сфере.

Разработка мер по борьбе с компьютерной преступностью невозможна без четкой доктрины, определяющей основные направления развития и основные принципы в регулируемой сфере, утвержденной на уровне государства. В России существует Доктрина информационной безопасности от 9 сентября 2000 г. № ПР-1895[1]. Необходимо отметить, что в целом национальная безопасность зависит и от информационной безопасности и с развитием технических средств и информационного общества данная зависимость будет расти. Под информационной безопасностью РФ в Доктрине понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. В Доктрине также выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере. Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны. Вторая составляющая – информационное обеспечение государственной политики РФ. Третья составляющая – развитие современных информационных технологий. Четвертая составляющая – защита информационных ресурсов и телекоммуникационных систем на территории России.

В 2016 г. планируется принятие новой Доктрины информационной безопасности. Секретарь Совета Безопасности РФ Н.П. Патрушев отмечает, что «наблюдается тенденция смещения военных угроз в информационное пространство, в целях актуализации концептуальных основ обеспечения национальной безопасности по решению Совета Безопасности РФ развернута работа по корректировке основных документов стратегического планирования — Стратегии национальной

[1] Российская газета. 28.09.2000. № 187.

безопасности РФ до 2020 года и Доктрины информационной безопасности РФ»[1].

Анализ положений проекта Доктрины информационной безопасности позволяет сделать следующие выводы: государство признает рост компьютерной преступности, особенно в кредитно-финансовой сфере; информационное пространство используется в целях разжигания межнациональной и религиозной ненависти; наблюдается тенденция милитаризации информационного пространства и наращивание гонки информационных вооружений, создающих угрозу международному миру, безопасности и стабильности.

Для выработки эффективных мер борьбы с данным видом преступлений необходимо продолжать исследовать теорию и практику применения законодательства о компьютерных преступлениях. Настоящая монография посвящена анализу общественных отношений, определяющих комплекс теоретических проблем уголовного права, а также обобщению практики применения норм уголовного законодательства, устанавливающего ответственность за преступные посягательства против компьютерной информации.

В ней осуществлен уголовно-правовой анализ составов компьютерных преступлений, предусмотренных ст. 272–274 УК РФ, сформулированы выводы и внесены конкретные предложения по совершенствованию нормативно-правового обеспечения безопасности компьютерной информации.

[1] Из-за новых угроз Россия меняет стратегию национальной безопасности до 2020 г. [Электронный ресурс]. – Режим доступа: https://russian.rt.com/article/89838. Дата обращения: 20.10.2015.

Глава 1. Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ)

§ 1.1. Объект неправомерного доступа к компьютерной информации

Для отграничения неправомерного доступа к компьютерной информации от других преступлений и правонарушений, определения характера и степени общественной опасности деяния, тяжести причиненного или возможного вреда, направленности преступного деяния необходимо установить и определить **объект преступного посягательства**. Установление объекта преступного посягательства служит как бы предварительной программой для выбора той группы смежных составов, среди которых нужно будет уже более тщательно искать необходимую норму[1].

По общему правилу **непосредственным объектом** является какое-либо отдельно взятое отношение[2]. Это положение является спорным. Проведенный анализ научных работ в этой области позволяет сделать вывод об отсутствии единого мнения относительно непосредственного объекта преступлений в сфере компьютерной информации. Точное понимание непосредственного объекта преступления необходимо для правильной квалификации преступления, для определения степени общественной опасности.

Ряд ученых определяют непосредственный объект преступления, предусмотренного ст. 272 УК РФ, через «состояние защищенности»: безопасность информационных систем, базирующихся на использовании ЭВМ, системе ЭВМ или их сети[3]; безопасность деятельности всех

[1] *Кудрявцев В.Н.* Объективная сторона преступления. М.: Госюриздат, 1960. С. 93.
[2] Там же.
[3] См.: *Алескеров В.И., Максименко И.А.* Уголовно-правовая и криминалистическая характеристика современных видов преступлений: Лекция. Домодедово: ВИПК МВД

субъектов, являющихся обладателями информации или операторами информационных систем, по созданию и использованию информации, т.е. по реализации ими своих полномочий в пределах, установленных законом[1]; безопасность использования компьютерной информации, информационных ресурсов и систем[2].

Другие исследователи относят к непосредственному объекту неправомерного доступа к компьютерной информации конкретные права и интересы по поводу ее использования: право владельца системы на неприкосновенность информации, содержащейся в системе[3]; конкретные права и интересы, охраняемые уголовным законом, подвергшиеся посягательству в результате совершения общественно опасного деяния[4]; права на информацию ее владельца и третьих лиц[5]; охраняемые законом права и интересы общества, государства, физических и юридических лиц в сфере владения, распоряжения, пользования компьютерной информацией[6]. Представляется не совсем верным определение непосредственного объекта преступления, предусмотренного ст. 272 УК РФ, через ущерб какому-либо социальному благу и через состояние защищенности информации, поскольку в теории уголовного права преступление направлено на изменение общественных отношений, а не на причинение вреда социальному объекту и не на нарушение какого-либо состояния.

Следует согласиться с теми учеными, которые определяют непосредственный объект неправомерного доступа к компьютерной информации через посягательство на общественные отношения как

России, 2011. С. 10; *Крылов В.В.* Криминалистические проблемы оценки преступлений в сфере компьютерной информации // Уголовное право. 1998. № 3. С. 83.

[1] *Зинина У.В.* Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Дис. ... канд. юрид. наук, М., 2007. С. 95.

[2] Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева и А.В. Наумова. М.: Юристь, 1997. С. 346. (Авторы главы – С.В. Бородин и С.В. Полубинская).

[3] *Клепицкий И.А.* Преступления в сфере компьютерной информации // Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. Б.В. Здравомилова. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2000. С. 352.

[4] *Дворецкий М.Ю.* Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография. Тамбов: Изд-во ТГУ, 2003, С. 46.

[5] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Отв. ред. В.М. Лебедев. 13-е изд., перераб. и доп. М.: Юрайт, 2013. С. 634, 640, 642.

[6] *Евдокимов К.Н.* Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации (по материалам Восточно-Сибирского региона): Дис. ... канд. юрид. наук. Иркутск, 2006. С. 68.

отношения, обеспечивающие безопасность (неприкосновенность) компьютерной информации[1]; как общественные отношения по соблюдению и обеспечению безопасности законного получения, обработки и использования компьютерной информации, а также нормального функционирования компьютерной техники[2]; как совокупность отношений, возникающих по поводу обеспечения безопасности компьютерной информации и ее носителей[3].

Под **непосредственным объектом** неправомерного доступа к компьютерной информации автор полагает возможным понимать общественные отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу.

При исследовании объектов непосредственного доступа к компьютерной информации целесообразно вкратце остановиться на таком понятии, как «дополнительный объект неправомерного доступа». Дополнительный объект — это общественные отношения, заслуживающие самостоятельной защиты применительно к целям и задачам издания конкретной нормы, которые охраняются законом лишь попутно, так как они неизбежно ставятся в опасность причинения вреда при посягательстве на основной объект[4].

Дополнительный объект повышает степень общественной опасности исследуемого преступления. Им могут быть отношения в области права собственности, в области авторского права, личные права и свободы граждан, неприкосновенность частной жизни. Как правило, наличие дополнительного объекта при совершении деяния, определяемого как неправомерный доступ к компьютерной информации, влечет за собой

---

[1] См.: *Числин В.П.* Уголовно-правовые меры защиты информации от неправомерного доступа: Дис. ... канд. юрид. наук. М., 2004. С. 9; Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. М.: ЮИ МВД РФ, 2003. С. 15; *Мазуров В.А.* Компьютерные преступления: классификация и способы противодействия: Учеб.-практ. пособие. М.: Палеотип; Логос, 2002. С. 27; *Ляпунов Ю., Максимов В.* Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9.

[2] *Буз С.А.* Уголовно-правовые средства борьбы с преступлениями в сфере компьютерной информации / С.А. Буз, С.Г. Спирина. Краснодар, 2002. С. 40.

[3] *Малышенко Д.Г.* Уголовная ответственность за неправомерный доступ к компьютерной информации: Дис. ... канд. юрид. наук. М., 2002. С. 56.

[4] *Фролов Е.А.* Объект уголовно-правовой охраны и его роль в организации борьбы с посягательствами на социалистическую собственность: Автореф. дис. ... д-ра юрид. наук. Свердловск, 1971. С. 25.

квалификацию по совокупности с соответствующими статьями УК РФ. Например, при неправомерном доступе, копировании и распространении компьютерной информации о частной жизни лица действия преступника будут квалифицироваться по совокупности ст. 272 и 137 УК РФ.

Большой научный и практический интерес вызывает вопрос определения **предмета неправомерного доступа** к охраняемой законом компьютерной информации. Под предметом преступления в отечественной уголовно-правовой науке обычно понимается элемент нормального правомерного общественного отношения, воздействуя на который, лицо нарушает (пытается нарушить) охраняемое законом общественное отношение[1]. В последнее время в предмет преступления ученые включают не только материальные объекты, но и объекты нематериального мира. Например, С.В. Землюков относит к предмету преступления как материальные, так и нематериальные блага, по поводу которых существуют общественные отношения: жизнь, здоровье, честь, достоинство, права и свободы, имущество и т.п.[2] А.В. Суслопаров считает предметом рассматриваемых составов «данные»[3].

Ряд отечественных исследователей относят к предмету неправомерного доступа к компьютерной информации технические устройства, на которых эта информация хранится. Существует точка зрения, что предметом любого компьютерного преступления следует признать компьютер как информационную систему, носитель информации[4]. Перекликается с ней позиция, в соответствии с которой предметом преступления выступает компьютерная информация, компьютер, компьютерная система или компьютерная сеть [5].

Однако большинство ученых считают такую точку зрения на предмет преступления, предусмотренного ст. 272 УК РФ, ошибочной.

[1] *Никифоров Б.С.* Объект преступления по советскому уголовному праву. М.: Госюриздат, 1960. С. 130.

[2] Российское уголовное право. Общая часть / Под ред. В.С. Комиссарова. СПб.: Питер, 2005. С. 154.

[3] *Суслопаров А.В.* Информационные преступления: Дис. ... канд. юрид. наук. Красноярск, 2008. С. 124.

[4] Новое уголовное право России. Особенная часть: Учеб. пособие / Г.Н. Борзенков, С.В. Бородин, Б.В. Волженкин, В.С. Комиссаров и др.; под ред. Н.Ф. Кузнецовой. М.: Зерцало, ТЕИС, 1996. С. 273–274.

[5] Информационная безопасность в органах внутренних дел и применение информационных технологий в борьбе с преступностью: Учеб. пособие / А.А. Гайдамакин, А.И. Горев, А.П. Корстов и др. Омск, 2010. С. 85–86.

Ю.В. Гаврилин указывает, что «физическое повреждение компьютера, повлекшее уничтожение информации, хранящейся в нем, не отвечает правовому содержанию общественно опасного действия, присущего преступлению, предусмотренного ст. 272 УК РФ, и, следовательно, не образует основания уголовной ответственности за его совершение»[1]. Представляется, что признание предметом рассматриваемого преступления технических устройств хранения компьютерной информации приведет к трудностям при разграничении преступлений в сфере компьютерной информации и преступлений против собственности.

Преступления, предметом посягательства которых являются технические средства хранения информации, должны относиться к преступлениям против собственности. Завладение персональным компьютером либо машинным носителем информации как имуществом не может квалифицироваться как доступ к компьютерной информации и влечет ответственность за преступления против собственности[2]. Причем даже если деяние, направленное на завладение компьютером, и повлекло за собой уничтожение хранящейся в нем информации, то квалификация по ст. 272 УК РФ неприменима[3]. Следует согласиться, что при совершении данных действий умысел виновного направлен на общественные отношения по охране собственности, а не против компьютерной информации.

В юридической литературе существует точка зрения, относящая к предмету преступного посягательства, предусмотренного ст. 272 УК РФ, «информационную среду, то есть деятельность субъектов, связанную с созданием, преобразованием и потреблением информации»[4]. Данная позиция отождествляет предмет неправомерного доступа к компьютерной информации с деятельностью субъектов отношений и неоправданно расширяет предмет преступного посягательства.

---

[1] *Гаврилин Ю.В.* Расследование неправомерного доступа к компьютерной информации: Учеб. пособие / Под ред. Н.Г. Шурухнова. М.: ЮИ МВД РФ, Книжный мир, 2001. С. 8.

[2] *Волеводз А.Г.* Противодействие к компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. С. 66.

[3] *Айсанов Р.М.* Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: Дис. ... канд. юрид. наук. М., 2006. С. 71.

[4] *Панфилова Е.И.* Компьютерные преступления / Е.И. Панфилова, А.Н. Попов; Науч. ред. проф. Б.В. Волженкин. СПб.: Изд-во СПб. юрид. ин-та Генеральной прокуратуры РФ, 2003. С. 563–564.

Признание предметом преступления деятельности участников отношений, являющейся содержанием объекта преступления, не позволяет отграничивать содержание общественных отношений от предметов материального мира[1].

Некоторые ученые, исследующие проблематику предмета анализируемого преступления, относят к предмету неправомерного доступа к компьютерной информации только компьютерную информацию. В.Ю. Максимов считает, что «информация, в том числе и компьютерная, является, без сомнения, общественным благом и в таком случае может быть определена как предмет компьютерного преступления»[2]. А.Е. Ратникова пишет, что «информация как предмет преступления – это сведения, сообщения о лицах, предметах, фактах, событиях, явлениях и процессах, зафиксированные или не зафиксированные на материальном носителе, воздействуя на которые виновный нарушает общественные отношения, охраняемые законом»[3].

Внутри группы, относящей к предмету неправомерного доступа к компьютерной информации саму компьютерную информацию, выделяется несколько направлений научной полемики вокруг следующих вопросов:

I. Какая компьютерная информация является предметом преступления, предусмотренного ст. 272 УК РФ: только охраняемая законом либо любая компьютерная информация?

II. Применима ли к компьютерной информации категория собственности?

III. Имеет ли компьютерная информация цену и, если имеет, влияет ли ее цена на привлечение к уголовной ответственности?

Рассмотрим все эти аспекты в отдельности.

I. По вопросу охраны информации законом Р.М. Айсанов полагает, что указание в законе на охраняемый характер информации излишне, а исключение из диспозиции ст. 272 УК РФ категории «охраняемая законом» «не приведет к излишнему расширению его границ, а, напротив, позволит более полно охватить уголовно-правовой охраной информацию, ограниченную законом или собственником в полном

[1] *Винокуров В.В.* Предмет преступления: отличие от смежных понятий // Журнал российского права. 2011. № 12. С. 56–63.

[2] *Максимов В.Ю.* Указ. соч. С. 23.

[3] *Ратникова А.Е.* Уголовно-правовое обеспечение права на информацию (сравнительно-правовое исследование): Автореф. дис. ... канд. юрид. наук. М., 2006. С. 8.

доступе»[1]. Автор полагает, что неохраняемой информации в современном информационном поле в условиях постинформационного общества не существует[2]. Перекликается с этой позицией точка зрения Ю. Гульбина, считающего понятие «охраняемая законом компьютерная информация» расплывчатым: неохраняемой информации практически нет, так как если информация не является объектом охраны одного из законодательных актов, то, как правило, она становится объектом охраны другого[3].

А.Г. Волеводз, считая, что «нормы ст. 272 УК РФ направлены на охрану государственных и корпоративных интересов»[4], предлагает ввести в сферу действия ст. 272 УК РФ «всю компьютерную информацию»[5]. А.Н. Копырюлин утверждает, что «уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб собственнику (владельцу, пользователю)[6]. По мнению А.Н. Ягудина, ст. 272 УК РФ защищает любую информацию, имеющую значение для собственника[7].

Сложно согласиться с теми, кто предлагает исключить из диспозиции ст. 272 УК РФ категорию «охраняемая законом» и относить к предмету преступления любую компьютерную информацию. Обратимся к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [8] (далее – ФЗ «Об информации, информационных технологиях и о защите информации»), разделившему информацию в зависимости от доступа к ней на общедоступную информацию и на информацию, доступ к которой ограничен. Согласно ст. 7 данного Закона «к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен», т.е. основными свойствами общедоступной информации являются общеизвестность и отсутствие ограничений

[1] *Айсанов Р.М.* Указ. соч. С. 59.

[2] Там же. С. 58.

[3] *Гульбин Ю.* Преступления в сфере компьютерной информации // Российская юстиция. 1997. № 10. С. 24.

[4] *Волеводз А.Г.* Указ. соч. С. 84.

[5] Там же.

[6] *Копырюлин А.Н.* Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: Дис. ... канд. юрид. наук. Тамбов, 2007. С. 72.

[7] *Ягудин А.Н.* Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: Дис. ... канд. юрид. наук. М., 2013. С. 114.

[8] http://base.garant.ru/12148555/#ixzz4AKOcjMQX. Дата обращения: 08.12.2015.