УДК 311(075.8)

© Ольга Шалагинова
доцент кафедры математики и информатики
Санкт-Петербургского университета
МВД России,
кандидат физико-математических наук, доцент

© Olga Shalaginova
Associate Professor of the Mathematics and Computer Science dept. of the St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation, Ph.D in Physical and Mathematical Sciences, Associate Professor

© Максим Кофейников
курсант факультета № 3
подготовки сотрудников для оперативных подразделений
Санкт-Петербургского университета
МВД России

© Maksim Kofejnikov
Cadet of the Faculty № 3 of Staff Training for operational Units of the St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation

СУБЪЕКТИВНАЯ СТОРОНА НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ЕГО СУБЪЕКТ

Человеческая цивилизация находится в постоянном развитии. Новые технологические разработки позволяют сделать жизнь человека значительно комфортнее. Однако параллельно проходит и иной процесс: по мере появления технических достижений многие из них начинают использоваться для облегчения криминальной деятельности. Так, всеобщая компьютеризация играет значительную роль в деле технологического оснащения преступности. Кроме того, в современном обществе информация закономерно перешла на новую ступень развития, стала товаром, получившим реальную стоимость, в связи с чем стала распространенным предметом посягательства.

Субъективную сторону любого преступления характеризуют такие признаки, как вина, мотив, цель общественно опасного и противозаконного поведения преступника. Все это дает представление

о психологическом состоянии субъекта, нарушающего закон, и отражает связь между сознанием самого преступника и реализуемым поведенческим актом. Касательно незаконного доступа к компьютерной информации уголовно-правовая ответственность этих признаков не равнозначна. Вина — субъективный признак каждого правонарушения. Без вины нет составляющей правонарушения, и для гражданина не может наступить уголовная ответственность. Другой смысл субъективной стороны приобретают такие признаки, как мотив и задача совершить это преступление, которые государство отнесло к факультативным.

Преступления в отношении компьютерной информации — это предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов.

Возникновение и быстрое развитие электронно-вычислительной техники проявили новые виды общественно опасных преступлений. Действенная борьба с ними возможна при наличии соответствующих уголовно-правовых средств.

В главе 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» выделяются преступления в сфере компьютерной информации трех составов:

1) неправомерный доступ к компьютерной информации (ст. 272 Уголовного кодекса Российской Федерации);

2) создание, использование и распространение вредоносных компьютерных программ (ст. 273 Уголовного кодекса Российской Федерации);

3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 Уголовного кодекса Российской Федерации) [1].

Конфиденциальность информации — субъективно определяемое свойство информации, указывающее на необходимость ограниченного круга субъектов, имеющих доступ к этой информации, и обеспечиваемое способностью системы сохранять данную информацию в тайне от субъектов, не имеющих полномочий доступа к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты их законных интересов от других субъектов информационных отношений.

Целостность информации — существование информации в неискаженном виде. Субъектов интересует обеспечение более широкого свойства — достоверности информации, которая складывается из полноты и

точности отображения состояния предметной области и непосредственно целостности информации.

Доступность информации — свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Следственно, для автоматизированных систем можно рассматривать три основных вида угроз:

1. Угроза нарушения конфиденциальности зключается в том, что информация становится известной тому, кто не обладает полномочиями доступа к ней. В компьютерной безопасности угроза нарушения конфиденциальности возникает всякий раз, когда получен доступ к любой секретной информации.

2. Угроза нарушения целостности включает в себя любое умышленное изменение информации. Когда злоумышленники преднамеренно изменяют информацию, это означает, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

3. Угроза отказа служб возникает, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реальное блокирование может быть постоянным: запрашиваемый ресурс никогда не будет получен или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

В уголовно-правовой сфере под субъектом преступления понимается лицо, виновное в совершении преступления и способное нести за свое действие или бездействие уголовную ответственность.

Согласно ст. 272 Уголовного кодекса Российской Федерации, есть следующие категории субъектов неправомерного доступа к охраняемой законом компьютерной информации: общий субъект и специальный субъект.

Так, в соответствии с ч. 1 ст. 272 Уголовного кодекса Российской Федерации, общим субъектом неправомерного доступа к компьютерной информации является вменяемое физическое лицо, достигшее возраста 16 лет, не имеющее права доступа к данной информации [1].

Специальным субъектом преступления является физическое вменяемое лицо, достигшее установленного законом возраста, наделенное или обладающее дополнительными признаками, присущими ему на момент совершения общественно опасного деяния, и способное нести уголовную ответственность за преступление.

Объективная сторона преступления, предусмотренного ст. 272 Уголовного кодекса Российской Федерации, включает в себя три обязательных признака:

1) противоправный доступ к охраняемой законом компьютерной информации;

2) результат в виде уничтожения, блокирования, копирования информации;

3) причинная связь между неправомерным доступом и последствиями, перечисленными в законе.

Доступ к информации — это ознакомление с информацией и ее обработка, в частности копирование, блокирование, преобразование или уничтожение информации, совершенные путем использования программно-технических средств компьютера.

Незаконным доступом будет ознакомление с информацией, ее копирование, блокирование, изменение и уничтожение, совершенные помимо воли собственника — владельца информации или вопреки его воле. Незаконным доступ будет в том случае, когда у виновного отсутствует право копирования, блокирования, изменения и уничтожения информации или он совершает подобные действия с нарушением установленных правил.

Субъективная сторона состава преступления обладает прямым умыслом. Виновный понимает, что создает, использует или распространяет вредоносные программу или файл, очевидно для него приводящие к противоправным действиям, и желает этого.

Раскрывая содержание, следует отталкиваться от распространенного в российской уголовно-правовой системе положения о том, что вина — это психическое отношение гражданина к совершенному опасному действию и его социально тяжелым последствиям, выраженное в форме умысла или неосмотрительности.

Несмотря на это, порядок ст. 272 Уголовного кодекса Российской Федерации не дает прямых указаний о индивидуальной стороне разбираемого преступления, то есть можно с твердостью заявлять о намеренной форме вины в виде прямого или косвенного умысла преступления.

В литературе упоминалась и иная точка зрения. Таким образом, неправомерный доступ к охраняемой законом компьютерной информации может быть произведен только с прямым умыслом. Между тем закон не имеет ограничения по привлечению личности к уголовной ответственности по ст. 272 Уголовного кодекса Российской Федерации в случае совершения такого правонарушения с прямым умыслом. Как показывает практика, преступник не всегда желает наступления катастрофических последствий. Особенно это характерно при совершении такого рода преступлений из мести.

В силу этого положения очевидно, что интеллектуальность момента вины, свойственный составу рассматриваемого преступления, заключается в осознании виновным результата неправомерного доступа к информации, охраняемой законом. Таким образом, виновный понимает не только недействительную суть поведения, но и его общественно тяжелый характер. Виновный понимает потенциал или неминуемость реального наступления социально опасных последствий в виде истребления, блокирования, видоизменения либо копирования компьютерной информации, нарушения работы электронной вычислительной машины (далее — ЭВМ), системы персонального компьютера или их сети. Стало быть, личность представляет характер следствий, осознает их социальную значимость и причинно-следственную зависимость.

Момент вины отражает либо влечение или умышленное допущение наступления указанных результатов, либо как минимум безразличное отношение.

Незаконный доступ к охраняемой законом компьютерной информации, совершенный по неосмотрительности, «опускает» правовое основание для привлечения личности к уголовной ответственности. Так, согласно ч. 2 ст. 24 Уголовного кодекса Российской Федерации, «деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части настоящего Кодекса» [1]. О неосторожности в диспозиции ст. 272 Уголовного кодекса Российской Федерации не сказано. Значит, такое деяние может быть совершено лишь умышленно. В силу этого условия трудно согласиться с мнением авторов научно-практического комментария к Уголовному кодексу Российской Федерации, в котором утверждается, что неправомерный доступ к информации

может совершаться как с умыслом, так и по неосторожности. Неосторожная форма вины может проявляться при оценке лицом правомерности своего доступа к компьютерной информации, а также в отношении неблагоприятных последствий доступа, предусмотренных диспозицией данной нормы уголовного закона. Эти точки зрения противоречат законодательному положению, закрепленному в ч. 2 ст. 24 Уголовного кодекса Российской Федерации, что, в свою очередь, может привести к безосновательному привлечению лица к уголовной ответственности за неосторожность поведения [2].

Поэтому можно сделать вывод о том, что при совершении неправомерного доступа к компьютерной информации выяснение интеллектуальности и волевого момента вины является предпосылкой правильной юридической оценки совершенного.

Задачи противоправного доступа к охраняемой законом компьютерной информации могут быть разнообразными. Признаком содержания анализируемого преступления они не являются, соответственно, на вид преступления не влияют. Все же более точное установление аргументов и целей незаконного доступа к охраняемой законом гиперинформации дает возможность не только обнаружить причины совершения лицом данного преступления, но и назначить виновному строгое наказание.

Чаще всего побуждающим фактором совершения неправомерного доступа к охраняемой законом компьютерной информации оказывается корысть, что поднимает степень указанного преступления. Так, корысть среди других мотивов преступлений в сфере компьютерной информации составляет 66 %. В качестве примера корыстного доступа к компьютерной информации можно привести случай, когда лицо путем подбора пароля внедряется в компьютерную сеть, отвечающую за банковские операции, и незаконно перечисляет определенную сумму денежных средств на свой счет.

Наряду с корыстью рассматриваемые преступления могут совершаться из-за чувства мести, зависти, желания испортить деловую репутацию конкурента, «спортивного интереса» или желания скрыть другое преступление.

Согласно ст. 20 Уголовного кодекса Российской Федерации, субъектом преступления, предусмотренного ч. 1 ст. 272 Уголовного кодекса Российской Федерации, может быть любое физическое лицо, достигшее к моменту преступной деятельности шестнадцатилетнего возраста. Необходимым условием привлечения лица к уголовной ответственности за совершенное незаконное деяние является вменяемость. Невменяемые

лица не могут подлежать уголовной ответственности по ст. 21 Уголовного кодекса Российской Федерации.

В том случае, когда противоправный доступ к охраняемой законом информации реализует представитель юридического лица, то ответственности подлежит непосредственный исполнитель этого преступления.

Формирование кредитных учреждений повлекло возникновение и рост новых видов злоупотреблений в данной сфере преступлений, не наблюдавшихся ранее.

Развиваются и такие новые виды преступлений, как хищения путем несанкционированного входа в компьютерную сеть с использованием векселей, кредитных карточек.

На первом этапе доминировали хищения денежных средств банков с использованием фиктивных платежных документов. Второй этап описывался совершением преступления с использованием финансовых и трастовых компаний. По данным МВД России, «пирамидами» было присвоено не менее 20 триллионов рублей, пострадавшими оказались от 3 до 10 миллионов человек.

Уголовным кодексом Российской Федерации предусмотрено наказание за создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (статья 274).

Можно произвести классификацию преступников (субъектов) по степени вовлеченности в противоправную деятельность, совершающих предусмотренные ст. 272 Уголовного кодекса Российской Федерации преступления [3]:

1. Начинающие. Возраст — от 18 до 30 лет. В основном это лица мужского пола. Образование — техническое: среднее, среднее специальное или высшее (иногда неоконченное). Они имеют средний достаток, позволяющий владеть одним или более компьютерными устройствами. Обладают существенными познаниями в области компьютерных технологий, включая языки программирования, а также программно-аппаратных частей компьютерных устройств. Вместе с тем эти лица не имеют постоянной работы либо их работа связана с компьютерными технологиями (специалисты компьютерных фирм, администраторы баз данных). Они увлекаются компьютерными технологиями. Противоправную деятельность они, как правило, начинают, еще не отдавая себе отчет в том, что их действия являются преступными. Установка на целенаправленное преступное поведение возникает внезапно — в основном под влиянием последовательности удачных взломов средств защиты

лицензионных программных продуктов на собственном и принадлежащих другим лицам компьютерных устройствах.

2. Профессиональные. Принадлежат к старшей возрастной категории. Их возраст — более 25 лет. Доля женщин составляет около 8 %. Их достаток выше среднего. Профессиональные преступники имеют высшее техническое образование, на высоком уровне обладают знаниями в области компьютеров и компьютерных технологий. Многие из профессиональных компьютерных преступников получают второе высшее образование, преимущественно по юридическим или экономическим специальностям. Лица, относящиеся к данной группе, обладают навыками программирования на нескольких языках, глубокими знаниями в области программных средств и устройства аппаратной части компьютерных систем, профессионально работают с различными компьютерными платформами, основными операционными системами и большинством пакетов специализированного программного обеспечения, в совершенстве владеют информацией об основных системах электронных коммуникаций и используют эти знания в противоправной деятельности. Такой тип личности характеризуется устоявшимися взглядами и системой ценностей, а также стойкостью к внешним воздействиям. Они амбициозны, но при этом четко знают цену своим навыкам. Формирование мотивации преступного поведения происходит обычно на стадии изучения компьютерных технологий и первоначально подкрепляется в основном желанием продемонстрировать свое интеллектуальное превосходство, нежели стремлением извлечь прибыль. Постоянно совершенствуются в области методик и средств противоправной деятельности, которые часто разрабатывают сами.

Результаты проведенного исследования позволяют сделать выводы:

1) о необходимости конкретизации состава преступления, предусмотренного ст. 272 Уголовного кодекса Российской Федерации, формы вины, криминализации незаконного владения компьютерной информацией, совершенного из корыстных побуждений;

2) о нецелесообразности снижения возраста уголовной ответственности за преступления против информационной безопасности; кроме того, состав незаконного завладения компьютерной информацией может быть дополнен квалифицирующими признаками и, соответственно, разделен на части, что потребует представления статьи в новой редакции, в которую целесообразно включить совершение таких действий группой лиц по предварительному сговору, сопряженность деяния с несанкционированным доступом к компьютерной информации.

Список основных источников

1. Уголовный кодекс Российской Федерации [Электронный ресурс] : 13 июня 1996 г., № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. Федер. закона от 29.12.2022 г. // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2023.
2. Чернова, Е. В. Информационная безопасность человека : учеб. пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — М. : Юрайт, 2021. — 243 с.
3. Внуков, А. А. Защита информации : учеб. пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — М. : Юрайт, 2023. — 161 с.

THE SUBJECTIVE SIDE OF ILLEGAL ACCESS TO COMPUTER INFORMATION AND ITS SUBJECT

Human civilization is in constant development. New technological developments allow you to make human life much more comfortable. However, in parallel, another process goes through: as technical achievements appear, many of them begin to be used to facilitate criminal activity. So, universal computerization plays a significant role in the technological equipment of crime. In addition, in modern society, the information naturally switched to a new level of development, became a product that received the real value, and therefore became a common subject of encroachment.