Известия Гомельского государственного университета
имени Ф. Скорины, № 5 (146), 2024

УДК 343.3/.7 EDN: UIHEBI

К вопросу об объективных и субъективных признаках несанкционированного доступа к компьютерной информации

О.Г. Шляхтова

В статье приведен анализ объективных и субъективных признаков несанкционированного доступа к компьютерной информации (ст. 349 Уголовного кодекса Республики Беларусь), дано авторское толкование некоторых терминов. Вносятся некоторые предложения по совершенствованию законодательства с учетом современных реалий развития науки и техники.
Ключевые слова: компьютерная информация, несанкционированный доступ, компьютерная система, защита информации, компьютерные данные.

The article contains an analysis of objective and subjective signs of unauthorized access to computer information (Article 349 of the Criminal Code of the Republic of Belarus), the author's interpretation of some terms is given. Some proposals are being made to improve legislation, taking into account the modern realities of the development of science and technology.
Keywords: computer information, unauthorized access, computer system, information protection, computer data.

Введение. В криминалистическом аспекте под объективными и субъективными признаками понимают способ совершения преступления, который характеризуется внешними и внутренними проявлениями поведения субъекта до, в момент и после совершения преступного деяния.

Основная часть. Частью 1 ст. 349 Уголовного кодекса Республики Беларусь (далее – УК) установлена уголовная ответственность за несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда.

Под компьютерной информацией понимается «информация, хранящаяся в компьютерной системе, сети или на машинных носителях, обрабатываемая компьютерной системой либо передаваемая в пространстве с помощью любых программно-технических средств» [1, ст. 4].

Определение термина «компьютерная информация» до сих пор является дискуссионным. Хотя разъяснения данного термина есть в ряде нормативных правовых актов, в том числе и международных, но единого мнения по этому поводу и унифицированного толкования он не получил. Такая неопределенность вызывает некоторое беспокойство. К примеру, в Уголовно-исполнительном кодексе Республики Беларусь есть статья, которая предусматривает осмотр компьютерной информации как самостоятельный вид осмотра [2, ст. 204^1]. В связи с этим необходимо четкое понимание, что выступает объектом осмотра.

В.Ю. Стромов полагает, что «под компьютерной информацией законодатель понимает сведения (данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [3, с. 69]. А.Л. Осипенко утверждает, что «компьютерная информация представляет собой особый вид данных, которые не могут существовать в материальном мире в их первоначальном виде» [4, с. 38].

В данном случае считаем целесообразным рассмотреть технический аспект термина «компьютерная информация». В научной литературе существует мнение, что информация представляет собой данные, закодированные в виде электрических сигналов. Эти данные передаются через каналы связи в форме сообщений, состоящих из символов и знаков. В процессе поступления в компьютер происходит кодирование данных в двоичный код (бинарное представление), в котором они сохраняются. Однако в этой форме данные не могут быть непосредственно восприняты и интерпретированы человеком, и, следовательно, не считаются информацией. Для того чтобы данные стали доступными для человеческого восприятия, осуществляется процесс декодирования, который преобразует двоичный код в форму, понятную человеку, например, текстовую или графическую. Однако даже после декодирования данные требуют дальнейшей когнитивной обработки и субъективной интерпретации для того, чтобы обрести статус информации. Таким образом, данные, которые становятся инфор-

мацией после осмысления человеком, изначально генерируются и обрабатываются с использованием компьютерных технологий. Эти данные сохраняются в оперативной памяти компьютера, передаются через каналы связи, могут быть скопированы, обработаны и модифицированы. Преобразование компьютерных данных в формы, доступные для восприятия, возможно исключительно благодаря использованию программно-аппаратных средств.

Поэтому необходимо сформировать и законодательно закрепить единый подход к определению данного понятия с учётом современных реалий развития науки и техники. Отметим, что в законодательстве зарубежных государств предпочтение отдается термину «данные» (data). В Великобритании к одному из основополагающих нормативных правовых актов, регулирующих правонарушения в информационной сфере, можно отнести Закон 1990 г. «О злоупотреблении компьютером», в котором выделены три вида преступлений, связанных с неправомерным использованием компьютерных технологий: 1) несанкционированный доступ к компьютерным данным; 2) несанкционированный доступ к компьютерным данным с намерением совершить или способствовать совершению дальнейших преступлений; 3) несанкционированное изменение компьютерных данных [5].

Уголовный кодекс Германии предусматривает наступление уголовной ответственности за:

– выведывание данных, особо защищённых от неправомерного доступа, посредством преодоления соответствующей защиты (§202^{a}) и перехват данных (§202^{b}), передаваемых любым непубличным способом, т. е. посредством телекоммуникации (телефон, факс, телетайп и пр.) или компьютерной коммуникации (электронная почта и пр.), независимо от избранной формы (Internet, LAN, VPN и пр.) и независимо от кодировки этих данных или её отсутствия;

– фальсификация данных, существенных для доказательств, введение в заблуждение при оформлении правовых отношений посредством обработки данных (§§ 269, 270);

– изменение данных, компьютерный саботаж (§§ 303^{a}, 303^{b}) [6, с. 314, 382–383, 406] и др.

В международных стандартах понятие данных раскрывается как «представление фактов, понятий или инструкций в форме, приемлемой для общения, интерпретации, обработки человеком или с помощью автоматических средств» [7], а также как «формы представления информации, с которыми имеют дело информационные системы и их пользователи» [8].

В Модельном Уголовном кодексе для государств-участников СНГ также используется термин «компьютерные данные – любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию» [9, ст. 286 прим.].

Конвенция о кибепреступлениях содержит следующее определение данных: «компьютерные данные означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию» [10, ст. 1].

Таким образом, компьютерные данные и компьютерная информация – это взаимосвязанные, но не тождественные понятия. Основные различия состоят в следующем:

1) Природа:

– данные – это необработанные, необобщенные факты, сведения, показатели, которые не несут смысловой нагрузки сами по себе;

– информация – это данные, которые были обработаны, систематизированы и интерпретированы для придания им смысла и значения.

2) Форма представления:

– данные обычно представлены в виде текста, чисел, графиков, аудио/видео записей и т. д.;

– информация представлена в форме сведений, знаний, выводов, умозаключений, которые получены по результатам анализа и разъяснения данных.

3) Назначение:

– данные – это исходный материал, из которого получают информацию;

– информация – это сведения, выводы, интерпретации, полученные на основе анализа данных.

4) Ценность:

– данные сами по себе не имеют большой ценности, пока не будут обработаны и осмыслены;

– информация является более ценной, т. к. она несет смысловую нагрузку и может быть использована для принятия решений и совершения действий.

В связи с этим отличие информации от данных состоит в том, что данные – это фиксированные сведения о чем-либо, хранящиеся на определенном носителе. Информация в свою очередь является результатом обработки этих данных. Например, в базах данных хранятся различные данные, а по определенному запросу система управления базой данных выдает требуемую информацию.

С целью унификации подходов к определению термина и применения в деятельности органов, ведущих уголовный процесс, считаем целесообразным в гл. 31 УК вместо термина «компьютерная информация» использовать термин «компьютерные данные».

Также нет и легального определения понятия «компьютерная система». Н.Ф. Ахраменка понимает под компьютерной системой «организационно упорядоченную совокупность массивов информации и информационных технологий, реализующую информационные процессы, образующим элементом которой является хотя бы одна ЭВМ» [11, с. 815]. В.В. Хилюта трактует данное понятие как «электронно-вычислительную машину и связанное с ней оборудование, функционирующее как единое целое для решения вычислительных задач» [12].

В.В. Лосев считает компьютерную систему синонимом автоматизированной информационной системы «в виде комплекса информационных ресурсов, информационных технологий и программно-технических средств, осуществляющих процессы в человеко-машинном или автоматическом режиме» [13, с. 18].

Ю.В. Харчейкина предлагает «для исключения ошибок в правоприменительной деятельности законодателю следует использовать понятие «информационная система», легальное толкование которого содержится в Законе Республики Беларусь «Об информации, информатизации и защите информации» [14, с. 243].

В целом можно согласиться с мнением Ю.В. Харчейкиной, но отождествлять понятия «компьютерная система» и «информационная система» не стоит. В Законе Республики Беларусь от 10.11.2008 г. № 455-З «Об информации, информатизации и защите информации» под информационной системой понимается «совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств» [15, ст. 1]. Считаем, что компьютерная система и информационная система в целом, взаимосвязанные концепции, но имеющие определенные отличия, которые состоят в следующем:

1) Задачи:

– компьютерная система представлена комплексом аппаратных и программных средств для обработки информации;

– информационная система подразумевает под собой комплексное объединение людей, технологий и процессов для сбора, хранения, обработки, распространения и использования информации.

2) Направленность:

– компьютерная система сконцентрирована на аппаратном и программном обеспечении;

– информационная система кроме технологий охватывает людей, бизнес-процессы и организационные аспекты.

3) Функции:

– компьютерная система выполняет вычислительные, коммуникационные и информационные функции;

– информационная система решает задачи сбора, хранения, обработки и распространения информации для поддержки принятия решений.

4) Применение:

– компьютерная система может быть частью информационной системы;

– информационная система охватывает более широкий спектр организационных задач.

Таким образом, компьютерные системы являются ключевым компонентом информационных систем, но информационные системы включают в себя гораздо больше элементов, нежели только технические средства обработки данных.

Основными компонентами компьютерной системы являются:

1) аппаратное обеспечение (центральный процессор, оперативная память, постоянная память, устройства ввода-вывода (клавиатура, мышь, монитор, принтер), сетевые адаптеры);

2) программное обеспечение (операционная система, прикладные программы (приложения, браузеры, медиаплееры и т. д.), драйверы устройств, системные утилиты);

3) системное программное обеспечение (компиляторы и интерпретаторы, библиотеки, средства разработки).

Таким образом, под компьютерными системами предлагаем понимать комплекс взаимосвязанных аппаратных и программных компонентов, предназначенных для обработки, хранения и передачи информации.

Состав этого преступления материальный. Оно считается оконченным с момента наступления указанных последствий от совершенного действия – несанкционированного доступа к компьютерной информации, сопровождающегося нарушением системы защиты.

Для деяния, предусмотренного ст. 349 УК характерна умышленная форма вины по отношению к совершаемым действиям и неосторожная форма – по отношению к последствиям, поскольку принято считать, что лицо не может заранее предвидеть, какой ущерб последует за деянием, соответственно, желать его наступления также не может.

Статья 1 Закона от 10.11.2008 г. № 455-З «Об информации, информатизации и защите информации» раскрывает содержание понятия доступа к информации как «возможность получения информации и пользования ею» [15].

Согласно Положению о технической и криптографической защите информации, утвержденному Указом Президент Республики Беларусь № 196 от 16.04.2013 г., «несанкционированный доступ к информации – доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа» [16, п. 33]. При этом данное деяние совершается лицом, у которого нет прав на доступ к информации либо лицом, имеющим такое право, но реализовывающее его с нарушением установленного порядка.

Диспозиция ч. 1 ст. 349 говорит о несанкционированном доступе только к компьютерной информации, не указывая при этом на носители, хранящие информацию. Иными словами, можно не иметь доступа к хранящейся информации на компьютере, и при этом иметь доступ к самому компьютеру.

Существует несколько способов несанкционированного доступа: 1) прямой контакт лица с компьютерным оборудованием; 2) дистанционно [17, с. 773].

Такой способ доступа как «с нарушением системы защиты» является обязательным признаком объективной стороны ч. 1 ст. 349. «Защита информации – это комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации» [15, ст. 1]. Как видно из определения, меры по защите информации весьма многообразны. Закон Республики Беларусь «Об информации, информатизации и защите информации» к правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий. К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации. К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации [15, ст. 29].

Защита информации организуется собственником информации, лицом, осуществляющим распространение и (или) предоставление информации, оператором информационной системы либо обладателем информации.

Способами доступа с нарушением защиты могут быть использование чужого имени/пароля, маскировка под законного пользователя, изменение физических адресов технических устройств, взлом системы защиты, хищение носителя информации и др.

Так как состав этого преступления материальный, то обязательным признаком его объективной стороны является понятие «существенный вред», который может быть материальным и нематериальным. Поэтому само по себе ознакомление с информацией, не образующее состава другого преступления (например, коммерческого шпионажа), преступлением не является.

Понятие «существенный вред» – оценочный признак, определяемый судом с учетом всех обстоятельств конкретного дела. В случае материального характера ущерба логично его оценивать на сумму в 40 и более раз превышающую размер базовой величины на день совершения преступления [1, п. 3 гл. 24]. В случае нематериального характера ущерба существенный вред может выражаться в нарушении прав, свобод и законных интересов гражданина, в нарушении общественных и государственных интересов (например, несанкционированный доступ к информационной сети с целью ознакомления с информацией, предназначенной исключительно для служебного пользования).

По субъективной стороне преступление, предусмотренное ч. 1 ст. 349 УК, является неосторожным. Если действие – несанкционированный доступ к компьютерной информации путем нарушения системы защиты – совершается умышленно, то отношение виновного лица к последствиям – неосторожное, что прямо указано в диспозиции рассматриваемой статьи.

Объективная сторона преступления, предусмотренного ч. 2 ст. 349 УК, характеризуется совершением двух альтернативных действий: 1) несанкционированный доступ к компьютерной информации; 2) самовольное пользование компьютерной системой или сетью.

В этой части статьи не указан способ совершения преступления, являющийся обязательным признаком состава, предусмотренного ч. 1, – с нарушением системы защиты.

Часть 2 ст. 349 предусматривает ответственность за два самостоятельных преступления: несанкционированный доступ к компьютерной информации, повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия и самовольное пользование компьютерной системой или сетью, повлекшее по неосторожности те же последствия.

Можем предположить, что признак «самовольности» говорит о несанкционированном доступе к компьютерной системе или сети без разрешения на то владельца, собственника, законного пользователя или уполномоченного лица. По Закону Республики Беларусь от 07.05.2021 г. № 99-З «О защите персональных данных» уполномоченным лицом по защите персональных данных считается «государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах» [17, ст. 1].

При доступе к компьютерной информации в первую очередь представляет опасность возможность ознакомления лица с информацией и в связи с этим устанавливается ограничение на доступ к ней. При самовольном пользовании содержание информации может и не представлять для виновного никакого интереса. Общественная опасность данного деяния заключается в том, что лицо пользуется компьютерной системой или сетью без разрешения, самовольно, для удовлетворения каких-либо потребностей и интересов, в результате чего наступают последствия, перечисленные в ч. 2 ст. 349 [18, с. 775].

Под иными тяжкими последствиями понимаются причинение ущерба в особо крупном размере, уничтожение информации особой ценности, нарушение графиков движения транспортных средств, подачи энергоносителей, создание политической или социальной напряженности в обществе и т. п.

Субъективная сторона преступления, предусмотренного ч. 2 ст. 349, характеризуется неосторожной формой вины по отношению к общественно опасным последствиям в виде легкомыслия или небрежности.

Заключение. Объективная сторона преступления, предусмотренного ст. 349 УК, характеризуется совершением двух альтернативных действий: 1) несанкционированный доступ к компьютерной информации; 2) самовольное пользование компьютерной системой или сетью.

Состав этого преступления материальный. Оно признается оконченным с момента наступления указанных последствий от совершенного действия – несанкционированного доступа к компьютерной информации, сопровождающегося нарушением системы защиты.

Для деяния, предусмотренного ст. 349 УК, характерна умышленная форма вины по отношению к совершаемым действиям и неосторожная форма – по отношению к последствиям, поскольку принято считать, что лицо не может заранее предвидеть, какой ущерб последует за деянием, соответственно, желать его наступления также не может.

Под компьютерными системами предлагаем понимать комплекс взаимосвязанных аппаратных и программных компонентов, предназначенных для обработки, хранения и передачи информации.

С целью унификации подходов к определению понятия и применению в деятельности органов, ведущих уголовный процесс, а также учитывая примеры законодательства зарубежных государств, считаем целесообразным в гл. 31 УК вместо термина «компьютерная информация» использовать термин «компьютерные данные».

Литература

1. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 4 июня 1999 г. : одобрен Советом Республики 24 июня 1999 г. : в ред. Закона Республики Беларусь от 09.03.2023 г., № 256-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

2. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : принят Палатой представителей 24 июня 1999 г. : одобрен Советом Республики 30 июня 1999 г. : в ред. Закона Республики Беларусь от 17.07.2023 г., № 286-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

3. Стромов, В. Ю. Оптимизация уголовной ответственности за несанкционированный доступ к компьютерной информации / В. Ю. Стромов // Преступления в информационной сфере : проблемы расследования, квалификации, реализации ответственности и предупреждения : материалы Международной научно-практической конференции, Тамбов, 14–15 февраля 2013 г. – Тамбов, 2013. – С. 69–73.

4. Осипенко, А. Л. Государственно-частное партнерство в сфере противодействия киберпреступности / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2016. – № 4. – С. 37–44.

5. Computer Misuse Act 1990 [Electronic resource]. – Access mode : https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf. – Accessed date : 18.07.2023.

6. Уголовный кодекс Федеративной Республики Германия – Strafgesetzbuch (StGB). Научно-практический комментарий и перевод текста закона ; пер. с нем. П. В. Головненков. – Потсдам, 2021. – 494 с.

7. ISO / IEC / IEEE 24765-2010 Systems and software engineering – Vocabulary: a representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means [Electronic resource]. – Access mode : https://www.cse.msu.edu/~cse435/Handouts/Standards/IEEE24765.pdf. – Accessed date : 18.07.2023.

8. ISO / IEC 2382: 2015 Information technology – Vocabulary: a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or communication, or processing [Electronic resource]. – Access mode : https://www.iso.org/standard/63598.html. – Accessed date : 18.07.2023.

9. Модельный Уголовный кодекс для государств-участников СНГ (принят постановлением Межпарламентской Ассамблеи государств-участников СНГ, 17.02.1996 г.) (с изм. и доп.) [Электронный ресурс]. – Режим доступа : https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti_i_rekomendatcii_mpa_sng/modelnie_kodeksi_i_zakoni. – Дата доступа : 14.07.2023.

10. Convention on Cybercrime (Budapest, 23.XI.2001) [Electronic resource]. – Access mode : https://rm.coe.int/1680aeb72a. – Accessed date : 14.07.2023.

11. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н. Ф. Ахраменка [и др.] ; под ред. А. В. Баркова, В. М. Хомича. – 2-е изд., с изм. и доп. – Минск, 2010. – 1064 с.

12. Хилюта, В. В. Хищении с использованием компьютерной техники : история и современность [Электронный ресурс]. – Режим доступа : https://bypravo.ru/hishhenie-s-ispolzovaniem-kompyuternoj-tehniki-istoriya-i-sovremennost/. – Дата доступа : 13.07.2023.

13. Лосев, В. В. Преступления против информационной безопасности : методические рекомендации к курсу «Уголовное право Республики Беларусь. Особенная часть» / В. В. Лосев. – Брест, 2000. – 45 с.

14. Харчейкина, Ю. В. Терминологические проблемы уголовного закона в сфере защиты информационной безопасности / Ю. В. Харчейкина // Проблемы укрепления законности и правопорядка: наука, практика, тенденции : сб. науч. тр. – Минск : Изд. центр БГУ, 2018. – Вып. 11. – С. 240–247.

15. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Республики Беларусь, 10 ноября 2008 г., № 455-З : в ред. Закона Республики Беларусь от 10.10.2022 г., № 209-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

16. Положение о технической и криптографической защите информации [Электронный ресурс] : утверждено Указом Президента Республики Беларусь от 16 апреля 2013 г., № 196 : в ред. Указа Президента Республики Беларусь от 22.06.2023 г., № 178 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

17. О защите персональных данных [Электронный ресурс] : Закон Республики Беларусь, 7 мая 2022 г., № 99-З : в ред. Закона Республики Беларусь от 01.06.2022 г., № 175-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

18. Уголовный кодекс Республики Беларусь : научно-практический комментарий / Т. П. Афонченко [и др.] ; под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. – Минск : НЦПИ РБ, 2019. – 1000 с.

Гомельский государственный
университет имени Франциска Скорины

Поступила в редакцию 10.12.2023