ЮРИДИЧНІ НАУКИ

УДК 343.3

К ПРОБЛЕМЕ ЗАКОНОДАТЕЛЬНОЙ ФОРМУЛИРОВКЕ ПРИЗНАКОВ ОБЪЕКТИВНОЙ СТОРОНЫ НЕСАНКЦИОНИРОВАННОГО ВМЕШАТЕЛЬСТВА В РАБОТУ ЭВМ

Дмитрук М.М.
Национальный университет «Одесская юридическая академия»

В статье рассматриваются такие признаки объективной стороны деяния, предусмотренного ст. 361 УК, как: утечка, потеря, подделка, блокирование, искажение процесса обработки, нарушение установленного порядка маршрутизации. Указанные признаки характеризуют такой признак как «общественно опасные последствия». Такое понимание указанных признаков является самым распространенным в литературе. Более детальное исследование этих признаков деяния свидетельствует, что эта точка зрения ошибочна. Такое неверное понимание этих признаков обусловлено их неправильной законодательной формулировкой в ст. 361 УК. Обосновывается, что эти признаки характеризуют действия, а не общественно опасные последствия.
Ключевые слова: несанкционированное вмешательство, работа ЭВМ, преступление, последствия, деяние, статья 361 УК Украины.

За последние несколько десятилетий жизнь большинства людей и общества, в целом, была существенно автоматизирована, в связи с чем, любая повседневная деятельность человека не представляется без электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи (далее – ЭВМ).

Постановка проблемы. Тотальная опосредованность всех общественных отношений информационными технологиями привела к увеличению количества преступлений, совершаемых как с помощью ЭВМ, так и преступлений совершаемых относительно общественных отношений, возникающих в результате использования ЭВМ.

Анализ последних исследований и публикаций. Вопросы уголовной ответственности за несанкционированное вмешательство в работу ЭВМ исследовали в своих работах такие ученые, как: Н.В. Карчевский [1, с. 528], В.Н. Бутузов [2, с. 67-71], Д.С. Азаров [3, с. 304], А.А. Васильев, Д.В. Пашнев [4, с. 34-42], Н.С. Козак [5, с. 154-159] и другие. Однако в указанных работах значение данных признаков объективной стороны рассматривалось в контексте либо всей системы преступлений, ответственность за которую предусмотрена Разделом XVI О. ч. УК Украины либо в контексте общепринятой трактовки признаков объективной стороны указанного деяния.

Выделение нерешенных ранее проблем. В теории уголовного права учеными обращается внимание на проблемы терминов в определении системы деяний, совершаемых с помощью ЭВМ («компьютерные преступления», «преступления в сфере ИТ», «киберпреступления»), а также на проблемы понятий, которые используются для определения признаков преступлений в сфере IT [1, с. 528; 3, с. 304]. Другие ученые, например, В.М. Бутузов, обращают внимание на необходимость системно-структурного противодействия компьютерным преступлениям, выделяя два таких основных аспекта, как: 1) работа с множественными составляющими (объектами, субъектами, мерами) в противодействии компьютерным преступлениям; 2) противодействие компьютерной преступности в рамках системы противодействия общей преступности путем определения особенностей исследуемого вида преступлений [2, с. 67-71]. Выделенные проблемы актуальны, однако состояние обобщения судебной практики и постоянные изменения в информационном законодательстве Украины требуют большего внимания признакам отдельных преступлений в сфере IT, в частности, несанкционированного вмешательства в работу ЭВМ. Рассмотрим некоторые проблемы в определении признаков объективной стороны указанного преступления, в частности, последствий и деяния.

В научной литературе распространено мнение, что объективная сторона несанкционированного вмешательства в работу ЭВМ характеризуется такими последствиями, как: 1) утечка; 2) потеря; 3) подделка; 4) блокирование информации; 5) искажение процесса обработки информации; 6) нарушение установленного порядка маршрутизации компьютерной информации [6, с. 606]. Однако более детальное рассмотрение данных признаков исследуемого деяния свидетельствует, что такая точка зрения ошибочна, поскольку противоречит пониманию этих же признаков в других категориях преступлений, положениям судебной практики, в которых эти признаки трактуются по-иному. По нашему мнению, данные признаки (кроме «уничтожения») характеризуют «деяние», а не «последствие» объективной стороны данного состава преступления.

Целью статьи является исследование значения и роли ряда признаков объективной стороны (утечка, потеря, подделка, блокирование, искажение процесса обработки, нарушение установленного порядка маршрутизации) деяния, ответственность за которое предусмотрена ст. 361 УК,

путем анализа положений информационного законодательства, материалов судебной практики.

Изложение основного материала исследования. Содержание вышеуказанных признаков объективной стороны исследуемого деяния заключается в следующем:

1. «Утечка» определяется как результат действий, которое заключается в том, что информация в системе становится известной или доступной лицам, не имеющим права доступа к ней [7, ст. 1]. Например, лицо К. с целью незаконного получения и дальнейшего использования информации с банковских карточек граждан, вмешалась в работу ЭВМ, установив на банкомате, несанкционированное считывающие устройство для снятия информации с банковских платежных карточек [8] т. е. утечка в судебной практике трактуется как снятие и считывания информации или иными словами – это получение доступа к информации. Однако «снятие» и «считывание» – это действия, а «утечка» в учебной [6, с. 606] и научной литературе [3, с. 125] трактуется как «общественно опасное последствие» несанкционированного вмешательства.

2. «Потеря» информации определяется как «действие, в результате которого информация в автоматизированной системе перестает существовать для физических или юридических лиц, имеющих право собственности на нее в полном или ограниченном объеме» [8 (в редакции закона до 27.03.2014 г.), ст. 1]. Например, лицо С., работая инженером программного обеспечения банка, намереваясь «уничтожить» информацию на его сервере, разместило вредоносное программное обеспечение в активном состоянии в каталогах ОС сервера банка, но реализовать до конца свой умысел не смогло, поскольку в день подачи заявления об увольнении ему было отказано в допуске к серверу [9]. Указанное деяние является оконченным покушением, а понятие «потеря» толкуется как «уничтожение» и свидетельствует, что указанный признак в судебной практике действительно играет роль «преступного последствия».

3. «Подделка» определяется как влияние на носитель информации, передаваемой сетью электросвязи в результате, которого абонент получает сведения, которые не совпадают с теми, что были ему направлены [6, с. 607]. Например, Лицо Д. не санкционированно вмешалась в работу автоматизированной системы компьютерного программного комплекса «Единая система статистики и анализа работы органов прокуратуры Украины» путем предоставления незаконных указаний внести изменения в нее, чем подделало сведения о своевременной подаче апелляционной жалобы [10]. При этом, «подделка» согласно ч. 1 ст. 358 УК Украины в этом же авторитетном учебнике определено как деяние с формальным составом, которое является оконченным с момента совершения действий альтернативно составляющих его объективную сторону [6, с. 590]. Не понятно почему в одном случае «подделка» – это преступное последствие, а в другом – характеристика действий виноватой лица. Использование одного и того же понятия в противоположном значении, как правило, не присуще для науки.

4. Блокирование информации в системе определяется как «действия, в результате которых исключается доступ к информации в системе» [7, ст. 1]. Гражданин Ч., используя телефонное устройство для осуществления несанкционированного вмешательства в работу сетей электросвязи, через электрощитовые, расположенных в подъездах многоэтажных домов, не имея на это разрешения, подключился к сети электросвязи чем блокировал доступ гражданину Г. как абоненту к сети электросвязи [11]. Указанный признак больше характеризует действия, нежели преступное последствие.

5. «Искажение процесса обработки компьютерной информации». Понятие указанного признака в информационном законодательстве отсутствует. Однако в судебной практике этот способ «несанкционированного вмешательства в работу сетей электросвязи» раскрывается, в частности, через понятие «нарушение установленного порядка обработки информации» в виде «монтажа» вредных программных устройств. Например, лицо В. за материальное вознаграждение установила гражданину С. спутниковую антенну, предназначенную для приема спутникового радиосигнала, к которому подключили модифицированный роутер и конвертор, что позволило осуществить несанкционированное декодирования телепрограмм с ограниченным доступом и последующий их просмотр [11].

6. «Нарушение установленного порядка маршрутизации компьютерной информации». «Маршрутизацией» является обмен данными при выполнении операций, в том числе по переводу средств между участниками платежной системы [12], а «нарушение работы автоматизированной системы» определяется как действия или обстоятельства, которые приводят к искажению процесса обработки информации. Указанные определения о нарушении установленного порядка маршрутизации компьютерной информации свидетельствуют, что «искажение» является одним из случаев «нарушения порядка обработки компьютерной информации». Об отражении в судебной практике этого «преступного последствия» можно привести следующий пример. Лицо А., будучи ответственным за построение и настройку каналов связи для ГМС Украины и ГП «Документ», несанкционированно изменил настройки и конфигурацию маршрутизатора путем подключения Центра обработки данных Единого государственного демографического реестра ГМС Украины через сеть Интернет «напрямую» в обход Национальной системы конфиденциальной информации в связи, чем совершил несанкционированное вмешательство в работу ЭВМ ГМС Украины, что привело к искажению процесса обработки и порядка маршрутизации информации [13]. Такая формулировка признаков объективной стороны исследуемого преступления свидетельствует, что «нарушение установленного порядка маршрутизации компьютерной информации» характеризует то каким образом осуществляется «несанкционированное вмешательство в работу ЭВМ» т. е. способ совершение деяния, а не его «преступное последствие».

Рассмотрение признаков несанкционированного вмешательства в работу ЄВМ в информационном законодательстве и их толкование в материалах судебной практики, свидетельствует, что

эти признаки описывают способы несанкционированного вмешательства. Еще раз обратим внимание на понимание этих признаков учеными, которые специально занимались этим вопросом.

А.А. Васильев, Д.В. Пашнев указывают: «Результат преступного воздействия на компьютерную информацию или компьютерную систему следует оценивать в тесной связи с признаками объективной стороны, которые относится к последствиям преступления (утечка, утрата, подделка, блокирование компьютерной информации, нарушение установленного порядка ее маршрутизации (ст. 361 УК), ...» [4, с. 35]. Н.С. Козак указывает: «Составы преступлений, предусмотренные ст. 361, ст. ст. 362-363-1, сконструированы как материальные, а оставшиеся – формальные» [5, с. 156], Далее автор к деяниям, которые причиняют существенный вред, но за которые, по мнению ученого, не установлена ответственность Разделом XVI О. ч. УК Украины, относит «...деяния, которые привели к последствиям указанным в ст. 361 УК, если им не предшествовало несанкционированное вмешательство в работу средств обработки информации (например, воздействие мощным электромагнитным излучателем)» [5, с. 157]; т. е. указанные ученые относят исследуемые признаки деяния к его общественно опасным последствиям.

Д.С. Азаров, характеризуя признаки объективной стороны всех деяний ответственность, за которые предусмотрена Разделом XVI О. ч. УК, в целом, указывает: «Останні зміни ст. 361 КК, внесені 23.12.2003 р. ЗУ № 2289-VI, торкнулися, зокрема, обсягу відповідних суспільно небезпечних наслідків. Нині такими наслідками є витік, втрата, підробка, блокування інформації, спотворення процесу оброблення інформації, порушення встановленого порядку її маршрутизації» [3, с. 124]. Указанное утверждение Д.С. Азарова является спорным, в частности, потому, что на страницу выше ученый указывает: «Способами вчинення втручання може бути введення, зміна, пошкодження, знищення чи блокування інформації, а також інший вплив на інформаційні процеси» [3, с. 123].

Н.В. Карчевский пишет: «Диспозиция ст. 361 УК дает возможность сделать вывод о том, что объективна сторона несанкционированного вмешательства характеризуется такой структурой: деяние – несанкционированное вмешательство...; общественно опасное последствие – утечка, утрата, подделка, блокирование информации, искажение процесса обработки информации, нарушение установленного порядка маршрутизации информации...» [1, с. 124], однако в новой предложенной им редакции ст. 361 «Несанкционированные действия с компьютерными данными» и ст. 362 «Причинение неосторожного вреда через незаконные действия с компьютерными данными» эти же признаки автор указывает в диспозициях статей в качестве способов совершения деяния, а не в качестве последствий [1, с. 516, с. 520].

Выводы и перспективы дальнейшего развития. Исследование признаков несанкционированное вмешательство в работу ЭВМ, по нашему мнению, указывает на ошибочное определение значения «утечки», «подделки», «блокирование информации», «искажения процесса обработки информации», «нарушения установленного порядка маршрутизации информации»: указанные признаки характеризуют способ совершения несанкционированного вмешательства, а не его преступные последствия. Неверное понимание указанных признаков обусловлено их ошибочной законодательной формулировкой в диспозиции ст. 361 УК Украины («несанкционированное вмешательство..., что привело к утечке, потере, подделке, блокированию информации, искажению процесса обработки информации или к нарушению установленного порядка ее маршрутизации»). «Потеря компьютерной информации» является преступным последствием несанкционированного вмешательства в работу ЭВМ (ст. 361 УК).

Пример формулировки объективной стороны деяния, предусмотренного ст. 361 УК, к сожалению, свидетельствует об оторванности законодательного процесса от науки уголовного права. Перспективами дальнейшего исследования данной проблемы могут быть изучение признаков несанкционированного вмешательства в законодательстве других стран, более детальное сопоставление признаков этого деяния с аналогичными понятиями в других системах преступлений УК Украины.

Список литературы:

1. Кримінально-правова охорона інформаційної безпеки України: монограф. / М.В. Карчевський; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. – 528 с.
2. Бутузов В.М. Системно-структурний аналіз як метод дослідження комп'ютерної злочинності // Правова інформатика. – 2011. – № 1. – С. 67-71.
3. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): Монографія. – К.: Атіка, 2007. – 304 с.
4. Васильєв А.А., Пашнєв Д.В. Особливості кваліфікації злочинів у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку // Вісник Кримінологічної асоціації України. – 2013. – № 5. – С. 34-42.
5. Козак Н.С. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку // Збір. наук. праць Ірпінської фінансово-юридичної академії. – Вип. 2. 2013. – С. 154-159.
6. Кримінальне право (Особлива частина): підручник / за ред. О.О. Дудорова, Є.О. Письменського. – [2-ге вид.] – К.: «ВД «Дакор», 2013. – 786 с.
7. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР: [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
8. Вирок Приморського районного суду м. Одесса від 27.06.2013 р., по справі № 522/14602/13-к: http://www.reyestr.court.gov.ua/Review/33870506.

9. Судова практика розгляду справ про злочини у сфері використання ЕОМ, АС та КМ і МЕ: Узагальнення судді ВС України М.І. Гриців та Головного консультанта Управління ВУСП ВС України В.В. Антощук: http://clc. to/JiDkzw.
10. Вирок Печерського районного суду м. Києва від 04.03.2015 р. по справі № 757/3752/15-к: http://www.reyestr.court.gov.ua/Review/42987287.
11. Узагальнення судової практики судами м. Харкова та Харківської області кримінальних справ та проваджень про злочини у сфері використання ЕОМ, систем та КМ і МЕ за період 2012-2014 роки: https://hra.court.gov.ua/sud2090/inf_court/generalization/uzag15k5.
12. Про платіжні системи та переказ коштів в Україні: Закон України від 05.04.2001 р. № 2346-III: [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2346-14.
13. Вирок Солом'янського райсуду м. Києва від 22.01.2018 р., по справі № 760/1167/18: http://reyestr.court.gov.ua/Review/71736592.

Дмитрук М.М.
Національний університет «Одеська юридична академія»

ДО ПРОБЛЕМИ ЗАКОНОДАВЧОГО ФОРМУЛЮВАННЯ ОЗНАК ОБ'ЄКТИВНОЇ СТОРОНИ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕОМ

Анотація
У статті розглядаються такі ознаки об'єктивної сторони діяння передбачено ст. 361 КК, як: витік, втрата, підробка, блокування, спотворення процесу обробки, порушення встановленого порядку маршрутизації інформації. Вказані ознаки характеризують таку ознака як «суспільно небезпечні наслідки». Таке розуміння вказаних ознак є найпоширенішим у літературі. Більш детальне вивчення цих ознак діяння свідчить, що ця точку зору є помилковою. Таке невірне розуміння цих ознак обумовлено їх неправильним законодавчим формулюванням у ст. 361 КК. Обґрунтовується, що вищевказані ознаки, крім «втрати», характеризують діяння, а не соціально небезпечні наслідки.
Ключові слова: несанкціоноване втручання, робота ЕОМ, злочин, наслідки, діяння, стаття 361 КК України.

Dmytruk M.M.
National University «Odessa Law Academy»

TO THE PROBLEM OF LEGISLATIVE FORMULATION OF THE OBJECTS OF THE OBJECTIVE SIDE OF UNAUTHORIZED INTERVENTION IN THE OPERATION OF THE COMPUTER

Summary
The article considers such signs of the objective side of the criminal act provided for in Art. 361 of the Criminal Code of Ukraine, as: leakage, loss, forgery, blocking, failure of the processing process, violation of the established routing order. These signs characterize such at attribute as «socially dangerous consequences». Such an understanding of these features is the most common in the literature. A more detailed study of these signs of the criminal act indicates that this view is erroneous. Such an incorrect understanding of these signs is due to their incorrect legislative formulation in Art. 361 of the Criminal Code. It is substantiated that these signs, except for "loss", characterize actions, and not socially dangerous consequences.
Keywords: unauthorized interference, computer operation, crime, criminal consequences, criminal act, Article 361 of the Criminal Code of Ukraine.