А. Ранзебова,
студентка юридического факультета Ярославского государственного университета им. П.Г. Демидова, Российская Федерация

ФОРМА ЗАКОНОДАТЕЛЬНОГО ВЫРАЖЕНИЯ СПОСОБА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ В ДИСПОЗИЦИИ УГОЛОВНО-ПРАВОВОЙ НОРМЫ

Под способом совершения преступления в теории уголовного права традиционно понимается "совокупность приемов и методов, которые использует преступник в процессе осуществления своего преступного намерения"[1] либо "определенный порядок, последовательность движений и приемов, применяемых для совершения преступления"[2] (операциональный подход). Поскольку преступное деяние есть акт волевого поведения лица, оно обладает двумя взаимосвязанными сторонами: субъективной (внутренней, связанной с психическим отношением лица к совершаемому преступлению, мотивами, эмоциями, целью) и объективирующей ее внешней, исполнительской (действия, последствия, причинная связь). Преступное действие (бездействие) утратило бы свою общественную опасность, если бы не обладало способностью причинять вред социальным отношениям. Характер преступного последствия обусловлен объектом, преступным действием, способом и средствами его совершения. Качественную определенность объективным признакам придают место, время, обстановка, образуя т.н. "объективную обстановку" совершения преступления.

Среди факультативных признаков состава преступления способ выделяется более тесной взаимосвязью с действием. Не выступая лишь объективированной формой последнего, способ представляет собой иное действие, характеризуя основное. Уголовно-правовое значение этой взаимосвязи – в изменении уровня общественной опасности преступления, т.к. способ не только раскрывает качественное своеобразие основного действия (например, особая жестокость), но и свидетельствует о дополнительных силах и факторах, которые применяет лицо для осуществления преступного посягательства на объект уголовно-правовой охраны (использование средств, орудийный способ) либо об особых негативных свойствах личности преступника (использование ядов и т.п.). Указанные свойства способа детерминируют необходимость его закрепления в уголовном законе. В УК 1996 г. 77 статей. из 254, содержащих состав преступления (30%), включают указание на тот или иной способ. В 34 случаях он является конститутивным признаком основного состава, в 67 – квалифицированного, в 16 – особо квалифицированного и в 1-м (ч.4 ст.166 УК РФ) – элементом "особо" особо квалифицированного. Использование способа совершения преступления при конструировании 118 составов обусловливает актуальность анализа законодательной техники при характеристике данного признака объективной стороны.

Традиционно в зависимости от описания способа диспозиции уголовно-правовых норм подразделяются на:

1. содержащие указание на единственный способ;
2. содержащие точный перечень возможных способов совершения преступления;
3. содержащие примерный перечень способов;
4. из формулировки которых может вытекать возможность совершения преступления любым способом[3].

Думается, что гносеологическая ценность данной классификации снижена ввиду неясного основания деления. Очевидно, подразумевается количественный критерий (деление диспозиций в зависимости от количества устанавливаемых способов), возможно указание на единственный способ совершения преступления (ст.161 ч.1 УК РФ), либо формулируется дизъюнктивно с применением союзов "или", "либо" в виде перечня. Перечни как прием

формулировки диспозиции подразделяются на открытое (ст.167 ч.2: "…деяния, совершенные путем поджога, взрыва или иным общеопасным способом…") и закрытые (ст. 230 ч.2).

Открытый перечень может содержать родовой признак указанных способов (ст. 261 ч.2: "…путем поджога или иным общеопасным способом…", либо ссылку на "иные способы" (ст.267 ч.1 УК РФ).

Возможна классификация по наличию указания на способ в диспозиции. Смысл ее в том, что способ подчас закрепляется по умолчанию (implicite), скрыт без отражения в законодательной формулировке. Общественно опасное действие в данном случае объективно совершено без соответствующего способа его исполнения: не может быть истязания без физического насилия, заведомо ложного доноса – без обмана[4]. Данная позиция представляется спорной, поскольку речь идет о фактической имманентности способа действию и о признании указанных диспозиций бланкетными.

Способ также не описан в диспозиции, если не является необходимым признаком состава. К примеру, простое убийство (ч.1 ст.105 УК РФ) может быть совершено многими способами (физическими, химическими, биологическими – в зависимости от средств), но этот признак не будет влиять на квалификацию , а подлежать учету лишь при индивидуализации уголовной ответственности. Кроме того, возможно указание на способ в диспозиции двух видов:

1. указание "позитивное" (т.е. характеристика наличия определенного способа – ст. 105 ч.2 п. "д");
2. "негативное указание", выражающееся в юридической значимости отсутствия того или иного способа совершения преступления (ст.135 УК РФ "совершение развратных действий без применения насилия", где "негативное указание позволяет разграничивать составы ст.132 и 135 УК).

Література

1. Уголовное право России. Часть Общая./ Под ред. Л.Л. Кругликова. – М., 2000. - С. 165.
2. Кудрявцев В.Н. Способ и средства совершения преступления // Сов. гос-во и право. - 1997. - №8.- с.60.
3. См.: Наумов А.В. Российское уголовное право. Часть Общая.- М., 2000. - С.195-196.
4. Панов Н.И. Способ совершения преступления и уголовная ответственность. - Харьков, 1980. - С.91.

Н. Розенфельд,
здобувач наукового ступеня кандидата юридичних наук Інституту держави і права ім. В.М. Корецького НАН України, м. Київ

ПРОГРАМНО-МАТЕМАТИЧНІ ЗАХОДИ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ ЯК ПРЕДМЕТ ЗЛОЧИНУ "НЕЗАКОННЕ ВТРУЧАННЯ В РОБОТУ ЕОМ (КОМП'ЮТЕРІВ), ЇХ СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ"

Сучасний світ неможливо уявити собі без систем зв'язку, серед яких головніше місце займають телекомунікації, які, крім інших систем, включають в себе комп'ютерні мережі: локальні, глобальні та всесвітню мережу Internet. Всесвітня комп'ютерна мережа Internet поповнюється щоденно тисячами користувачів в усьому світі.

При такому зростi суб'єктів зв'язку пропорційно збільшується кількість осіб, які спрямовують свої протиправні дії на шкоду не лише власникам, а й користувачам комп'ютерної інформації.

Комп'ютерна злочинність сучасного світу не знає кордонів, віртуальні злочини належать повною мірою до транснаціональних. При цьому відсутність єдиної системи законодавства щодо кримінальної караності діянь комп'ютерних злочинців робить таку проблему також міжнародною (транснаціональною).

Значні проблеми з приводу кваліфікації діянь комп'ютерних злочинців виникають і з приводу розбіжностей тлумачення норм, що передбачають комп'ютерні злочини. Зокрема, такі складності виникають з приводу тлумачення поняття предмету окремих комп'ютерних злочинів, до яких, насамперед, належить злочин "незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), їх систем та комп'ютерних мереж, що призвело до перекручення або знищення комп'ютерної інформації або носіїв такої інформації", відповідальність за яке передбачено статтею 361 КК України.

Так, з моменту прийняття КК України 2001 року, фахівцями було висловлено низку думок з приводу тлумачення предмет комп'ютерних злочинів, визначених в Розділі XVI КК України.

Окремими фахівцями предмет злочину "Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин (комп'ютерів), їх систем та мереж", передбаченого ст. 361 КК України було визначено: "1. автоматизовані електронно-обчислювальні машини (комп'ютери, АЕОМ); 2. їх системи; 3. комп'ютерні мережі"[1].

Іншою групою укладачів коментаря КК України було зазначено предмет вказаного злочину, як "кілька елементів сфери електронного інформаційного забезпечення життя суспільства: електронно-обчислювальні машини (ЕОМ); програмні матеріали, що забезпечують нормальне функціонування ЕОМ; носії інформації; системи ЕОМ та комп'ютерні мережі"[2].

Крім того, були висловлені два відокремлені визначення поняття предмету даного злочину, в яких альтернативними предметами даного злочину передбачались:

" 1) електронно-обчислювальна машина (...); 2) автоматизовані комп'ютерні системи (АСК) (...); 3) комп'ютерні мережі (...); 4) носії комп'ютерної інформації (...); 5) комп'ютерна інформація (...)" (1)[3];

" 1) автоматизовані електронно-обчислювальні машини (...); 2) системи АЕОМ або автоматизовані системи (...); 3) комп'ютерна мережа (...); 4) носії комп'ютерної інформації (...); 5) Комп'ютерні віруси (...); 6) Комп'ютерна інформація (...); 7) програмні і технічні засоби, призначені для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи та комп'ютерні мережі" (2)[4].

Щодо поняття "комп'ютерна інформація» фахівцями висловлювались формулювання, які значним чином відрізнялись одне від одного, хоча такі тлумачення базувались на нормі Закону України «Про захист інформації в автоматизованих системах», яка була сформульована як « інформація в АС - сукупність усіх даних і програм, які використовуються в АС незалежно від форми їх логічного представлення"[5].

Фахівцями вказувалось, що комп'ютерна інформація - це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному виді, зберігається в відповідних електронних носіях і може використовуватися, оброблятися або змінюватись за допомогою ЕОМ[6].

На нашу думку, комп'ютерна інформація - це авторизована інформація, яка зберігається в електронних носіях, або пересилається між ними, незалежно від її фізичного або логічного представлення, і може використовуватися, оброблятися або змінюватися за допомогою ЕОМ.

Особливу увагу на практиці привертає питання: чи належать захисні паролі, коди, режими доступу до інформації до предмета вказаного злочину? Вирішення такого питання впливатиме на визначення стадії вчинення злочину "Незаконне втручання в роботу електронно-обчислювальних машин, їх систем та комп'ютерних мереж". Це питання постає, насамперед, через те, що вказаний злочин за ознакою покарання належить до злочинів незначної тяжкості, і в відповідності із ст. 15 КК України, кримінальна відповідальність за готування до вчинення якого не наступає.

В.О. Голубєв, В.А. Говловський та В.С. Цимбалюк в переліку інженерно-технічних заходів захисту інформації в автоматизованих системах включають такі види:

- апаратний захист (за допомогою технічних пристроїв);
- програмно-математичний захист (паролі доступу, режими доступу користувачів тощо);
- апаратно-програмний захист (комплексне застосування апаратних і програмних засобів)[7].

Виходячи з визначення поняття "комп'ютерна інформація", засоби програмно-математичного захисту, а саме паролі, коди та режима доступу до ЕОМ, їх систем та комп'ютерних мереж, а також до комп'ютерної інформації та її носіїв, також слід відносити до предмету злочину, передбаченого статтею 361 КК України, через те, що вони:

1. відповідають ознакам "комп'ютерної інформації»;
2. здійснюють захисну функцію інших предметів вказаного злочину.

Захисні системи що належать до апаратно-програмного захисту повинні в частині програмного забезпечення тлумачитись, як різновид комп'ютерної інформації.

При цьому поза увагою залишаються інші захисні заходи, які належать до суто апаратного захисту та, апаратно-програмні заходи в частині апаратного забезпечення.

На нашу думку, програмно-математичні та апаратно-програмні заходи в програмній частині захисту ЕОМ, їх систем та комп'ютерних мереж належать до різновиду комп'ютерної інформації; апаратні та апаратно-програмні заходи захисту в апаратній частині належать до технічного устаткування ЕОМ, їх систем а комп'ютерних мереж.

---

[1] Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року. / За ред. М.І.МЕЛЬНИКА, М.І.ХАВРОНЮКА. – К., "Каннон" "А.С.К." – 2001р. - С. 902.

[2] Науково-практичний коментар до Кримінального кодексу України. Особлива частина. / Під заг. Ред. Потебенька М.О., Гончаренка В.Г. – К., "Форум" – 2001 р. - С 721.

[3] Кримінальне право України. Особлива частина. / За ред. М.І.Бажанова, В.В.Сташиса, В.Я.Тація. –К. –Х. "Юрінком Інтер"–"Право" –2001. - С. 363.

[4] Кримінальне право України. Особлива частина. / За ред. М.І.Бажанова, В.В.Сташиса, В.Я.Тація. –К. –Х. "Юрінком Інтер"–"Право" –2001 р. - С. 363.

[5] Закон України "Про захист інформації в автоматизованих системах". Стаття 1. /ВВР № 31. –1994 р. – С. 286.

[6] Кримінальне право України. Особлива частина. / За ред. М.І.БАЖАНОВА, В.В.СТАШИСА, В.Я.ТАЦІЯ. –К. –Х. "Юрінком Інтер"–"Право" –2001 р. - С. 385.

[7] Кримінальне право України. Особлива частина. / За ред. М.І.БАЖАНОВА, В.В.СТАШИСА, В.Я.ТАЦІЯ. –К. –Х.: "Юрінком Інтер–Право", 2001. - С. 385.