жливість застосування штрафу навіть тоді, коли це не передбачено санкцією статті. Норми, що регулюють призначення умовного засудження містяться у Загальній частині Кримінального кодексу, а норми, які знаходяться у загальній частині розповсюджуються на норми, що знаходяться у Особливій частині Кримінального кодексу. Отже, закріплення у нормах загальної частини того, що при умовному засудженні застосовується штраф, розповсюджується і на норми Особливої частини.

Потрібно зазначити, що вказівка законодавця у ст. 45 КК України на те, що незастосування штрафу при умовному засудженні можливе лише при наявності підстав, передбачених у ст. 44, яка передбачає призначення більш м`якого покарання, чим передбачено законом за даний злочин, є невірним розумінням природи умовного засудження та суперечить загальним положенням кримінального права. При такому викладенні статті закону виходить, що норми загального права визначають однакове додаткове покарання незалежно від злочину, його обставин та особи винного. Доцільним було б зазначити у статті, що штраф не застосовується, якщо суд дійде висновку про недоцільність та неможливість сплати штрафу засудженим.

Слід мати на увазі, що законодавець встановив розмір штрафу в залежності від неоподатковуваних мінімумів прибутків громадян. З таким викладенням виникає ось таке запитання: від часу скоєння злочину до моменту призначення покарання може пройти деякий час, збільшиться неоподатковуваний мінімум прибутків громадян. Тобто, сума штрафу визначається законом не на момент скоєння злочину, а за законом на момент визначення покарання. Це протирічіть ст.6 КК України, в якій сказано, що карність діяння визначається законом, діючим під час скоєння злочину. Доцільним було б у статті закону зазначити, що розмір штрафу визначається виходячи з неоподатковуваного мінімуму прибутку громадян на момент скоєння злочину. Таку точку зору підтримують й практики [5].

*Надійшла до редколегії 21.03.2000*

**Список літератури:**

1. Саввин Н.Ф., Ефимов М.А Условное осуждение и условно-досрочное освобожение от наказания. М., 1963. 2. Ткачевский Ю.М. Освобождение от отбывания наказания. М., 1970. 3. Советское уголовное право. Часть общая. М., 1972.; Наказания, не связанные с лишением свободы / Под ред. И.М. Гальперина / М., 1972. 4. Ломако В.А. Применение условного осуждения. 1976.; Пионтковский А.А. Об условном осуждении или системе испытания. Одесса, 1894. 5. Камынин И., Колесников А. О трудностях толкования нового уголовного законодательства // Законность. 1998. № 11.

*С.О.Орлов*

## Кримінальна відповідальність за комп'ютерні злочини у деяких країнах СНД

По оцінках експертів, у наступному десятилітті країнам що розвиваються, до яких відносяться і країни СНД, буде потрібно забезпечити суттєвий технологічний зріст, щоб стати економічно самостійними і більш конкурентноспроможними на світових ринках. По мірі підвищення залежності

від комп'ютерної технології в усіх країнах виникне необхідність забезпечення того, щоб темпи зросту технологічної залежності не випереджали темпи розвитку відповідних соціальних, юридичних і політичних структур. Тому важливе значення набуває планування заходів безпеки і попередження злочинності паралельно з упровадженням комп'ютерної техніки [1, п. 13].

Однією з основних мір по попередженню та профілактиці злочинності, у тому числі і комп'ютерної, є існування відповідного кримінально-правового законодавства. Єдина норма в українському кримінальному законодавстві, яка безпосередньо встановлює відповідальність за злочини пов`язані з комп'ютерною технікою – це норма статті 198[1] КК України [2]. В диспозиції статті передбачено відповідальність за два самостійних складу злочину: навмисне втручання в роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації; розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації.

Частина друга статті 198[1] КК України передбачає такі кваліфікуючі ознаки: спричинення шкоди у великих розмірах, вчинення злочину повторно, а також за попередньою змовою групою осіб.

Поняття автоматизованих систем, носіїв інформації та інших термінів містяться у законі України "Про захист інформації в автоматизованих системах" від 05 липня 1994 року та в "Положенні про технічний захист інформації в Україні", затвердженого постановою Кабінету Міністрів України від 9 вересня 1994 року [3, 4].

В проекті кримінального кодексу України введено відповідний розділ XVI "Злочини у сфері використання автоматизованих електронно-обчислювальних систем", якій включає три складу злочинів пов'язаних з комп'ютерами [5].

Перший склад міститься у статті 332 "Умисне втручання в роботу автоматизованих електронно-обчислювальних систем", яка практично відтворює статтю 198[1] діючого КК України. Термін "автоматизовані системи" змінено на "автоматизовані електронно-обчислювальні системи" та добавлено таке поняття як комп'ютерна мережа.

Криміналізовані у новому КК України і такі діяння як викрадення, привласнення, вимагання комп`ютерної інформації або заволодіння нею шахрайством, які складають склад злочину передбаченого статтею 333 проекту КК України. В цій статті передбачені такі кваліфікуючи ознаки як вчинення таких дій повторно або за попередньою змовою групою осіб та заподіяння злочином шкоди у великому розмірі.

Третя стаття, яка включена до вищезазначеного розділу є бланкетною нормою, та встановлює відповідальність за порушення правил експлуатації автоматизованих електронно-обчислювальних систем. До об'єктивної сторони цього злочину диспозиція норми статті 334 відносить такі дії як порушення правил експлуатації автоматизованих електронно-обчислювальних систем та настання таких наслідків: викрадення, перекручення чи знищення комп'ютерної

інформації, засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких систем. Суб'єкт злочину у даному випадку спеціальний – це особа яка відповідає за експлуатацію цих систем.

Російське кримінальне законодавство почало достатньо ефективно протидіяти посяганням в сфері комп'ютерної інформації вже з 1 січня 1997 року зі вступом в дію нового кримінального кодексу [6]. До глави 28 КК Російської Федерації "Злочини в сфері комп'ютерної інформації" внесені наступні три склади злочинів:

Неправомірний доступ до комп'ютерної інформації (ст. 272). Дана стаття захищає право володаря на недоторканість інформації в комп'ютерній системі. Цей склад злочину матеріальний та має привести до таких наслідків як знищення, блокування, модифікація або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі.

Створення, використання та розповсюдження шкідливих програм для ЕОМ (ст. 273). В диспозиції цієї статті передбачені такі ж наслідки як і в попередній. Під шкідливими програмами в ст.273 КК РФ розуміються програми спеціально створені для порушення нормального функціонування комп'ютерних програм. Під нормальним функціонуванням розуміється виконання операцій для яких ці програми призначені, визначені в документації на програму.

Порушення правил експлуатації ЕОМ, системи ЕОМ або їх мережі (ст. 274). Норма цієї статті є бланкетною як і відповідна стаття проекту КК України. Але наслідки до яких приводять порушення правил експлуатації ЕОМ відрізняються від тих, які передбачені в статті 334 проекту КК України, до них відносяться: знищення, блокування або модифікація охороняємої законом інформації ЕОМ, якщо це спричинило суттєву шкоду.

Кримінальне законодавство Республіки Бєларусь було оновлене з прийняттям 9 липня 1999 року нового кримінального кодексу [7]. Велика увага в ньому приділяється боротьбі з комп'ютерними злочинами, відповідальність за які передбачена в семі статтях розділу XII "Злочини проти інформаційної безпеки" та ще у деяких статтях особливої частини.

Стаття 349 КК Республіки Бєларусь встановлює відповідальність за несанкціонований доступ до комп'ютерної інформації. В цілому, приведена стаття подібна до статті 272 КК Російської Федерації, але ж вона більш досконала і приведена у відповідність з міжнародними вимогами [1, п.121].

Відповідальність за модифікацію комп'ютерної інформації або внесення заздалегідь неправдивої інформації у комп'ютерну систему, мережу або машинний носій, яке спричинило суттєву шкоду, при відсутності ознак злочину проти власності, встановлює стаття 350 КК Республіки Бєларусь.

Винна особа підлягає відповідальності за комп'ютерний саботаж згідно зі статтею 351 КК Республіки Бєларусь. Під комп'ютерним саботажем розуміється умисне знищення, блокування, приведення у непридатне становище комп'ютерної інформації або програми, або вивід зі строю комп'ютерного обладнання, або руйнування комп'ютерної системи, мережі або машинного носія.

Неправомірне заволодіння комп'ютерною інформацією, як самостійний склад злочину передбачено статтею 352 КК Республіки Бєларусь. Однією із умов при якій данні дії будуть кваліфікуватися як злочин, є настання суттєвої шкоди.

Виготовлення або збут спеціальних засобів для одержання неправомірного доступу комп'ютерної системи або мережі та розробка, використання або розповсюдження шкідливих комп'ютерних програм (так звані "комп'ютерні віруси") складають два самостійних складів злочину, які передбачені статтями 353 та 354 КК Республіки Бєларусь відповідно.

Відповідальність за такий склад злочину як порушення правил експлуатації комп'ютерної системи або мережі встановлюється статтею 355 КК Республіки Бєларусь. На відміну від подібних статей проекту КК України та КК Російської Федерації, суб'єктивна сторона цього злочину визначається змішаною формою вини, тобто саме порушення правил здійснюється умисно, а настання наслідків у вигляді знищення, блокування, модифікації інформації, порушення роботи комп'ютерного обладнання або іншої суттєвої шкоди – з необережності.

На тринадцятому пленарному засіданні восьмого Конгресу ООН по попередженню злочинності і поводженню з правопорушниками, який відбувся в 1990 році була прийнята резолюція, котра закликала активізувати зусилля держав з метою боротьби з комп'ютерними злочинами шляхом розгляду можливості прийняття ряду мір з удосконалення національних законів та процедур, спрямованих на боротьбу з комп'ютерною злочинністю [1, п.18]. Аналізуючи сучасне кримінальне законодавство вищезазначених країн можна визначити, що ведучі держави СНД виконують частково вимоги міжнародних організацій.

*Надійшла до редколегії 24.03.2000*

**Список літератури:**

1. Руководство ООН по предупреждению преступлений, связанных с применением компьютеров, и борьбе с ними // Международный обзор уголовной политики (ООН). - № 43 – 44. – 1994; 2. Уголовный кодекс Украины. – Харьков, 1999; 3. Закон України "Про захист інформації в автоматизованих системах" від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України. – 1994. - № 31, ст.286; 4. Положення "Про технічний захист інформації в Україні" затверджено постановою Кабінету Міністрів України від 9 вересня 1994 року № 632; 5. Кримінальний кодекс України: Проект підготовлений робочою групою КМ України. – 1998; 6. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ; 7. Уголовный кодекс Республики Беларусь от 9 июля 1999 года № 275-З // Ведомости Национального Собрания республики Беларусь от 25 августа 1999 года. - № 24 (314)