Розділ XVI

ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

(Назва розділу XVI із змінами, внесеними згідно із Законом № 908-IV від 05.06.2003)

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, –

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Примітка. Значною шкодою у статтях 361–363[1], якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

(Стаття 361 в редакції Законів № 908-IV від 05.06.2003, № 2289-IV від 23.12.2004)

1. Основним безпосереднім об'єктом злочину є два різні види суспільних відносин. По-перше, це суспільні відносини у сфері інформаційної діяльності щодо комп'ютерної інформації. Така діяльність полягає у здійсненні *інформаційних процесів*, тобто створенні, збиранні, накопиченні, зберіганні, пошуку, розповсюдженні, використанні, споживанні, перетворенні, введенні, копіюванні, зчитуванні, знищенні, реєстрації комп'ютерної інформації тощо. По-друге, це суспільні відносини у сфері обміну інформацією (не лише комп'ютерною) мережами електрозв'язку (телекомунікаційними мережами). *Телекомунікації* – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків чи повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах (ст. 1 ЗУ від 18 листопада 2003 р. №1280–IV «Про телекомунікації»).

Додатковим безпосереднім об'єктом злочину є відносини власності щодо певної інформації, **додатковим факультативним безпосереднім** – відносини у сфері забезпечення режиму обмеженого доступу до певної інформації.

У ст. 361 КК прямо не вказано, яка інформація може бути *предметом* відповідного злочину, але зі змісту норми випливає, що мається на увазі комп'ютерна інформація та (або) інформація, яка передається мережами електрозв'язку.

Комп'ютерна інформація – це відомості про навколишній світ і процеси, які в ньому відбуваються, представлені у формі даних, зафіксованих в електронному вигляді.

Комп'ютерну інформацію слід розглядати одночасно у двох аспектах: інформація як *відомості* про навколишній світ і процеси, які в ньому відбуваються, повідомлення про стан справ, про стан будь-чого тощо; інформація як *дані,* тобто сукупність символів, кодів, сигналів, команд тощо, які знаходять свій вираз у різноманітних комп'ютерних програмах, що забезпечують функціонування та керування комп'ютерною технікою, а також за допомогою

яких певні відомості набувають електронної форми, з ними здійснюються різні операції, вони отримують свій прояв назовні.

Інформація, що передається мережами електрозв'язку, – це відомості, подані у вигляді знаків, сигналів, письмового тексту, рухомих або нерухомих зображень, звуків чи в інший спосіб, що передаються по радіо, проводових, оптичних або інших електромагнітних системах. Отже, зазначене поняття є ширшим за поняття «комп'ютерна інформація» і повністю охоплює останнє, але винятково в частині, що стосується передавання та приймання інформації з використанням мереж електрозв'язку. Відмінність між цими поняттями потрібно шукати передусім у формі фіксування інформації. Комп'ютерна інформація фіксується лише в електронному вигляді, інші види інформації, що передаються мережами електрозв'язку, – в інший спосіб (наприклад, при передаванні інформації телеграфом вона фіксується на папері) чи не фіксуються взагалі (приміром, усне передавання відомостей за допомогою телефонного зв'язку).

Предметом аналізованого злочину не можуть вважатися електронно-обчислювальні машини (комп'ютери) (далі у цьому розділі – ЕОМ), автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку. Адже аналізований злочин вчиняється шляхом впливу на інформацію та (або) з приводу неї, а не вказаного устаткування. У разі фізичного впливу безпосередньо на цю техніку (наприклад, знищення жорсткого диска, викрадення дисків для лазерних систем зчитування) вчинене за наявності підстав має кваліфікуватися за іншими кримінально-правовими нормами, зокрема тими, що передбачені статтями розд. VI Особливої частини або ст. 360 КК.

2. Об'єктивної сторони злочин характеризується: *дією* у вигляді несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; *наслідками*, що можуть проявлятися у формі витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації; *причинним зв'язком* між зазначеними діями та наслідками.

Застарілим терміном **«електронно-обчислювальна машина»** позначається комп'ютер, тобто електронний пристрій, призначений для оброблення (у тому числі зберігання) інформації з використанням програмного забезпечення.

У ст. 1 ЗУ від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» уживається термін **«інформаційна (автоматизована) система»**, що означає організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Відповідно до ДСТУ 226-93 «Автоматизовані системи. Терміни та визначення» автоматизована система – це організаційно-технічна система, що складається із засобів автоматизації певного виду чи кількох видів діяльності людей та персоналу, що здійснює цю діяльність.

Комп'ютерна мережа – сукупність телекомунікаційних каналів та засобів зв'язку, що об'єднують кілька комп'ютерів і забезпечують обмін комп'ютерною інформацією між ними.

Мережа електрозв'язку (телекомунікаційна мережа) – це комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням (ст. 1 ЗУ «Про телекомунікації»).

Під **несанкціонованим втручанням** у роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку слід розуміти вплив на інформаційні процеси за умови, що він є несанкціонованим. Такий вплив може вчинятися шляхом уведення, зміни, пошкодження, знищення, блокування інформації тощо. Про поняття *інформаційного процесу* див. п. 1 коментарю до цієї статті.

Несанкціонованими є дії, що провадяться з порушенням порядку доступу до інформації, установленого відповідно до законодавства; *доступ до інформації* – це отримання користувачем можливості обробляти інформацію в системі; *порядок доступу до інформації в системі* – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації (ст. 1 ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах»). Поняття *«несанкціоновані дії»* не можна ототожнювати з поняттям

«незаконні дії». За вчинення несанкціонованих, але законних дій не може наставати кримінальна відповідальність.

Витік інформації має місце у випадках, коли вона стає відомою хоча б одній особі, яка не має права доступу до неї. У ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» визначено поняття «виток» (а не «витік») інформації – це результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. У такому разі може йтися лише про інформацію з обмеженим доступом. Про витік загальнодоступної, відкритої інформації йтися не може, оскільки право доступу до неї має будь-яка особа.

Відповідно до ст. 21 ЗУ від 2 жовтня 1992 р. № 2657-XII «Про інформацію» ***інформація з обмеженим доступом*** поділяється на конфіденційну, таємну та службову. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

До інформації з обмеженим доступом не можуть бути віднесені такі відомості: про стан довкілля, якість харчових продуктів і предметів побуту; про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей; про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення; про факти порушення прав і свобод людини і громадянина; про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб; інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана ВР.

Аналогічним чином визначено види інформації з обмеженим доступом у ст. 6 ЗУ від 13 січня 2011 р. № 2939-VI «Про доступ до публічної інформації», згідно з якою обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог: 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. Зазначене положення не поширюється на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину (за умови дотримання вимог, що ставляться до обмеження доступу до інформації).

Не належать до інформації з обмеженим доступом відомості, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, оформленої за формою і в порядку, що встановлені ЗУ від 7 квітня 2011 р. № 3206-VI «Про засади запобігання і протидії корупції», крім відомостей, зазначених в абз. 2 ч. 2 ст. 12 цього ЗУ, а саме: відомості щодо реєстраційного номера облікової картки платника податків або серії та номера паспорта громадянина України, а також реєстрації місця проживання, дати народження декларанта, місцезнаходження об'єктів, які наводяться в декларації про майно, доходи, витрати і зобов'язання фінансового характеру.

Конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов (ст. 7 ЗУ «Про доступ до

публічної інформації»). До конфіденційної інформації не може бути віднесено: відомості щодо використання бюджетних коштів; інформацію, пов'язану з виконанням обов'язків з надання освітніх, оздоровчих, соціальних або інших державних послуг; інформацію щодо умов постачання товарів, послуг та цін на них, якою володіють суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями; інформацію про стан довкілля, про якість харчових продуктів і предметів побуту, про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян; іншу інформацію, що становить суспільний інтерес (суспільно необхідну інформацію).

Таємна інформація – інформація, доступ до якої обмежується відповідно до ч. 2 ст. 6 ЗУ «Про доступ до публічної інформації», розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю. Порядок доступу до таємної інформації регулюється цим ЗУ та спеціальними законами (ст. 8 ЗУ «Про доступ до публічної інформації»). До останніх належать, наприклад, ЗУ від 21 січня 1994 р. № 3855-XII «Про державну таємницю», від 7 грудня 2000 р. № 2121-III «Про банки і банківську діяльність», від 2 вересня 1993 р. № 3425-XII «Про нотаріат», від 5 липня 2012 р. № 5076-VI «Про адвокатуру та адвокатську діяльність».

До *службової* може належати інформація: що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; зібрана у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці (ст. 9 ЗУ «Про доступ до публічної інформації»).

Інформація з обмеженим доступом є предметом злочинів, передбачених статтями 111, 114, 132, 145, 159, 168, 182, 231, 232, 232^1, 328, 329, 330, 361^2, 381, 387, 397 КК та ін.

Втрата інформації – це припинення існування інформації для фізичних або юридичних осіб, які мають право власності на неї у повному чи обмеженому обсязі. Втрата інформації матиме місце й тоді, коли її можна відновити за допомогою спеціальних програмних чи технічних засобів.

Підробкою інформації є викривлення змісту існуючої або створення нової інформації, яка за змістом не відповідає дійсності. Підробку інформації необхідно відрізняти від її зміни (див. п. 3 коментарю до ст. 362 КК).

Блокування інформації – дії, внаслідок яких унеможливлюється доступ до інформації в системі (ст. 1 ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах»).

Спотворення процесу обробки інформації – це зміна перебігу оброблення інформації, порядок якого визначений її власником чи власником ЕОМ, автоматизованої системи, комп'ютерної мережі, мережі електрозв'язку або уповноваженою ними особою. У ст. 1 ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» обробку інформації визначено як виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Порушення встановленого порядку маршрутизації інформації полягає у зміні визначеного відправником інформації адресата інформації, яка передається телекомунікаційними каналами, унаслідок чого адресат не отримує інформацію або крім нього її отримують інші особи, яким вона не призначалася. Слід мати на увазі, що склад злочину утворює зміна лише *встановленого* порядку маршрутизації інформації, тобто такого, який визначено відправником інформації або власником ЕОМ, автоматизованої системи, комп'ютерної мережі чи мережі електрозв'язку.

Коментованою статтею охоплюється винятково «зовнішній» вплив на відповідну інформацію, тобто такий вплив, що здійснюється *без використання права доступу* до неї. У разі спричинення зазначених вище наслідків щодо інформації, яка оброблюється в ЕОМ, автоматизованих системах, комп'ютерних мережах або зберігається на відповідних носіях, особою, яка має право доступу до неї, вчинене може кваліфікуватися за ст. 362 КК.

Аналізований склад злочину сконструйовано як *матеріальний,* отже посягання, ознаки якого ним охоплюються вважається *закінченим* з моменту настання суспільно небезпечних наслідків.

3. Суб'єкт злочину – *загальний.*

4. Суб'єктивна сторона злочину характеризується виною у формі *прямого або непрямого умислу.*

5. Кваліфікуючими ознаками злочину є заподіяння ним значної шкоди, вчинення його повторно чи за попередньою змовою групою осіб.

Визначення поняття **значної шкоди** міститься у примітці до ст. 361 КК і тлумачиться лише в контексті заподіяння матеріальних збитків. Останні можуть мати характер як прямої шкоди, так і втраченої вигоди, і повинні визнаватися кваліфікуючою ознакою лише в разі, коли їх розмір у сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

При встановленні цієї кваліфікуючої ознаки і залежно від суспільно небезпечних наслідків, що настали, необхідно враховувати, зокрема: вартість інформації; збитки, завдані неможливістю використання знищеної (втраченої), зміненої (підробленої) чи заблокованої інформації; витрати на відновлення змісту цієї інформації; збитки від використання не справжньої, а підробленої чи зміненої інформації; шкоду від витоку певної інформації; збитки, зумовлені спотворенням процесу оброблення інформації, порушенням або припиненням роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Проте не можуть враховуватися витрати на забезпечення захисту інформації від протиправних посягань.

Аналізована кваліфікуюча ознака в частині, що не стосується збитків, має оціночний характер. Тому завдана злочином шкода може визнаватися значною з урахуванням й інших обставин, зокрема, важливості інформації, її значення для потерпілого, функціонального призначення. Психічне ставлення суб'єкта злочину до спричинення наслідків у вигляді значної шкоди може бути як умисним, так і необережним. Незалежно від цього злочин загалом вважається умисним.

Про поняття **повторності** див. коментар до ст. 32 КК, а про вчинення злочину за попередньою змовою групою осіб – до ст. 28 цього Кодексу.

6. Злочин, передбачений ч. 1 коментованої статті, належить до злочинів середньої тяжкості, а ч. 2 – до тяжких, що необхідно брати до уваги при застосуванні значної кількості норм кримінального процесуального права.

7. Втручання в роботу Державного реєстру виборців слід кваліфікувати за ст. 158 КК, автоматизованої системи документообігу суду – за ст. 376[1] КК, втручання в роботу технологічного обладнання магістральних або промислових нафто-, газо-, конденсатопроводів чи нафтопродуктопроводів, відводів від них, технологічно пов'язаних з ними об'єктів, споруд, засобів обліку, автоматики, телемеханіки, зв'язку, сигналізації – за ст. 292 КК.

Несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку може бути способом вчинення інших злочинів, відповідальність за які встановлено, наприклад, статтями 111, 113, 114, 163, 182, 231, 256, 330 КК. У таких випадках вчинене слід кваліфікувати за сукупністю злочинів, передбачених однією чи кількома із цих статей та ст. 361 КК.

Несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку з метою незаконного заволодіння чужим майном чи правом на нього може кваліфікуватись як шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК). Втручання у роботу банківських автоматів з використанням підроблених електронних платіжних інструментів або платіжних карток кваліфікується за ст. 200 КК. У разі, коли зазначені дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку її маршрутизації, вчинене потрібно кваліфікувати за сукупністю злочинів, передбачених ст. 361 та ст. 200 КК або, якщо такі дії були способом заволодіння чужим майном чи придбання права на нього (за наявності всіх інших ознак шахрайства), – за ст. 190 КК (ст. 200 КК заволодіння чужим майном не передбачає).

Стаття 361[1]. **Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут**

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, –

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

(Кодекс доповнено статтею 361[1] згідно із Законом № 2289-IV від 23.12.2004)

1. Основний безпосередній об'єкт аналізованого злочину за змістом аналогічний об'єкту злочину, передбаченого ст. 361 КК (див. п. 1 коментарю до неї).

Предметом злочину є шкідливі програмні чи технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Поняття **«програмні засоби»** у вітчизняному законодавстві відсутнє, натомість у ст. 1 ЗУ від 23 грудня 1993 р. № 3792-XII «Про авторське право і суміжні права» вживається термін ***«комп'ютерна програма»*** – набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його в дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах).

Технічні засоби – це певне обладнання, устаткування, єдиною або основною функцією якого є забезпечення несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

У законі вказано на дві ознаки предмета цього злочину: програмні і технічні засоби мають бути **шкідливими**, тобто забезпечувати можливість незаконно вплинути на процес оброблення інформації та спричинити наслідки, передбачені ст. 361 КК; їх єдиним або основним призначенням має бути **несанкціоноване втручання** в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (див. п. 2 коментарю до ст. 361 КК).

Фактично у ст. 361[1] КК встановлено кримінальну відповідальність за створення, розповсюдження та збут знарядь вчинення злочину, ознаки якого передбачено у ст. 361 КК. Отже, шкідливі властивості програмних і технічних засобів проявляються не при розповсюдженні чи збуті останніх, а при їх використанні, тобто втручанні в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Законодавчий опис властивостей шкідливих програмних засобів не повною мірою відповідає типовим характеристикам комп'ютерних вірусів, що, як правило, не використовуються для втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Про поняття **«електронно-обчислювальна машина (комп'ютер)»**, **«автоматизована система»**, **«комп'ютерна мережа»** та **«мережа електрозв'язку»** див. п. 3 коментарю до ст. 361 КК.

2. Об'єктивна сторона злочину характеризується лише однією ознакою – суспільно небезпечними *діями*, що можуть полягати у створенні, розповсюдженні або збуті шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Створення – це дії, внаслідок яких виникає новий, такий, що раніше не існував, шкідливий програмний або технічний засіб, призначений для такого втручання.

У контексті коментованої статті під **розповсюдженням** шкідливих програмних і технічних засобів слід розуміти їх оплатну чи безоплатну передачу будь-яким способом широкому, невизначеному колу осіб. Розповсюдження програмних засобів може відбуватися шляхом надання доступу до них через Інтернет.

Виходячи зі змісту актів судового тлумачення кримінально-правових норм термін «збут» означає оплатну чи безоплатну передачу певних предметів хоча б одній особі (див., наприклад, пункти 15, 16 ППВСУ від 26 квітня 2002 р. № 3 «Про судову практику в справах про викрадення та інше незаконне поводження зі зброєю, бойовими припасами, вибуховими речовинами, вибуховими пристроями чи радіоактивними матеріалами» та п. 4 ППВСУ від 26 квітня 2002 р. № 4 «Про судову практику в справах про злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів»).

Отже, поняття «збут» шкідливих програмних чи технічних засобів є ширшим за змістом, ніж поняття «розповсюдження» цих засобів, оскільки охоплює їх оплатну чи безоплатну передачу не лише невизначеному колу осіб, а й одній особі. Використання шкідливих програмних і технічних засобів не охоплюється цим складом злочину і за наявності підстав може кваліфікуватися за ст. 361 КК.

Аналізоване посягання належить до злочинів із *формальним* складом і вважається *закінченим* з моменту вчинення суспільно небезпечної дії.

3. Суб'єкт злочину – *загальний*.

4. Суб'єктивна сторона злочину характеризується виною у формі *прямого умислу*, а створення шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – ще й *метою* використання, розповсюдження або збуту цих засобів.

5. Кваліфікуючими ознаками злочину є заподіяння ним **значної шкоди** (див. п. 5 коментарю до ст. 361 КК), вчинення його **повторно** (див. коментар до ст. 32 КК) чи **за попередньою змовою групою осіб** (див. коментар до ст. 28 КК).

6. Злочин, передбачений ч. 1 коментованої статті, належить до злочинів невеликої тяжкості, а ч. 2 – до злочинів середньої тяжкості, що необхідно брати до уваги при застосуванні значної кількості норм кримінального процесуального права.

Стаття 361^2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, –

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

(Кодекс доповнено статтею 361^2 згідно із Законом № 2289-IV від 23.12.2004)

1. Основним безпосереднім об'єктом злочину є відносини у сфері інформаційної діяльності щодо комп'ютерної інформації (про їх зміст див. п. 1 коментарю до ст. 361 КК), **додатковим безпосереднім об'єктом** – відносини власності щодо певної інформації та відносини у сфері забезпечення режиму обмеженого доступу до неї.

Предмет злочину – інформація з обмеженим доступом, яка зберігається в ЕОМ, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створена і захищена відповідно до чинного законодавства.

Про поняття **інформації з обмеженим доступом** див. п. 2 коментарю до ст. 361 КК.

У ч. 1 ст. 361^2 КК йдеться про інформацію з обмеженим доступом, яка **створена та захищена відповідно до чинного законодавства**. Тому при кваліфікації аналізованого злочину не можуть братися до уваги будь-які інші нормативно-правові акти, в яких визначений порядок створення і захисту інформації з обмеженим доступом. Згідно з Рішенням КСУ від 9 липня 1998 р. № 12-рп/98 терміном «*законодавство*» охоплюються лише закони України, чинні міжнародні договори України, згода на обов'язковість яких надана ВР, а також постанови ВР, укази Президента України, декрети і постанови КМУ, прийняті в межах їх повноважень та відповідно до КУ і законів України.

Оскільки у ст. 361^2 КК між словами «створена», «захищена» вжито сполучник «та», відповідна інформація має бути і створена, і захищена згідно з чинним законодавством. Порядок створення інформації, навіть з обмеженим доступом, в Україні на законодавчому рівні не регламентується. Отже, у цьому контексті може йтися лише про те, що певні відомості одержані чи зібрані без порушень чинного законодавства.

Законодавець прямо не вказує на форму представлення інформації. Очевидно, що насамперед мається на увазі *комп'ютерна інформація* (див. п. 2 коментарю до ст. 361 КК). Варто пам'ятати, що предметом цього посягання може бути лише та **інформація, яка зберігається в ЕОМ, автоматизованих системах, комп'ютерних мережах і на відповідних носіях,** і не може – інформація яка не зберігається, а в інший спосіб обробляється в ЕОМ, автоматизованих системах, комп'ютерних мережах, а також будь-яка інформація в мережах електрозв'язку. Відмінність між інформацією, яка зберігається, і тією, що обробляється в ЕОМ, автоматизованих системах, комп'ютерних мережах, випливає з порівняльного аналізу статей 361^2 і 362 КК.

Про поняття **«електронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа»** та **«мережа електрозв'язку»** див. п. 2 коментарю до ст. 361 КК**.**

Носії такої інформації – буквально це носії інформації, яка зберігається в ЕОМ, автоматизованих системах, комп'ютерних мережах. Носіями комп'ютерної інформації слід вважати будь-яке обладнання, призначене для постійного або тимчасового зберігання її у сталому вигляді. Канали електрозв'язку не є носіями комп'ютерної інформації, позаяк вони за своїми технічними характеристиками не здатні зберігати інформацію у постійному, незмінному стані. Так само не можуть бути визнані її носіями різноманітні сигнали (електронні, світлові, звукові тощо), оскільки за їх допомогою інформація не зберігається, а передається від одного носія до іншого.

2. З об'єктивної сторони злочин характеризується діями, що можуть проявлятися у несанкціонованих збуті або розповсюдженні інформації. Про поняття **несанкціонованих діянь** див. п. 3 коментарю до ст. 361 КК, а про поняття **збуту** та **розповсюдження** – п. 3 коментаря до ст. 361^1 КК.

Злочин вважається *закінченим* з моменту вчинення суспільно небезпечної дії, а отже, має *формальний* склад.

3. Суб'єкт злочину – *загальний*.

4. Суб'єктивна сторона злочину характеризується виною у формі *прямого умислу*.

5. Кваліфікуючими ознаками злочину є заподіяння ним **значної шкоди** (див. п. 6 коментарю до ст. 361 КК), вчинення його **повторно** (див. коментар до ст. 32 КК) чи **за попередньою змовою групою осіб** (див. коментар до ст. 28 КК).

6. Злочин, передбачений ч. 1 коментованої статті, належить до злочинів невеликої тяжкості, а ч. 2 – до злочинів середньої тяжкості. Це має істотне значення при застосуванні значної кількості норм кримінального процесуального права.

Стаття 361[3]. ***(Виключена на підставі Закону № 767-VII від 23.02.2014)***

Стаття 361[4]. ***(Виключена на підставі Закону № 767-VII від 23.02.2014)***

Стаття 362. **Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї**

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, –

караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, –

караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

(Стаття 362 в редакції Закону № 2289-IV від 23.12.2004)

1. Основним безпосереднім об'єктом злочину є відносини у сфері інформаційної діяльності щодо комп'ютерної інформації (про їх зміст див. п. 1 коментарю до ст. 361 КК), **додатковим безпосереднім** – відносини власності щодо певної інформації, а злочину, передбаченого ч. 2 цієї статті, – також суспільні відносини у сфері забезпечення режиму обмеженого доступу до певної інформації.

Предмет злочину – інформація, яка оброблюється в ЕОМ, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації. Очевидно, в цій статті йдеться насамперед про *комп'ютерну інформацію* (її поняття розкрито у п. 1 коментарю до ст. 361 КК). Інформація, яка оброблюється в мережах електрозв'язку, не може бути предметом цього посягання.

Предметом злочину, передбаченого ч. 2 цієї статті, може бути лише та *комп'ютерна інформація, доступ до якої обмежений* (див. коментар до ст. 361 КК), оскільки єдиним наслідком відповідного злочину є витік інформації. Говорити про витік загальнодоступної, відкритої інформації не коректно, оскільки право доступу до неї має будь-яка особа.

Про поняття **«електронно-обчислювальна машина (комп'ютер)»**, **«автоматизована система»** та **«комп'ютерна мережа»** див. п. 2 коментарю до ст. 361 КК; **«носії такої інформації»** – п. 1 коментарю до ст. 361[2] КК.

2. У ч. 1 коментованої статті терміни «зміна», «знищення» і «блокування» одночасно позначають суспільно небезпечні несанкціоновані дії та їх наслідки.

Зміна інформації – це будь-яка модифікація інформації, що не спричинила втрату її основних якостей. Мається на увазі передусім модифікація змісту інформації, її доповнення. Унаслідок таких дій інформація не перестає існувати, не змінюються її основні атрибути (призначення, формат тощо), а головне – вона може використовуватися. Водночас не можна

розглядати як зазначений суспільно небезпечний наслідок доповнення і модифікацію інформації, що міститься у службових протоколах комп'ютерних програм, якщо останні здійснюють такі зміни автоматично.

Згідно зі ст. 1 ЗУ від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» під **«знищенням інформації»** розуміються дії, внаслідок яких інформація в системі зникає. Це поняття за змістом збігається з поняттям **«втрата інформації»**, яке розглядалося у п. 2 коментарю до ст. 361 КК. Там само визначено поняття **«блокування інформації»**.

У ч. 2 ст. 362 КК встановлена кримінальна відповідальність за вчинення суспільно небезпечних *дій* у вигляді несанкціонованих перехоплення або копіювання інформації, *наслідком* яких є витік останньої.

Копіювання інформації та її **перехоплення** за своїм змістом є подібними і полягають в одержанні копії певної інформації, її відтворенні з оригінального примірника. При цьому копія може створюватися як на іншому, так і на тому самому носієві. Відмінність між копіюванням і перехопленням інформації слід шукати у способі одержання копії. При копіюванні інформація відтворюється з використанням доступу до неї. Перехоплення відбувається за відсутності доступу до інформації, як правило, під час передавання каналами зв'язку або у процесі іншого оброблення (наприклад, шляхом сканування й аналізу випромінювання, що створює комп'ютер). З огляду на зазначене, перехоплення інформації не можна кваліфікувати за коментованою статтею, оскільки суб'єктом цього злочину є особа, яка має право доступу до інформації. Кримінально-правову оцінку аналізованих діянь необхідно здійснювати з урахуванням положень ст. 361 КК, тобто вони можуть кваліфікуватись як несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що спричинило витік інформації.

У статтях 361 і 362 КК термін **«витік інформації»** має однаковий зміст (див. п. 2 коментарю до ст. 361 КК).

Аналізованою статтею не охоплюється заволодіння інформацією, коли остання незаконно вибуває з володіння власника (у разі її викрадення, привласнення тощо). Якщо такі діяння були вчинені шляхом безпосереднього впливу на носій інформації (наприклад, його викрадення), вчинене потрібно кваліфікувати за відповідними статтями розд. VI Особливої частини КК «Злочини проти власності». Аналогічно слід кваліфікувати знищення інформації шляхом знищення чи пошкодження її носія. У таких випадках розмір майнової шкоди необхідно визначати з урахуванням вартості як інформації, так і носія.

Злочин має *матеріальний* склад, тобто вважається *закінченим* з моменту настання суспільно небезпечних наслідків.

3. Суб'єкт злочину – *спеціальний.* Ним може бути фізична осудна особа, яка до моменту вчинення злочину досягла 16-річного віку і має право доступу до інформації, що є предметом цього посягання. У законі прямо не вказано на те, що суб'єкт під час вчинення злочину використовує зазначене право. Проте в разі умисного вчинення аналізованих діянь особою, яка не має права доступу до інформації, вчинене може кваліфікуватися за ст. 361 КК.

4. Суб'єктивна сторона злочину, коли він полягає у перехопленні інформації, характеризується *умислом,* а в разі вчинення інших діянь, передбачених аналізованою статтею КК, – *як умислом,* так і *необережністю*. Такий висновок зумовлений двома обставинами. По-перше, законодавець прямо не визначив форму вини, з якою може вчинятися аналізоване посягання. По-друге, сутність останнього така, що допускає будь-яке психічне ставлення суб'єкта до вчинюваного ним діяння та його наслідків.

5. Кваліфікуючими ознаками злочину є заподіяння ним **значної шкоди** (див. п. 5 коментарю до ст. 361 КК), вчинення його **повторно** (див. коментар до ст. 32 КК) чи **за попередньою змовою групою осіб** (див. коментар до ст. 28 КК).

6. Злочин, передбачений ч. 1 коментованої статті, належить до злочинів невеликої тяжкості, а частинами 2 і 3 – до злочинів середньої тяжкості. Це має істотне значення при застосуванні значної кількості норм кримінального процесуального права.

Стаття 362[1]. ***(Виключена на підставі Закону № 767-VII від 23.02.2014)***

Стаття 363. **Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється**

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, –

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

(Стаття 363 в редакції Закону № 2289-IV від 23.12.2004)

1. Про **основний безпосередній об'єкт** злочину див. п. 1 коментарю до ст. 361 КК. **Факультативним безпосереднім об'єктом** є відносини власності щодо певної інформації.

Предмет злочину у статті прямо не вказаний, проте його наявність підтверджується аналізом відповідного складу злочину, зокрема, суспільно небезпечних наслідків. Ним може виступати *комп'ютерна інформація* або *інформація, що передається мережами електрозв'язку* (див. п. 1 коментарю до ст. 361 КК).

2. Об'єктивна сторона злочину характеризується: суспільно небезпечним *діянням* (дією чи бездіяльністю) у вигляді порушення правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється; суспільно небезпечним *наслідком*, який проявляється у заподіянні значної шкоди; *причинним зв'язком* між цими діянням та наслідком.

Диспозиція ст. 363 КК є *бланкетною*, оскільки для встановлення змісту об'єктивної сторони злочину відсилає до інших правових документів – **правил експлуатації** ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або **порядку чи правил захисту** інформації, яка в них обробляється.

Нормативно-правового акта, який би визначав правила використання згаданих машин, систем і мереж на рівні держави не існує. Загальні засади захисту лише окремих видів інформації передбачені ЗУ від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах», Положенням про порядок здійснення криптографічного захисту інформації в Україні і Положенням про технічний захист інформації в Україні, затвердженими відповідно Указами Президента України від 22 травня 1998 р. № 505/98 та від 27 вересня 1999 р. № 1229/99, а також Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженими постановою КМУ від 29 березня 2006 р. № 373.

Отже, правила, які регламентують порядок роботи з ЕОМ, автоматизованими системами, комп'ютерними мережами та мережами електрозв'язку, а також порядок чи правила захисту інформації, не зазначеної у згаданих нормативно-правових актах, можуть бути встановлені та затверджені лише відповідним наказом, розпорядженням, іншим документом, виданим власником або уповноваженою ним особою чи органом. Відсутність на підприємстві, в установі чи організації таких правил виключає наявність у діяннях особи складу аналізованого злочину. Такі діяння за наявності всіх інших підстав можуть кваліфікуватися, зокрема, за ст. 367 КК.

Про поняття **«електронно-обчислювальна машина (комп'ютер)»**, **«автоматизована система»**, **«комп'ютерна мережа»** та **«мережа електрозв'язку»** див. п. 2 коментарю до ст. 361 КК.

Суспільно небезпечні наслідки у вигляді заподіяння **значної шкоди** визначено у п. 5 коментарю до ст. 361 КК. Варто зробити лише таке застереження: значною шкодою не може вважатися знищення чи пошкодження ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також протиправне заволодіння відповідним технічним облад-

нанням. Заподіяння таких наслідків за наявності підстав має кваліфікуватися за статтями розд. VI Особливої частини КК «Злочини проти власності» або ст. 360 КК.

Злочин має *матеріальний* склад, тобто вважається *закінченим* з моменту настання суспільно небезпечного наслідку.

3. Суб'єкт аналізованого злочину – *спеціальний*. Ним може бути лише особа, яка відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Як правило, це їх адміністратор, який згідно з посадовими обов'язками має забезпечувати належне функціонування зазначених машин, систем чи мереж у цілому або їх частини чи інших інфраструктур, що безпосередньо пов'язані з функціонуванням вказаного обладнання і впливають на його роботу.

Суб'єктом цього злочину не може бути особа, яка забезпечує дотримання лише порядку чи правил захисту інформації і не відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

4. Суб'єктивна сторона злочину характеризується умисним або необережним психічним ставленням суб'єкта до своєї дії чи бездіяльності, а до наслідків – виключно необережним. У цілому ж злочин вважається *необережним*. У разі умисного ставлення і до суспільно небезпечного діяння, і до його наслідків кримінально-правову оцінку вчиненого потрібно здійснювати залежно від змісту наслідків, що настали. Такі діяння можуть кваліфікуватися, зокрема, за ст. 362 КК.

5. Передбачене коментованою статтею посягання належить до злочинів невеликої тяжкості, що слід брати до уваги при застосуванні значної кількості норм кримінального процесуального права.

Стаття 363[1]. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, –

карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, –

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи.

(Кодекс доповнено статтею 363[1] згідно із Законом № 2289-IV від 23.12.2004)

1. Про **основний безпосередній об'єкт** злочину див. п. 1 коментарю до ст. 361 КК. **Факультативним безпосереднім об'єктом** є відносини власності щодо певної інформації.

Предмет злочину у статті прямо не вказаний, проте його існування випливає зі змісту диспозиції ч. 1 та аналізу суспільно небезпечних наслідків. Масове одержання повідомлень електрозв'язку впливає на комп'ютерну інформацію в ЕОМ, автоматизованій системі, комп'ютерній мережі чи мережі електрозв'язку адресата. Отже, предметом злочину є *комп'ютерна інформація* або *інформація, що передається мережами електрозв'язку* (див. п. 1 коментарю до ст. 361 КК).

2. Об'єктивна сторона злочину характеризується: суспільно небезпечними *діями* у вигляді масового розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів; суспільно небезпечними *наслідками*, що проявляються у порушенні або припиненні роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електро-

зв'язку; *причинним зв'язком* між зазначеними діями та наслідками; *знаряддям* вчинення злочину, яким є повідомлення електрозв'язку.

Масове розповсюдження повідомлень електрозв'язку має місце, коли такі повідомлення розсилаються широкому, невизначеному колу адресатів без їхньої згоди. Передавання одного чи багатьох повідомлень одному адресатові або незначній, чітко визначеній їх кількості не може становити склад цього злочину.

Повідомлення електрозв'язку – це певні відомості, що сповіщаються комусь, письмова чи усна інформація, яка передається мережами електрозв'язку. Отже, сигнали, які не містять певних відомостей для когось, не охоплюються аналізованим поняттям. Передавання таких сигналів мережами електрозв'язку за наявності підстав може кваліфікуватися за ст. 361 КК.

Як **порушення роботи** ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку потрібно розуміти збій у процесі їх функціонування, повну або часткову втрату контролю над ними. **Припинення роботи** вказаного обладнання має місце у випадках, коли воно взагалі перестає працювати. Від порушення та припинення роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку слід відрізняти *спотворення процесу обробки інформації* (див. коментар до ст. 361 КК), коли змінюється, тобто спрямовується в іншому напрямі або припиняється, лише процес обробки інформації, проте робота техніки залишається сталою, не припиняється, у ній відсутні збої.

За ст. 363[1] КК не може кваліфікуватися розповсюдження так званого *спаму*, тобто розсилання електронною поштою повідомлень, як правило, комерційного, рекламного змісту. Зазначені діяння не порушують і не припиняють роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, адже приймання і передавання повідомлень є звичайною функцією цього обладнання. ЗУ від 3 вересня 2015 р. № 675-VIII «Про електронну комерцію» (зокрема ст. 10) передбачено вимоги до комерційних електронних повідомлень та загальні правила їх поширення. Однак жодної відповідальності за порушення цих вимог чи правил у законодавстві наразі не встановлено.

Про поняття **«електронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа», «мережа електрозв'язку»** див. п. 2 коментарю до ст. 361 КК.

Злочин має *матеріальний* склад, тобто вважається *закінченим* з моменту настання суспільно небезпечних наслідків.

3. Суб'єкт злочину – *загальний*.

4. Суб'єктивна сторона злочину характеризується виною у формі *прямого чи непрямого умислу*.

5. Кваліфікуючі ознаки аналізованого злочину сформульовано інакше, ніж у попередніх статтях цього розділу: «Ті самі дії, вчинені повторно або за попередньою змовою групою *осіб, якщо (курсив авт.)* вони заподіяли значну шкоду». У статтях 361–363 КК між словами «осіб» та «якщо» вжито сполучник *«або»*. У коментованій статті цього сполучника немає. Виходячи із зазначеного інкримінування кваліфікуючих ознак у вигляді вчинення злочину повторно або за попередньою змовою групою осіб можливе лише в разі, коли таким злочином заподіяно значної шкоди. За її відсутності вчинене не може кваліфікуватися за ч. 2 ст. 363[1] КК.

Про зміст ознаки **«повторно»** див. коментар до ст. 32 КК, **«за попередньою змовою групою осіб»** – до ст. 28 КК, **«значна шкода»** – до ст. 361 КК.

6. Злочин, передбачений ч. 1 коментованої статті, належить до злочинів невеликої тяжкості, а ч. 2 – до злочинів середньої тяжкості. Це має істотне значення при застосуванні значної кількості норм кримінального процесуального права.

Перелік основних наукових джерел до розділу

Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис... канд. юрид. наук : 12.00.08 / Д. С. Азаров. – К., 2003. – 246 с.

Азаров Д. С. Нові зміни до розділу XVI Особливої частини Кримінального кодексу України – нові проблеми / Д. С. Азаров // Юридичний вісник України. Інформаційно-правовий банк. – 2005. – № 502 (12). – 12–18 лютого.

Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія / Д. С. Азаров. – К. : Атіка, 2007. – 304 с.

Азаров Д. С. Теоретичні основи розроблення законопроекту, спрямованого на реформування норм про відповідальність за «комп'ютерні» злочини / Д. С. Азаров // Наука і правоохорона. – 2008. – № 1. – С. 63–69.

Азаров Д. С. Кримінальна відповідальність за «комп'ютерні» злочини: стан наукових досліджень та основні напрями удосконалення / Д. С. Азаров // 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали Міжн. наук.-практ. конф. 13–14 жовт. 2011 р. / Редкол. : В. Я. Тацій (голов. ред.), В. І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2011. – С. 347–350.

Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : дис. ... канд. юрид. наук : 12.00.08 / М. В. Карчевський. – Луганськ, 2002. – 175с.

Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж / М. В. Карчевський; Луганська академія внутрішніх справ ім. 10-річчя незалежності України. – Луганськ : РВВ ЛАВС, 2002. – 144 с.

Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський. – Луганськ : РВВ ЛДУВС ім. О. Е. Дідоренка, 2012. – 528 с.

Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : дис. ... докт. юрид. наук : 12.00.08 / М. В. Карчевський. – К., 2013. – 536 с.

Музика А. А., Азаров Д. С. Законодавство України про відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров. – К. : Вид. Паливода А. В., 2005. – 120 с.

Орлов С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : дис... канд. юрид. наук : 12.00.08 / С. О. Орлов. – Х., 2004. – 213 с.

Плугатир М. В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації : дис. ... канд. юрид. наук : 12.00.08 / М. В. Плугатир. – К., 2010. – 240 с.

Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис. ... канд. юрид. наук : 12.00.08 / Н. А. Розенфельд. – К., 2003. – 222 с.

Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : дис. ... канд. юрид. наук : 12.00.08 / М. В. Рудик. – Х., 2007. – 229 с.

Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія / Н. А. Савінова. – К. : ДКС, 2012. – 342 с.

Савінова Н. А. Кримінально-правова політика та убезпечення інформаційного суспільства в Україні : монографія / Н. А. Савінова. – К. : Ред. журн. «Право України»; Х. : Право, 2013. – 292 с.