слуг: загальна характеристика // Вісник Асоціації кримінального права України, 2015, вип. 1 (4).

Ю. В. Гродецький.

НЕСАНКЦІОНО́ВАНЕ ВТРУЧА́ННЯ В РОБО́ТУ ЕЛЕКТРО́ННО-ОБЧИ́СЛЮВАЛЬНИХ МАШИ́Н (КОМП'Ю́ТЕРІВ), АВТОМАТИЗО́ВАНИХ СИСТЕМ, КОМП'Ю́ТЕРНИХ МЕРЕ́Ж ЧИ МЕРЕ́Ж ЕЛЕКТРОЗВ'ЯЗКУ́ – злочин, передбачений ст. 361 КК, в якій встановлено відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (ЕОМ), 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.

Осн. безпосереднім об'єктом злочину є 2 різновиди сусп. відносин: 1) сусп. 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; 2) сусп. відносини у сфері обміну інформацією (не лише комп'ютерною) мережами електрозв'язку (телекомунікацій). Телекомунікації – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків чи повідомлень будь-якого роду по радіо, проводових, оптичних або ін. електромагнітних системах. Дод. безпосереднім об'єктом злочину є відносини власності щодо певної інформації, факультативним безпосереднім об'єктом – відносини у сфері забезпечення режиму обмеженого доступу до певної інформації.

Предметом злочину слід вважати комп'ютерну інформацію та (або) інформацію, яка передається мережами електрозв'язку. Комп'ютерну інформацію слід розглядати у 2-х аспектах: 1) як відомості про навколишній світ і процеси, які в ньому відбуваються, зафіксовані в електронному вигляді; 2) як дані, тобто сукупність символів, кодів, сигналів, команд тощо, які виражаються у різноманітних комп'ютерних програмах, за допомогою яких певні відомості набувають електронної форми, проявляються назовні й із якими здійснюються різні операції. Інформація, що передається мережами електрозв'язку, – відомості, подані у вигляді знаків, сигналів, письмового тексту, рухомих або нерухомих зображень, звуків чи в ін. спосіб, що передаються по радіо, проводових, оптичних або ін. електромагнітних системах. Мережами електрозв'язку може передаватися як комп'ютерна інформація, так й ін. інформація. Відмінність між цими поняттями полягає передусім у формі фіксування інформації. Комп'ютерна інформація фіксується лише в електронному вигляді, ін. види інформації, що передаються мережами електрозв'язку, – в ін. спосіб (напр., при передаванні інформації телеграфом вона фіксується на папері) чи не фіксується взагалі (приміром, усне передавання відомостей за допомогою телефон. зв'язку).

Електронно-обчислювальна машина – комп'ютер, тобто електронний пристрій, призначений для оброблення (у т. ч. зберігання) інформації з використанням програмного забезпечення. Автоматизована система – організаційно-тех. система, в якій реалізується технологія обробки інформації з використанням тех. і програмних засобів. 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) – комплекс тех. 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 ін. електромагнітних системах між кінцевим обладнанням.

З об'єктивної сторони злочин характеризується суспільно небезпеч. діянням, наслідками та причин. зв'язком між ними. Діяння характеризується дією у вигляді несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Під втручанням у роботу вказаних об'єктів слід розуміти вплив на інформаційні процеси, що вчиняється шляхом уведення, зміни, пошкодження, знищення, блокування інформації тощо. Несанкціонованим є таке втручання, що здійснюється з порушенням порядку доступу до інформації, установленого відповідно до зак-ва.

Суспільно небезпеч. наслідками є витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації. Витік інформації має місце у випадках, коли вона стає відомою чи доступною хоча б одній особі, яка не має права доступу до неї. Втрата інформації – припинення існування інформації для фіз. або юрид. осіб, які мають право власності на неї в повному чи обмеженому обсязі. Втрата інформації матиме місце й тоді, коли її можна відновити за допомогою спец. програмних чи тех. засобів. Підробкою інформації є викривлення змісту існуючої або створення нової інформації, що за змістом не відповідає дійсності. Підробку інформації необхідно відрізняти від її зміни (ст. 362 КК), під якою слід розуміти будь-яку модифікацію інформації, що не спричинило втрату її осн. якостей. Блокування інформації – дії, внаслідок яких унеможливлюється доступ до інформації в системі. 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. Обробку інформації в зак-ві 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 тех. 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 ін-

формацію або крім нього її отримують ін. особи, яким вона не призначалася. Склад злочину може утворювати зміна лише встановленого порядку маршрутизації інформації, тобто такого, який визначено відправником інформації або власником ЕОМ, автоматизованої системи, комп'ютерної мережі чи мережі електрозв'язку.

Складом злочину, передбаченим ст. 361 КК, охоплюється винятково «зовнішній» вплив на відповід. інформацію, тобто такий, що здійснюється без використання права доступу до неї. У разі спричинення зазначених вище наслідків щодо інформації, яка обробляється в ЕОМ, автоматизованих системах, комп'ютерних мережах або зберігається на відповід. носіях, особою, яка має право доступу до неї, вчинене може кваліфікуватися за ст. 362 КК.

Злочин вважається закінченим з моменту настання суспільно небезпеч. наслідків.

Суб'єкт злочину – заг., суб'єктивна сторона злочину характеризується виною у формі прямого або непрямого умислу.

Ч. 1 ст. 361 КК передбачено злочин серед. тяжкості, вчинення якого може каратися штрафом від 600 до 1 тис. н. м. д. г. або обмеж. волі на строк від 2-х до 5-ти років, або позбавл. волі на строк до 3-х років, з позбавл. права обіймати певні посади чи займатися певною діяльністю на строк до 2-х років або без такого.

У ч. 2 ст. 361 КК передбачено кваліфікуючі ознаки у вигляді заподіяння злочином значної шкоди, вчинення його повторно чи за попер. змовою групою осіб.

Поняття значної шкоди, якщо вона полягає у заподіянні матеріальних збитків, розкрито у примітці до ст. 361 КК. Такі збитки можуть бути як прямою шкодою, так і втраченою вигодою, і мають визнаватися кваліфікуючою ознакою в разі, коли їх розмір у 100 і більше разів перевищує н. м. д. г. При встановленні цієї кваліфікуючої ознаки 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 можна брати до уваги витрати на забезпечення захисту інформації від протиправних посягань. Зазначена кваліфікуюча ознака в частині, що не стосується матеріальних збитків, має оціночний характер. Тому завдана злочином шкода може визнаватися значною з урахуванням й ін. обставин, зокрема важливості інформації, її значення для потерпілого, функц. призначення.

Поняття повторності див. *Повторність злочинів*, вчинення злочину за попер. змовою групою осіб див. *Вчинення злочину групою осіб за попередньою змовою*.

Злочин, передбачений ч. 2 ст. 361 КК, належить до тяжких, за його вчинення передбачено покарання у виді позбавл. волі на строк від 3-х до 6-ти років з по-

збавл. права обіймати певні посади чи займатися певною діяльністю на строк до 3-х років.

Втручання в роботу Держ. реєстру виборців слід кваліфікувати за ч. 1 ст. 158 КК, автоматизованої системи документообігу суду – за ст. 376[1] КК, втручання в роботу технол. обладнання магістральних або пром. 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 з метою незакон. заволодіння чужим майном чи правом на нього може кваліфікуватися як шахрайство, вчинене шляхом незакон. операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК). Втручання у роботу банк. автоматів з використанням підроблених електронних платіжних інструментів або платіжних карток кваліфікується за ст. 200 КК. У разі, коли ті або ін. 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 ін. ознак шахрайства) – за ст. 190 КК.

Літ.: Азаров Д. С. Злочини у сфері комп'ютерної інформації. К., 2007; Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія / І. Р. Шинкаренко, В. О. Голубєв, М. В. Карчевський та ін. Д., 2007; Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України. Луганськ, 2012.

Д. С. Азаров.

НЕСАНКЦІОНО́ВАНІ ДІЇ З ІНФОРМА́ЦІЄЮ, ЯКА́ ОБРО́БЛЮЄТЬСЯ В ЕЛЕКТРО́ННО-ОБЧИ́СЛЮВАЛЬНИХ МАШИ́НАХ (КОМП'Ю́ТЕРАХ), АВТОМАТИЗО́ВАНИХ СИСТЕ́МАХ, КОМП'Ю́ТЕРНИХ МЕРЕ́ЖАХ АБО́ ЗБЕРІГА́ЄТЬСЯ НА НОСІЯ́Х ТАКО́Ї ІНФОРМА́ЦІЇ, ВЧИ́НЕНІ ОСО́БОЮ, ЯКА́ МА́Є ПРА́ВО ДО́СТУПУ ДО НЕ́Ї – злочин, передбачений ст. 362 КК. У ч. 1 цієї статті встановлено відповідальність за несанкціоновані зміну, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (ЕОМ) (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї. Ч. 2 передбачено несанкціоновані перехоплення або копіювання інформації, яка обробляється в ЕОМ (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.

Визначення понять ст. 362 КК містяться у законах України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації».

Осн. безпосереднім об'єктом злочину є відносини у сфері інформаційної діяльності щодо комп'ютерної інформа-