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 ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ 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-

ції (див. *Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*), дод. безпосереднім об'єктом – відносини власності щодо певної інформації. Дод. безпосередній об'єкт злочину – сусп. відносини у сфері забезпечення режиму обмеженого доступу до певної інформації.

Предметом злочину є інформація, яка оброблюється в ЕОМ, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації. У цій статті йдеться насамперед про комп'ютерну інформацію. Інформація, яка оброблюється в мережах електрозв'язку (за винятком комп'ютерних мереж), не може бути предметом цього посягання. Предметом злочину, передбаченого ч. 2 цієї статті, може бути лише та комп'ютерна інформація, доступ до якої обмежений, оскільки єдиним наслідком відповід. злочину є витік інформації. Не є витоком загальнодоступна, відкрита інформація, оскільки право доступу до неї має будь-яка особа.

Носієм комп'ютерної інформації слід вважати будь-яке обладнання, призначене для постій. або тимчасового зберігання її у сталому вигляді. Канали електрозв'язку не є носіями комп'ютерної інформації, бо за своїми тех. характеристиками вони не здатні зберігати інформацію у постій., незмінному стані. 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 ін.

Поняття «комп'ютерна інформація», «електронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа» див. *Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*.

У ч. 1 ст. 362 КК терміни «зміна», «знищення» і «блокування» інформації одночасно позначають суспільно небезпеч. несанкціоновані дії та їх наслідки.

Зміна інформації – будь-яка модифікація інформації, що не спричинила втрату її осн. якостей. Це передусім модифікація змісту інформації, її доповнення. Унаслідок таких дій інформація не перестає існувати, не змінюються її осн. атрибути (призначення, формат тощо), а головне – вона може використовуватися. Водночас не можна розглядати як суспільно небезпеч. наслідок доповнення і модифікацію інформації, що міститься у служб. протоколах комп'ютерних програм, якщо ост. здійснюють такі зміни автоматично.

Знищення інформації – дії, внаслідок яких інформація в системі зникає. Зазначене поняття за змістом збігається з поняттям «втрата інформації», яке міститься у ст. 361 КК.

Блокування інформації – дії, внаслідок яких унеможливлюється доступ до інформації в системі.

У ч. 1 ст. 362 КК передбачено злочин невеликої тяжкості, вчинення якого карається штрафом від 600 до 1 тис. н. м. д. г. або випр. роботами на строк до 2-х років.

Ч. 2 ст. 362 КК передбачено суспільно небезпеч. дії у вигляді несанкціоно-

ваних перехоплення або копіювання інформації, наслідком яких є витік ост.

Копіювання інформації та її перехоплення за своїм осн. змістом є однаковими і полягають в одержанні копії певної інформації, її відтворенні з ориг. примірника. При цьому копія може створюватися як на ін., так і на тому самому носієві. Відмінність між копіюванням і перехопленням інформації полягає 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 ін. оброблення (напр., шляхом сканування й аналізу випромінювання, що створює комп'ютер). З огляду на зазначене, перехоплення інформації не можна кваліфікувати за ст. 362 КК, оскільки суб'єктом цього злочину є особа, яка має право доступу до інформації. Крим.-прав. оцінку зазначених діянь необхідно здійснювати з урахуванням положень ст. 361 КК, тобто вони можуть кваліфікуватися як несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що спричинило витік інформації.

Витік інформації має місце у випадках, коли вона стає відомою чи доступною хоча б одній особі, яка не має права доступу до неї. Ст. 362 КК не охоплюється заволодіння інформацією, коли ост. незаконно вибуває з володіння власника (у разі її викрадення, привласнення тощо). Якщо такі діяння були вчинені шляхом безпосереднього впливу на носій інформації (напр., його викрадення), вчинене потрібно кваліфікувати за відповід. статтями розд. VI Особл. част. 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.

Посягання, ознаки якого виписано у ч. 2 ст. 362 КК, належить до злочинів серед. тяжкості, його вчинення карається позбавл. волі на строк до 3-х років з позбавл. права обіймати певні посади або займатися певною діяльністю на той самий строк.

Злочин вважається закінченим з моменту настання суспільно небезпеч. наслідків.

Суб'єкт злочину – спец. Ним може бути фіз. 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 зазначених діянь особою, яка не має права доступу до інформації, вчинене може кваліфікуватися за ст. 361 КК.

Суб'єктивна сторона злочину, вчиненого у формі перехоплення інформації, характеризується умислом, ін. діянь, передбачених цією статтею КК, – як умислом, так і необережністю.

У ч. 3 ст. 362 КК передбачено такі кваліфікуючі ознаки: заподіяння злочином значної шкоди (див. *Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*); вчинення злочину по-

вторно (див. *Повторність злочинів*); вчинення злочину за попередньою змовою групою осіб (див. *Вчинення злочину групою осіб за попередньою змовою*). Такі дії караються позбавл. волі на строк від 3-х до 6-ти років з позбавл. права обіймати певні посади або займатися певною діяльністю на строк до 3-х років.

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.

НОВИ́Й СОЦІА́ЛЬНИЙ ЗА́ХИСТ У КРИМІНА́ЛЬНОМУ ПРА́ВІ – напрям, який сформувався у повоєн. період у розвиток соціол. школи крим. права. Остання, услід за антропологічною школою крим. права, з'явилася внаслідок т. зв. позитивістського повороту в крим. юстиції, де осн. дилемою було встановлення балансу між індивід. правами особи і гарантіями безпеки для сусп-ва. У 1889 відомими представниками соціол. школи Ф. фон Лістом, Ж. А. Ван-Гамелем, А. Принсом був заснований Міжнар. союз криміналістів, де і формувалися погляди на соціал. захист. А. Принс у роботі «Соціальний захист і трансформація кримінального права» (1910) розвинув першу самост. теорію соціал. захисту. Доктринальним підґрунтям його розробок стала праця Е. Феррі «Кримінальна соціологія». Осн. метою критики соціологів було крим. право, що розглядало злочин не як живу людську поведінку, а як абстрактну юрид. сутність. Одним із центр. понять, що розроблялися доктриною соціал. захисту, було поняття небезпеч. стану особи. Небезпеч. стан розглядався в аспекті захисту інтересів д-ви та сусп-ва, а не індивіда. Відповіддю на небезпеч. стан мали стати заходи, які застосовувалися не за конкр. злочин, а з урахуванням потенційної загрози, що цей індивід становив. Цей напрям сприяв поширенню ідей профілактики злочинів, попередженню злочинності на основі більш повного вивчення особистості. Проте вже в період між 2-ма світ. війнами згадані ідеї зазнали згортання, д-ви повертались до принципу відплати у крим. праві, а ідеї заходів безпеки фактично використовувалися для посилення заходів репресії.

Новий імпульс доктрина соціал. захисту отримала після Другої світ. війни. У м. Генуя (Італія) виник Центр досліджень соціал. захисту, орієнтований на ресоціалізацію злочинця. Його засновником виступив італійський граф Ф. Граматика (нагородж. медаллю ім. Ч. Беккаріа, що присуджується з 1964 і вважається еквівалентом Нобелівської премії у кримінології). «Соціальний захист» як незалежний ідейний рух поставив завдання перегляду в рамках концепції ефективної крим.-прав. політики всієї крим.-прав. системи, разом з крим. відповідальністю, режимом санкцій, правилами судочинства та розробкою рац. методів випр. впливу на злочинців. У 1948 при Гол. Секретаріаті ООН була заснована секція соціал. захисту, що організовувала міжнар. і регіональні конгреси, сприяла орг-ції