УДК 343.346.8

Савченко Андрій Володимирович – начальник кафедри кримінального права Національної академії внутрішніх справ, доктор юридичних наук, професор,

Карчевський Микола Віталійович – професор кафедри кримінального права Луганського державного університету внутрішніх справ імені Е. О. Дідоренка, кандидат юридичних наук, доцент

Особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем

У статті проаналізовано питання, що стосуються особливостей кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем. Обґрунтовано відповідні формули кримінально-правової кваліфікації такого роду діянь у різних варіантах їх проявів.

Ключові слова: кримінально-правова кваліфікація, несанкціоноване втручання, вбудовані комп'ютерні системи, електронно-обчислювальні машини, інформація.

Постановка проблеми. У реаліях сьогодення важко знайти більш динамічний соціальний процес ніж інформатизація. Темпи розвитку комп'ютерних технологій забезпечили стрімке падіння ціни та вартості експлуатації разом з постійним зростанням продуктивності сучасних електронно-обчислювальних машин (далі – ЕОМ). Технологічні успіхи дозволили досягти без перебільшення вибухових темпів розширення сфери застосування електронно-обчислювальної техніки. Тут слід пригадати влучний вислів Біла Гейтса: "Якби автомобіль розвивався так само швидко, як комп'ютер, "Роллс-ройс" коштував би зараз менше долара, а на літрі бензину можна було б проїхати тисячу кілометрів". Зрозуміло, що настільки важливі соціальні зміни отримали кримінально-правове відображення: Кримінальний кодекс (далі – КК) України було доповнено відповідними нормами, а проблеми криміна-

льної відповідальності за злочини в сфері використання комп'ютерної техніки стали предметом значної кількості наукових досліджень.

Аналіз останніх досліджень і публікацій. Незважаючи на те, що важливі результати для правозастосовної та законотворчої роботи щодо кримінально-правової протидії "комп'ютерним злочинам" були відображені у працях Д. С. Азарова, П. П. Андрушка, В. М. Бутузова, В. О. Голубєва, С. В. Дрьомова, Т. В. Міхайліної, А. А. Музики, С. О. Орлова, М. І. Панова, М. В. Плугатиря, М. В. Рудик, Н. А. Савінової (Розенфельд) та інших науковців, чимало питань досі залишаються дискусійними. Одним із таких питань є специфіка кримінальної відповідальності за несанкціоноване втручання в роботу вбудованих комп'ютерних систем, що наразі є об'єктом посиленої уваги теоретиків і практиків через новизну цієї проблеми.

Мета статті – встановлення особливостей кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем.

Виклад основного матеріалу. Сучасні технології дозволяють розробляти та ефективно використовувати спеціалізовані ЕОМ для вдосконалення керування різноманітними пристроями та устаткуванням. Як стверджують Д. Д. Грицай та А. І. Роговенко, це "засоби на основі управління, контролю, диспетчеризації в системах тепло та енергозбереження, комп'ютерні системи управління виробництвом, касові апарати, апаратура діагностики, побутові прилади тощо" [1]. Практичні та експлуатаційні характеристики таких систем визначаються особливостями і характеристиками об'єктів управління, які вони обслуговують. Саме цим вони відрізняються від комп'ютерів у звичайному розумінні (персональних комп'ютерів), головною характеристикою яких є універсальність призначення [2, с. 9]. Для позначення таких ЕОМ використовуються терміни "вбудована система" (англ. "embedded system") або "вбудована комп'ютерна система".

Одним з найбільш поширених визначень такої системи є наступне: "спеціалізована комп'ютерна система або обчислювальний пристрій, призначений для виконання обмеженої кількості функцій" [3]. Достатньо інформативним є і визначення, запропоноване фахівцями Інституту вбудованих систем (Embedded Systems Institute, Eindhoven, Netherlands): "комбінація технічного обладнання та програмних компонентів, які вбудовані у виріб, для того, щоб створювати можливість його інформаційної взаємодії з оточуючим середовищем" [4]. Тобто, вбудована система становить собою спеціалізовану комп'ютерну систему управління, яка конструктивно поєднана, є частиною того пристрою, керування яким забезпечує.

Ураховуючи наведені вище положення, а також наявне у національному правовому полі визначення ЕОМ (функціональний пристрій, що складається з одного або декількох взаємопов'язаних центральних процесорів і периферійних пристроїв і може виконувати розрахунки без участі людини) [5, с. 7], можемо сформулювати наступний висновок: несанкціоноване втручання в роботу вбудованих комп'ютерних систем може, за наявності відповідних підстав, розглядатися як несанкціоноване втручання в роботу ЕОМ (ст. 361 КК України). Тобто, під ЕОМ, у контексті ст.ст. 361–363-1 КК України, слід розуміти не тільки комп'ютери в їх "класичному", можна сказати, звичному вигляді, тобто "системний блок – монітор – клавіатура – принтер", але й інше устаткування, яке містить процесор і може виконувати розрахунки без участі людини. Типовим прикладом такого устаткування є мобільний телефон. Саме тому незаконну зміну чи знищення інформації, що зберігається в мобільному телефоні, можна кваліфікувати як несанкціоноване втручання в роботу ЕОМ.

Проте, на цьому зовсім не вичерпуються особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем. Наведемо кілька прикладів.

Працівник станції технічного обслуговування автомобілів П. під час діагностики транспортного засобу, обладнаного бортовим комп'ютером, вирішив шляхом обману заволодіти грошима його власника В. З цією метою П. повідомив В. завідомо неправдиві відомості щодо можливості обладнання його транспортного засобу додатковим устаткуванням, яке забезпечить істотну економію пального. В. погодився і залишив транспортний засіб на станції технічного обслуговування. Невдовзі П. вчинив несанкціоноване втручання в роботу бортового комп'ютера автомобіля В., що призвело до спотворення процесу обробки інформації. Внаслідок дій зловмисника бортовий комп'ютер автомобіля став повідомляти неправдиву інформацію щодо витрат пального. Наступного дня П. запевнив В. у тому, що додаткове устаткування для економії пального було успішно встановлене на його транспортний засіб і запропонував переконатися в цьому, перевіривши показники бортового комп'ютера. Задоволений господар автомобіля сплатив П. гроші за "виконану роботу".

Наступний приклад. Аналогічні маніпуляції з бортовим комп'ютером зробив власник автомобіля задля того, щоб продати свій транспортний засіб по завищеній ціні.

Третій приклад. Підприємець, здійснив несанкціоноване втручання у роботу належного йому електронного контрольно-касового апарату. Такі дії призвели до спотворення процесу обробки інформації,

оскільки до фіскальної пам'яті апарату заносилися не всі відомості про здійснені розрахункові операції.

Сукупність наведених прикладів наочно демонструє, що кримінально-правова оцінка несанкціонованого втручання в роботу вбудованої комп'ютерної системи має даватися з урахуванням питання про власника об'єкта, в який вбудовано систему. Так, очевидно, що дії працівника станції технічного обслуговування (про що йшлося у першому прикладі) слід кваліфікувати за сукупністю злочинів, передбачених відповідними частинами ст.ст. 190 та 361 КК України.

У той же час, підстав для кваліфікації за ст. 361 КК аналогічних дій власника транспортного засобу (другий приклад) немає, оскільки об'єктом несанкціонованого втручання в роботу ЕОМ є право власності на комп'ютерну інформацію, а його предметом – відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника й ціну [6, с. 113–119]. Природно, що власник певного пристрою з вбудованою системою є і власником інформації, що обробляється такою системою. Саме тому в більшості випадків, коли власник приладу з вбудованою комп'ютерною систему знищує або перекручує інформацію, що обробляється такою системою, немає підстав говорити про наявність складу злочину, передбаченого ст. 361 КК України.

Останній приклад відноситься до тих випадків, які становлять виключення зі сформульованих вище положень. Маємо зазначити, що подібні випадки неодноразово зустрічалися у практиці російських правоохоронних органів. Інформація, яка зберігалася в пам'яті реєстраторів розрахункових операцій (до них, у тому числі, відносяться й електронні контрольно-касові апарати), знищувалася або перекручувалася. У результаті такого втручання забезпечувалося приховування реальних доходів від податкових органів [7]. Вчинене, за наявності для цього підстав (зокрема, несплати необхідної для початку кримінального провадження суми грошових коштів), може кваліфікуватися як ухилення від сплати податків, зборів (обов'язкових платежів), але, крім цього, подібні дії необхідно додатково кваліфікувати як втручання в роботу ЕОМ, що призвело до знищення або перекручення комп'ютерної інформації. Обґрунтування тут полягає у наявності спеціальних норм законодавства, які, можна сказати, "виводять" інформацію, що обробляється вбудованою системою, з власності особи, якій належить певне устаткування.

Стосовно реєстраторів розрахункових операцій, то до таких норм слід відносити положення Закону України "Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг". Відповідно до цього Закону України, особи, які внесли непередбачені конструкторсько-технологічною та програмною

документацією виробника зміни у конструкцію чи програмне забезпечення реєстраторів розрахункових операцій, що можуть призвести до знищення чи зміни накопичених даних про розрахункові операції за товари (послуги), притягаються до відповідальності згідно із законом (ст. 27) [8]. Тобто, незважаючи на те, що певний реєстратор розрахункових операцій належить конкретній особі, вона не є власником інформації, що обробляється вбудованою у реєстратор комп'ютерною системою, та, відповідно, може підлягати кримінальній відповідальності за несанкціоноване втручання в роботу ЕОМ.

Висновки. Підсумовуючи викладене, слід констатувати, що особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем полягають у наступному:

1. Оскільки вбудовані комп'ютерні системи становлять собою ЕОМ за визначенням, то несанкціоноване втручання в роботу вбудованих комп'ютерних систем, може, за наявності відповідних підстав, бути кваліфіковане за ст. 361 КК України.

2. Якщо власник приладу з вбудованою комп'ютерною системою знищує або перекручує інформацію, що обробляється такою системою, то немає підстав вести мову про наявність складу злочину, передбаченого ст. 361 КК України, за виключенням випадків, передбачених спеціальними нормами законодавства, які "виводять" інформацію, що обробляється вбудованою системою, з власності особи, якій належить певний прилад.

3. Беручи до уваги той факт, що сьогодні близько 60,0 % технологічних процесів керуються безпосередньо вбудованими системами управління, які функціонують автономно або в складі більш складних систем [9], очевидною є тенденція до розширення сфери застосування вбудованих комп'ютерних систем у побутових приладах. Звідси обґрунтовано можна прогнозувати зростання кількості посягань, пов'язаних з несанкціонованим втручанням у роботу вбудованих систем. Чи свідчить це про потребу більш ретельної розробки питання про особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем у контексті норм розділу XVI Особливої частини КК? Можливо так. У той же час, є необхідність внесення відповідних змін до законодавства з метою відмови від окремого розгляду таких діянь, забезпечення їх кримінально-правової оцінки в межах шахрайства, ухилення від сплати податків тощо. Який підхід є більш перспективним з позицій ефективності кримінальної юстиції? Вважаємо, що окреслені питання потребують свого подальшого розв'язання як науковцями, так і практиками.

Список використаних джерел

1. Грицай Д. Д. Особливості побудови комп'ютерної системи тестування цифрових пристроїв на базі SOFT-процесорів [Електронний ресурс] / Д. Д. Грицай, А. І. Роговенко // Вісник Чернігівського державного технологічного університету. "Технічні науки". – 2011. – № 2(49). – Режим доступу : http://archive.nbuv.gov.ua/portal/natural/vcndtu/2011_49/.

2. Проектування спеціалізованих комп'ютерних систем : навч. посіб. / Я. М. Николайчук, Н. Я. Возна, І. Р. Пітух. – Тернопіль : Терно-граф, 2010. – 392 с.

3. Barr M. Embedded Systems Glossary [Electronic resourse] / Michael Barr // The Barr Group site. – Mode of access : http://www.barrgroup.com/Embedded-Systems/Glossary.

4. Embedded systems [Electronic resourse] // Embedded systems institute / Mode of access : http://www.esi.nl/research/embeddedsystems.dot.

5. Системи оброблення інформації. Основні положення. Терміни та визначення : ДСТУ 2938-94. – [Чинний від 1 січ. 1996 р.]. – К. : Держспоживстандарт України, 1996. – 20 с.

6. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.

7. Лукина Н. Для регистрации ККТ договор аренды помещения не нужен [Электронный ресурс] / Н. Лукина // Главбух. – 2011. – 25 дек. – Режим доступа : http://www.glavbukh.ru/art/19724.

8. Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг : Закон України від 6 лип. 1995 р. № 265/95-ВР (зі змін. і доп.) / [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/265/95-%D0%B2%D1%80.

9. Заквасов В. В. Програмно-апаратний комплекс для дослідження вбудованих систем керування [Електронний ресурс] / В. В. Заквасов // Електромеханічні і енергозберігаючі системи. – 2010. – № 1(9). – Режим доступу : http://archive.nbuv.gov.ua/portal/natural/Ees/2010_1/66.pdf.

В статье проанализированы вопросы, касающиеся особенностей уголовно-правовой квалификации несанкционированного вмешательства в работу встроенных компьютерных систем. Обоснованы соответствующие формулы уголовно-правовой квалификации такого рода деяний в различных вариантах их проявлений.

The issues regarding the specific features of criminal-legal qualification of unauthorized intervention in the embedded computer systems are analyzed. The appropriate formulas of criminal-legal qualification of such acts in various forms of their displaying are grounded.

Стаття надійшла до редакції журналу 19 вересня 2013 року.