думку слідчого, істотної шкоди (чи її загрози) при такому діяння, цілком можна пояснити, але наявність реальної шкоди (чи загрози її завдання), яка нормативно визначена при крадіжці - не заперечує наявність відповідного складу злочину. По-друге, дослідимо чи є малозначність діяння видом звільнення від кримінальної відповідальності. Судова практика має негативну відповідь на це питання: Пленум Верховного Суду України у п. 2 своєї постанови «Про практику застосування судами України законодавства про звільнення особи від кримінальної відповідальності» від 23 грудня 2005 р. № 12 не визначав такий вид звільнення особи від кримінальної відповідальності. В теорії кримінального права загальноприйнятою є аналогічна позиція. Відомий фахівець з вказаного питання Ю.В. Бауліна також не відносить малозначність до видів звільнення від кримінальної відповідальності [1, с. 174]. Викладене свідчить про невідповідність законодавству рішень суду про закриття проваджень у зв'язку зі звільненням особи від кримінальної відповідальності через малозначність діяння. Тому є необхідним закріпити нову умову для закриття провадження в п. 9 в ч. 1 ст. 284 КПК «встановлена малозначність діяння».

Викладене дозволяє запропонувати певні нормативні напрями удосконалення проблеми розуміння та застосування поняття малозначності діяння: 1) передбачити в ст. 11 КК нову ч. 3 у такій редакції: «Малозначність діяння не встановлюється при завданні злочином достатніх та визначених фізичних та майнових наслідків для відповідного складу»; 2) заміна терміна «істотна шкода» в диспозиціях норм Особливої частини КК на інший - «значна шкода»; 3) доповнити ч. 1 ст. 284 КПК пунктом 9 такого змісту: «встановлена малозначність діяння».

Список використаних джерел:

1. Кримінальний кодекс України. Науково-практичний коментар : у 2 т. / [за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна]. - 5-те вид., допов. - Х. : Право, 2013. - Т. 1 : Загальна частина / [Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін.]. - 2013. - 376 с.
2. Севастьянова Т. Є. Малозначність діяння за кримінальним законодавством України: дис. ... кандидата юрид. наук : 12.00.08 / Севастьянова Тетяна Євгенівна. - Запоріжжя, 2002. - 183 с.
3. Маломуж С. І. Напрями удосконалення малозначного діяння / С. І. Маломуж // Часопис Академії адвокатури України. -2014. - №3 (24) ; том 7. - С. 61-64.

Інформаційна диверсія та інформаційний саботаж - інструменти кібертероризму

Кузьменко Б.В., доктор технічних наук, професор, професор кафедри автоматизації та комп'ютерно-інтегрованих технологій Академії муніципального управління

Серед всієї множини злочинів у галузі в інформаційно-комп'ютерній сфері одними з найнебезпечніших є інформаційний (комп'ютерний) саботаж та інформаційна (комп'ютерна) диверсія, які є важливими інструментами кібертероризму. Комп 'ютерний саботаж (QS) складають наступні види злочинів: QSH - саботаж з використанням апаратного забезпечення: введення, зміна, знищення комп'ютерних даних або програм; втручання в роботу комп'ютерних систем з наміром перешкодити функціонуванню комп'ютерної або телекомунікаційної системи. QSS - комп'ютерний саботаж з програмним забезпеченням: знищення, пошкодження, погіршення або стримування комп'ютерних даних або програм без права на те. До інших видів комп 'ютерних злочинів (QZ) відносяться: QZB - використання електронних дошок об'яв (BBS) для зберігання, обміну і розповсюдження матеріалів, що мають відношення до злочинної діяльності. QZE - розкрадання інформації, що є комерційною

таємницею: придбання незаконними засобами або передача інформації, що становить комерційну таємницю, без права на те або іншого законного обґрунтування з наміром заподіяти економічного збитку або одержати незаконні економічні переваги.QZS - використання комп'ютерних систем або мереж для зберігання, обміну, розповсюдження або переміщення інформації конфіденційного характеру.

«Внесення, зміна, пошкодження або знищення комп'ютерний даних або програм, а також втручання в комп'ютерну систему, з наміром перешкоджати функціонуванню комп'ютера або телекомунікаційної системи». Головна мета в цьому злочині - перешкоджати звичайному функціонуванню комп'ютера або телекомунікаційної системи. Це є ширшим, ніж пошкодження комп'ютерних даних. Комп'ютерний саботаж включає всі види втручання в комп'ютерну систему. Зокрема введення неправильних даних, для того, щоб порушити роботу системи. Сюди також відносяться всі види фізичного пошкодження комп'ютера, а також такі дії, як виключення напруги. Хакери можуть також досягти цієї мети за допомогою модифікації системних файлів. Відомий також комп'ютерний (інформаційний) саботаж програмного забезпечення. «Внесення, зміна, пошкодження або знищення комп'ютерний даних або програм, а також втручання в комп'ютерну систему, з наміром перешкоджати функціонуванню комп'ютера або телекомунікаційної системи». Головна мета в цьому злочині - перешкоджати звичайному функціонуванню комп'ютера або телекомунікаційної системи. Це є ширшим, ніж пошкодження комп'ютерних даних. Комп'ютерний саботаж включає всі види втручання в комп'ютерну систему. Зокрема введення неправильних даних, для того, щоб порушити роботу системи. Сюди також відносяться всі види фізичного пошкодження комп'ютера, а також такі дії, як виключення напруги. Хакери можуть також досягти цієї мети за допомогою модифікації системних файлів. QSH - саботаж з використанням апаратного забезпечення: введення, зміна, знищення комп'ютерних даних або програм; втручання в роботу комп'ютерних систем з наміром перешкодити функціонуванню комп'ютерної або телекомунікаційної системи.

Злочини проти основ національної безпеки - найбільш тяжкі злочини, відомі кримінальному законодавству. Шкоду, яку вони можуть заподіяти, не можна недооцінювати. Державна зрада, шпигунство, диверсія, можуть спричинити знищення об’єктів, що мають важливе економічне і військове значення, дезорганізацію роботи державних або громадських організацій, і що найголовніше - до загибелі великої кількості людей. Безпосередньо диверсійні акти заподіюють державі не тільки серйозний матеріальний збиток але і негативно впливають на психологічний стан населення, можуть викликати паніку та інші негативні явища. У сучасних умовах, з урахуванням створення нових засобів масового ураження величезної руйнівної сили, хімічної і бактеріологічної зброї великої потужності, небезпека диверсії ще більше зростає. Тому відповідні органи держави спрямовують свої зусилля на попередження диверсії ще на ранніх стадіях здійснення цього злочину. На жаль, рамки статті 113 КК України не дозволяють здійснити більш детальний аналіз сучасних форм та видів диверсійної діяльності залежно від способів та засобів її здійснення. Тому наше наукове дослідження має бути спрямоване саме на вивчення нових форм диверсійних актів в умовах сучасності. Особливим видом диверсії, який з’явився відносно недавно, є так звана інформаційна диверсія - кібердиверсія (диверсія, що має відношення до комп’ютерів та комп’ютерних мереж). Швидкий розвиток Інтернету відкрив широкий спектр можливостей як у сфері пропаганди, так і безпосередньо у сфері озброєної боротьби. Способи

здійснення комп'ютерних злочинів можна поділити на три групи: 1) способи безпосереднього доступу до комп'ютерної інформації; 2) способи віддаленого доступу до комп'ютерної інформації; 3) способи розповсюдження технічних носіїв інформації, які вміщують у собі шкідливі програми для ЕОМ.

Будь-яке індустріально розвинене суспільство характеризується високим ступенем залежності від комп'ютерних мереж. Водночас чимала кількість американських дослідників намагається переконати у зворотному. Мовляв, загроза вторгнення є мінімальною, і кіберзлочинці здатні застосувати хіба що «зброю не масового ураження, а зброю масового роздратування». Один із аргументів такої позиції ґрунтується на тому, що кібератаки, за досвідом, дуже рідко спричиняють фізичні збитки, що потребують довготривалого ремонту. Дж. Льюїс зазначає, що «в контексті макроекономіки збої в системах водопостачання, електроенергії та повітряного руху, так само інші сценарії кібертерору, видаються стандартними подіями». Стандартними, тобто такими, що не торкаються системи національної безпеки країни. На думку цього автора, для національної економіки, де десятки чи навіть сотні систем забезпечують роботу найважливіших інфраструктур, збої в системах, коли обслуговування споживачів припиняється на години та навіть дні - є «стандартним випадком на регіональному рівні».

Інформаційна диверсія та інформаційний саботаж є небезпечними інструментами, зокрема, кібертероризму. Кібертероризм - це один з напрямків тероризму, в якому об'єктом деструктивної дії для досягнення цілей використовують інформаційно-обчислювальну техніку, комплекси та мережеві сегменти, які підтримують критично важливі, з точки зору національної безпеки, системи. Як предмет дії використовують засоби обчислювальної техніки та їх програмне забезпечення. Для України нині ця проблема постає гостро, а з приєднанням до глобального інформаційного простору потенційна загроза посилюватиметься. І поки кібертероризм з розряду «потенційної» загрози переходить до розряду реальної загрози, слід застосовувати всю множину заходів для недопущення його становлення. Основою забезпечення боротьби з кібертероризмом повинно бути створення ефективної загальнонаціональної системи заходів із запобігання,виявлення та припинення такого виду злочинних посягань.

Європеїзація прокуратури України: доктринально-правові засади та інституційно-функціональна трансформація

Проневич О.С., доктор юридичних наук, професор, головний науковий співробітник відділу наукового забезпечення організації роботи та управління в органах прокуратури Науково-дослідного інституту Національної академії прокуратури України

Європейська інтеграція є невід'ємною складовою глобалізації як процесу становлення ґрунтованих на загальноцивілізаційних засадах структур, зв'язків і відносин у різних сферах людської життєдіяльності. Розбудова незалежної української держави здійснюється у контексті європейської інтеграції, що передбачає реалізацію системних реформ відповідно до норм і стандартів Європейського Союзу. Євроінтеграційний вибір України об'єктивно зумовлений прагненням забезпечити належний рівень захисту прав і свобод людини та громадянина, створити умови для ствердження класичної моделі ринкової економіки та інтенсифікації зовнішньоекономічного співробітництва,