Міністерство освіти і науки України
Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем'янчука

А. В. БОРОВИК, І. М. КОПОТУН

КІБЕРЗЛОЧИНИ В УКРАЇНІ

(кримінально-правова характеристика)

НАВЧАЛЬНИЙ ПОСІБНИК

Луцьк
ВолиньПоліграф
2019

УДК 343.9.024:004(477)
Б 83

Рекомендовано до друку вченою радою
Міжнародного економіко-гуманітарного університету
імені академіка Степана Дем'янчука
(протокол № 11 від 26.06.2019 р.)

Рецензенти:

Стрельцов Євген Львович – доктор юридичних наук, доктор теології, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки;

Головач Андрій Володимирович – доктор юридичних наук, доцент, заслужений юрист України;

Литвинов Олексій Миколайович – доктор юридичних наук, професор, заслужений працівник освіти України;

Шаблистий Володимир Вікторович – доктор юридичних наук, доцент.

Боровик А. В.

Б 83 Боровик А. В., Копотун І. М. Кіберзлочини в Україні (кримінально-правова характеристика): навч. посіб. Луцьк: СПД Гадяк Ж. В. друкарня «Волиньполіграф»™, 2019. 304 с.
ISBN 978-617-7129-76-8

У навчальному посібнику на основі сучасних наукових підходів, структури та змісту кримінологічних знань розглянуто предмет, систему й кваліфікацію злочинів у сфері кіберзлочинності, та перспективи розвитку. Сформульовано низку нових концептуальних положень, висновків і рекомендацій, що мають важливе теоретичне та практичне значення.

Для студентів, аспірантів, викладачів юридичних факультетів та вишів, працівників науково-дослідних установ, адвокатів, суддів, працівників правоохоронних органів, усіх, кого цікавлять проблеми запобігання злочинам у сфері кіберзлочинності.

УДК 343.9.024:004(477)

ISBN 978-617-7129-76-8
DOI

ЗМІСТ

Перелік умовних позначень

КВК – Кримінально-виконавчий кодекс

ККУ – Кримінальний кодекс України

КПК – Кримінальний процесуальний кодекс

МВС – Міністерство внутрішніх справ

ОВС – Орган внутрішніх справ

ООН – Організація Об'єднаних Націй

ОРД – Оперативно-розшукова діяльність

РЄ – Рада Європи

ОЧ ККУ – Особлива частина кримінального кодексу України

ЗЧ ККУ – Загальна частина кримінального кодексу України

НМДГ – Неоподаткований мінімум доходу громадян

ІТС – Інформаційно-телекомунікаційні системи

ШПЗ – Шкідливі програмні засоби

ШТЗ – Шкідливі технічні засоби

ДБО – Махінації в системах дистанційно банківського обслуговування

Передмова

Сьогодні важливу роль в соціальному й економічному розвитку багатьох країн світу відіграють кібернетичний та інформаційний простори, а також інформаційне суспільство, яке сформувалося внаслідок стрімкого розвитку науково-технічного прогресу та комп'ютеризації.

Проте існування глобального інформаційного простору призвело до появи інформаційних загроз. Отже, тема кібербезпеки надзвичайно актуальна і відкрита, особливо для України, враховуючи сучасний стан держави.

Кібербезпекою є стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також вчасне виявлення, запобігання та нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним або національним інтересам.

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» кібербезпекою є захищеність життєво важливих інтересів людини і громадянина, суспільства й держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, вчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

До складників кібернетичної безпеки належать: кібернетичні впливи; розвідка інформаційно-теле-

комунікаційних систем та криптосистем протиборчих сторін; захист власної інформаційної сфери.

Досягається такий стан завдяки сукупності активних захисних і розвідувальних дій, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційних ресурсів, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем.

Кібербезпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм.

Вибір конкретних засобів і шляхів забезпечення кібербезпеки України зумовлений необхідністю вчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз життєво важливим інтересам людини і громадянина, суспільства та держави.

Основні напрями забезпечення кібербезпеки України:

– розвиток інформаційної інфраструктури держави, гарантування безпечного функціонування об'єктів критичної інформаційної інфраструктури;

– розвиток міжнародного співробітництва у сфері кібербезпеки; зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з проявами кіберзлочинності та кібертероризму;

– забезпечення ефективного застосування Збройних сил України для адекватної відповіді реаль-

ним та потенційним кіберзагрозам національному сегменту кіберпростору;

– розвиток пріоритетних напрямів науки й техніки як основи створення високих інформаційних технологій; підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників;

– адаптація законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення її стійкості до кібератак, спроможності держави ефективніше захищати національні інтереси в кіберпросторі;

– забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних; підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі.

Проблематика кібербезпеки являє собою проблеми пов'язані з такими поняттями, як «кіберзлочин», «кіберзлочинець», «кіберпростір», «кіберзахист».

У сучасному світі ці поняття є дуже важливими, тому що кожен день ми стикаємося з необхідністю використання інформаційних технологій. Щодня ми заходимо на велику кількість вебсторінок і на більшості з них надаємо персональні дані про себе. Постає питання: наскільки захищені наші персональні дані? Чи є можливість захистити себе в мережевому просторі?

Питання кіберпезпеки ніколи не втрачало актуальності на всьому шляху історичного розвитку людства незалежно від форми організації суспільного життя.

Однак у нашій країні з цими питаннями виникають складнощі, при аналізі нашого законодавства було визначено, що такі поняття, як «кіберпростір», «кіберзлочинець», «кіберзахист», «кіберзлочин» досі не визначені.

За перші 6 місяців 2019 року в Україні було порушено 4041 кримінальних порушень у сфері порушень кіберзлочинності: 1336 – у сфері платіжних систем; 810 – кібербезпеки; 1380 – у сфері електронної комерції; 515- у сфері протиправного контенту. Отже, у сфері платіжних систем кількість злочинів у 2018 році зросла порівняно з 2017-м у 1,4 раза. У сфері протиправного контенту кількість злочинів у 2019 році порівняно із 2018-м також зросла.

Кіберзахист залежить не тільки від держави, а й від самих нас.

Оскільки більшість людей легковажно і не дуже обережно ставиться до цього питання, це стосується тих випадків, коли людина реєструється на сайтах, які їм невідомі, тим самим віддаючи персональні дані зловмиснику, а щодо платежів у мережі всі ми хочемо купити речі якомога дешевше і тому частіше всього ми потрапляємо в пастку людей, які розробили сайт із «дешевими» речами.

Купуючи речі на цих сайтах, ми переводимо деяку суму грошей на банківський рахунок зловмисника. Це один із прикладів, а їх можна на-

вести тисячі. А також підключивши до Free Wi-fi в публічних місцях, через відкритий wi-fi зловмисник може отримати доступ до ваших даних.

Стрімкий розвиток технологій інтернету зумовлює появу та розвиток нових видів кіберзлочинів, які мають серйозні та незворотні наслідки. Величезний технічний потенціал та безмежні можливості у віртуальному просторі все частіше використовуються кіберзлочинцями для шахрайства, тероризму та реалізації політичної мети.

Саме тому ми повинні налагоджувати співробітництво з іншими державами, міжнародними експертними організаціями в цій сфері, а особливо воно повинно активізуватися при розробленні відповідних нормативно-правових актів і прийнятті на рівні держави міжнародних норм та стандартів.

Положенням Стратегії національної безпеки на законодавчому рівні було деталізовано пріоритети державної політики у сфері гарантування кібербезпеки та безпеки інформаційних ресурсів, до яких належать: реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Розвиток безпечного, стабільного й надійного кіберпростору має полягати в підтримці міжнарод-

них ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні її співпраці з ЄС та НАТО для посилення можливостей нашої країни у сфері кібербезпеки, участі в заходах зі зміцнення довіри в кіберпросторі, які проводяться під егідою ОБСЄ.

Категорії «кібер» і «безпека» взаємопов'язані між собою. Збільшення потреб людського розвитку закономірно і логічно супроводжується збільшенням кількості загроз на шляху до їх реалізації. Загрози з виходом людства на кожний новий рівень цивілізаційного розвитку усе більше набувають економічного спрямування і закономірно виходять на перший план.

Вивченню проблем кіберпезпеки присвячено безліч фундаментальних досліджень, сотні монографій, тисячі статей. Незважаючи на те, що кібербезпека розглядалася багатьма вченими, дослідження її природи не втрачає актуальності. Традиційно питання розглядається через тріаду: національна безпека, державна безпека – безпека регіону.

Це зрозуміло і логічно з позицій класичної ієрархії. Змінюється тільки напрям залежно від завдань дослідження цього питання: від національної безпеки держави до економічної безпеки підприємства або навпаки. Це різні аспекти дослідження проблеми. А тому включаються різні механізми переходу від одного рівня безпеки до іншого.

Першопричиною появи загроз для безпеки можна назвати порушення балансу фактично на всіх рівнях розвитку суспільства: економічному, соціальному, екологічному, енергетичному, демографічному, технологічному тощо.

Упровадження нових технологій у сферу людської продуктивної діяльності зумовило виникнення технологічно нових загроз з вищим потенціалом деструктивного впливу.

Сучасний світ характеризується високим рівнем інформаційно-телекомунікаційного забезпечення економічного розвитку країн світу, серед яких Україна з її потенціалом цифрових технологій.

На їх основі відбуваються процеси акумулювання цифрових технологій, створення необхідних баз даних, системи захисту економічної безпеки, техніко-технологічне забезпечення стабільного функціонування IT-інфраструктур підприємств.

Технології, методи і способи гарантування безпеки можуть бути найрізноманітнішими. Це залежить від того, в якій сфері життєдіяльності виникла загроза. Наприклад, можна закрити кордони, організувати тотальний контроль і встановити відповідний режим, створити спільну систему безпеки, розробити й упровадити високотехнологічні системи захисту, увести суворо регламентовану систему розподілу ресурсів, заборонити певні види діяльності тощо.

Країни Західної Європи для гарантування національної безпеки почали використовувати економічні методи. Намітилися два підходи до боротьби із загрозами безпеки взагалі й економічної зокрема. Перший із них полягає в тому, що загроза як фактор може і не виникнути. Навіщо ж витрачати час і гроші на їх попередження. З'явиться загроза, усуватимемо її. Інший підхід полягає в тому, щоб завчасно спрямувати зусилля на виявлення потен-

ційних загроз та створення ефективних механізмів їх усунення.

І перший, і другий підходи цілком зрозумілі. Перший більше пов'язаний із ризиком втрат і для підприємства, і для регіону або країни загалом. Водночас, якщо все буде організовано грамотно, професійно і керівництво буде далекоглядним, то ймовірність виникнення загроз буде мінімальною. Однак якщо виникне загроза, то доведеться вжити заходів щодо її усунення і передбачити можливість повторення, закріпивши набутий досвід.

Розвивається телекомунікаційна галузь, і не відстає в розвитку телекомунікаційне шахрайство. Розвиток шахрайства стимулює роботу над створенням ефективних і надійних систем захисту. На створення цих систем захисту оператори витрачають значні кошти, щоб запобігти навмисному несанкціонованому доступу до послуг зв'язку.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації, Національна поліція України, СБУ, Міністерство оборони України та Генеральний штаб ЗСУ, розвідувальні органи, Національний банк України, Державний комітет фінансового моніторингу України, ФАТФ (FATF).

Дослідження проблеми захищеності кіберпростору України дає підстави зробити висновки про те, що для гарантування безпеки необхідний комплекс заходів, інфраструктур, технічних засобів, програмного забезпечення та організаційно-юридичних процедур, спрямованих на виявлення, нейтралізацію та запобігання кіберпорушенням у кіберпросторі.

Отже, можна стверджувати, що в час глобалізаційних процесів інформаційно-телекомунікаційні системи стають уразливими, тому кібернетична безпека України є пріоритетним напрямом, що захищає інтереси держави, підтримує обороноздатність, забезпечує повноцінну діяльність економічних та інших сфер, отож сприяє збалансованому існуванню суспільства та нейтралізації дії внутрішніх і зовнішніх загроз та небезпек.

Навчальний посібник розроблено на основі сучасних наукових підходів до структури та змісту кримінологічних знань. Розглянуто предмет, систему й кваліфікацію злочинів у сфері кіберзлочинності, перспективи розвитку, сформульовано низку нових концептуальних положень, висновків і рекомендацій, що мають важливе теоретичне та практичне значення.

Сподіваємося, що навчальний посібник буде корисний студентам, аспірантам, викладачам юридичних факультетів та вишів, працівникам науково-дослідних установ, адвокатам, суддям, працівникам правоохоронних органів, усім, кого цікавлять проблеми запобігання злочинам у сфері кіберзлочинності.

Вдячний професорам О. Г. Колбу, О. М. Литвинову, В. В. Шаблистому за їхні корисні наукові побажання, які дали змогу комплексніше дослідити нам цю правову проблематику.

Доктор юридичних наук, професор,
заслужений юрист України **І. М. Копотун**

Розділ 1

Поняття та принципи кримінально-правової кваліфікації

Використання інтернету має низку позитивних переваг та необезпечене його використання призводить до негативних наслідків.

Розвиток глобальних систем призвів до багатократного збільшення кількості користувачів і росту кількості атак на комп'ютери, підключені до інтернету. Тому при підключенні до інтернету необхідно потурбуватися про гарантування інформаційної безпеки підключених локальних чи корпоративних мереж.

Через інтернет порушник може:

– проникнути до внутрішньої мережі підприємства та отримати несанкціонований доступ до конфіденційної інформації;

– незаконно скопіювати важливу і цінну для підприємства інформацію;

– отримати паролі, адреси серверів і навіть їх зміст;

– заходити до інформаційної системи підприємства під іменем користувача, раніше зареєстрованого тощо.

З допомогою отриманої правопорушниками інформації може бути серйозно підірвана конкурентоспроможність підприємства і довіра клієнтів до нього.

Однією з актуальних тем у сфері кібербезпеки є вдосконалення систем безпеки, що захищають ІТ-системи від атак із вимогами.

У деяких країнах знову з'являються повідомлення про кіберзлочинців із *Ransomware*. Ці віруси поширюються електронною поштою, яка автоматично відправляє себе із заражених облікових записів електронної пошти і розсилає інфіковані електронні листи всім контактам електронної пошти вірусної поштової скриньки, інфікованої вірусом. Він є дуже небезпечним, оскільки після відкриття підробленої електронної пошти встановлюється глибоко в комп'ютер і шифрує доступ до дисків, блокуючи доступ до вмісту дисків.

Аналіз банківських троянів полягає в дослідженні методів кіберзлочинності у сфері зараження інформаційних систем банку – і тих, які є внутрішньобанківськими, і тих, які обслуговують клієнтів банку як частину інтернет-мобільного банкінгу. Аналіз атак кіберзлочинців, наприклад, популярних останнім часом вірус-троян типу вимагання, який після шифрування комп'ютерів шифрує дані дисків. Крім того, інші типи троянських коней використовуються для крадіжки конфіденційних даних, особистих клієнтів або розкрадання коштів із банківських рахунків клієнтів, вимагання кредитів тощо.

Після аналізу методів, що використовують кіберзлочинці, банки зміцнюють системи безпеки, захищають банківські системи від цих атак, поліпшують безпеку та інструменти авторизації клієнтів онлайн-банкінгу. Крім того, наступним кроком

є вдосконалення процесу управління ризиками ІТ-систем.

Крім того, атаки на комп'ютерні злочини на електронних банківських системах, імовірно, набагато більше, ніж надає офіційна статистика, оскільки банки не похвалилися цими подіями, якщо їм не потрібно. Це пояснюється тим, що багато з цих атак на кіберзлочинність неефективні або мають відносно низькі витрати, а виявлені прогалини в системі електронного банкінгу швидко відновлюються. Однак якщо клієнти банку знали всі ці події кіберзлочинців, це може знизити рівень довіри до банків. Тоді клієнти банку могли б почати виводити банківські депозити з банків у масовому масштабі, тоді серйозною проблемою для банків з'явилося б пов'язане з різким зростанням рівня ризику ліквідності.

Ще однією з актуальних тем у сфері кібербезпеки є аналіз систем безпеки, розроблених у порталах соціальних медіа. Однак, незважаючи на запевнення компаній, які працюють на порталах соціальних медіа, інформація, що міститься на цих вебсайтах, не завжди повністю захищена від діяльності кіберзлочинців. Крім того, для того, щоб обробляти їх для маркетингових цілей, слід додати питання про завантаження даних великих компаній із порталів соціальних медіа.

Питання конфіденційності в соціальних мережах дуже важливе і стосується безпеки особистої інформації. Конфіденційність перебуває під загрозою з точки зору інформації, розміщеної на порталах соціальних медіа.

1.1. Зміст поняття «кримінально-правова кваліфікація»

Поняття «кримінально-правова кваліфікація» розглядають у нерозривній сукупності двох значень:

– це інтелектуальна діяльність зі встановлення відповідності між фактичними обставинами вчиненого діяння та положеннями кримінального закону (кваліфікація як процес);

– це остаточна юридична та суспільно-політична оцінка вчиненого особою діяння як злочину чи незлочину (кваліфікація як результат);

Отже, *кримінально-правова кваліфікація* – це оцінка вчиненого особою діяння, яка включає в себе обґрунтування та процесуальне закріплення висновку про те, чи таке діяння передбачене відповідною статтею (статтями, частиною, пунктом) кримінального закону і, відповідно, що воно є (не є) злочином чи іншим діянням, передбаченим кримінальним законом.

Визначення положення (положень) кримінального закону, яке підлягає застосовуванню до конкретного випадку, зазвичай, здійснюється за таким алгоритмом:

1) проводиться оцінка фактичних обставин справи. Для цього, діяння, яке підлягає кримінально-правовій оцінці «розкладається» за ознаками елементів складу злочину (об'єкт, предмет, потерпілий, суспільно небезпечне діяння, суспільно небезпечний наслідок, причинний зв'язок між суспільно небезпечним діянням та суспільно небезпечним наслідком, час, місце, спосіб, знаряддя, засоби, обстановка, ознаки суб'єкта, форма та вид вини, мотив, мета, емоційний стан особи тощо) та з'ясо-

вуються інші обставини, які можуть мати кримінально-правове значення (причини, чому злочин не доведено до кінця, наявність співучасників тощо). При цьому встановлюється не лише наявність чи відсутність таких ознак, а з'ясовується їх фактичний зміст;

2) здійснюється «вибір» статті (статей, їх частин або пунктів) ККУ, які містять кримінально-правове положення, яке найбільш імовірно може бути застосоване в ситуації, яка підлягає кримінально-правовій оцінці. При цьому слід мати на увазі, що застосуванню можуть підлягати і положення ОЧ ККУ і положення ЗЧ ККУ;

3) обґрунтовується необхідність застосування конкретного положення ККУ (встановлюється наявність чи відсутність складу злочину, обставин, що виключають злочинність діяння тощо).

Очевидно, що кожен із названих вище кроків можна розподілити на більш детальні, які в науковій літературі називаються етапами процесу кримінально-правової кваліфікації.

За результатами кримінально-правової оцінки діяння особи приймається процесуальне рішення, яке відображається у відповідних актах від початку кримінального провадження до постанови вироку чи іншого рішення суду.

1.2. Поняття і види підстав кримінально-правової кваліфікації

Підстави кримінально-правової кваліфікації – правові явища, відповідно до яких здійснюється

кримінально-правова оцінка діяння, те, що лежить в її основі.

У теорії кримінального права прийнято виділяти фактичну і юридичну підстави кримінально-правової кваліфікації.

Фактична підстава кваліфікації – вчинене діяння, фактичні обставини, які підлягають правовій оцінці, зіставляються з правовою нормою.

Такою підставою виступає не саме вчинене діяння, а доказова інформація про нього, яка стала відома відповідним органам і здобута ними в законному порядку. Доказуванню обов'язково підлягають ті фактичні ознаки злочину, які прямо вказані в диспозиції статті ОЧ ККУ, а в разі, якщо є підстави вважати, що діяння не є злочином – ознаки, які обґрунтовують такий висновок (відсутність ознак суб'єкта, дотримання умов необхідної оборони тощо). При кваліфікації можуть враховуватися лише ті фактичні обставини справи, закріплені доказами, що належно процесуально оформлені.

Окрім цього, слід наголосити, що відповідно до положень ЗУ «Про оперативно-розшукову діяльність» від 18.02.1992 р. матеріали такої діяльності також використовуються для отримання фактичних даних, які можуть бути доказами у кримінальному провадженні (п. 2 ст. 10). Однак для того, щоб такі матеріали бути використані при кримінально-правовій кваліфікації, вони повинні або перевірятися слідчим шляхом, або ж бути отримані у встановленому КПК України порядку.

Юридична підстава кримінально-правової кваліфікації – це юридичний склад злочину – сукуп-

ність встановлених у законі юридичних ознак (об'єктивних і суб'єктивних), котрі визначають учинене суспільно небезпечне діяння як злочинне.

Ці ознаки, зазвичай, містяться в статті ОЧ ККУ, але іноді доповнюються за допомогою положень ЗЧ ККУ. Саме вони відображаються, в кінцевому результаті, у формулі кримінально-правової кваліфікації.

При цьому, за стосунком до *процесу* кваліфікації статті ЗЧ ККУ поділяються на три групи:

– статті, до яких у процесі кваліфікації не звертаються ніколи (які регламентують питання покарання, його призначення, звільнення від покарання та його відбування тощо);

– статті, які використовуються в процесі кваліфікації окремих видів діянь (наприклад, статті 14, 15, 24, 25, 27 ККУ);

– статті, які використовуються при кваліфікації будь-якого діяння (осудність (ст. 19 ККУ), вік, з якого може наставати кримінальна відповідальність (ст. 22 ККУ) тощо).

Натомість у *результаті* кваліфікації (у формулі кримінально-правової кваліфікації), використовуються лише *обмежена кількість* перерахованих статей ЗЧ ККУ та їх частин (взагалі-то, лише ч. 2 ст. 14 або ч. 3 ст. 15, частини 3, 4 або 5 ст. 27 ККУ). Інші не вказуються ніколи.

Водночас, не слід забувати, що для з'ясування змісту статей ККУ в багатьох випадках потрібно звертатися і до інших джерел, які називають *додатковими юридичними підставами кримінально-правової кваліфікації*:

– інші кримінально-правові норми (якщо на них прямо вказує відсильна диспозиція чи коли в іншій нормі витлумачено зміст понять, які використовуються в «основній» нормі);

– нормативні акти інших галузей права (за наявності бланкетних норм кримінального закону чи в разі субсидіарного застосування правових норм тоді, коли прямих відсилок у нормі ОЧ ККУ немає, але їх використання випливає зі змісту відповідних норм);

– норми суспільної моралі, звичаї, правові принципи, загальні уявлення про право (при з'ясуванні змісту оцінних понять, які використовуються в кримінально-правових нормах);

– акти офіційного тлумачення Конституції України та кримінального закону;

– прецеденти (якщо це відповідає вимогам забезпечення правильного й одностайного застосування кримінального закону).

Джерела з останніх двох пунктів містяться в матеріалах узагальнення правозастосовної практики, які існують у вигляді і неписаних, і формалізованих приписів. У першій формі – це положення, які передаються від досвідчених працівників до початківців, поширюються серед колег одного рівня. У другій формі практика існує як:

– рішення Конституційного Суду України;

– постанови Пленуму Верховного Суду України (а з 2010 року – Пленуму Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ) з тих чи тих категорій кримінальних проваджень;

– узагальнення практики застосування законодавчих норм стосовно певних категорій злочинів;

– листи, роз'яснення, відповіді на запитання, що надходять до керівних правоохоронних органів;

– методичні вказівки щодо розслідування, розгляду окремих категорій кримінальних проваджень.

Роз'яснення Пленуму Верховного Суду України (Пленуму Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ) із питань застосування законодавства де-факто сприймаються суддями та працівниками правоохоронних органів на рівні з законом. Але ж зауважимо: де-юре вони є актами *тлумачення* кримінального закону, причому не належать до офіційного (правом на здійснення якого володіє тільки Конституційний Суд України), а тому такі роз'яснення не повинні ставитися вище положень ККУ.

Від підстав кримінально-правової кваліфікації слід відрізняти підстави перекваліфікації, якими можуть виступати:

А) зміна обсягу процесуально встановленої інформації про факти, які підлягають кримінально-правовій оцінці;

Б) зміна кримінального закону внаслідок якої новий кримінальний закон набуває зворотної сили. Причому зміна кваліфікації може бути здійснена й у справах, де вироки вже винесені;

В) помилка, або виявлені зловживання працівників, які здійснюють кримінально-правову кваліфікацію;

Г) зміна правил кваліфікації того чи іншого діяння.

1.3. Принципи кримінально-правової кваліфікації

Кримінально-правова кваліфікація, як і будь-яка цілеспрямована свідома діяльність людини, підпорядковується певним правилам. Ці правила за рівнем їх використання можуть бути класифіковані на:

1) загальні, які поширюються на кримінально-правову оцінку будь-якого діяння;

2) типові, що стосуються кваліфікації певних типів злочинних діянь (попередньої злочинної діяльності, злочинів, учинених у співучасті, повторних злочинів тощо);

3) конкретні, які застосовуються при кваліфікації окремих видів злочинів (крадіжки, тілесних ушкоджень, хуліганства і тощо).

Положення першого виду складають принципи кримінально-правової кваліфікації – систему науково обґрунтованих, стабільних, таких, що застосовуються свідомо, найбільш загальних правил, на підставі яких здійснюється обґрунтування та процесуальне закріплення висновку про те, чи таке діяння передбачене відповідною статтею (статтями, частиною, пунктом) кримінального закону і, відповідно, що воно є (не є) злочином чи іншим діянням, передбаченим кримінальним законом.

Найбільш часто до принципів кримінально-правової кваліфікації належать такі:

Принцип законності. Зміст цього принципу полягає в тому, що кримінально-правова кваліфікація як вид застосування кримінального закону повинна здійснюватися лише на підставі закону і в

точній відповідності до нього. Саме закон є вищим критерієм правильності рішень, які приймаються в ході правозастосування. Застосування права не лише здійснюється на підставі закону, а й регламентоване ним. Усі – і загальні положення, відповідно до яких здійснюється кримінально-правова кваліфікація і її принципи, і конкретні правила кваліфікації випливають із окремих правових норм чи їх сукупності, які містяться в законі.

Принцип законності має визначальний вплив на зміст усіх інших принципів кваліфікації, є головним серед них.

Принцип стабільності кримінально-правової кваліфікації. Зміст цього принципу полягає в тому, що в процесі кримінально-правової оцінки діяння має бути прийнято об'єктивне рішення, яке, в ідеалі, не змінюється в ході досудового слідства судового розгляду тощо. Водночас, виходячи із прагнення забезпечити стабільність зафіксованих у процесуальних документах висновків про оцінку діяння, чинне законодавство передбачає можливість та певну процедуру зміни кваліфікації на різних стадіях кримінального процесу.

Принцип офіційності кримінально-правової кваліфікації полягає в тому, що така діяльність це прерогатива спеціально на те уповноважених державних органів. Тому й кваліфікація виступає як форма державно-владної діяльності, як діяльність офіційна. Більше того правова оцінка вчиненого є одним із важливих завдань держави, виступає не правом, а обов'язком її компетентних органів. Кримінально-правова кваліфікація спрямована і

на визначення правомірності вчиненого з точки зору кримінального закону, і на забезпечення кримінального переслідування тих, хто вчиняє злочини. При цьому очевидно, що передумовою застосування стосовно особи будь-яких правових заходів, передбачених кримінальним законом, є кваліфікація скоєного від імені держави.

Чинне процесуальне законодавство визначає коло органів, які здійснюють кримінально-правову оцінку діяння особи від імені держави, встановлює їх повноваження, передбачає порядок закріплення результатів кримінально-правової кваліфікації в процесуальних документах. З відповідних норм випливає, що лише така – офіційна – кваліфікація має правове значення. Тому вказаний принцип прямо випливає з головного принципу кримінально-правової кваліфікації – принципу законності;

Принцип повноти кримінально-правової кваліфікації. Кваліфікація повинна відображати кримінально-правову оцінку вчиненого діяння в повному обсязі. Якщо ж піддати оцінці лише частину вчиненого особою діяння (діянь), оцінити його з позицій не всіх наявних кримінально-правових норм, а лише окремих із них, то очевидно, що така кваліфікація не буде об'єктивною і правильною.

Необхідність повноти кваліфікації випливає також із принципу законності. Він може вважатися реалізованим, коли закон застосований у повному обсязі, всі норми, які поширюються на це діяння враховані при оцінці відповідної поведінки особи.

Принцип точності кримінально-правової кваліфікації. Його дотримання полягає в тому, що

кримінально-правова кваліфікація, що має бути проведена відповідно до закону, є правильною коли вибрано саме те положення, яке передбачає скоєне діяння, а у формулі відображена не лише стаття (статті), а також її (їх) відповідна частина, пункт тощо. У разі вчинення, наприклад, незакінченого злочину чи злочину вчиненого у співучасті це також обов'язково має бути відображене у формулі кримінально-правової кваліфікації.

Принцип індивідуальності кримінально-правової кваліфікації. Указаний принцип кваліфікації безпосередньо виходить із конституційного положення про те, що «юридична відповідальність кожної особи має індивідуальний характер» (ч. 2 ст. 61 Конституції України). Тому в ході кваліфікації має бути: а) проведена індивідуальна правова оцінка кожного діяння окремо, б) диференційована роль кожної особи у вчиненні злочину, в) неможливість притягнення до кримінальної відповідальності інших осіб.

Принцип недопустимості подвійного інкримінування. Указаний принцип кримінально-правової кваліфікації базується на конституційному положенні, згідно з яким «ніхто не може бути двічі притягнений до юридичної відповідальності одного виду за одне й те саме правопорушення» (ч. 1 ст. 61 Конституції України). Виходячи з цього, кваліфікація діяння за певною нормою виключає застосування до цього ж діяння іншої норми, норм (статей ККУ), якщо скоєне повністю отримало кримінально-правову оцінку.

Принцип об'єктивності кримінально-правової кваліфікації. Запорукою об'єктивності кваліфіка-

ції є використання в її ході об'єктивно установлених підстав. Тому при кваліфікації слід виходити з встановлених у процесуальному порядку обставин справи, а не з власних догадок, припущень, уподобань. Водночас необхідно керуватися кримінальним законом, актами його офіційного тлумачення, а не своєю суб'єктивною оцінкою скоєного та розумінням закону, уявленнями про оцінку скоєного потерпілим чи іншими особами.

Принцип гуманності проявляється при кваліфікації в тому, що всі сумніви та суперечності при застосуванні кримінально-правових норм повинні тлумачитися на користь обвинуваченого (підсудного, засудженого). Отже, кваліфікація повинна в такому разі схилятися до пом'якшення кримінальної відповідальності особи.

1.4. Вирішення колізії та конкуренції норм у кримінальному праві

У праві колізією звичайно розуміють як таке співвідношення між двома чи більше юридичними положеннями, коли вони спрямовані на регламентацію одного і того ж питання, але по-різному його вирішують, тому застосування одного з них виключає застосування іншого.

Конкуренція як правове поняття означає наявність кількох правових положень, які «претендують» на застосування до певного випадку. При цьому суперництво між ними виникає лише в ході їх застосування до конкретних фактичних обста-

вин. Поза правозастосуванням вони між собою не суперечать і можуть існувати одночасно.

Колізія та конкуренція в кримінальному праві, хоча і мають спільні риси, оскільки в обох випадках має місце наявність кількох статей (частин статей, пунктів статей) нормативно-правових актів, які одночасно передбачають (охоплюють) діяння, яке підлягає кримінально-правовій кваліфікації, але все ж таки відрізняються за своєю юридичною природою в наступному:

– колізія може існувати між кількома нормативно-правовими актами (відповідними статтями кількох таких актів) або різними частинами кримінального закону, а конкуренція лише між статтями (їх структурними частинами) одного кримінального закону;

– при колізії статті закону (викладені в них положення) суперечать одна одній, при конкуренції – ні;

– при колізії одне положення виключає дію іншого, а конкуруючі статті закону існують паралельно;

– подолання колізії та конкуренції відбувається в різний спосіб.

У кримінальному праві України виділяють такі можливі види *колізій та шляхи їх вирішення*:

1) Колізії між положеннями Конституції України та статтями ККУ. Прямої невідповідності між положеннями, закріпленими в Конституції України, та статтями чинного ККУ не простежується. Однак окремі розбіжності між нормами, закріпленими в статтях ККУ та Конституції

все ж таки мають місце. Це розбіжності, суть яких полягає в тому, що в ККУ формально передбачена відповідальність за певні діяння, а з КУ випливає правомірність відповідної поведінки. Наприклад, передбачені у ч. 1 ст. 34 Конституції України права кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір, можуть бути обмежені тільки у випадках, передбачених у ч. 2 цієї статті. Одне з таких обмежень виражено в ст. 363-1 ККУ. Проте такі обмеження можуть стояти на заваді реалізації інформаційних прав людини, гарантованих Конституцією України. Річ у тому, що ознаки «спаму», вказані у наведеній статті, сформульовані неправильно, не відповідно до загальноприйнятих у цивілізованому світі правил визнання розсилок «спамом». Ця колізія підтверджена життям, практикою – за весь час існування вказаної норми (з 2004 р.) були лише одиничні випадки її застосування.

Правило вирішення колізії в таких випадках: дія кримінально-правових норм обмежується – вони не можуть застосовуватися в тій частині, у якій не відповідають конституційним положенням.

2) Колізії між положеннями чинних для України міжнародно-правових договорів та статтями ККУ. Про такі колізії можна говорити, скоріше, гіпотетично, оскільки аналіз чинного ККУ та міжнародно-правових договорів не дозволяє, як видається, констатувати наявність суперечностей між ними з огляду на особливий порядок ратифікації міжнародно-правових договорів та специфічною

роллю міжнародно-правових договорів, які містять положення кримінально-правового характеру, які по суті передбачають лише рекомендації щодо встановлення кримінальної відповідальності за певні діяння.

Водночас, можливі колізії між положеннями міжнародно-правових актів і ККУ мають вирішуватися так:

– якщо міжнародно-правовий акт передбачає встановлення кримінальної відповідальності, а в ККУ вона не передбачена, то пріоритет віддається ККУ;

– якщо з положень міжнародно-правового акта вбачається, що відповідальність за певні дії, криміналізовані в ККУ, не повинна наставати, то перевагу мають положення міжнародно-правового акта.

3) Колізії між статтями ККУ та інших законів й підзаконних нормативно-правових актів слід вирішувати так:

1) якщо діяння є правомірним відповідно до положень чинних нормативно-правових актів, то воно не може бути визнане злочином, хоча б формально й було передбачене в ККУ;

2) діяння, на злочинність чи щодо кримінально-правової оцінки якого є вказівка в нормативно-правових актах інших галузей права кваліфікується відповідно до положень, регламентованих у ККУ.

4) Колізії між статтями ЗЧ ККУ та ОЧ ККУ. ЗЧ ККУ має пріоритет над його Особливою частиною. Це стосується і питань законотворчості, і правозастосування. Інакше кажучи, законодавець

зобов'язаний так формулювати статті ОЧ ККУ, щоб вони не виходили за межі, не вступали у суперечність зі статтями ЗЧ ККУ, а наявні колізії повинні усуватися з ККУ через внесення до нього змін.

До того моменту, поки такі колізії не усунуті, особа, уповноважена на застосування кримінально-правових норм, мусить при виявленні колізії між частинами одного і того ж закону вирішувати певні питання так, як цього вимагає ЗЧ ККУ.

5) Колізії між окремими статтями (частинами статей) ОЧ ККУ. У таких випадках потрібно керуватися принципом, відповідно якого всі неясності, суперечливості закону вирішуються на користь особи, щодо якої застосовується кримінальний закон. Тому у разі колізій між різними частинами статей, окремими статтями ОЧ ККУ слід застосовувати статтю, її частину, яка найбільш «сприятлива» для особи, дії якої кваліфікуються.

При виділенні видів *конкуренції*, слід брати до уваги, що їй як правовому явищу притаманні такі істотні та необхідні ознаки: 1) існують принаймні дві статті (її (їх) структурні частини) ККУ, які спрямовані на урегулювання одного і того ж питання; 2) вчинено один злочин, який підпадає під ознаки двох (або більше) статей (її (їх) структурних частин) ККУ; 3) конкуруючі положення одночасно претендують на застосування при вирішенні цього конкретного випадку; 4) наявний функціональний зв'язок між конкуруючими нормами.

Характер функціонального зв'язку між конкуруючими нормами може проявлятись у таких

формах: 1) підпорядкування за об'ємом; 2) підпорядкування за змістом; 3) відсутність підпорядкування між конкуруючими спеціальними нормами, але наявність такого підпорядкування між кожною з них із єдиною загальною нормою.

Відповідно до цих форм взаємозв'язку норм і можна виділити основні види конкуренції кримінально-правових норм:

1) Конкуренція статей, які містять загальну та спеціальну норми. При конкуренції такого виду одна зі статей (яка містить загальну норму) охоплює визначене коло діянь, а інша (яка містить спеціальну норму) – частину цього кола, тобто різновиди діянь, передбачених загальною нормою. При цьому може бути цілий ряд статей, які містять ознаки спеціальних норм. Ці статті (норми) можуть бути між собою рівнозначними за обсягом (не підпорядковані) – відповідно, однаково розташованими щодо загальної, а можуть своєю чергою перебувати у співвідношення загальної та спеціальної (підпорядковані). Тоді певна норма є водночас і спеціальною щодо якоїсь більш широкої за обсягом – загальної, і загальною щодо вужчої – спеціальної.

Правила кваліфікації, які використовуються у правозастосовній практиці при конкуренції статей, які передбачають загальну та спеціальну норми:

– одночасна кваліфікація за статтями ОЧ ККУ, які передбачають загальну та спеціальну норми, не допускається. Така кваліфікація можлива лише у випадках реальної сукупності злочинів;

– при конкуренції двох статей, одна з яких містить загальну, а інша – спеціальну норму,

застосуванню підлягає лише стаття ОЧ ККУ, яка передбачає ознаки спеціальної норми;

– при конкуренції статті, яка передбачає загальну норму та декількох статей, які передбачають підпорядковані спеціальні норми, застосовується стаття, яка передбачає норму, найменшу за обсягом – інакше кажучи, «найбільш спеціальну»;

– при конкуренції статті, яка передбачає загальну норму та декількох статей, які передбачають не підпорядковані спеціальні норми, застосовується стаття, яка передбачає одну зі спеціальних норм, а яка саме вирішується за правилами подолання конкуренції статей, які містять спеціальні норми;

– якщо діяння повністю не охоплюється жодною зі статей, що передбачають спеціальні норми, то воно кваліфікується за статтею про загальну норму. Однак потрібно зважати на те, що статті про загальні норми не виступають резервними щодо статей, які передбачають так звані привілейовані норми (їх ще називають нормами про привілейовані склади злочинів чи нормами про привілейовані види злочинів). Тому якщо скоєне не охоплюється статтею, яка передбачає привілейовану норму, то стаття, яка передбачає ширшу за обсягом норму не застосовується – у такому разі відповідні діяння повинні взагалі не визнаватися кримінально караними. Наприклад, у ККУ передбачена відповідальність за умисне тяжке тілесне ушкодження, заподіяне в стані сильного душевного хвилювання (ст. 123) чи в разі перевищення меж необхідної оборони або в разі перевищення

заходів, необхідних для затримання злочинця (ст. 124). Заподіяння при цих же обставинах легкого або середньої тяжкості тілесного ушкодження не означає, що скоєне слід кваліфікувати за статтями, які передбачають «прості» види цих злочинів – ст. 125 або 122 ККУ.

2) Конкуренція цілого і частини (цілого і частин). За такої конкуренції вчинений злочин підпадає під дію принаймні двох (або більше) статей (їх частин) ККУ, одна з яких охоплює вчинене загалом та разом, а інша (інші) визнає як самостійні злочини лише частину (частини) вчиненого суспільно небезпечного посягання.

У теорії кримінального права до конкуренції статей, які передбачають норми про ціле і частину (чи частини), належать:

1) конкуренція статей про складені злочини та їх елементи;

2) конкуренція статей про закінчений злочин та попередню злочинну діяльність;

3) конкуренція статей про співучасть у злочині та «самостійний злочин».

Кваліфікація при конкуренції цілого і частини або частин будь-якого з названих видів здійснюється відповідно до таких *загальних правил*:

А) повинна застосовуватися стаття ОЧ ККУ, яка найбільш повно охоплює всі ознаки вчиненого посягання (охоплює посягання загалом);

Б) статті, які передбачають лише частину вчиненого посягання, не інкримінуються, якщо є стаття, яка охоплює все посягання.

Окрім цих загальних правил, при вирішенні питань при конкуренції частин і цілого застосовуються і *спеціальні правила*:

1) При вирішенні питань про *конкуренцію статей про складені злочини та їх елементи* слід виходити з того, що складені злочини (або врахована законодавцем сукупність злочинів) мають місце тоді, коли законодавець у диспозиції однієї статті ОЧ ККУ передбачає відповідальність за діяння, які і так криміналізовані, причому відповідальність за них встановлена в інших статтях.

Правила вирішення конкуренції при кваліфікації складених злочинів зводяться до наступного: посягання, передбачене статтею про складений злочин, кваліфікується лише за статтею про такий злочин; статті ОЧ ККУ, які передбачають діяння, які входять до складеного злочину не застосовуються за сукупністю зі статтею про складений злочин.

2) При вирішенні випадків *конкуренції статей про закінчений злочин та попередню злочинну діяльність* слід виходити із загального правила про те, що кожна наступна стадія одного і того ж злочину поглинає (включає в себе) попередню. Тобто конкуренція статей про більш ранню і більш пізню стадію одного і того ж злочину вирішується на користь статті, яка передбачає пізнішу стадію.

Коли в ході замаху вчиняється інший закінчений злочин, який менш небезпечний, ніж той, щодо якого має місце відповідна попередня стадія, то за загальним правилом скоєне кваліфікується за статтею, яка передбачає відповідальність за замах на більш небезпечний злочин.

Можлива і зворотна ситуація – коли закінчений злочин становить собою готування до іншого злочину. Наприклад, готуючись до умисного вбивства, винний вчиняє придбання вогнепальної зброї. У таких випадках ситуації конкуренції статей ОЧ ККУ немає: скоєне кваліфікується як сукупність злочинів – закінченого і готування до іншого злочину.

Як конкуренція частини та цілого розглядається і конкуренція статей, які передбачають співучасть у злочині та «самостійний» злочин. Така ситуація має місце, якщо діяння, які становлять собою співучасть у злочині, передбаченому певною статтею ОЧ ККУ, можуть бути передбачені іншою його статтею як «самостійний» злочин. Так, фінансування не передбаченого законом воєнізованого формування водночас передбачене і ч. 3 ст. 260 ККУ як «самостійний» злочин, і становить собою пособництво у злочині, яке передбачене ч. 5 ст. 27 – ч. 1 ст. 260 ККУ.

У такому разі скоєне зазвичай кваліфікується за статтею, яка передбачає «самостійний» злочин.

Як співучасть діяння кваліфікується тоді, коли воно становить собою більш небезпечне посягання.

3) Конкуренція статей, які передбачають кілька спеціальних норм.

Такий вид конкуренції характеризується тим, що: 1) одне діяння охоплюється ознаками принаймні трьох статей ОЧ ККУ; 2) статті, які передбачають спеціальні норми, підпорядковуються за обсягом з тією, що передбачає загальну норму; 3) у кримінальному законі відсутня стаття, яка б пе-

редбачала вчинення діяння, що підпадає під ознаки одночасно всіх конкуруючих статей, які передбачають спеціальні норми.

Водночас, статті, які передбачають спеціальні норми, можуть бути:

– підпорядковані за обсягом – одна з них є спеціальною стосовно іншої, і водночас загальною стосовно третьої. Умовно їх можна назвати: загальною, спеціальною, найбільш спеціальною;

– не пов'язані між собою – кожна з них є цілком самостійною і перебуває в підпорядкуванні за обсягом лише зі статтею, яка містить ознаки загальної норми, так би мовити, конкуренція статей, які передбачають спеціальні норми в чистому вигляді.

Очевидно, що правила вирішення конкуренції у двох випадках різнитимуться.

Щодо кваліфікації при конкуренції статей, які передбачають кілька спеціальних норм, які підпорядковані за обсягом, то в теорії кримінального права як такі види конкуренції розглядають:

А) конкуренцію статей (щодо чинного ККУ – завжди частин статей) про простий, кваліфікований та особливо кваліфікований склади злочину. В таких випадках застосовується частина статті кримінального закону, яка передбачає найбільш тяжкий вид злочину. Інакше кажучи, має перевагу частина статті про:

1) кваліфікований вид злочину – над тією, яка передбачає простий вид злочину;

2) особливо кваліфікований вид злочину – над тією, що передбачає кваліфікований вид злочину;

3) найбільш тяжчу особливо кваліфікуючу ознаку.

Одночасно діє правило про те, що один злочин, учинений при наявності кількох кваліфікуючих, особливо кваліфікуючих ознак не може кваліфікуватися за сукупністю різних частини однієї статті ОЧ ККУ. Тобто конкуренція статей чи частин статті про різні види одного і того ж злочину не може перерости в їх сукупність.

Б) конкуренцію статей про привілейований та особливо привілейований склади злочинів. Вирішується така конкуренція відповідно до правила про необхідність застосовувати статтю про найбільш привілейований склад злочину. Так, у разі, коли вбивство вчинене в стані сильного душевного хвилювання (ст. 116 ККУ) та одночасно при перевищенні меж необхідної оборони (ст. 118 ККУ), скоєне кваліфікується за ст. 118 ККУ.

В) конкуренцію статей про привілейований та кваліфікований склади злочинів. Тут діє правило, згідно з яким повинна застосовуватись стаття ОЧ ККУ, що передбачає привілейований склад злочину. Зокрема, вбивство при перевищенні меж необхідної оборони (ст. 118 ККУ) двох або більше осіб (п. 1 ч. 2 ст. 115 ККУ) або ж вчинене способом, небезпечним для життя багатьох осіб (п. 5 ч. 2 ст. 115 ККУ) має кваліфікуватися як привілейований склад умисного вбивства, а не як кваліфікований вид цього злочину.

Ситуації конкуренції статей, які передбачають кілька спеціальних норм, які не підпорядковані за обсягом, не пов'язані між собою, є найбільш складними для розв'язання на сьогодні. Йдеться про те, що чинний ККУ містить низку випадків, коли

вчинене діяння може одночасно містити ознаки кількох статей, які своєю чергою закріплюють норми, які є за суттю спеціальними, проте за різними ознаками і передбачені в різних статтях ОЧ ККУ. Наприклад, особа, яка має право доступу до бази даних Державного реєстру виборців, учиняє несанкціоновані дії з інформацією, що в ній міститься. У такому разі є ознаки і складу злочину, передбаченого ч. 1 ст. 158 ККУ, і складу злочину, передбаченого ч. 1 ст. 362 ККУ, як спеціальних норм відносно ст. 361 ККУ. При чому ці норми спеціальні за різними ознаками: норма ч. 1 ст. 158 ККУ спеціальна за ознакою діяння (несанкціоновані дії з інформацією, що міститься в базі даних Державного реєстру виборців, розглядаються за змістом диспозиції як вид несанкціонованого втручання у роботу цієї бази даних), а норма ч. 1 ст. 362 ККУ – за ознакою суб'єкта (особа, яка має право доступу до бази даних Державного реєстру виборців).

У схожих ситуаціях наявності описаних видів конкуренції, щодо вирішення яких у самому кримінальному законі жодних вказівок немає, а наука і практика дають суперечливі рекомендації, слід застосовувати правило, що всі сумніви при застосуванні кримінально-правових норм, зокрема про пріоритет однієї з конкуруючих норм, повинні тлумачитися на користь обвинуваченого (підсудного, засудженого). А отже такі випадки повинні вирішуватись за правилом, згідно з яким застосовуватись повинна норма, що передбачає привілейований склад злочину (тобто з пом'якшеною санкцією).

1.5. Розмежування та відмежування злочинів у ході кримінально-правової кваліфікації

Як вже відзначалося, в ході кваліфікації злочинів здійснюється вибір статті (частини, пункту) ОЧ ККУ, адже саме в них передбачаються визначальні ознаки складу того чи того злочину. Очевидно, що вибрати «потрібну» статтю, без розмежування її з подібними неможливо. Такий вибір здійснюється через послідовне «відкидання» тих ознак юридичного складу, які не відповідають виявленим ознакам фактичного складу правопорушення.

Роль ознак, за якими проводиться розмежування злочинів відіграють ознаки складу злочину. Збіг ознак говорить про те, що порівнювані злочини є суміжними. Відмінність між окремими ознаками свідчить про те, що злочини відрізняються між собою.

Очевидно, що роль розмежувальних ознак можуть відігравати лише такі, які в різних складах злочинів відрізняються. До них належать насамперед предмет злочину і потерпілий, суспільно небезпечне діяння та його наслідки, спосіб вчинення злочину, ознаки спеціального суб'єкта, форма вини тощо. Причому при розмежуванні злочинів до уваги слід брати ознаки, які прямо вказані в диспозиції статті (частини) чи випливають з її змісту, тобто є конститутивними ознаками складу злочину.

У ході кримінально-правової кваліфікації здійснюються такі основні види розмежування: 1) ок-

ремих видів злочинів між собою; 2) різних видів одного і того ж злочину, виділених за ступенем суспільної небезпеки.

Розмежування окремих видів злочинів полягає у:

1) встановленні обов'язкових ознак основних складів злочинів, за якими очевидно відрізняються два чи більше посягання. Ця розмежувальна дія полягає у виясненні того, які ознаки складу злочину є обов'язковими для кожного зі складів і їх «кількісному» порівнянні. Або, інакше кажучи, з'ясовуються, за котрими саме не ознаками, які відрізняються, склади злочинів, які розмежовуються. Наприклад, при розмежуванні несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ (ст. 361 ККУ) і несанкціонованих дій з інформацією… (ст. 362 ККУ) такими ознаками будуть суб'єкт – відповідно загальний і «особа, що має право доступу до інформації», а також спосіб – відповідно «несанкціоноване втручання» і «дії з використанням права доступу»;

2) перевірці змісту формально ознак, які збігаються. Відбувається порівняння одних і тих же ознак (наприклад, предмета, суб'єкта злочину) за змістом. Наприклад і в ст. 361 ККУ і в ст. 362 ККУ як предмета виступає інформація. Однак у складі ст. 361 ККУ таким предметом може бути будь-яка інформація, то в складі злочину, передбаченого ст. 362 ККУ, предметом виступає інформація, яка оброблюється в ЕОМ (комп'ютерах), АС, КМ чи МЕ або зберігається на носіях такої інформації.

Розмежування різних складів злочинів звичайно проводиться за однією або ж за кількома

ознаками. Чим більше розмежувальних ознак, тим чіткішим і більш очевидним є розмежування між ними.

Специфіка розмежування складів злочинів, виділених за ступенем суспільної небезпеки, полягає в тому, що такі злочини збігаються за ознаками основного складу.

Розмежування таких складів злочинів залежить насамперед від змісту кваліфікуючої ознаки. У зв'язку з цим можна виділити принаймні два випадки.

Перший, якщо кваліфікований склад відрізняється від основного складу злочину «додатковою» ознакою, яка не є конститутивною ознакою складу основного злочину. Очевидно, що в такому разі саме вона виступає розмежувальною. За її наявності діяння кваліфікується як злочин із кваліфікованим складом, за її відсутності – як з основним складом. Наприклад, несанкціоноване втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ (ч. 1 ст. 361 ККУ) та вчинене повторно (ч. 2 ст. 361 ККУ).

Така ж ситуація має місце, якщо кваліфікований (особливо кваліфікований) вид злочину має матеріальний склад, а простий вид цього ж складу злочину – формальний. Наприклад, створення з метою використання, розповсюдження або збуту, а також поширення або збут шкідливих програмних чи технічних засобів (ч. 1 ст. 361-1 ККУ) та ті самі дії, якщо вони заподіяли значну шкоду (ч. 2 ст. 361-1 ККУ).

Другий вид ситуацій розмежування злочинів з основним та кваліфікованим складом – випадки,

коли вони відрізняються за ознакою, яка є конститутивною ознакою і основного, і кваліфікованого складу. Водночас, ця ознака має різний зміст, різний якісний чи кількісний вираз. Наприклад, конститутивною ознакою основного складу несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ є суспільно небезпечний наслідок – виток, втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації, а кваліфікованого складу – ті ж самі наслідки, які за розміром становлять значну шкоду.

Якщо ж розмежувальна ознака має кількісний вираз, то в процесі розмежування слід виходити з такого: 1) верхня межа простого виду злочину є нижньою межею кваліфікованого виду цього ж злочину; 2) верхня межа кваліфікованого виду злочину є нижньою межею особливо кваліфікованого виду цього ж злочину.

Указані правила наочно видно при розмежуванні, наприклад, складів злочинів передбачених у частини 3, 4, 5 ст. 185 ККУ, за ознакою вартості викраденого майна. У Розділі 16 також нижня межа значної шкоди (100 НМДГ) є верхньою межею простого (основного) складу злочину.

У літературі майже як аксіома сприймаються положення, що правильне вирішення питання про відмежування злочинів від інших правопорушень має важливе значення для дотримання і загальних, і галузевих принципів кримінального права і критеріями такого відмежування є: 1) суспільна небезпека; 2) суб'єкт правопорушення; 3) винність;

4) кримінальна протиправність; 5) кримінальна караність.

Вирішуючи питання відмежування злочинів від адміністративних правопорушень, слід виходити з таких засадничих положень, із яких виходять при визначенні співвідношення положень кримінального й адміністративного права, які давно відомі та сприймаються як аксіоми, а саме:

– одні й ті ж діяння не можуть бути і злочином, і адміністративним правопорушенням;

– якщо за певне діяння передбачена і адміністративна, і кримінальна відповідальність, то верхня межа шкоди, заподіяної адміністративним правопорушенням, є, водночас, нижньою межею шкоди, за наявності якої настає кримінальна відповідальність;

– суперечливість, неясність, інші недоліки законодавства тлумачаться на користь особи, щодо якої застосовується закон;

– однакові терміни та термінологічні звороти в межах усієї системи права позначають одні й ті ж поняття і мають однакове значення.

На основі врахування наведених вище положень та з урахуванням положень КпАП та ККУ є підстави виділити певні правила відмежування злочинів від адміністративних правопорушень:

– при вирішенні питань адміністративної відповідальності недопустиме застосування тих положень, які притаманні лише кримінальному праву, і спрямовані на встановлення відповідальності. Йдеться про те, що КпАП не передбачає низки норм та інститутів, характерних для кримінального

законодавства, наприклад інститути стадій та співучасті. А, отже, адміністративна відповідальність не може наставати в разі лише готування до адміністративного правопорушення чи замаху на нього, а також коли особа безпосередньо не виконувала об'єктивну сторону посягання, описану в диспозиції статті Особливої частини КпАП;

– при вирішенні адміністративно-правових питань слід застосовувати положення, притаманні лише кримінальному праву, і спрямовані на виключення відповідальності за певні діяння. Ідеться про те, що ККУ містить статті про норми, на підставі яких виключається відповідальність, але ці норми невідомі КпАП, то викладені в них положення слід застосовувати і щодо адміністративно-правових питань. Наприклад, коли адміністративне правопорушення вчинене внаслідок фізичного або психічного примусу, у зв'язку з виконанням наказу або розпорядження тощо, то підстави правомірності діянь, закріплені в ККУ, поширюються і на діяння, передбачені КпАП;

– якщо в статті ККУ чи КпАП розкрито зміст певних ознак, а в статті нормативно-правового акту іншої галузі, яка встановлює відповідальність за суміжне посягання, вони лише названі – в таких випадках тлумачення поняття, яке міститься в одному з таких актів повністю поширюється на відповідне положення іншого акту. Наприклад, у статтях 185, 190, 191 ККУ є визначення відповідних злочинів: крадіжки, шахрайства, привласнення чи розтрати. Водночас, в ч. 1 ст. 51 КпАП, яка передбачає відповідні адміністративні правопору-

шення, будь-які роз'яснення відсутні. Отже, ці адміністративні правопорушення розуміються так само, як і в ККУ;

– якщо в статтях (примітках) КпАП чи ККУ роз'яснюється зміст понять, то ті з них, які мають кількісний вираз (розкривають вартісні чи інші критерії) встановлюють межу між кримінальними й адміністративними правопорушеннями. Наприклад, у разі дрібного розкрадання чужого майна, якщо воно вчинене при ознаках, визначених в ст. 51 КпАП України, то має місце адміністративне правопорушення, а не злочин, передбачений ч. 1 ст. 185, ч. 1 ст. 190, ч. 1 ст. 191 ККУ. І навпаки, наприклад, значний розмір коштів згідно з примітками до ст. 212 ККУ має місце тоді, коли суми податків, зборів й інших обов'язкових платежів у тисячу і більше разів перевищують НМДГ. Відповідно, за наявності цього розміру настає кримінальна відповідальність, а за меншого – адміністративна за ст. 126 Податкового кодексу України;

– при «дублюванні» відповідальності, коли за певні діяння відповідальність водночас передбачена і в КпАП, як за адміністративне правопорушення, і в ККУ, як за злочин, більш правильно керуватися принципами правозастосування, відповідно до яких усі сумніви, неясності, суперечності законодавства, тлумачаться на користь особи, дії якої оцінюються і кваліфікувати скоєне не як злочин, а як адміністративне правопорушення.

Очевидно, що наведені правила не охоплюють усіх можливих питань, які можуть виникнути в ході відмежування злочинів від адміністративних

правопорушень, і стосуються лише ситуацій, які найчастіше трапляються у правозастосуванні.

Відмежування злочинів від цивільних деліктів. У ході правозастосування нерідко доводиться визначати, який вид правових відносин стає об'єктом правової оцінки – існують лише цивільно-правові відносини (у вирішення яких кримінально-правовими засобами втручатися неприпустимо), чи вчинено злочин і, отже, виникли кримінально-правові відносини. Зазвичай, це має місце у випадках заволодіння і розпорядження майном, при заподіянні майнової шкоди. Особливо складно проводити розмежування щодо відносин, які виникають у зв'язку з діяльністю господарських товариств, використанням спільного майна одним із співвласників.

При відмежуванні злочинів від цивільних деліктів важливо враховувати такі міркування:

1) невиконання чи неналежне виконання договірних зобов'язань не може оцінюватися як злочин;

2) кримінальна відповідальність може наставати тоді, коли встановлено, що цивільно-правова угода укладена без мети її виконання, маскує намір винного протиправно збагатитися за рахунок партнера. Причому така мета існує ще до моменту укладення договору. Це, наприклад, отримання речей у тимчасове користування з метою звернути її на свою користь (ст. 192 ККУ);

3) розпорядження своїм майном чи часткою в сумісній власності не становить злочину. Це, зокрема, стосується дій власника, який вилучає своє майно з володіння іншої особи (кримінальна відповідальність може наставати лише тоді, коли вико-

ристовуються способи впливу на іншу особу, які заборонені ККУ, насамперед насильство, погрози). Так само не становить собою злочину дії співвласника щодо майна, управління яким здійснюється спільно, яке не виділене, наприклад, перебуває в спільній сумісній власності подружжя;

4) кримінально-караними є протиправні дії щодо майна, співвласником якого є винний, але яке відокремлене від його власного (зокрема, це майно господарського товариства, кооперативу);

5) факт заподіяння майнової шкоди, якщо це водночас оцінюється як суспільно небезпечні наслідки злочину, повинен бути констатований власником чи уповноваженим ним органом. Неприпустимо визнавати наявність злочинних наслідків, при тому, що сам власник в установленому порядку не визнає, що йому заподіяна шкода.

Слід також зауважити, що кримінальна відповідальність може поєднуватися із застосуванням заходів цивільно-правового характеру, в тому числі й із притягненням до цивільної відповідальності. Наприклад, у разі розкрадання окремих видів майна його вартість відшкодовується в «кратному порядку», крім того винний підлягає і кримінальній відповідальності. Інколи стверджують, що в такому разі за одне порушення настає два види юридичної відповідальності. Виявляється, що це не так – у таких випадках має місце ідеальна сукупність злочину і цивільного делікту, тобто одним діянням вчиняються два правопорушення. За кожне з них настає юридична відповідальність різних видів, а «подвійної» відповідальності не виникає.

При відмежуванні злочинів від цивільних деліктів слід також враховувати, що злочином є лише винне діяння, а цивільно-правова відповідальність може наставати також за спричинення шкоди за відсутності вини.

Основні поняття

Кримінально-правова кваліфікація – це оцінка вчиненого особою діяння, яка включає в себе обґрунтування та процесуальне закріплення висновку про те, чи таке діяння передбачене відповідною статтею (статтями, частиною, пунктом) кримінального закону і відповідно, що воно є (не є) злочином чи іншим діянням, передбаченим кримінальним законом.

Юридична підстава кримінально-правової кваліфікації – це юридичний склад злочину – сукупність установлених у законі юридичних ознак (об'єктивних і суб'єктивних), котрі визначають вчинене суспільно небезпечне діяння як злочинне.

Контрольні запитання та завдання

1. Назвіть зміст та поняття кримінально-правової кваліфікації.
2. Вкажіть, у якому акті вказано поняття і види підстав кримінально-правової кваліфікації.
3. Сформулюйте принципи кримінально-правової кваліфікації.
4. Які передумови вирішення колізії та конкуренції норм у кримінальному праві?
5. У чому основано розмежування та відмежування злочинів у ході кримінально-правової кваліфікації?

Розділ 2

Загальна характеристика та види кіберзлочинів

Статистика свідчить, що у 2018 році кіберзлочини зайняли друге місце з усіх зареєстрованих злочинів у світі. В Україні їх кількість, що можуть кваліфікуватись як кіберзлочини, за даними Національної поліції, щороку збільшується на 2,5 тис. За 2018 рік хакери викрали понад 16,7 млрд дол. США по всьому світу. Крім того, персональні дані щонайменше 40 млн людей були викрадені різними угрупованнями. Тому питання кібербезпеки людини надзвичайно актуальне сьогодні.

Ситуація ускладнена тим, що загального визначення кіберзлочинів не існує ні в національному законодавстві, ні в міжнародному. Це призводить до відсутності єдиного підходу до визначення підстав віднесення протиправних діянь до таких злочинів, розроблення спільних заходів щодо їх ліквідації та розроблення превентивних заходів.

Європейське законодавство за останні п'ять років посилило відповідальність щодо обробки персональних даних та захисту конфіденційності в різних сферах. Україна поки що розробляє тільки проекти таких документів.

Аналіз чинних стратегічних документів держави та проектів, що розробляються, а саме відсутність

у них заходів і відповідальних органів за реалізацію політики у сфері цифрової економіки, розвитку цифрових навичок і цифрової гігієни, доводить необхідність розроблення окремої стратегії із розвитку цифрових навичок населення та плану її реалізації якнайшвидше. Інакше відставання населення в цьому питанні призведе до відставання країни, яке надолужити буде вкрай важко.

Цифровий розрив сьогодні приводить до іншого поділу країн на рівні, що загалом негативно позначиться місці України у світі та призведе до неможливості потрапити із третього світу в перший.

2.1. Поняття «кіберзлочин» та його ознаки

Термін «кіберзлочинність» з'явився у вітчизняному офіційному нормативному обігу завдяки підписанню Україною «Конвенції про кіберзлочинність». Проте цей документ не містить визначення цього поняття і окреслює його обсяг, лише надаючи перелік видів правопорушень, які до нього входять. ККУ, як і інше законодавство України, також не містить визначення такого виду злочинів, а отже на шляху розроблення правил їх кваліфікації з урахуванням найбільш повного обсягу їх особливостей постає питання про відмежування таких злочинів від інших. Але спочатку відійдемо від положень Конвенції та спробуємо дати визначення кіберзлочину, відповідно до буквального тлумачення терміна.

Взагалі «кібер» (*cyber*, що походить від *cybernetics*) – префікс, який додають до повсякденних слів, щоб показати їхню причетність до інтернету, комп'ютерів тощо. А кібернетику (*cybernetics* (від грец. *cybernos* – рульовий)) зараз розглядають як науку про зв'язки, керування й організацію в об'єктах різноманітної природи. У сучасних умовах інформаційно-телекомунікаційні технології (далі – ІТТ) є основними засобами забезпечення вказаних процесів.

Отже, семантичний аналіз поняття «кіберзлочинність» указує на те, що інтегруючим елементом складників цього явища є ІТТ, які різним чином задіяні при вчиненні відповідних діянь. І взагалі *основною сутнісною ознакою кіберзлочину є те, що це є діяння, сама можливість вчинення якого випливає з особливих можливостей інформаційно-телекомунікаційних технологій, які використовуються для завдання шкоди суспільним відносинам.*

Застосувавши вказану ознаку до поняття «злочину» можна дати таке визначення з позицій Кримінального права України:

Кіберзлочин – передбачене ККУ суспільно небезпечне винне діяння, вчинене суб'єктом злочину з використанням ІТТ.

Для розуміння терміна *«інформаційно-телекомунікаційні технології»* слід звернутися до основного нормативно-правового акту в сфері захисту інформації – Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (далі – Закон).

Інформаційно-телекомунікаційні технології реалізовані в програмному забезпеченні, яке призначене для обробки інформації в інформаційно-телекомунікаційній системі і є об'єктом захисту відповідно до ст. 2 Закону. Звичайно, слід звернути увагу, що поряд із програмним забезпеченням об'єктом захисту є і сама вказана інформація, а відповідно до Конвенції кіберзлочин може бути вчинений із використанням не тільки комп'ютерної системи, а й даних у ній. Але все ж таки використання цих даних у процесі вчинення злочину неможливе без застосування програмного забезпечення, а тому у визначенні й фігурують тільки самі технології їх обробки, які реалізовані в цьому програмному забезпеченні.

Інші важливі для розуміння цього поняття терміни містяться в ст. 1 Закону:

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформаційна (автоматизована) система – організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією через передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

2.2. Міжнародні нормативні акти у сфері протидії кіберзлочинності

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 року в Будапешті Конвенція Ради Європи про кіберзлочинність. Це один із найважливіших документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі й поки єдиний документ такого рівня.

Конвенція про кіберзлочинність є комплексним документом, який містить норми, покликані суттєво вплинути на різні галузі права: кримінальне, кримінально-процесуальне, авторське, цивільне, інформаційне. Вона ґрунтується на основних принципах міжнародного права: дотримання прав людини, співпраці та сумлінного виконання зобов'язань. Конвенція охоплює три основні напрями: узгодження національних норм, що визначають склади злочинів, визначення порядку розслідування щодо злочинів у світових комп'ютерних мережах і створення оперативної та дієвої системи міжнародної співпраці по боротьбі з кіберзлочинністю.

Норми Конвенції спрямовані на врегулювання трьох основних блоків питань:

– зближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації;

– зближення національних кримінально-процесуальних заходів, спрямованих на забезпечення збирання доказів при розслідуванні таких злочинів;

– міжнародне співробітництво в кримінально-процесуальній діяльності, спрямованої на збирання доказів вчинення таких злочинів за кордоном.

У частині кримінально-правових питань Конвенцією пропонується включити в законодавство країн-учасниць єдині норми про кримінальну відповідальність за «кіберзлочини», що включає перелік таких діянь. Ми їх розглянемо в наступному питанні, тут же зупинимося на загальній характеристиці.

Конвенція про кіберзлочинність на сьогодні є одним із базових міжнародно-правових актів у сфері права телекомунікацій. Її можна поставити в один ряд з Окінавською хартією глобального інформаційного суспільства. Однак якщо в хартії йдеться, скоріше, про закріплення загальної концепції розвитку інформаційно-комунікаційних технологій, то в Конвенції пропонується реальний механізм правового регулювання.

Конвенція встановлює процедури для підвищення ефективності проведення розслідувань:

– завдяки негайному збереженню комп'ютерних даних;

– надання владі можливостей запитувати передачу зазначених комп'ютерних даних;

– надання слідчим можливості збирати дані про трафік і перехоплювати контент у реальному часі.

Ця Конвенція також створює процедури й системи, що сприяють міжнародному співробітництву, наприклад:

– формується цілодобова щоденно діюча мережа (24/7), яка дає змогу надавати негайну допомогу слідчим;

– конвенція сприяє екстрадиції та обміну інформацією;

– конвенція допомагає владі однієї країни збирати дані в іншій, а також заохочує взаємну юридичну допомогу між країнами.

Наша держава також приєдналася до згадуваної Конвенції. Парламент України встановив у Законі «Про ратифікацію Конвенції про кіберзлочинність», що країна приєднується до її норм з такими застереженнями і заявами.

По-перше, що стосується встановленого Конвенцією переліку кримінально караних діянь, то Україна залишає за собою право не застосовувати п. 1 ст. 6 Конвенції в частині встановлення кримінальної відповідальності за виготовлення, придбання для використання, надання для використання іншим чином пристосувань, включаючи комп'ютерні програми, створені або адаптовані задля вчинення будь-якого зі злочинів, перерахованих у Конвенції, а також виготовлення і придбання для використання комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у Конвенції про кіберзлочинність.

Крім того, Україна, по-перше, залишає за собою право не застосовувати повністю норми ст. 9 Конвенції в частині встановлення кримінальної відповідальності за навмисне вчинення без права на це наступних дій: отримання дитячої порнографії за допомогою комп'ютерних систем для себе

чи іншої особи або володіння дитячою порнографією, розміщеною у комп'ютерній системі або на комп'ютерному носії інформації.

По-друге, в Україні органами, які відповідальні за підготовку запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам і т. д., є Міністерство юстиції України (щодо доручень судів) і Генеральна прокуратура України (щодо доручень органів досудового слідства).

Продовженням Конвенції став *додатковий протокол до Конвенції про кіберзлочинність*, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (далі – Протокол).

У принципі з його назви зрозуміло, що в ньому містяться положення щодо криміналізації дій расистського та ксенофобного характеру. Крім того, визнаються кримінальними правопорушеннями в національному законодавстві держави у разі умисного вчинення без права на це, пособництво або підбурювання до вчинення будь-якого з правопорушень, визначених відповідно до Протоколу, з наміром учинити такий злочин.

Ратифікуючи цей Протокол, Україна заявила, що відповідно до підпункту «а» п. 2 ст. 6 Протоколу вона вимагатиме, щоб заперечення чи значна мінімізація, про які йдеться в пункті 1 цієї статті, були вчинені з наміром підбурити до ненависті, дискримінації чи насильства проти будь-якої особи чи групи осіб на підставі ознак раси, кольору шкіри, національного чи етнічного походження, а

також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій.

Отже, Україна привела положення Протоколу у відповідність до ККУ, а саме статей 161 та 300.

2.3. Види кіберзлочинів відповідно до міжнародних нормативних актів

Об'єктом кіберзлочинів відповідно до Конвенції є широкий спектр охоронюваних нормами права суспільних відносин, що виникають при провадженні інформаційних процесів із приводу виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, поширення та споживання комп'ютерної інформації, а також в інших сферах, де використовуються комп'ютери, комп'ютерні системи та мережі. Серед них, ураховуючи підвищену суспільну значущість, виділяються правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності та доступності комп'ютерних даних і систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського та суміжних прав.

Об'єктивна сторона кіберзлочинів характеризується виділенням чотирьох груп суспільно небезпечних діянь.

Конвенція поділяє злочини в кіберпросторі на чотири групи.

У першу групу злочинів, спрямованих *проти конфіденційності, цілісності та доступності комп'ютерних даних і систем*, входять:

– протизаконний доступ – отримання доступу до комп'ютерної системи загалом або її частини без права на це, який може розглядатися як злочин, якщо вчинено в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними або іншим безчесним наміром, або щодо комп'ютерної системи, поєднаної з іншою комп'ютерною системою (ст. 2);

– протизаконне перехоплення даних, здійснене з використанням технічних засобів перехоплення без права на це непублічних передач комп'ютерних даних у комп'ютерну систему, з неї або всередині такої системи, у тому числі електромагнітні випромінювання комп'ютерної системи, що несе такі комп'ютерні дані, якщо він зроблений в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними або іншим безчесним наміром, або щодо комп'ютерної системи, поєднаної з іншою комп'ютерною системою (ст. 3);

– порушення цілісності даних – ушкодження, стирання, псування, зміну або блокування комп'ютерних даних без права на це, у тому числі виключно у випадках, які спричинили серйозні наслідки (ст. 4;

– втручання у функціонування системи – створення без права на це серйозних перешкод функціонуванню комп'ютерної системи через уведення, передачу, пошкодження, знищення, псування, зміну або приховування комп'ютерних даних (ст. 5);

– протиправне використання пристроїв – (а) виробництво, продаж, придбання для використання, імпорт, оптова продаж або інші форми надання в користування: (1) пристроїв, у т. ч. комп'ютерних

програм, розроблених або адаптованих, насамперед для цілей вчинення злочинів, (2) комп'ютерних паролів, кодів доступу або інших подібних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи загалом або її частини, з наміром використовувати їх для вчинення злочинів, та (3) володіння одним із предметів, що згадуються вище, з наміром використовувати його для вчинення злочинів (ст. 6).

Об'єктом злочину виступають не тільки комп'ютерні програми, розроблені або адаптовані для вчинення злочинів, передбачених у статтях 2–5 Конвенції, а й комп'ютерні паролі, коди доступу та їх аналоги, за допомогою яких може бути отримано доступ до комп'ютерної системи загалом або її частини (з урахуванням злочинного наміру). Норми ст. 6 Конвенції застосовуються лише в тому разі, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на вчинення протиправних діянь.

У другу групу входять *злочини, пов'язані з використанням комп'ютерних засобів*: фальсифікація та шахрайство з використанням комп'ютерних технологій (статті 7, 8 Конвенції):

– підроблення з використанням комп'ютерів – уведення, зміну, знищення або блокування комп'ютерних даних, що призводять до порушення автентичності даних із наміром, щоб вони розглядалися або використовувалися в юридичних цілях, як ніби вони залишаються справжніми, незалежно від того, чи є ці дані безпосередньо читабельні і зрозумілі (ст. 7);

– шахрайство з використанням комп'ютерів – позбавлення іншої особи його власності через уведення, зміну, стирання або приховування комп'ютерних даних або втручання у функціонування комп'ютера або системи задля неправомірного отримання економічної вигоди для себе чи для іншої особи (ст. 8).

Третю групу складають *злочини, пов'язані з контентом (змістом) даних*.

Правопорушення, пов'язані з дитячою порнографією (порнографічними матеріалами, візуально відображають участь неповнолітнього чи удаваної повнолітньої особи в сексуально відвертих діях, а також реалістичні зображення, що представляють неповнолітніх у сексуально відвертих діях), а саме: виробництво задля поширення через комп'ютерні системи; пропозиція або надання через комп'ютерні системи; поширення або передача через комп'ютерні системи; придбання через комп'ютерну систему для себе чи іншої особи; володіння дитячою порнографією, що міститься в комп'ютерній системі або в середовищі для збереження комп'ютерних даних.

У четверту групу ввійшли *порушення авторського права і суміжних прав*:

– порушення авторського права, передбаченого нормами внутрішньодержавного законодавства з урахуванням вимог Паризького акта від 24 липня 1971 р. до Бернської конвенції про захист творів літератури та мистецтва, Угоди про пов'язані з торгівлею аспекти прав на інтелектуальну власність і Договору про авторське право Всесвітньої

організації інтелектуальної власності (ВОІВ), за винятком будь-яких моральних прав, що надаються цими Конвенціями, коли такі дії навмисно відбуваються в комерційному масштабі й за допомогою комп'ютерної системи;

– порушення прав, пов'язаних з авторським правом (суміжними правами), передбачених нормами внутрішньодержавного законодавства, з урахуванням вимог Міжнародної конвенції про захист прав виконавців, виробників звукозаписів та радіомовних організацій (Римська конвенція), Угоди про пов'язані з торгівлею аспекти прав інтелектуальної власності та Договору ВОІВ про виконавців і звукозаписи, за винятком будь-яких моральних прав, які надаються цими Конвенціями, коли такі дії вчинені умисно в комерційному масштабі та за допомогою комп'ютерної системи.

Шкідливими наслідками перерахованих діянь Конвенцією визнається порушення прав законних користувачів комп'ютерної інформації, комп'ютерів, їх систем чи мереж. Установлення як обов'язкової ознаки більш тяжких наслідків (матеріального збитку, протиправного використання отриманої комп'ютерної інформації тощо) Конвенцією залишено на розсуд держав. Загалом норми Конвенції не передбачають обов'язковості настання шкідливих наслідків.

Суб'єктом кіберзлочинів може бути фізична особа, яка вчинила означені вище дії.

Виходячи з усталеної в різних країнах практики, ст. 12 Конвенції вимагає встановлення відповідальності юридичних осіб за правопорушення,

передбачені нею. Умовами настання відповідальності юридичної особи є: (1) вчинення дії (2) задля отримання вигоди на користь юридичної особи (3) його посадовою особою, яка займає керівну посаду, (4) з використанням його повноважень за поданням юридичної особи, прийняття рішень або здійснення контролю за його діяльністю. Крім того, конвенція наказує встановлювати відповідальність юридичних осіб також у разі вчинення протиправних дій іншим працівником, який перебуває під керівництвом посадової особи, яка займає керівний пост, задля отримання вигоди на користь юридичної особи.

Суб'єктивна сторона. У всіх злочинах, згаданих у Конвенції, відповідальність настає тільки в разі вчинення їх умисно. У деяких статтях, із посиланням на «традиційні» злочини, вчинені з використанням комп'ютера або комп'ютерної інформації, передбачено, що умисна форма вини має характеризувати не тільки саме діяння, а й протиправне їх використання, хоча це і є кваліфікуючою ознакою таких злочинів (наприклад, ст. 8 – шахрайство з використанням комп'ютера).

Поряд із закінченими злочинами Конвенцією передбачається необхідність установлення відповідальності за замах, співучасть чи підбурювання до його вчинення (ст. 11).

Згідно з ч. 1 ст. 13 Конвенції встановлення конкретних санкцій за вчинення зазначених діянь віднесено до відання держав. На їх розсуд може встановлюватися кримінальна відповідальність для фізичних осіб, а також кримінальна, цивільно-

правова або адміністративна відповідальність юридичних осіб. Передбачені внутрішньодержавним законодавством санкції повинні бути ефективні, пропорційні та переконливі.

Згідно з Додатковим протоколом до Конвенції про кіберзлочинність, який стосується криміналізації *дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи* до кіберзлочинів слід додати п'яту групу діянь:

– поширення або в інший спосіб надання громадськості доступу через комп'ютерні системи до расистського та ксенофобного матеріалу;

– погроза, зроблена через комп'ютерну систему, вчинення тяжкого злочину, визначеного в національному законодавстві, проти (I) осіб через їх належність до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (II) групи осіб, котра відрізняється за будь-якою з цих характеристик;

– публічна образа через комп'ютерну систему (I) осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (II) групи осіб, яка відрізняється за будь-якою з цих характеристик;

– поширення або в інший спосіб надання громадськості доступу через комп'ютерні системи до матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або

злочинами проти людства, як це визначено в міжнародному праві та як це визнано заключними та обов'язковими рішеннями Міжнародного військового трибуналу, заснованого згідно з Лондонською угодою від 8 серпня 1945 року, або будь-якого іншого міжнародного суду, заснованого відповідними міжнародними документами, юрисдикція якого визнана Стороною угоди (вчинені з наміром підбурити до ненависті, дискримінації чи насильства проти будь-якої особи чи групи осіб на підставі ознак раси, кольору шкіри, національного чи етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій).

2.4. Види кіберзлочинів відповідно до Кримінального кодексу України

Відповідно до кримінально-правової класифікації (загальним критерієм якої, як відомо, є родовий об'єкт) кіберзлочини можуть бути виділені серед інших та, отже, відмежовані, за їх *об'єктом*, тобто суспільними відносинами, яким ними завдається шкода або створюється реальна загроза завдання шкоди.

Такими діяннями шкода може завдаватися за трьома варіантами:

1) суспільним відносинам, які виникають у ході забезпечення за допомогою ІТТ життєдіяльності людини, суспільства, держави (відносини у сфері використання ЕОМ (комп'ютерів), їх систем, КМ, МЕ);

2) традиційним суспільним відносинам, охоронюваним кримінальним законодавством, які забезпечуються за допомогою ІТТ, цілеспрямований шкідливий вплив на які використовується для завдання шкоди цим відносинам;

3) традиційним суспільним відносинам, охоронюваним кримінальним законодавством, для нанесення шкоди яким використовуються ІТТ, які, своєю чергою, не зазнають при цьому шкоди.

Відповідно можна виділити три групи кіберзлочинів, які будуть мати свої особливості кваліфікації. Не важко побачити паралель із видами кіберзлочинів у Конвенції, але з одним зауваженням – кіберзлочини другої та третьої груп, за практикою діяльності Департаменту боротьби з кіберзлочинністю, включають набагато ширше коло діянь, ніж передбачено в Конвенції. Вони ще включають кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання ЕОМ (комп'ютерів), АС, КМ чи МЕ (у сферах платіжних систем; обігу інформації протиправного характеру із використанням ЕОМ (комп'ютерів), АС, КМ чи МЕ (протиправного контенту); економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також заборонені види господарської діяльності у цій сфері (електронної комерції); надання телекомунікаційних послуг; а також шахрайства і легалізацію (відмивання) доходів, одержаних від означених вище кримінальних правопорушень тощо).

Отже, у цьому курсі ми розглянемо кваліфікацію трьох умовних видів кіберзлочинів:

1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

2. Злочини, пов'язані з комп'ютерами.

3. Інші кіберзлочини.

Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем кваліфікуються за статтями (їх частинами) Розділу 16 ОЧ ККУ або подібними їм спеціальними статтями (наприклад, ст. 158):

– несанкціоноване втручання в роботу комп'ютерної системи (ст. 361 ККУ);

– створення задля використання, поширення або збуту шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу комп'ютерної системи (ст. 361^1 ККУ);

– поширення або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу комп'ютерної системи (ст. 361^1 ККУ);

– несанкціонований збут або поширення інформації з обмеженим доступом, яка зберігається в комп'ютерній системі, або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (ст. 361^2 ККУ);

– несанкціонована зміна, знищення або блокування інформації, яка оброблюється в комп'ютерній системі, або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ч. 1 ст. 362 ККУ);

– несанкціоноване перехоплення або копіювання інформації, яка оброблюється в комп'ютерній системі, або зберігається на носіях такої інформації, вчинене особою, яка має право доступу до такої інформації (ч. 2 ст. 362 ККУ);

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації (ст. 363 ККУ);

– умисне масове поширення повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерної системи (ст. 363^1 ККУ).

Кваліфікація другої групи кіберзлочинів (злочини, пов'язані з комп'ютерами) найчастіше відбувається за сукупністю зі статтями (їх частинами) Розділу 16 ОЧ ККУ. Іноді така сукупність вже закріплена Законом (наприклад, ч. 3 ст. 190 ККУ), а отже кваліфікується як одиничний злочин. Крім того, у цю групу ми віднесли і злочини, при вчиненні яких використання ІТТ стає невід'ємною і необхідною частиною їх способу, і які *можуть* кваліфікуватися без посилань на статті Розділу 16 ККУ.

Такі діяння можуть належати до таких видів злочинів:

– злочини проти власності (статті 185, 189–192 ККУ);

– злочини проти інформації з обмеженим доступом, яка не зберігається на комп'ютерних носіях (статті 111, 114, 132, 145, 328, 330, 381, 387 ККУ);

– злочини у сфері господарської діяльності (статті 200, 208, 209, 212, 217, 225, 229, 231, 232 ККУ);

– злочини проти особистих прав і свобод людини (статті 163, 168, 176, 177, 182 ККУ);

– злочини проти громадської безпеки і громадського порядку (статті 258, 295 ККУ) та ін.

Кваліфікація другої групи злочинів повинна відбуватися за сукупністю відповідно до ККУ, зміст положень якого пояснено в Постанові Пленуму Верховного Суду України № 7 від 04.06.2010 «Про практику застосування судами кримінального законодавства про повторність, сукупність і рецидив злочинів та їх правові наслідки».

До інших кіберзлочинів ми відносимо всю решту діянь, які не належать до перших двох груп. Такі діяння *завжди* кваліфікуються без посилань на статті Розділу 16 ККУ, а елементи ІТТ в їх складі утворюють специфічні факультативні ознаки об'єктивної сторони:

– обстановку вчинення злочину – кіберпростір;

– засіб вчинення злочину.

Тут можна виділити такі злочини:

– порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (ст. 161 ККУ);

– порушення авторського права і суміжних прав (ст. 176 ККУ);

– виготовлення підроблених грошей (ст. 199 ККУ);

– підроблення документів на переказ, платіжних карток для доступу до банківських рахунків (ст. 200 ККУ);

– легалізація (відмивання) доходів, одержаних злочинним шляхом (ст. 209 ККУ);

– підроблення знаків поштової оплати і проїзних квитків (ст. 215 ККУ);

– підроблення марок акцизного збору або контрольних марок (ст. 216 ККУ);

– виготовлення підроблених недержавних цінних паперів (ст. 224 ККУ);

– виготовлення фальсифікованих вимірювальних приладів (ст. 226 ККУ);

– виготовлення порнографічних матеріалів, матеріалів, що пропагують культ насильства чи жорстокості (статті 300, 301 ККУ);

– підроблення документів на отримання наркотичних засобів чи психотропних речовин (ст. 318 ККУ);

– підроблення документів, печаток, штампів та бланків (ст. 358 ККУ) та ін.

Із цієї групи кіберзлочинів ми розглянемо тільки злочини, пов'язані зі змістом даних або порушенням авторського права та суміжних прав, та злочини расистського та ксенофобного характеру, вчинені через комп'ютерні системи.

2.5. Міжнародний досвід із кібербезпеки та уроки для України

1. Досвід США

Загроза кібервійни призвела до вражального факту: в США урядовий зв'язок відмовився від IP-телефонії. Поворотним моментом послугував

теракт 11 вересня 2001 р. в Нью-Йорку, і як міра протиборства була сформована надпотужна структура – Міністерство внутрішньої безпеки, хоча боротьба з тероризмом розпочалася значно раніше.

Було поставлено завдання розробити всеохопну національну стратегію по захисту інфраструткури від фізичних і кіберзагроз.

Спеціальна комісія із п'яти команд, що представляли 9 інфраструктур, виділила п'ять напрямів захисту:

– телекомунікації, ПЕОМ і програмне забезпечення, інтернет, супутники і оптоволокно;

– залізниці, повітряний і морський транспорт, трубопроводи;

– електроенергія, газ, нафта, виробництво, зберігання і транспортування;

– фінансові операції, фондові й ринки облігацій;

– вода, аварійні служби, державна служба.

Відповідно до вказаних напрямів було розроблено стандартизований опис критичної інфраструктури для полегшання контролю й підготовки до ліквідації надзвичайних ситуацій.

Відпрацьована рамочна концепція, яка складається з п'яти функцій кіберзахисту: виявити – відпрацювати ризики й управління ними; захистити – розробити заходи по кіберзахисту об'єктів; виявити – впровадити відповідні заходи; відповісти – здійснити заходи кіберзахисту; відновити порушені функції і забезпечити стійкість роботи системи.

Ці 5 функцій складаються з 22 заходів та включають множину стандартів, методик, процедур і

процесів, що детально описані й підлягають виконанню операторами критичної інфраструктури. Крім того, вони зобов'язані повідомляти про інциденти IT-безпеки.

Невиконання приписів передбачає досить строгі покарання:

– до 20 років позбавлення волі – за розкрадання інтелектуальної власності американських компаній із використанням інформаційних технологій;

– до 30 років позбавлення волі без права дострокового звільнення – за проникнення в державні мережі, енергомережі, транспортні канали зв'язку або системи управління водоспоживанням;

– до 100 років позбавлення волі – за кіберзлочини.

Окрім того, Президент США Барак Обама у 2015 р. затвердив нову Стратегію національної безпеки держави і політику в інформаційній сфері, згідно з якою військове керівництво США розглядає кіберпростір як одну зі сфер проведення військових операцій поряд із наземною, морською, повітряною і космічною операціями. Потенційними противниками називають Росію, Китай, Північну Корею, Іран.

2. Досвід Китаю

У Китаї політика в кіберпросторі визначається з 2005 р. стратегією розвитку інформатизації, яка просуває інтернет у народне господарство задля розвитку економіки.

При цьому китайці застосовують обмежувальні заходи в кіберпросторі. Так, наприклад, користу-

вачі не мають права реєструватися в соціальних мережах, використовуючи псевдонім. Окрім того, в рамках фільтрації інтернет-контенту «Вогняна стіна» в Китаї офіційно заборонені найбільша в світі соціальна мережа «Facebook», відеохостингова компанія «You Tube» та соціальна мережа мікроблогів «Twitter».

3. Досвід Великобританії та ФРН

Великобританія прийняла стратегію у сфері кібербезпеки у 2011 році й реалізує інформаційну політику задля виводу країни на перше місце за інноваціями, інвестиціями і якістю сервісу у сфері IT-технологій.

У Німеччині відповідний документ щодо кібербезпеки прийнято у 2011 році й передбачає створення внутрішньої системи звітності про інциденти IT-безпеки.

Невиконання вимог про вказану звітність підлягає штрафу в розмірі 100 тисяч євро, які можуть бути накладені на оператора критичної інфраструктури, який не зміг реалізувати вказані заходи IT-безпеки.

4. Досвід Росії

У Росії Доктрина інформаційної безпеки РФ була затверджена у 2016 році. До основних її положень належить стратегічне стримування і відвертання військових конфліктів, які можуть виникнути внаслідок застосування інформаційних технологій. Росія належить до пятірки країн, що володіють потужними кібервійськами (у 2014 р.

були створені війська інформаційних операцій РФ). До таких країн належать США, Китай, Росія, Велика Британія, Південна Корея.

5. Уроки та завдання для України

Отже, розвиток інформаційних технологій зумовлює появу нових видів кібератак.

Відповідно однією з основних складників національної безпеки держави стає гарантування інформаційної безпеки. В Україні почалася активна робота в цьому напрямі. Для реалізації інформаційної безпеки необхідно застосовувати не лише інфраструтуру, стійку до кібератак (квантові комп'ютери можуть стати одним із компонентів вирішення цього завдання), водночас і забезпечувати цифровий суверенітет (розвивати українське програмне й апаратне забезпечення).

Крім того, потрібно прискорити міжнародне співробітництво за напрямами протидії кібератакам із боку терористичних організацій і країн та застосування кіберзброї для боротьби з ними. Але на сучасному етапі найбільш перспективним напрямом удосконалення інформаційної безпеки об'єктів управління і зв'язку та інформації в рамках нинішніх технологій є багаторівневий багатопозиційний захист (ББЗ) із використанням апаратно-програмних засобів і способів захисту об'єктів та інформації.

Звичайно, що технічна основа ББЗ повинна ґрунтуватися на таких основних принципах:

– незалежно від фізичної природи потенційних загроз система захисту повинна протидіяти їх реалізації з певною (необхідною) мірою надійності;

– у системі повинен здійснюватися моніторинг стану захищеності об'єкта захисту, основна функція якого вчасне й достовірне виявлення небезпечних подій;

– у системі повина здійснюватися ідентифікація виявленої небезпечної події та прийняття заходів щодо її нейтралізації;

– система в будь-якому разі завжди реалізує умови припинення (нейтралізації) загрози;

– система повина забезпечувати припинення дій дестабілізуючих факторів із заданою мірою надійності.

Рівні захисту

Відповідно до розглянутих принципів ББЗ має містити такі рівні: рівень безпосереднього захисту, що забезпечує відвертання фізичних чи логічних атак; рівень виявлення, що забезпечує вчасне й достовірне виявлення небезпечної події і передачі інформації органу, який приймає рішення про її нейтралізацію; рівень збору й оброблення інформації; рівень оперативного реагування системи захисту, що забезпечує створення вчасних умов для нейтралізації небезпечної події; рівень нейтралізації небезпечної події.

Кожен із указаних рівнів захисту може бути реалізований із використанням різних технічних і програмних засобів, які забезпечують високу логічну, технічну й оперативну стійкість роботи системи захисту. При цьому можливі такі підходи для розв'язання завдання ідентифікації.

Перший заснований на використані додаткових спеціальних засобів, таких, як засоби відеоконтролю для систем фізичного захисту, вимірювальні прилади й апаратура для засобів захисту інформації від витоку та спеціальні програмні продукти для верифікації й ідентифікації комп'ютерних програм.

Другий підхід ґрунтується на застосуванні шаблону ситуацій. Ці шаблони повинні включати в собі параметри, які описують стан системи та об'єкта захисту, поведінку порушників, зовнішні чинники. Збіг ситуацій із заданим в одному із шаблонів указує на наявність небезпечної події.

Далі здійснюється вироблення варіанта реагування на небезпечну подію. Його реалізація полягає в синтезі можливих варіантів, що задовольнять критерій виконання вимог до ефективності нейтралізації небезпечної події й процесів, які її реалізують. Завдання синтезу може формуватися як оптимізаційне. У цьому разі відшукується єдине найкраще рішення.

На четвертому рівні здійснюється оперативне реагування на небезпечну подію задля її нейтралізації (видалення). Реалізація процедур цього рівня залежить від організації управління захистом і від просторово-технологічних можливостей системи захисту щодо припинення небезпечних подій. Заходи, які реалізуються на цьому рівні, обов'язкові лише для систем захисту інформації.

Останній п'ятий рівень захисту передбачає безпосередню нейтралізацію небезпечних подій. Складність заходів цього рівня полягає у вирішенні

конфліктної ситуації, яка вимагає використання спеціальних ресурсів. Завершує цю послідовність контроль результатів нейтралізації небезпечної події й оцінка за заданим критерієм.

З наведеного вище можливо зробити такий висновок: кіберпростір має стати інструментом нашої асиметричної відповіді на агресію; добиватися управління не лише своїми засобами, а й супротивником; створювати й удосконалювати інтелектуальний потенціал (де чільне місце займає підготовка кадрів), мислити по-новому; всі органи й системи управління «тримати у формі» через проведення впорядкованих тренувань з управління в кризових ситуаціях з охопленням усіх можливих варіантів розвитку подій; багаторівневий захист може використовуватися для розв'язання завдань забезпечення інформаційної безпеки об'єктів різного призначення і для захисту самого об'єкта, і для захисту інформації, яка в ньому циркулює.

Відповідно до висновків кібербезпека сьогодні набуває значення нової галузі в нашому ВПК і призначена гарантувати національну безпеку держави. Тому вчасне планування й реалізація заходів забезпечення кібербезпеки та інформаційного протиборства на глобальному й регіональному рівнях стає одним із пріоритетних завдань держави. Україна не просто може, а вимушена перестати концентруватися лише на оборонних заходах. Маючи один із найкращих у світі людських потенціалів, фахівців з IT, здатність працювати швидко та ефективно, високу мотивацію до протистояння зовнішній агресії, держава повинна робити ставку

не лише на оборонні технології, а й на наступальні, у тому числі кіберозброєння.

Основні поняття

Основною сутнісною ознакою кіберзлочину є те, що це є діяння, сама можливість вчинення якого випливає з особливих можливостей інформаційно-телекомунікаційних технологій, які використовуються для завдання шкоди суспільним відносинам.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією через передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Контрольні завдання

1. Розкрийте зміст поняття «кіберзлочину» та назвіть його ознаки.

2. Вкажіть, у якому акті вказано міжнародні нормативні акти у сфері протидії кіберзлочинності.

3. Сформулюйте види кіберзлочинів відповідно до міжнародних нормативних актів.

4. Сформулюйте види кіберзлочинів відповідно до Кримінального кодексу України.

Розділ 3

Загальні положення кваліфікації кіберзлочинів

Аналіз зареєстрованих в Україні кіберзлочинів показує постійне зростання рівня кіберзлочинності та суми збитків, які завдаються кіберзлочинцями державі та бізнесу.

Відповідно до цього потрібно усвідомлювати, що рівень латентності у сфері розслідування кіберзлочинів надзвичайно високий: передовсім через те, що злочини, які мають за мету втручання в роботу комп'ютеризованих систем без їх очевидного пошкодження, або викрадення коштів здебільшого лишається непоміченим, або не повідомляється до органів правопорядку. Тому зазвичай, офіційна статистика за даними кримінальних справ становить менше половини від кількості кіберзлочинів.

Для попередження необ'єктивності у своєму аналізі динаміки розвитку ситуації з кібербезпекою в Україні ми також спираємося на відомості Державного центру кіберзахисту, що діє на базі Державної служби спецзв'язку та захисту інформації, а також на дослідження приватних компаній, які спеціалізуються у сфері надання послуг із забезпечення кібербезпеки та моніторингу кіберзагроз.

Верховна Рада ухвалила Закон України «Про основні засади забезпечення кібербезпеки України», який заклав правове підґрунтя для віднесення приватних підприємств до критично важливих об'єктів інформаційної інфраструктури зі спеціальним статусом та запровадив поняття і основні характеристики державно-приватної взаємодії у сфері кібербезпеки.

Відповідно до положень ст. 1 та ст. 6 означеного Закону до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність і надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки й безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Стаття 10 Закону, своєю чергою, визначає шляхи здійснення державноприватної взаємодії у сфері кібербезпеки:

1) створення системи вчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів із підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу задля забезпечення безпеки в інтернеті;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, у т. ч. страховиків, аудиторів, юристів, визначення

їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями для виконання заходів кібероборони в кіберпросторі.

Також Законом України «Про основні засади забезпечення кібербезпеки України» встановлюється обов'язок державних органів та органів місцевого самоврядування, їх посадових осіб, підприємств, установ та організацій незалежно від форми власності, осіб, громадян та об'єднання громадян сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.

На сьогодні все ще не завершена розроблення необхідних підзаконних нормативних актів, які б визначили порядок та способи реалізації положень закону. Не склалася правозастосовна практика та корпоративні традиції в цій сфері. Все ще не вирішеним залишається більшість питань щодо визначення конкретних суб'єктів, які забезпечуватимуть реалізацію положень цього закону та підготовки належної кількості спеціалістів у цій сфері.

З огляду на викладене, найбільш пріоритетними завданнями на цьому етапі вважаються:

– завершення формування нормативно-правової бази у сфері кібербезпеки через прийняття необхідних підзаконних актів у частині регулювання порядку віднесення підприємств до об'єктів критичної інфраструктури та проведення їх незалежного аудиту;

– підготовка та популяризація рекомендаційних вимог щодо кібербезпеки та стандартів реагування на кіберінциденти, для запровадження належного рівня кіберзахисту інформаційних систем держави та створення достатніх передумов для швидкого та ефективного реагування на кіберінциденти та розслідування кіберзлочинів.

Представники індустрії інформаційних технологій і власники підприємств віднесених до об'єктів критичної інфраструктури повинні відповідальніше ставитися до своїх обов'язків щодо забезпечення кібербезпеки держави та відповідно до світової практики розпочати роботу над національними стандартами корпоративної етики та принципів взаємодії і обміну інформацією з державою та міжнародними акторами в цій сфері.

3.1. Результати кваліфікації кіберзлочинів

Процесуальне рішення щодо кваліфікації кіберзлочину може приймати один із таких змістів:

1. Діяння є:

– закінченим злочином, учиненим особою за відсутності ознак співучасті у злочині або вико-

навцем (співвиконавцем) за їх наявності (застосуванню підлягає певна стаття (частина, пункт, пункти) ОЧ ККУ);

– готуванням до злочину середньої тяжкості, тяжкого чи особливо тяжкого злочину, вчиненим особою за відсутності ознак співучасті у злочині або виконавцем (співвиконавцем) за їх наявності (застосуванню підлягає певна стаття (частина, пункт, пункти) ОЧ ККУ) з попереднім посиланням на ч. 1 ст. 14 ККУ);

– замахом на злочин, учиненим особою за відсутності ознак співучасті у злочині або виконавцем (співвиконавцем) за їх наявності (застосуванню підлягає певна стаття (частина, пункт, пункти) ОЧ ККУ) з попереднім посиланням відповідно на частини 2 або 3 ст. 15 ККУ (залежно від виду замаху на злочин));

– співучастю (у виді організації, підбурювання чи пособництва) в закінченому чи незакінченому злочині (застосовуються наведені вище правила з попереднім посиланням на частини 3, 4 або 5 ст. 27 ККУ – відповідно);

– множинністю злочинів (щодо кожного з епізодів застосовується наведені вище правила);

2. Діяння не є злочином, оскільки:

– відсутні всі необхідні й достатні ознаки будь-якого складу злочину, передбаченого ККУ (відсутні ознаки суб'єкта, має місце казус тощо);

– воно формально передбачене кримінальним законодавством, але у зв'язку з малозначністю (ч. 2 ст. 11 ККУ) не становить суспільної небезпеки;

– воно передбачене кримінальним законодавством, але вчинене за наявності обставин, що виключають злочинність діяння;

– має місце підготовка до злочину невеликої тяжкості, відповідальність за яке виключається (ч. 2 ст. 14 ККУ);

– має місце добровільна відмова від доведення конкретного злочину до кінця, а фактично вчинене складу іншого злочину не містить (ч. 2 ст. 17 ККУ).

Найчастіше діяльність правоохоронних органів спрямована на перший випадок кваліфікації, що не виключає обов'язковості звернення уваги на підстави для прийняття другого рішення. Але все ж таки друге рішення приймається найчастіше в ході діяльності спрямованої на прийняття першого виду рішення про кваліфікацію.

Отже, розглянемо послідовно загальні положення прийняття такого рішення. У ході розгляду матеріалу буде проаналізоване якомога ширше коло особливостей кримінально-правової кваліфікації. Звичайно, пояснення будуть даватися максимально наближено до специфіки діяльності кіберполіції. Але з огляду на те, що з розвитком ІТТ все більше видів традиційних злочинів вчиняються з їх використанням (навіть проти життя та здоров'я), увага буде приділятися всім видам злочинів.

3.2. Кваліфікація незакінчених кіберзлочинів

Нині галузь ІТ, і програмування БД зокрема, і далі стрімко розвиваються. Проте з розвитком ІТ

все гостріше стоїть питання безпеки ПЗ та БД, якими оперують ІС. Одна з найбільш актуальних проблеми сучасних баз даних, написаних за допомогою SQL, – це SQL-injection.

SQL ін'єкція – один із поширених способів злому сайтів та програм, що працюють із базами даних, заснований на впровадженні в запит довільного SQL-коду.

Перед самою атакою зловмисник вивчає поведінку скриптів сервера при маніпуляції вхідними параметрами задля виявлення їх аномальної поведінки. Маніпуляція відбувається всіма можливими параметрами:

– даними, переданими через методи post і get;

– значеннями (http-cookie);

– http_referer (для скриптів);

– auth_user та auth_password (при використанні аутентифікації).

Зазвичай, маніпуляція зводиться до підстановки в параметри символу одинарної (рідше подвійний або зворотної) лапки.

Аномальною поведінкою вважається будь-яка поведінка, за якої сторінки, одержувані до і після підстановки лапок, розрізняються (і при цьому немає повідомлення про неправильний формат параметрів). Найчастіші приклади аномальної поведінки:

– виводиться повідомлення про різні помилки;

– при запиті даних (наприклад, новини або списку продукції), дані про які здійснювався запит не виводяться взагалі, хоча сторінка відображається і т. д.

Слід ураховувати, що відомі випадки, коли повідомлення про помилки, через специфіку розмітки сторінки, не видно в браузері, хоча і присутні в її HTML-коді.

Упровадження SQL, залежно від типу СУБД та умов впровадження, може дати можливість атакувальнику виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері. Атака типу впровадження SQL може бути можлива за некоректної обробки вхідних даних, що використовуються в SQL-запитах, поділяється на кілька типів:

1. *UNION query SQL injection*. Класичний варіант упровадження SQLкоду, коли в уразливий параметр передається вираз, який починається з «UNION ALL SELECT». Ця техніка працює, коли вебдодатки напряму повертають результат вводу команди SELECT на сторінку: з використанням циклу for або схожим способом, так що кожен запис отриманої з БД вибірки послідовно виводиться на сторінку.

2. *Error-based SQL injection*. Цей спосіб ґрунтується на виведенні інформації в тексті помилки виконання запиту. Для цього потрібно прямо виводити текст помилки на саму сторінку. Однак цим «грішить» значна частина починаючих розробників.

3. *Stacked queries SQL injection*. Цей прийом переважно використовується для впровадження SQL-команд, відмінних від SELECT, наприклад,

для маніпуляції даними (за допомогою INSERT або DELETE). Примітним є те, що техніка потенційно може привести до можливості читання/запису з файлової системи, а також виконанню команд в ОС.

4. *Boolean-based blind SQL injection.* Реалізація так званої «сліпої ін'єкції»: дані з бази даних у «чистому» вигляді уразливим вебдодатком не повертаються. Цей прийом також іноді називають дедуктивним.

5. *Time-based blind SQL injection.* Повністю сліпа ін'єкція. Як і в минулому прикладі, «гра» проводиться з уразливим параметром. Але до нього додається підзапит, який призводить до паузи роботи DBMS на певну кількість секунд (наприклад, за допомогою команд SLEEP) або BENCHMARK). Використовуючи цю специфіку, хакер може посимвольно вилучити інформацію з бази даних, порівнюючи час відповіді на оригінальне питання й на запит з упровадженим кодом. Також тут використовується алгоритм бінарного пошуку. Крім того, використовується спеціальний метод верифікації даних, щоб зменшити ймовірність неправильного вилучення символу через нестабільне з'єднання.

Якщо сайт було зламано, то слід урахувати, що, використовуючи інформацію в своїх цілях, хакери залишають так звані backdoors – приховані точки входу. Це можуть бути файли з будь-яким розширенням, навіть jpg, але в них буде закодовано php-код для проникнення в систему. Нині існує багато антивірусів, програм, які сканують файлову систему сайту на предмет підозрілих файлів.

У теорії кримінального права та у кримінальному законодавстві виділяють три стадії злочину, які враховуються при кваліфікації посягання:

1) підготовка до злочину;

2) замах на злочин;

3) закінчений злочин.

Так зване «виявлення умислу», тобто намір вчинити злочин, який не виразився зовні в конкретних діяннях, не є злочином, не тягне кримінальної відповідальності. Адже злочин, відповідно до ст. 11 ККУ, – це дія або бездіяльність.

Підготовка до злочину та замах на нього у ККУ називається незакінченим злочином, у теорії та на практиці їх ще прийнято називати попередньою злочинною діяльністю (або попередніми стадіями вчинення злочину).

Посягання кваліфікується як підготовка до злочину чи замах на нього лише тоді, коли злочинна діяльність перервана на відповідній стадії. Якщо ж злочин продовжується, після підготовчих дій вчиняються ті, що оцінюються як замах, або має місце закінчений злочин, то стадії готування до злочину, замаху на нього самостійній кваліфікації не підлягають. Відбувається так зване поглинання пізнішою стадією вчинення злочину попередньої стадії.

Урахування стадії вчинення злочину при його кваліфікації полягає:

– у побудові формули кваліфікації, яка щодо кожної зі стадій має специфічний зміст;

– в оцінці певних видів злочинної діяльності як незакінчених злочинів;

– у розв'язанні питань конкуренції закінчених та незакінчених злочинів;

– у визнанні наявності сукупності у випадках, коли попередня злочинна діяльність є самостійним закінченим злочином.

Закінчений злочин – це типовий вид злочину, ознаки котрого встановлені у нормах ОЧ ККУ, стосовно якого сконструйовані основні інститути ЗЧ ККУ (вина, співучасть, причетність тощо).

За загальним правилом *злочин визнається закінченим, якщо у фактично скоєному є всі ознаки складу злочину, передбачені статтею ОЧ ККУ.*

З наведеного вище випливає, що при визначенні моменту закінчення злочину потрібно враховувати:

1) *описання злочину в ОЧ ККУ* – чим більше ознак злочину названо в диспозиції статті ККУ, тим більше їх потрібно для того, щоб були підстави вважати злочин закінченим;

2) *фактичне виконання об'єктивної сторони злочину* – злочин може бути визнаний закінченим лише тоді, коли є всі обов'язкові ознаки об'єктивної сторони.

Відповідно до різних видів злочинів момент закінчення визначається так:

1) злочин з матеріальним складом (у конструкції якого законодавець передбачає обов'язкову наявність суспільно небезпечного діяння, суспільно небезпечного наслідку та причинного зв'язку між ними) вважається закінченим тоді, коли настали суспільно небезпечні наслідки посягання, передбачені диспозицією статті ОЧ ККУ;

2) злочин із формальним складом (у конструкції якого законодавець передбачає обов'язкову наявність тільки суспільно небезпечного діяння) вважається закінченим тоді, коли повністю виконане (завершене) діяння, що назване в диспозиції статті ОЧ ККУ як ознака складу такого посягання;

3) злочин з усіченим складом (є різновидом злочинів із формальним складом, які у зв'язку з їх підвищеною суспільною небезпечністю, вважаються закінченими на більш ранніх стадіях вчинення злочину: на стадії підготовки або замаху) вважається закінченим з моменту початку виконання суспільно небезпечного діяння, вказаного в диспозиції статті ОЧ ККУ;

4) триваючі злочини, які в чинному законодавстві передбачені лише з формальним складом, кваліфікуються як закінчені тоді, коли виконане діяння, яке є обов'язковою ознакою об'єктивної сторони;

5) при кваліфікації продовжуваного злочину, який складається з декількох діянь, потрібно виділяти дві ситуації.

Перша має місце тоді, коли закон пов'язує кримінальну відповідальність з учиненням декількох дій, тобто коли відбувається формальний склад злочину. Такий злочин кваліфікується як закінчений тоді, коли виконана остання з дій, достатніх для визнання посягання злочином; друга – при повторності (неодноразовості); третя – при систематичності.

Друга з таких ситуацій полягає у вчиненні посягань із матеріальним складом. Такого роду

продовжуваний злочин є закінченим тоді, коли розмір шкоди стає достатнім для визнання посягання, що складається з кількох деліктів, злочином.

Кваліфікуючи продовжуваний злочин, що складається з посягань, кожне з яких може оцінюватися як окремий злочин, також треба розрізняти дві ситуації.

Перша має місце тоді, коли вчинено декілька діянь, спрямованих на досягнення єдиного результату, але сумарні наслідки не перетворюють злочин на кваліфікований. У такому разі скоєне кваліфікується за частиною статті, яка передбачає простий вид цього злочину незалежно від того, скільки вчинено дій. Учинення першої ж дії (за умови, що вона тягне за собою наслідки, при наявності яких настає кримінальна відповідальність), дає підстави кваліфікувати злочин як закінчений.

Друга – коли вчинення другого, третього чи наступного діяння призводить до заподіяння наслідків, характерних для кваліфікованого чи особливо кваліфікованого виду цього злочину. При цьому вчинення хоча б першої з кількох запланованих дій, які повинні привести до відповідних наслідків, слід кваліфікувати як замах на кваліфікований (особливо кваліфікований вид злочину). Після вчинення діяння, внаслідок якого заподіяна шкода, що є ознакою складу кваліфікованого або особливо кваліфікованого складу злочину, скоєне має оцінюватися як відповідний закінчений злочин;

б) складений злочин кваліфікується як закінчений за умови, що є закінченими всі посягання, які його утворюють;

7) дії кожного зі співучасників кваліфікуються як посягання за тією стадією, яку вчинив виконавець злочину.

Закінчений злочин кваліфікується лише за статтею ОЧ ККУ.

Кваліфікація злочину як закінченого посягання означає:

1) у скоєному є всі обов'язкові ознаки відповідного складу злочину;

2) діяння, вчинені до моменту закінчення даного посягання, але у зв'язку з ним, підлягають додатковій (самостійній, окремій) кваліфікації за умови, що вони не охоплюються ознаками даного злочину – коли має місце сукупність злочинів;

3) діяння, скоєні після закінчення злочину, не впливають на кваліфікацію цього посягання, якщо вони не становлять іншого злочину;

4) діяння, вчинені після закінчення злочину, підлягають додатковій кваліфікації тоді, коли вони утворюють самостійний злочин.

Формула кваліфікації готування до злочину чи замаху на злочин повинна відповідати таким вимогам:

1) містити посилання на ч. 1 ст. 14 або частини 2 чи 3 ст. 15 ККУ. Потрібно наголосити, що посилатися слід не просто на статті 14 чи 15 ККУ, а й на відповідні частини цих статей, оскільки ознаки, яких бракує, підстави кримінальної відповідальності за окремі стадії попередньої злочинної діяльності різні. Крім того, посилання на відповідні частини статей 14 або 15 ККУ робить формулу кваліфікації більш інформативною;

2) посилання на статтю ЗЧ ККУ має міститися перед вказівкою на статтю ОЧ ККУ. Завдяки цьому акцентується увага на те, що має місце незакінчений злочин, об'єктивна сторона якого «недорозвинута»;

3) містити посилання на відповідну частину, пункт статті ОЧ ККУ, котрі передбачають закінчений злочин, щодо якого мало місце готування чи замах;

4) якщо винному інкримінується вчинення кількох незакінчених злочинів, передбачених кількома статтями ОЧ ККУ, то посилання на відповідні частини статей 14 або 15 ККУ повинно бути перед кожною зі статей ОЧ ККУ, причому незалежно від того, мають місце однакові чи різні стадії вчинення злочину;

5) у формулі кваліфікації попередньої злочинної діяльності розділові знаки повинні бути розставлені так, щоб було видно, до якої статті ОЧ ККУ належить посилання на ч. 1 ст. 14, частини 2 або 3 ст. 15 ККУ. Особливо це важливо у випадках учинення винним декількох злочинів, передбачених різними статтями ОЧ ККУ. Оптимальним видається відділяти посилання на статті ЗЧ ККУ і ОЧ ККУ комою, посилання ж на окремі статті ОЧ ККУ – крапкою з комою. При цьому формула кваліфікації (наприклад, дій А., який учинив підготовку до вмисного вбивства без обтяжуючих обставин та закінчений замах на крадіжку чужого майна з проникненням у житло) матиме такий вигляд:

А.: ч. 1 ст. 14; ч. 1 ст. 115; ч. 2 ст. 15; ч. 3 ст. 185 ККУ.

Якщо ж формулу кваліфікації цього посягання записати так, як це нерідко трапляється на практиці: *А.: статтях 14; 15 ч. 2; 115 ч. 3; 185 ККУ,* то з неї не вбачається, яка конкретна стадія попередньої злочинної діяльності має місце, який злочин є закінченим, а який – ні.

Готування до злочину кваліфікується з урахуванням загальних правил кваліфікації попередньої злочинної діяльності, підстав кримінальної відповідальності за неї. Тобто скоєне кваліфікується за статтею ОЧ ККУ, яка передбачає відповідний закінчений злочин, із посиланням на ч. 1 ст. 14 ККУ. При цьому має бути констатована наявність усіх ознак складу відповідного закінченого злочину з урахуванням незавершеності його об'єктивної сторони, а також вчинення діяння, яке відповідає ознакам готування до злочину.

Замах на злочин кваліфікується за ч. 2 (закінчений замах) або ч. 3 (незакінчений замах) ст. 15 ККУ та статтею ОЧ ККУ, яка передбачає відповідний закінчений злочин. При цьому потрібно встановити наявність усіх ознак складу закінченого злочину з урахуванням незавершеності об'єктивної сторони – відсутності суспільно небезпечних наслідків або закінченого діяння в матеріальних складах злочинів; незавершеності діяння у формальних складах злочинів. Якщо замаху передували дії, у яких полягає підготовка до цього ж злочину, то все скоєне кваліфікується лише як замах на злочин, оскільки, як вже зазначалося, кожна наступна стадія «поглинає» собою попередні стадії посягання.

3.3. Кваліфікація кіберзлочинів, учинених у співучасті

При кваліфікації злочинів, вчинених у співучасті, потрібно:

1) установити, чи має місце співучасть;

2) визначити вид співучасті та встановити: кваліфікується вона з посиланням на ст. 27 ККУ чи лише за статтею ОЧ ККУ;

3) установити вид співучасника і при необхідності здійснити посилання на ст. 27 ККУ (та визначити частину цієї статті);

4) установити форму співучасті відповідно до ст. 28 ККУ (визначити частину цієї статті);

5) з'ясувати, який злочин вчинено співучасниками і якою статтею (частиною статті) ОЧ ККУ він передбачений з урахуванням форми співучасті;

6) визначити, чи всі співучасники відповідають за однією і тією ж статтею ОЧ ККУ чи за різними і за якими саме.

Діяння кожного зі співучасників кваліфікуються окремо. До того ж самостійній кваліфікації підлягає кожний з учинених у співучасті чи без неї злочинів.

Зупинимось коротко на цих етапах.

По-перше, співучастю називається умисна спільна участь декількох суб'єктів злочину у вчиненні умисного злочину (ст. 26 ККУ). Отже, є ознаки, які свідчать про відсутність співучасті: 1) учинення злочину лише одним суб'єктом злочину; 2) спільне вчинення кількома особами необережного злочину; 3) використання необережності іншої особи для

вчинення злочину; 4) відсутність сумісності посягання; 5) відсутність двостороннього суб'єктивного зв'язку між особами, з участю яких вчиняється злочин; 6) у злочинах із подвійною формою вини, кваліфікованих за наслідками.

Багато з цих ознак трапляється при вчиненні кіберзлочинів, а тому при їх кваліфікації слід приділити увагу відсутності їх всіх. Зокрема, найчастіше виникає питання про відсутність двостороннього суб'єктивного зв'язку між особами, з участю яких вчиняється злочин, – при вчиненні кіберзлочину його учасники іноді навіть не бачили один одного ніколи і не спілкувалися в реальному житті. А тому слід установити факт їх спілкування в кіберпросторі про вчинення злочину, який або передував йому (група за попередньою змовою, організована група, злочинна організація), або відбувався під час його вчинення (група осіб). Якщо такий факт відсутній, то діяння всіх цих осіб кваліфікуються за відсутності ознак співучасті.

Наприклад, така ситуація була при DDOS-атаці на сайт ex.ua – тисячі осіб, лише побачивши призив до атаки, почали його відкривати в браузері та активно ним користуватися, від чого він і зупинив роботу. Вони не знали про дії інших своїх «колег», ніколи не бачили один одного, не спілкувалися щодо сумісних дій, не знали про конкретні дії інших, не планували і не координували їх, а отже не мали суб'єктивного зв'язку – обов'язкової ознаки співучасті.

Також часто вік правопорушників у мережі не досягає межі, з якої настає кримінальна відпові-

дальність. Отже, слід пам'ятати, що вчинення злочину лише одним суб'єктом злочину не є співучастю, скільки б у нього не було малолітніх «помічників».

Види співучасті, які враховуються у кваліфікації злочинів:

1) співучасть *за формою її відображення і врахування (вираження) у кримінальному законі.* Співучасть, передбачену ЗЧ ККУ, називають ще *співучастю у власному (у вузькому) розумінні слова.* Вона характерна тим, що окремі учасники злочину (підбурювач, організатор, пособник) не виконують складу посягання, передбаченого статтями ОЧ ККУ, тому виникає потреба обґрунтувати відповідальність за таку злочинну діяльність. При цьому загальновизнано, що в цих випадках караність посягання визначається сукупністю положень, які містяться і у ЗЧ ККУ (ст. 27), і в ОЧ ККУ (що стосуються спільно вчинюваного посягання, об'єктивну сторону якого завершує виконавець злочину). Специфіку суспільної небезпеки такої співучасті слід ураховувати, виходячи передовсім із небезпеки посягання виконавця, у межах санкції статті, яка передбачає вчинений ним злочин. При цьому всі злочини, вчинені у співучасті, яка передбачена ЗЧ ККУ, можуть бути скоєні й без співучасті – одноособово.

Стаття ОЧ ККУ регламентує співучасть (її прийнято називати *співучастю особливого роду)* в тих випадках, коли об'єднання декількох осіб для вчинення злочину збільшує суспільну небезпеку сумісної злочинної діяльності настільки, що це по-

трібно врахувати при побудові санкції кримінально-правової норми. Відповідні злочини можуть бути вчинені лише у співучасті, вона для цих посягань є необхідною ознакою. Отже, злочини, щодо яких ОЧ ККУ передбачено їх вчинення у співучасті, не можуть бути скоєні однією особою. Це стосується і тих випадків, коли відповідні норми передбачають діяльність кількох осіб, які спільно виконують об'єктивну сторону злочину (для їх позначення закон використовує вказівку на вчинення злочину «групою осіб», «групою осіб за попередньою змовою», «організованою групою», а також окремими видами злочинних організацій), так і тих, коли одна особа спонукає інших до злочинної діяльності, керує їх злочинами, надає сприяння (а у відповідних статтях передбачена відповідальність за «організацію», «керівництво», «фінансування», «постачання» тощо).

Для кваліфікації співучасті, передбаченої статтями ОЧ ККУ, немає потреби посилатися на відповідний інститут, передбачений ЗЧ ККУ (ст. 27), однак немає й підстав вважати, що в таких випадках взагалі немає необхідності в інституті співучасті. Адже кваліфікація співучасті, встановленої статтями ОЧ ККУ, передбачає врахування специфічних положень, вироблених стосовно саме такої співучасті – співучасті особливого роду.

2) співучасть *за характером ролей, що їх виконують окремі співучасники.* Види співучасників – виконавця, організатора, підбурювача, пособника – виділяє закон у ст. 27 ККУ. Вид співучасника має відображатися при кваліфікації через посилання

на відповідну частину цієї статті (крім виконавця). Слід зазначити, що характер поведінки учасників спільного злочину враховується лише при кваліфікації співучасті, передбаченої ЗЧ ККУ. Для співучасті, передбаченої в ОЧ ККУ, специфічним є те, що незалежно від характеру виконуваних ролей кожен учасник такого злочину прирівнюється до виконавця, його дії повністю охоплюються статтями ОЧ ККУ і не кваліфікуються з посиланням на ст. 27 ККУ. При кваліфікації дій співучасника, який поєднує декілька функцій, слід посилатися на кожну із частин ст. 27 ККУ, що передбачає діяльність певних видів співучасників, та відповідну статтю ОЧ ККУ.

3) співучасть *за ступенем згуртованості учасників спільно вчинюваного злочину, організованості, стійкості їх об'єднання.* Така класифікація в теорії кримінального права називається класифікацією за *формою співучасті.* Чинним ККУ вона відображена у ст. 28. Ця співучасть враховується у кваліфікації тільки у разі, якщо прямо вказана в ККУ, і додатково (посиланням на ст. 28 ККУ) у формулі кваліфікації не відображається.

Правила кваліфікації кіберзлочинів, учинених групою осіб:

1) діяння учасників групи – виконавців, тобто осіб, які, діючи погоджено, виконують об'єктивну сторону злочину, кваліфікуються безпосередньо за статтею ОЧ ККУ, що передбачає вчинення злочину групою осіб;

2) посягання організаторів, підбурювачів та пособників злочину, вчиненого групою осіб – неучас-

ників такої групи – кваліфікуються з посиланням на відповідну частину ст. 27 ККУ та статтю ОЧ ККУ, яка передбачає злочин, учинений групою осіб;

3) але якщо стаття не передбачає такої кваліфікуючої ознаки, то діяння виконавців кваліфікуються за статтею ОЧ ККУ, так, як у разі вчинення злочину однією особою, а діяння «неучасників» – ще додатково за відповідною частиною ст. 27 ККУ.

При кваліфікації кіберзлочину, вчиненого за попередньою змовою групою осіб, можливі такі варіанти:

1) у диспозиції статті передбачене вчинення злочину за попередньою змовою групою осіб (тобто ця форма співучасті виступає як співучасть особливого роду) – *діяння учасників групи кваліфікуються лише за відповідною частиною статті ОЧ ККУ, без посилання на статті ЗЧ ККУ. Участь у вчиненні такого злочину осіб, які не входять до складу групи, кваліфікується з посиланням на частини 3–5 ст. 27 ККУ*;

2) у диспозиції статті вчинення злочину за попередньою змовою групою осіб взагалі не передбачене (тобто має місце співучасть у власному розумінні слова) або передбачена вища форма співучасті – вчинення злочину організованою групою. У таких випадках *скоєне учасниками групи кваліфікується як вид злочину, вчиненого однією особою. Участь у вчиненні злочину осіб, які не є учасниками групи, кваліфікується з посиланням на частини 3–5 ст. 27 і статтю ОЧ ККУ про відповідний вид злочину, вчинений однією особою.*

Таблиця 1

Кваліфікація при організованій співучасті в кіберзлочині

Принцип, відповідно до якого настає кримінальна відповідальність	**Організована група**	**Злочинна організація**
Випадки врахування при вирішенні питань кримінальної відповідальності	1) коли це передбачено в диспозиції статті ОЧ ККУ (33 випадки); 2) у випадках учинення умисних злочинів (додаткова кваліфікація за ч. 3 ст. 28 ККУ)	У випадках, прямо передбачених статтями ОЧ ККУ (5 статей: 255–257, 258-3, 260)
Момент закінчення злочину	Визначається залежно від того, коли є закінченим злочин, учинений організованою групою	Початок організаційних дій, спрямованих на створення угруповання чи вступ до нього
Відповідальність організаторів	За всі злочини, вчинені організованою групою або злочинною організацією, якщо вони охоплювалися умислом організаторів	
Відповідальність інших учасників	За злочини, у підготовці або вчиненні котрих вони брали участь, незалежно від тієї ролі, яку виконував кожен із них	

Злочини, вчинені в складі злочинної організації, слід кваліфікувати самостійно, за сукупністю за вказаними статтями. Слід пам'ятати, що ці статті передбачають відповідальність не тільки саме за створення злочинних організацій або за

участь у скоєних ними злочинах, а й лише за участь у них, що вважається закінченим злочином, якщо особа тільки дала згоду на це.

Випадки, коли посягання співучасників кваліфікуються за різними статтями ОЧ ККУ:

1. Виконавець та інші співучасники або декілька співвиконавців неоднаково усвідомлюють суспільно небезпечний характер своєї дії чи бездіяльності. Якщо певні обставини не охоплювалися виною особи, то вони як обов'язкові ознаки складу злочину не можуть бути враховані при кваліфікації її діяння.

2. Окремі співучасники допускають помилку у визначенні фактичних обставин справи. При цьому дії того з них, хто допустив помилку у визначенні об'єкта посягання, кваліфікуються як замах на вчинення того злочину, який він прагнув виконати.

3. Учинення посягання з альтернативним чи неконкретизованим умислом. Діяння тих співучасників, які беруть участь у незавершеному посяганні, діючи з неконкретизованим чи альтернативним умислом, кваліфікуються за статтею ОЧ ККУ, що передбачає найменш небезпечний вид злочину. Співучасники, які вчиняють посягання з конкретизованим чи безальтернативним умислом, відповідають за статтею ОЧ ККУ, що передбачає фактично заподіяну шкоду.

4. Має місце ексцес у діях певного співучасника. Діяння особи, яка допустила ексцес (не обов'язково виконавця, як про це переважно пишуть у літературі), кваліфікують відповідальність також за статтями, що передбачають такий ексцес.

5. Має місце відхилення дії. Лише виконавець злочину може нести відповідальність за злочини, вчинені у зв'язку з відхиленням дії.

6. Існують індивідуальні особливості, які характеризують особу певного учасника спільного злочину і впливають лише на його відповідальність, а отже за загальним правилом, не враховуються при кваліфікації дій інших співучасників. Тому статті ОЧ ККУ, які передбачають врахування таких особливостей, інкримінуються лише певному співучаснику, і за ними не кваліфікується посягання інших учасників того ж самого злочину. Такими індивідуальними особливостями можуть бути ознаки спеціального суб'єкта, повторність посягання, рецидив тощо.

7. Одні зі співучасників досягли віку, з якого може наставати кримінальна відповідальність за злочин, вчинюваний у співучасті, а інші – ні.

3.4. Кваліфікація множинних кіберзлочинів

Множинність злочинів має місце у разі вчинення однією особою або співучасниками двох або більше злочинних діянь (дії чи бездіяльності) кожне з яких має ознаки самостійного складу злочину.

Фактично головним у кваліфікації множинності злочинів є відмежування множинності від одиничних злочинів. Одиничний, або один злочин (на відміну від множини злочинів), – поняття власне юридичне, а не кількісне за рахунком дій, наслідків, що настали, вчинених епізодів тощо.

Одиничним називається злочин, передбачений однією кримінально-правовою нормою, яка містить лише один склад злочину. Одиничний злочин характеризується єдністю всіх його елементів: а) має один і той же безпосередній об'єкт посягання і злочинні наслідки; б) вчинюється однією або кількома тотожними діями; в) вчинюється за одним видом вини – умисно чи необережно.

Простий одиничний злочин складається з однієї дії або з однієї дії й одного виду наслідків. Прикладом першого може бути зайняття гральним бізнесом (ст. 203-2 ККУ), а другого – порушення правил, що заподіяло значну шкоду (ст. 363 ККУ).

Складні одиничні злочини мають декілька видів:

1) злочин, склад якого включає дві чи більше альтернативні різноманітні дії, наприклад злочин, передбачений ст. 361-1 ККУ: створення задля використання, поширення або збуту шкідливих програмних чи технічних засобів, їх розповсюдження або збут, всі ці дії мають загальну єдність, мету та вид вини;

2) злочин, що має додаткові тяжкі наслідки, що наступають слідом за основними, наприклад у ч. 3 ст. 362 ККУ, значна шкода наступає за зміною, знищенням, блокуванням (наслідки за ч. 1) або витоком (наслідок за ч. 2) інформації (див. також ст. 363-1);

3) складений злочин, що має:

а) безпосередній об'єкт, що включає декілька об'єктів посягання, наприклад відносини у сфері використання комп'ютерних систем та власність на інформацію при несанкціонованих діях з ІОД (ст. 361-2);

б) два види дій, які є де-юре складами окремих злочинів, але органічно поєднані в одному, наприклад застосування насильства чи погроза його застосування та використання малолітньої дитини для заняття жебрацтвом у ч. 2 ст. 150-1 ККУ, або вимога передачі чужого майна чи права на майно, або вчинення будь-яких дій майнового характеру та погроза розголошення відомостей, які потерпілий чи його близькі родичі бажають зберегти в таємниці в ст. 189 ККУ;

в) декілька видів альтернативних злочинних наслідків, наприклад виток, втрата, підроблення, блокування інформації, спотворення процесу оброблення інформації або порушення встановленого порядку її маршрутизації в ч. 1 ст. 361 ККУ.

До складних також належать продовжувані та триваючі злочини.

Продовжуваний злочин складається з кількох тотожних злочинних актів, поєднаних одним умислом і спрямованих на досягнення однієї загальної мети. Всі злочинні акти продовжуваного злочину мають спільну (одну) суб'єктивну сторону, і тому вони утворюють один злочин. Продовжуваним злочином може бути, зокрема, викрадення певної суми грошей окремими частинами за кілька незаконних транзакцій, кожна з яких є несанкціонованим утручанням. Початком продовжуваного злочину є вчинення першого злочинного акту. Закінчується продовжуваний злочин: 1) вчиненням останнього злочинного акту; або 2) явкою з повинною; або 3) затриманням винного і припиненням його злочинної діяльності.

Триваючий злочин – така злочинна дія чи бездіяльність, після якої настає тривале невиконання особою свого важливого юридичного обов'язку. Наприклад, особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), АС, КМ чи МЕ, після порушення правил їх експлуатації або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 ККУ), що, наприклад, систематично заподіює значну шкоду потерпілій особі, може перебувати в стані вчинення триваючого злочину поки не буде встановлено, що ця шкода заподіюється її діями чи бездіяльністю, або поки сама не виправить цих порушень.

Видами множинності злочинів є повторність, сукупність та рецидив злочинів.

У кримінальному праві повторністю злочинів (ст. 32 ККУ) називається вчинення особою вдруге злочину, в якому згідно з кримінальним законом передбачено ознаку повторності незалежно від того, чи була ця особа притягнута до відповідальності за попередній (перший) злочин.

Практичне значення поняття повторності злочинів полягає в тому, що в одних кримінально-правових нормах одиничний злочин (учинок) не відрізняється від злочину-діяльності, а в інших закон значно посилює кримінальну відповідальність за вчинення злочину вдруге, повторно. Так, статті 361–362 та 363-1 ККУ встановлюють кримінальну відповідальність і за такі діяння, вчинені як одиничний злочинний акт, і за множину – повторність і неодноразовість таких злочинних актів. Кількість злочинних актів при цьому не

впливає на міру відповідальності, кваліфікацію діяння і має значення лише для призначення міри покарання.

Чинне кримінальне законодавство України передбачає два види повторності:

1) повторність як обставина, що обтяжує покарання (п. 1 ст. 67 ККУ);

2) повторність як кваліфікуюча ознака злочину, що передбачена статтями ОЧ ККУ.

Повторність як обставина, що обтяжує кримінальну відповідальність і покарання, не впливає на кваліфікацію діяння, її враховує суд лише при призначенні міри покарання за злочин, учинений вдруге (втретє і більше). Ця повторність має загальний характер – вона поширюється на всі без винятку випадки вчинення двох чи більше злочинів.

Наявність у чинному законодавстві двох видів повторності призводить до їх конкуренції. Вирішується вона на користь повторності як кваліфікуючої ознаки.

Повторність як кваліфікуюча обставина, що передбачена кримінальним законом, має свої характерні ознаки:

1. Вчинення двох або більше одиничних злочинів однією особою (групою осіб).

2. Повторні злочини є однорідними або становлять один і той же склад злочину. В Розділі 16 майже всі статті містять кваліфікуючу ознаку «ті самі дії, вчинені повторно», яка означає другий вид – *повторність тотожних злочинів*. Але, наприклад, примітка до ст. 185 ККУ зазначає, що повторність у вказаних у ній статтях охоплює не

тільки вчинення злочинів із всього наведеного в ній переліку, а й одного зі злочинів, передбачених статтями 187, 262 ККУ, що означає *повторність однорідних злочинів*.

При цьому злочин кваліфікується повторно незалежно від того, чи був цей другий злочин (як і попередній) закінченим, чи це був лише замах на вчинення злочину, а також незалежно від тієї ролі, яку виконував винний при вчиненні злочину – чи був він виконавцем, організатором, підмовником, чи пособником злочину. Повторна спроба вчинити один і той же злочин (убити, зґвалтувати, викрасти, одержати чи дати хабар тощо) без перерви в часі не утворює повторності як кваліфікуючої ознаки злочину.

У разі вчинення особою кількох злочинів, одні з яких були закінчені, а інші – ні, незакінчені злочини кваліфікуються окремо з посиланням на статті 14 чи 15 ККУ. Повторне вчинення одного і того ж виду посягання, передбаченого статтями 361–362 та 363-1 ККУ, кваліфікується лише за частинами 2 або 3 (для ст. 362) цих статей. Додатково кваліфікувати перший злочин ще й за частинами 1 або 2 (для ст. 362) статті непотрібно. Але якщо особа вчинила кілька посягань у цій сфері, які передбачені різними статтями, то перший злочин кваліфікується окремо за ч. 1 (або 2) відповідної статті, а інші, як учинені повторно, – за ч. 2 (або 3) цієї ж статті ККУ.

За загальним правилом, учинення особою двох злочинів, передбачених різними частинами однієї статті ККУ, кваліфікується лише за тією частиною

цієї статті, яка передбачає більш тяжкий злочин і суворіше покарання, тому що кримінальний закон, встановлюючи відповідальність за повторний злочин, ураховує цю кваліфікуючу ознаку, що значно обтяжує вчинення злочину і відповідальність та суттєво підвищує міру покарання за нього.

3. Злочини, що утворюють повторність, вчиняються в різний час, послідовно, а не одночасно. Ця особливість повторності визначається законом. У багатьох статтях кримінального закону повторність визначена словами: «вчинення злочину особою, яка раніше вчинила такий злочин» (ч. 2 ст. 203; ч. 2 ст. 204; ч. 2 ст. 213; ч. 2 ст. 249; ч. 3 ст. 296; ч. 2 ст. 302 та ч. 2 ст. 309 ККУ), тобто між злочинами, що утворюють повторність, є якась певна перерва в часі. Ще більшою є перерва в часі між злочинами, повторність яких у законі визначається словами: «вчинення злочину особою, раніше судимою за такий же злочин» (ч. 2 ст. 79; ч. 2 ст. 80; ч. 2 ст. 125; ч. 2 ст. 161; ч. 2 ст. 162; ч. 3 ст. 168; ч. 2 ст. 170; ч. 2 ст. 206 та ч. 2 ст. 296 ККУ).

4. Повторність як кваліфікуюча ознака злочину утворюється вчиненням злочину вдруге не взагалі, не в будь-якому випадку, але лише тоді, коли повторність безпосередньо вказана в диспозиції кримінально-правової норми. Зокрема шахрайство, вчинене після розбою, є повторним (ч. 2 ст. 190 ККУ), а розбій, учинений після шахрайства, повторним не буде; зґвалтування, вчинене після зґвалтування, є повторним (ч. 2 ст. 152 ККУ), а заподіяння тілесних ушкоджень, учинене після заподіяння тілесних ушкоджень, не є повторним, оскільки така

повторність законом не передбачена, та потребує додаткової кваліфікації за статтями 121–125 ККУ.

Будь-яка повторність утворюється, якщо не минули строки притягнення особи до кримінальної відповідальності за перший (попередній) злочин, або якщо особу не було звільнено на законних підставах від кримінальної відповідальності за перший злочин, або якщо судимість за перший злочин ще не було знято чи погашено.

Слід також мати на увазі, що чинний ККУ України не визнає повторними деякі злочини, зокрема передбачені статтями 111–114, 117, 121, 146, 147, 155, 156, 239–242, 257, 271–275, 286, 287, 293, 295, 298, 338–347 і за повторне (неодноразове, систематичне) вчинення їх не посилює відповідальності. Отже, незалежно від кількості епізодів діяння кваліфікується як одиничний злочин.

Сукупністю злочинів у кримінальному праві називається вчинення особою двох або більше злочинів, передбачених різними кримінально-правовими нормами, за жоден із яких її не було засуджено.

Згідно зі ст. 33 ККУ України сукупність злочинів характеризується такими ознаками: 1) вчинення однією особою двох або більше злочинів, передбачених різними статтями кримінального закону (різними кримінально-правовими нормами); скоєне не охоплюється одним складом злочину; 2) вчинені однією особою злочини мають різні юридичні ознаки, підпадають під ознаки різних статей кримінального закону або різних частин однієї статті

кримінального закону; 3) за вчинені злочини особа ще не притягалася до кримінальної відповідальності й не була за них покараною.

Сукупність можуть утворювати лише ті злочини, які згідно із законом тягнуть за собою кримінальну відповідальність, тобто злочини, щодо яких: 1) не закінчилися строки давності притягнення особи до кримінальної відповідальності (ст. 49 ККУ); 2) немає акта амністії (ст. 86 ККУ); 3) немає інших обставин, що виключають кримінальну відповідальність, наприклад відсутність заяви потерпілого при вчиненні злочинів, передбачених ч. 1 ст. 152; ч. 1 ст. 125; ч. 1 ст. 126 ККУ (ч. 1 і ч. 2 ст. 27 КПК); 4) особа не звільнена від кримінальної відповідальності на підставі статей 44–49 ККУ.

Сукупність утворюють:

1) різні злочини, передбачені різними кримінально-правовими нормами, які мають власні санкції. Не буде сукупності злочинів у тих випадках, коли вчинені діяння передбачені різними пунктами однієї статті (наприклад ч. 2 ст. 115 ККУ), якщо ці пункти не мають власних санкцій. Таке діяння кваліфікується як один злочин, але до вини надаються всі ті пункти ч. 2 ст. 115 ККУ, які є в діях винної особи;

2) злочини, передбачені однією й тією ж статтею кримінального закону, – коли однією статтею кримінального закону передбачається відповідальність за різні злочини, наприклад за несанкціоновані зміну, знищення або блокування інформації (ч. 1 ст. 362 ККУ) і за несанкціоновані перехоплення або копіювання інформації (ч. 2 ст. 362 ККУ);

3) злочини, передбачені різними частинами однієї й тієї ж статті кримінального закону, одна з яких передбачає основний склад злочину, а інші – кваліфікований. Зокрема, вчинення несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ без обтяжуючих ознак, а потім повторного несанкціонованого втручання за наявності значної шкоди доцільно кваліфікувати за сукупністю злочинів, передбачених ч. 1 ст. 361 ККУ та ч. 2 цієї статті.

Не утворюють сукупності:

1) етапи вчинення злочину, які є окремими складовими частинами об'єктивної сторони цього злочину. Наприклад, у тому ж випадку несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ, яке в результаті заподіяло значну шкоду, спочатку вчиняються дії, передбачені ч. 1. Але все заподіяне кваліфікується лише за ч. 2 ст. 361 ККУ як один злочин, оскільки всі інші зазначені злочини були невід'ємним складником цього «кінцевого» злочину. З цієї ж причини не утворюють сукупності злочинів різні стадії вчинення одного і того ж злочину (готування, замах та закінчений злочин);

2) спосіб учинення злочину із самим цим злочином. Наприклад, знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації задля ослаблення держави через несанкціоноване втручання, яке спричинило значну шкоду, є диверсією, і повинне кваліфікуватися лише за ст. 113 ККУ України, без додаткової кваліфікації за ч. 2 ст. 361 ККУ України. Кваліфі-

кація в таких випадках, крім злочину, ще й додатково способу його вчинення необґрунтована, оскільки в одних випадках учинення певних злочинів можливе лише певними способами, без цього способу не може бути цього злочину: шахрайства без обману, розбою без нападу тощо, а в інших – спосіб, який включив учинення окремого злочину, знову ж таки, був невід'ємною, органічною частиною об'єктивної сторони більш тяжкого злочину;

3) причетність до злочину із самим цим злочином, зокрема: приховування злочинцями вчинених ними злочинів (ст. 396 ККУ); неповідомлення співучасниками про вчинений злочин (ст. 383 ККУ); неповідомлення про злочин, як спосіб приховування злочину; придбання майна, завідомо здобутого злочином (ст. 198 ККУ), задля приховування злочину;

4) загальні (основні) та кваліфіковані склади злочину. Усякий кваліфікований вид складу злочину має перевагу (пріоритет) над загальним видом, а особливо кваліфікований – над кваліфікованим. При цьому в обвинуваченні враховуються всі ознаки вчиненого діяння – і основні, і кваліфікуючі, й особливо кваліфікуючі, – але кваліфікація відбувається лише за частиною, яка передбачає найбільш кваліфікований склад злочину;

5) загальна і спеціальна норми кримінального закону. За наявності у вчиненому діянні ознак обох норм застосуванню підлягає лише спеціальна норма.

У кримінальному праві та кримінально-правовій практиці розрізняють два види сукупності злочинів – реальну сукупність злочинів та ідеальну.

Реальною сукупністю злочинів називається вчинення різними, окремими самостійними діями двох або більше злочинів, передбачених різними кримінально-правовими нормами, за жоден із яких винний ще не був засуджений. Для реальної сукупності характерне різночасне вчинення злочинів. Але тривалість перерви між злочинами юридичного значення не має. Кваліфікація злочинів, що утворюють реальну сукупність, жодних особливостей не має.

Ідеальною сукупністю злочинів називається вчинення однією дією (бездіяльністю) двох або більше злочинів одночасно, одноразово. Класичним прикладом ідеальної сукупності є вчинення посадовою особою кількох злочинів лише одним словом або навіть одним кивком голови на знак згоди незаконно відпустити покупцям наркотичні засоби чи психотропні речовини завідомо для перепродажу за винагороду. Таке діяння кваліфікується як три злочини: за статтями 308, 364 та 368 ККУ.

Ідеальну сукупність злочинів, наприклад, утворюють: крадіжка, поєднана з несанкціонованим утручанням у роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ (ч. 1 ст. 185 і ч. 1 ст. 361 ККУ) або з несанкціонованими діями з інформацією, яка оброблюється в ЕОМ (комп'ютерів), АС, КМ чи МЕ (ч. 1 ст. 185 і ч. 1 ст. 362 ККУ); порушення недоторканності приватного життя, вчинене під час несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ (ч. 1 ст. 182 та ч. 1 ст. 361 ККУ); умисне масове поширення повідомлень електрозв'язку,

здійснене без попередньої згоди адресатів, що призвело до такого порушення роботи ЕОМ (комп'ютерів), АС, КМ чи МЕ, яке спричинило порушення таємниці кореспонденції, що передається через комп'ютер (ч. 1 ст. 363-1 і ч. 2 ст. 163 ККУ); зловживання повноваженнями службовою особою юридичної особи приватного права, поєднані з порушенням правил експлуатації ЕОМ (комп'ютерів), АС, КМ чи МЕ (статті 364-1 і 363 ККУ); втягнення неповнолітнього у злочинну діяльність, поєднане з погрозою вчинити вбивство (ст. 304 та ст. 129 ККУ).

Ідеальна сукупність злочинів відрізняється від одиничного злочину множиною об'єктів посягання (кількома), різними злочинними наслідками діяння, а в деяких випадках – і видами вини.

Найкоротший шлях вирішення дилеми кваліфікації – вчинене утворює один злочин чи воно є сукупністю кількох злочинів – обґрунтування з позиції об'єкта злочинного посягання: якщо вчинене є посяганням на різні безпосередні об'єкти кримінально-правової охорони, то його належить кваліфікувати як сукупність злочинів.

Відповідно до ст. 34 ККУ України рецидивом злочинів визнається вчинення нового умисного злочину особою, яка має судимість за умисний злочин. Рецидив злочинів є видом повторності злочинів, яка пов'язана із засудженням за попередній злочин, тому рецидиву притаманні ознаки повторності злочинів і такі ж правила кваліфікації.

3.5. Розмір НМДГ при кваліфікації кіберзлочинів

При кваліфікації кіберзлочинів для визначення розміру завданої шкоди застосовується поняття «неоподатковуваний мінімум доходів громадян».

Основні поняття

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією через передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Контрольні завдання

1. Сформулюйте кваліфікацію кіберзлочинів відповідно до Кримінального кодексу України.
2. Назвіть зміст та кваліфікацію незакінчених кіберзлочинів.
3. Назвіть кваліфікацію кіберзлочинів, учинених у співучасті.
4. Сформулюйте кваліфікацію множинних кіберзлочинів.
5. Назвіть розмір НМДГ при кваліфікації кіберзлочинів.

Розділ 4

Кваліфікація кіберзлочинів, які посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем

На сучасному етапі економічного розвитку України, коли управління інформацією стає функцією, критично важливою для бізнесу, а обсяги інформації невпинно зростають, усе гостріше стоїть питання інформаційної безпеки.

Сьогодні триває кібер-війна України з Росією, під час якої Україна перетворилась на тестовий полігон для російських хакерів. Щомісяця Україна піддається кібератакам 3000–3500 разів.

За останні 12 місяців кожна друга промислова компанія у світі пережила від одного до п'яти кібер-інцидентів. Втрати світової економіки в результаті кібер-атак становлять 445 000 000 000 USD. Збитки українського бізнесу, завдані кібер-атаками, складають 25 000 000 USD.

Домінуючою загрозою для промислових та критично важливих інфраструктур на сьогодні стало шкідливе програмне забезпечення (ШПЗ) – 53 % кібер-інцидентів пов'язані з ШПЗ, причому близько 36 % компаній піддавались таргетованим атакам.

Якщо підприємство працює з даними фізичних осіб, то кібер-атаки та крадіжка інформації – це фактори ризику, які завдають підприємству репутаційних та фінансових збитків.

При цьому 64 % підприємств не використовують спеціальних програм збору та аналізу інформації про кіберзагрози, обмежуються несистемними заходами в цій галузі. 86 % підприємств визнають, що їхня політика кібербезпеки не відповідає повною мірою потребам організації.

Основними причинами, які перешкоджають підвищенню кібербезпеки підприємств, є: недостатнє фінансування; нестача або відсутність кваліфікованих кадрів; нестача розуміння або підтримки з боку керівництва організації.

Отже, наразі *актуальною проблемою* при використанні комп'ютерних систем (КС) є надійний захист інформації від кібер-загроз і ШПЗ.

Відомі на сьогодні методи та системи виявлення кібер-загроз та шкідливого ПЗ неспроможні здійснювати достовірний та ефективний захист КС через недосконаліть методів, покладених в їх основу, та зростання кількості нових кібер-загроз та шкідливого ПЗ (кожні 4 секунди у світі з'являється нове, невідоме шкідливе ПЗ). Сучасні антивірусні засоби виявляють лише 46 % ШПЗ.

Для підвищення достовірності виявлення кіберзагроз та ШПЗ у комп'ютерних системах було розроблено інтелектуальну систему виявлення кіберзагроз та шкідливого ПЗ, яка складається з

– підсистеми діагностування КС на наявність троянських програм;

– підсистеми виявлення бот-мереж на основі аналізу DNS-трафіка.

Розроблена інтелектуальна система виявлення кібер-загроз та шкідливого ПЗ надає такі переваги:

– підвищує достовірність та ефективність виявлення кібер-загроз та ШПЗ, зменшуючи рівень хибних спрацювань та обчислювальну складність процесу виявлення;

– підвищує ефективність діагностування комп'ютерних систем на наявність нових троянських програм;

– підвищує достовірність виявлення ботів відомих та невідомих ботмереж на 8–22 % порівняно з відомими засобами виявлення бот-мереж;

– підвищує достовірність виявлення метаморфних вірусів на 7–14 %.

Розроблена інтелектуальна система може бути використана в державних установах, військових формуваннях та правоохоронних органах (зокрема в кіберполіції), оскільки вона спрямована на гарантування національної безпеки України в частині підвищення її кібербезпеки. При використанні в комерційних організаціях представлена система дає змогу захистити КС підприємства від кібер-загроз та шкідливого ПЗ.

4.1. Загальні питання кваліфікації кіберзлочинів, що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем

Назва цього виду кіберзлочинів взята з Конвенції, але вона не випадкова і засновується на трьох властивостях необхідним чином захищеної інформації:

– конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;

– цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

– доступність – властивість інформації бути захищеною від несанкціонованого блокування.

Отже, з огляду на це, до кіберзлочинів, що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем відповідно до ККУ належать злочини, передбачені Розділом 16 – «Злочини у сфері використання ЕОМ (комп'ютерів), АС та КМ і МЕ». На особливостях їх кваліфікації ми і зупинимося в цій темі. Також у другому питанні цієї лекції наведено інформацію щодо всіх ознак складів злочинів, передбачених цим розділом ККУ, яку, звичайно, слід знати і до якої слід звертатися при ознайомленні з основним матеріалом та в подальшому для ефективної кваліфікації цих злочинів.

Крім того, запам'ятайте: якщо ви побачите поняття чи терміни, які використовуються в статтях (їх частинах) Розділу 16 ОЧ ККУ, в статях інших розділів (наприклад ст. 158 ККУ), то ці, інші статті слід вважати спеціальними до статей Розділу 16, а вказані поняття та терміни слід розуміти так само, як і в загальних статтях.

Переважна більшість складів злочинів у сфері використання ЕОМ (комп'ютерів), АС та КМ і МЕ є матеріальними, а тому виявляються за наслідками. Тому під час кваліфікації цих злочинів та їх відмежуванні від суміжних складів злочинів потрібно

оцінювати розмір та характеристику заподіяної шкоди з точки зору предмета злочинів у цій сфері.

Так, предметом більшості злочинів у сфері використання ЕОМ (комп'ютерів), АС та КМ і МЕ є комп'ютерна інформація або комп'ютерна система (яку слід розуміти як будь-яку із систем: ЕОМ (комп'ютер), АС, КМ чи МЕ). Саме злочинний вплив на ці предмети або їх злочинне використання надає підстави визначити наявність об'єкта цих злочинів, тому що вони є невід'ємною частиною охоронюваних розглядуваними нормами суспільних відносин.

Результати злочинного впливу на комп'ютерну інформацію чи комп'ютерну систему слід оцінювати в тісному зв'язку з ознаками об'єктивної сторони, що належать до наслідків злочину (витік, втрата, підробка, блокування комп'ютерної інформації, порушення встановленого порядку її маршрутизації (ст. 361), зміна, знищення, блокування комп'ютерної інформації (ст. 362) тощо.

Зокрема, на практиці трапляються випадки кваліфікації внесення до комп'ютерної системи неправдивої інформації особою, яка має права доступу до неї, за ст. 362 ККУ України як несанкціонованої зміни інформації (наприклад при внесенні нотаріусом у реєстр даних про незаконно оформлену довіреність). У цьому разі фактично відбулося створення інформації в системі, а тому така кваліфікація помилкова.

На таких випадках слід зупинитися окремо, оскільки фактично вони не підпадають не під одну зі статей Розділу 16 ОЧ ККУ. Іноді суди кваліфі-

кують такі діяння як втручання в систему – за ст. 361 ККУ. Але несанкціоноване втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж розуміють як проникнення до цих машин, їх систем чи мереж і учинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі, або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а так само вплив на роботу ЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини, тобто ці дії повинні мати деструктивний характер.

У цьому разі особа не вчиняє таких дій – вона створює інформацію, тобто її поведінка не може бути оцінена за ст. 361 ККУ. І як ми вже вказали вище, інформація не змінюється, не знищується і не блокується, тобто неможлива кваліфікація і за ст. 362 ККУ.

Подібні дії, які фактично не містять указаних у статтях 361–363-1 ККУ наслідків для системи та комп'ютерної інформації, слід розцінювати як спосіб учинення іншого злочину і кваліфікувати їх за відповідними статтями інших розділів ККУ за наявності ознак складу злочину, наприклад за ч. 3 ст. 190, якщо шляхом такого внесення в систему завідомо неправдивої інформації вчинено заволодіння чужим майном.

При кваліфікації комп'ютерного злочину в будь-якому разі слід оцінювати розмір завданої шкоди, тому що це має критичне значення для наявності конкретного складу злочину. Зокрема, злочин, передбачений ст. 363 ККУ, вважається за-

кінченим, лише якщо заподіяно значну шкоду, а при наявності такого розміру шкоди при вчиненні злочину, передбаченого ст. 361 ККУ, кваліфікацію слід проводити за ч. 2 цієї статті. При цьому слід пам'ятати, що шкода у статтях 361–363-1 ККУ може полягати в заподіянні матеріальних збитків, які зазвичай є позитивними (позитивна майнова шкода), які оцінюються, виходячи з витрат власника на придбання комп'ютерної інформації, пропорційно зниженню цієї вартості, спричиненої злочином, або виходячи з вартості компонентів комп'ютерної системи (програмних чи технічних), які зазнали негативного злочинного впливу, або відповідно до витрат на відновлення комп'ютерної інформації чи компонентів комп'ютерної системи тощо, тобто це прямі збитки для потерпілого, підтверджені певними документами. Крім того, збитки від такого злочину можуть мати непряме вираження (опосередковане тощо) – в упущеній вигоді, наприклад в укладанні невигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в нематеріальних видах шкоди, що зумовлено використанням ЕОМ, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та керування ними. Така шкода може виражатися в порушенні нормальної роботи підприємств (установ чи організацій), зупиненні або порушенні складних технологічних процесів, погіршенні обороноздатності держави, підрив авторитету державних органів,

підприємств, установ або організацій, створенні загрози або заподіяння шкоди життю та здоров'ю громадян, порушенні безпеки руху транспорту тощо. Так, у практиці правоохоронних органів можуть виникати випадки, коли внаслідок незаконного втручання в роботу автоматизованих систем управління порушувався виробничий процес, створювалася загроза життю багатьох осіб.

Слід зауважити: визначити вичерпний перелік можливих наслідків злочину у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку надзвичайно важко, оскільки в кожному випадку ці наслідки залежать насамперед від змісту комп'ютерної інформації, яка зазнала шкоди. Характер шкоди в кожному конкретному злочині, зазвичай, залежить від тих суспільних відносини, які виступають додатковим об'єктом. Це можуть бути відносини в різних сферах життєдіяльності людини, пов'язані з використанням ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку. Перешкоджаючи інформаційним відносинам, злочинець завдає або загрожує завдати шкоди тим суспільним відносинам, для інтенсифікації яких застосовуються комп'ютерні технології. Отже, велике значення для кваліфікації має визначення додаткового обов'язкового або факультативного об'єкта злочину та шкоди, яку він зазнав.

До того ж визначення шкоди від злочину у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, особливо непрямої та нематеріальної, утворює велику складність на практиці. Суд досить рідко приймає

до уваги розмір шкоди, який не підтверджено документально, не обраховано обґрунтованими методиками, які на даний час для обчислення вартості втраченої комп'ютерної інформації, вартості робіт із відновлення роботи системи та іншої шкоди у сфері комп'ютерних технологій, відсутні. Тому розмір шкоди повинен бути підтверджений всіма можливими документами, що містять вартість, яку можна включити у вартість інформації (оплата роботи працівників, котрі створювали базу даних, вартість покупки частин бази даних для створення якісно нової бази даних тощо), або у втрати потерпілого від неробочої комп'ютерної системи (вартість робіт із відновлення, вартість необхідного для відновлення програмного та технічного забезпечення тощо).

Якщо ж предмет злочинного впливу не має необхідних ознак – інформація не представлена у вигляді, потрібному для її оброблення ЕОМ, чи інформаційна система не є комп'ютерною, – або шкода, яка їй завдана, не відповідає вказаній у відповідних нормах, або шкода цій інформації взагалі не завдана, хоча і були вчинені дії, які входять до об'єктивної сторони певного складу злочину, то не може йтися про злочин у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Якщо ж виявлені наслідки мають необхідні ознаки, то слід здійснити оцінку, розмежувати склади злочинів за такою ознакою об'єктивної сторони як діяння (дія або бездіяльність). Характер діянь, які вчинюються у сфері використання ЕОМ

(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку дає змогу виокремити щонайменше чотири моделі злочинного посягання на конфіденційність, цілісність та доступність комп'ютерних систем та даних:

1. Якщо наслідки спричинені діями особи, яка не мала права доступу до комп'ютерної інформації, – ці дії мають явні ознаки несанкціонованого втручання в систему, зокрема здійснені в порушення порядку доступу до інформації або з подоланням засобів захисту інформації тощо. У такому разі ці дії слід кваліфікувати за ст. 361 ККУ.

2. Якщо наслідки спричинені діями особи, яка мала право доступу до комп'ютерної інформації, але не мала права вчиняти з нею певні дії – змінювати, знищувати, блокувати, перехоплювати або копіювати її. Такі дії слід кваліфікувати за ст. 362 ККУ.

3. Якщо наслідки спричинені діями (бездіяльністю) особи, яка відповідає за експлуатацію ЕОМ (комп'ютерів), АС, КМ чи МЕ. Ці дії чи бездіяльність вчинені в порушення правил експлуатації або порядку чи правил захисту інформації, яка в них обробляється. У такому разі подія повинна отримати кримінально-правову оцінку за ст. 363 ККУ.

4. Якщо наслідки спричинені будь-якою особою через масове поширення повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів. Очевидно, що такі дії слід кваліфікувати за ст. 363-1 ККУ.

Злочини, склади яких належать до формальних (статті 361-1 та 361-2 ККУ), найчастіше виявляються в ході розслідування інших злочинів,

або через отримання правоохоронними органами інформації від заявників, які не є потерпілими від злочину, або з інших джерел.

У такому разі для отримання підтвердження ознак певного виду злочину слід провести слідчі (розшукові) дії (огляд, обшук), у необхідних випадках – негласні (контроль за вчиненням злочину). Під час їх здійснення потрібно оцінити дії запідозреної особи або їх результати на предмет наявності в них ознак об'єктивної сторони певного злочину (збут, поширення шкідливих програмних чи технічних засобів або ІОД). Крім того, слід звернути увагу і на виявлення необхідних ознак названих предметів цих злочинів.

Звичайно, кваліфікація діяння не повинна на цьому закінчуватися, адже фактично були оцінені тільки об'єкт та об'єктивний бік складу злочину. Велика увага повинна приділятися оцінці ознак суб'єкта та суб'єктивного боку складу злочину, оскільки їх невідповідність вимогам ККУ виключає кримінальну відповідальність.

Оцінка ознак суб'єкта злочину в сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку набуває великого значення також тому, що на поточному етапі проникнення комп'ютерних технологій у життя суспільства більшість їх користувачів неповнолітні, точніше, такими, що не досягли віку, з якого може наставати кримінальна відповідальність. Отже, слід чітко встановити, що підозрюваний досяг 16-річного віку.

У випадках наявності ознак спеціального суб'єкта (статті 362 та 363 ККУ) їх потрібно встановити та оцінити.

Слід мати на увазі, що останнім часом учені визнають наявність нових видів психічних хвороб, пов'язаних із використанням комп'ютерних технологій. Отже, слід приділити окрему увагу поведінці підозрюваного в ході слідства та відображенням її в слідах вчиненого діяння для оцінки осудності цієї особи.

При оцінці суб'єктивної сторони злочину у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку здебільшого (статті 361, 361-1, 361-2, 362, 363-1 ККУ) потрібно встановити ознаки вини у формі умислу в діях чи бездіяльності особи. Однак при цьому слід обмежуватися лише вказаною частиною об'єктивної сторони, адже щодо наслідків цих злочинів може бути й необережна форма вини (матеріальні склади цих злочинів можуть характеризуватися змішаною формою вини). Це стосується тільки тих злочинів, склади яких окремо передбачають діяння та наслідки (статті 361, 363-1 ККУ). Щодо складу злочину об'єктивна сторона якого описана за допомогою формулювань, які містять і діяння, і наслідки (ст. 362 ККУ): зміна, знищення або блокування інформації, – форма вини щодо обох цих ознак об'єктивної сторони повинна бути умисною.

Інша ситуація стосується складу злочину, передбаченого ст. 363 ККУ: він може характеризуватися умисною або необережною формою вини щодо діяння, щодо наслідків завжди має місце необережність. В іншому разі такі дії, за наявності

необхідних ознак, можуть кваліфікуватися за статтями 361 чи 362 ККУ.

У ході оцінки суб'єктивної сторони злочинів, передбачених статтями 361 та 362 ККУ, слід приділяти окрему увагу завідомості – усвідомленню запідозреною особою несанкціонованості її дій. Оскільки ознаки відсутності в неї такого усвідомлення або відсутність ознак того, що вона мала таке усвідомлення (відсутність підпису про інструктаж, відсутність будь-яких інструкцій з боку власника системи чи інформації тощо), зумовлює і відсутність відповідної форми вини цієї особи – умислу.

Склад злочину ст. 361-1 ККУ містить як обов'язкову ознаку суб'єктивної сторони мету вчинення злочину: використання, збут чи розповсюдження предметів злочину. Ця ознака повинна оцінюватися в тісному зв'язку з діянням, яке входить до об'єктивної сторони складу цього злочину – створенням шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ.

У разі посягання під час вчинення злочину й на інші суспільні відносини (крім родового об'єкту Розділу XVI ККУ), тобто за наявності ознак сукупності злочинів, слід ураховувати таке. За загальним правилом ідеальна сукупність злочинів відсутня, якщо вчиненим діянням виконуються злочини, які обов'язкові (конститутивними) ознаки посягання, передбаченого однією статтею ОЧ КК. Слід мати на увазі те, що інформаційні процеси пронизують усі суспільні відносини, і часто діяння, яке передбачено статтею Розділу XVI ККУ, є способом учинення іншого, більш тяжкого злочину, а

тому в деяких літературних джерелах містяться рекомендації, що в такому разі не слід кваліфікувати вчинене за сукупністю злочинів. Наприклад, знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації задля ослаблення держави через несанкціоноване втручання, яке спричинило істотну шкоду, розглядається тільки як диверсія і кваліфікується лише за ст. 113 ККУ, без додаткової кваліфікації за ч. 2 ст. 361 ККУ.

Законодавець навіть закріплює таке бачення в ч. 3 ст. 190 ККУ, передбачивши шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. У цьому разі значення має спрямованість умислу винної особи: особа, маючи умисел на заволодіння чужим майном, наприклад, вносить зміни у базу даних комерційного банку щодо розміру депозитного вкладу чи кредиту тощо, а працівник банку на підставі цих даних видає гроші. При цьому незаконні операції з використанням електронно-обчислювальної техніки повністю поглинаються обманом як способом шахрайства. Але законодавець виділив в окремій спеціальній нормі такі випадки, як такі, що мають підвищену суспільну небезпечність та поширеність.

Проте інші випадки закріплення не отримали, і практика іде все ж таки іншим шляхом, оскільки обґрунтувати відсутність потреби додаткової кваліфікації набагато складніше, ніж її присутність, адже в таких випадках ознаки злочину, передбаченого статтею Розділу XVI ККУ, явно присутні поряд з ознаками іншого діяння.

А тому до чітко виражених рекомендацій вищих судових інстанцій, заснованих на узагальненні судової практики, слід дотримуватись такого правила: в цих та інших випадках, коли своїми діями чи бездіяльністю особа порушила інформаційні відносини, забезпечені комп'ютерними технологіями, та будь-які інші суспільні відносини, кваліфікація повинна відбуватися за правилами сукупності злочинів.

У ході оцінки події, яка не містить достатніх ознак складу злочину, хоч в ній і фігурували ЕОМ (комп'ютер), система, комп'ютерна мережа або мережа електрозв'язку, слід мати на увазі, що вона може бути кваліфікована як незакінчений злочин або співучасть у злочині. Зокрема, досить поширені зараз діяння, передбачені ст. 6 Конвенції про кіберзлочинність, можуть бути кваліфіковані так: умисний продаж, поширення або надання для використання в інший спосіб комп'ютерних паролів, кодів доступу або подібних даних з метою подальшого вчинення злочинів, передбачених статтями Розділу XVI ККУ, є пособництвом у вчиненні відповідних злочинів (потрібно додатково посилатися на ч. 5 ст. 27 ККУ); володіння шкідливими засобами задля подальшого вчинення злочинів треба, відповідно до національного законодавства, вважати готуванням до відповідних злочинів (додаткове посилання на ч. 1 ст. 14 ККУ).

Отже, використовуючи особливості складів комп'ютерних злочинів, у ході їх кваліфікації слід дотримуватися певних правил:

1) кваліфікацію комп'ютерних злочинів, склади яких є матеріальними, слід розпочинати з оцінки їх наслідків щодо предмета злочину, далі оцінити причинно-наслідковий зв'язок із діяннями винної особи та ознаки цієї особи, і залежно від цього обрати відповідну статтю;

2) кваліфікацію комп'ютерних злочинів, склади яких є формальними, слід розпочинати із установлення відповідних ознак діяння та предмета злочину;

3) незалежно від складу злочину слід оцінити суб'єктивні ознаки з огляду на знижений вік комп'ютерних користувачів та вплив комп'ютерних технологій на психіку людини;

4) при оцінці сукупності злочинів звернути увагу на велику ймовірність входження діяння, яке містить ознаки комп'ютерного злочину, до самостійного складу іншого злочину;

5) при оцінці діянь у комп'ютерній сфері, які прямо не передбачені ККУ, потрібно спробувати застосувати до них правила кваліфікації незакінченого злочину або співучасті в злочині.

4.2. Спеціальні питання кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

4.2.1. Загальна характеристика Розділу XVI ККУ

Родовим об'єктом злочинів, передбачених у Розділі XVI КК «Злочини у сфері використання

електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», є *інформаційні процеси суспільних відносин, засобом забезпечення яких є інформаційно-телекомунікаційні системи (ІТС).*

Основним *безпосереднім об'єктом* цих злочинів виступають окремі аспекти інформаційних процесів суспільних відносин, зокрема пов'язані із забезпеченням конфіденційності, цілісності та доступності інформації, її оброблення та передачі (ст. 361 ККУ), порядок створення та обігу програмних та технічних засобів (ст. 361-1 ККУ), порядок доступу до інформації в ІТС (ст. 361-2 ККУ), порядок розділення доступу до інформації та її оброблення в ІТС (ст. 362 КК), безпека використання ІТС, а також порядок та правила захисту комп'ютерної інформації чи інформації в мережах електрозв'язку (ст. 363 КК). В окремих складах злочинів факультативним *додатковим об'єктом* є відносини, пов'язані з правом власності на інформацію (статті 362, 361-2, 363 ККУ) або правом власності на ІТС (ст. 363 ККУ).

Предмети злочинів можна згрупувати так:

– інформація – КІ та інформація МЕ (ст. 361 ККУ), ІОД, яка зберігається в ІТС або на носіях такої інформації, створена та захищена відповідно до чинного законодавства (ст. 361-2 ККУ), інформація, яка опрацьовується в ІТС або зберігається на носіях такої інформації (ст. 362 ККУ);

– шкідливі програмні та технічні засоби (ст. 361-1 ККУ);

– повідомлення електрозв'язку (ст. 363-1 ККУ).

З *об'єктивного боку* більшість злочинів у сфері використання ІТС вчиняються через дії. Виключення становить порушення правил експлуатації ІТС, а також порушення порядку чи правил захисту інформації (ст. 363 ККУ), які можуть бути вчинені і через дії, і шляхом бездіяльності.

За конструкцією *об'єктивного боку* розглядувані злочини в основному є злочинами з *матеріальним складом*. Тобто закінченими вони вважаються з моменту настання суспільно небезпечних наслідків, зокрема: витоку, втрати, підробки, блокування інформації, спотворення процесу оброблення інформації, порушення встановленого порядку маршрутизації інформації (ст. 361 ККУ) або порушення чи припинення роботи ІТС (ст. 363-1 ККУ).

Злочини, передбачені ч. 1 ст. 361-1 та ст. 361-2 ККУ, належать до злочинів із *формальним* складом, тобто вважаються закінченими з моменту вчинення діянь, зазначених у диспозиції.

Із *суб'єктивного боку* щодо діяння необхідна наявність умислу у всіх складах злочинів, за винятком ст. 363, де можливе і умисне, і необережне винне ставлення до діяння. У складах, де передбачені наслідки, до них можливе і умисне, і необережне ставлення, за винятком, знову ж таки, ст. 363, де можливе *тільки* необережне винне ставлення до наслідків. Тобто у всіх складах злочинів, де передбачені наслідки, можлива *змішана форма вини* – умисел щодо діяння та необережність щодо наслідків.

Суб'єкт злочинів, передбачених статтями 361, 361-1, 361-2, 363-1 ККУ – загальний, тобто фізична, осудна особа, яка на момент вчинення злочину досягла 16 років. Суб'єкт злочинів, передбачених статтями 362, 363 ККУ, спеціальний – особа, яка має право доступу до інформації (ст. 362 ККУ) або особа, яка відповідає за експлуатацію ІТС чи системи захисту інформації (ст. 363 КК).

Статті 361–362 та 363-1 ККУ містять такі спільні *кваліфікуючі ознаки*:

– вчинення комп'ютерного злочину повторно;

– вчинення комп'ютерного злочину за попередньою змовою групою осіб;

– вчинення комп'ютерного злочину, який заподіяв значну шкоду.

Значною шкодою в статтях 361–363-1 ККУ, якщо вона полягає в заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує НМДГ (примітка до ст. 361 ККУ).

4.2.2. Несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 ККУ)

Безпосереднім об'єктом несанкціонованого втручання в роботу ІТС є інформаційні суспільні відносини, у яких забезпечені конфіденційність, цілісність та доступність інформації, а також нормальний процес її оброблення та передачі.

Інформація як *предмет злочину*, передбаченого ст. 361 ККУ, включає комп'ютерну інформацію та інформацію мереж електрозв'язку.

Комп'ютерна інформація включає сукупність програм та даних в ІТС.

Програма – це набір інструкцій у вигляді слів, цифр, кодів, схем, символів або в 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 і системну, і прикладну програму, виражену в початковому, проміжному або об'єктному коді.

Дані – відомості у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб, які існують у формі, придатній для автоматизованої обробки засобами обчислювальної техніки.

Інформація мереж електрозв'язку – знаки, сигнали, письмовий текст, зображення та звуки або повідомлення будь-якого роду, які передаються, випромінюються та/або приймаються по радіо, проводових, оптичних або інших електромагнітних системах.

Об'єктивний бік: діяння – несанкціоноване втручання в роботу ІТС; *суспільно небезпечні наслідки* – витік, втрата, підроблення, блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку маршрутизації інформації (перелічені наслідки є альтернативними, тобто для наявності складу злочину достатньо настання хоча б одного з наслідків); *причинний зв'язок* між діянням та наслідками.

Несанкціоноване втручання в роботу ІТС – здійснена поза дозволом (санкцією) власника ком-

п'ютерної системи чи інформації в ній, зміна нормального режиму роботи ІТС, вчинена через вплив на її програмні чи технічні засоби у будь-якому вигляді (програмному, технічному, механічному тощо). Фактично про *несанкціонованість* таких дій свідчить наявність порушення встановленого власником розмежування доступу до системи: або взагалі відсутність прав доступу, або вихід за їх межі.

Наслідки несанкціонованого втручання в роботу ІТС:

1) *виток інформації* – ознайомлення чи отримання доступу до неї фізичних та/або юридичних осіб, які не мають права доступу;

2) *втрата інформації* – зникнення інформації в системі або її руйнування до втрати змісту;

3) *підроблення інформації* – цілеспрямована зміна змісту інформації;

4) *блокування інформації* – унеможливлення доступу до інформації;

5) *спотворення процесу обробки інформації* – порушення 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;

6) *порушення встановленого порядку маршрутизації інформації* – зміна правил вибору її маршруту(ів) в телекомунікаційних системах.

Злочин буде закінченим із моменту настання вказаних суспільно небезпечних наслідків у причинному зв'язку з діянням.

Суб'єктивний бік виражається у вигляді прямого або непрямого умислу.

Суб'єкт несанкціонованого втручання – загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Кваліфікуючими ознаками злочину (ч. 2 ст. 361 ККУ) є дії, передбачені частиною першою цієї статті, вчинені: 1) повторно; 2) за попередньою змовою групою осіб; 3) якщо вони заподіяли значну шкоду.

2.3. Незаконні дії зі шкідливими програмними або технічними засобами (ст. 361-1 ККУ)

Безпосередній об'єкт злочину, передбаченого ст. 361-1 ККУ, складає порядок створення та обігу програмних та технічних засобів, який забезпечує дотримання вимог конфіденційності, цілісності та доступності інформації в ІТС.

Предмети злочину:

– шкідливі програмні засоби (ШПЗ);

– шкідливі технічні засоби (ШТЗ).

Під *ШПЗ* слід розуміти програми (програмні блоки, програмне забезпечення), розроблені спеціально *для несанкціонованого втручання в роботу ІТС*, використання яких спричиняє або створює загрозу заподіяння шкоди конфіденційності, цілісності та доступності інформації в цій системі.

ШТЗ – це різного роду пристрої, устаткування, розроблені *для несанкціонованого втручання в роботу ІТС*, використання яких спричиняє або створює загрозу заподіяння шкоди конфіденцій-

ності, цілісності та доступності інформації в цій системі.

ШПЗ можна класифікувати на основі таких підстав:

1. За функцією саморозповсюдження:

1.1. Програми, що саморозповсюджуються, тобто такі, які мають в алгоритмі функцію, що дає змогу їм, незалежно від дій користувача, створювати свої копії (розмножуватися) і розповсюджуватися, тобто упроваджувати свої копії у файли, системні області носіїв інформації, зокрема в оперативну пам'ять тощо. Копії шкідливої програми можуть не збігатися за точністю з оригіналом, проте зберігають всі або велику частину введених в їх алгоритм функцій, включаючи функцію саморозповсюдження. До числа таких програм належать:

а) комп'ютерний вірус – шкідлива програма, що саморозповсюджується через включення свого програмного коду або деякої його частини в програмний код файлів, системні області або інший робочий простір носіїв інформації в ІТС;

б) комп'ютерний черв'як – шкідлива програма, що саморозповсюджується шляхом перенесення свого програмного коду або деякої його частини по мережі (телекомунікаційній системі).

Основна відмінність комп'ютерного черв'яка від вірусу полягає в механізмі його саморозповсюдження.

1.2. Програмні закладки – програми, не здатні до саморозповсюдження. Відсутність механізму саморозповсюдження – основна їх відмінна ознака, в іншому – вони можуть бути наділені аналогіч-

ними шкідливими функціями програм, що саморозповсюджуються. Їх можна умовно розділити на п'ять груп:

а) програмні закладки, які здійснюють збір інформації про інформаційні процеси, що протікають в ІТС;

б) програмні закладки, що забезпечують порушення порядку доступу до інформації в системі;

в) програмні закладки, що порушують або припиняють роботу програмних чи технічних засобів ІТС;

г) програмні закладки, що наділені деструктивними функціями;

ґ) комбіновані програмні закладки.

2. За наявністю недекларованих функцій:

2.1. Троянська програма – шкідлива програма, яка, крім прихованих шкідливих функцій, закладених в її алгоритм і здійснюваних відповідно до наперед визначених умов, має і відкрито декларовані функції, не пов'язані зі шкідливою дією.

2.2. Приховані шкідливі програми відрізняються від троянських програм відсутністю в них відкрито декларованих функцій. Зазвичай, про наявність, запуск і функціонування прихованої шкідливої програми користувачу невідомо.

3. За об'єктом шкідливого впливу:

3.1. На загальну працездатність ІТС.

3.2. На окремі програмні чи технічні засоби ІТС.

3.3. На конфіденційність, цілісність та доступність інформації.

3.4. На декілька об'єктів (комбіновані). Наприклад, вплив на носій інформації як на програмно-

технічний засіб задля порушення доступності інформації.

Об'єктивна сторона. Злочин, передбачений ч. 1 ст. 361-1 ККУ, належить до злочинів із *формальним* складом, тобто вважається закінченим із моменту вчинення одного з альтернативних діянь, зазначених у диспозиції. Розглядувана норма передбачає такі форми об'єктивного боку:

1) створення шкідливих програмних або технічних засобів задля використання, розповсюдження або збуту;

2) розповсюдження шкідливих програмних або технічних засобів;

3) збут шкідливих програмних або технічних засобів.

Створення ШПЗ або ШТЗ є творчою діяльністю, унаслідок якої отримується якісно нова програма або технічний засіб, що явно наділяються функціями, виконання яких може заподіювати шкоду конфіденційності, цілісності та доступності інформації в ІТС. Слід звернути увагу, що створення буде кримінально караним тільки за наявності відповідної ознаки суб'єктивної сторони – мети подальшого використання, розповсюдження або збуту.

Розповсюдження ШПЗ – це оплатне або безоплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а рівно їх «закладання» в програмне забезпечення, поширення за допомогою телекомунікаційних мереж чи через самовідтворення.

Розповсюдженням ШТЗ є дії, спрямовані на поширення використання цього засобу та його подальший збут, які можуть бути вчинені в будь-який спосіб (реклама, пропозиції придбати, показ його роботи, опублікування технічної документації, надання в пробне використання, підключення до технічних засобів інформаційно-телекомунікаційних систем за проханням іншої особи тощо), і стосовно однієї особи, і будь-якої кількості людей – і за платню, і безкоштовно.

Збут ШПЗ або ШТЗ – це їх оплатне або безоплатне відчуження, тобто повний перехід цього засобу у власність іншої особи.

Розповсюдження та збут ШТЗ чітко розрізняються. Розповсюдження ж ШПЗ відрізняється від їхнього збуту тим, що воно містить певні зусилля винної особи щодо якомога більшого розширення кола осіб, які мають можливість отримати цей засіб (викладення ШПЗ на мережевий ресурс, доступ до якого може відкриватися після оплати певної суми грошей, або бути відкритим; поштова розсилка з прикріпленим файлом або гіперпосиланням на нього тощо). Збут же характеризується певною обмеженістю за кількістю екземплярів ШПЗ та колом осіб, які їх отримали чи могли отримати (продаж дисків із записаними на них шкідливими програмами на одній торговій точці; передача програми знайомому).

Суб'єктивний бік характеризується виною у формі прямого умислу, при цьому свідомістю особи обов'язково охоплюється розуміння того, що створювані або розповсюджувані засоби спеціально

призначені для несанкціонованого втручання в роботу ІТС. Обов'язкова *мета* цього діяння – подальше використання, розповсюдження або збут ШПЗ чи ШТЗ.

Суб'єкт цього злочину – загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Кваліфікуючими ознаками злочину (ч. 2 ст. 361-1 ККУ) є дії, передбачені частиною першою цієї статті, вчинені: 1) повторно; 2) за попередньою змовою групою осіб; 3) якщо вони заподіяли значну шкоду.

4.2.4. Незаконні дії щодо інформації з обмеженим доступом (ст. 361-2 ККУ)

Основним безпосереднім об'єктом злочину виступає встановлений порядок доступу до інформації в ІТС. *Факультативним додатковим об'єктом* є відносини, пов'язані із правом власності на інформацію.

Предметом злочину є ІОД, яка зберігається в ІТС або на носіях такої інформації, створена та захищена відповідно до чинного законодавства. Така інформація може бути комп'ютерною або належить до мереж електрозв'язку і має додаткові ознаки:

– є *інформацією з обмеженим доступом*, до якої згідно зі ст. 30 Закону України «Про інформацію» належить таємна, конфіденційна та службова інформація;

– *зберігається в ІТС або на носіях такої інформації. Носій інформації* – фізичне тіло, яке

використовується під час запису для збереження в ньому або на його поверхні сигналів інформації, може бути вбудованою або знімною частиною технічного засобу;

– *створена відповідно до чинного законодавства*, тобто розповсюдження або збут такої інформації, якщо вона отримана з порушенням законодавства, не є злочином, передбаченим ст. 361-2 ККУ. Для встановлення цієї ознаки слід звернутися до відповідних нормативних актів;

– *захищена відповідно до чинного законодавства.* Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (далі – Закон) *інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом*, повинна оброблятися із застосуванням «комплексної системи захисту інформації з підтвердженою відповідністю» (ч. 2 ст. 8 Закону). В іншому разі «*умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації*» (ч. 1 ст. 8 Закону). Отже, склад злочину, передбачений цією статтею, буде мати місце тоді, коли в першому випадку будуть відповідні заходи захисту, а в другому – ці заходи будуть ужиті відповідно до договору. У разі ж відсутності будь-яких заходів захисту ця необхідна ознака предмета цього злочину відсутня, отже немає і складу злочину.

За конструкцією *об'єктивної сторони* злочин, передбачений ст. 361-2 ККУ, є формальним. Він вважається закінченим із моменту вчинення несанкціонованого збуту або несанкціонованого роз-

повсюдження комп'ютерної інформації з обмеженим доступом.

Збут або поширення інформації буде *несанкціонованим*, коли він вчиняється без дозволу її власника.

Поширення комп'ютерної інформації з обмеженим доступом являє собою оплатне або безоплатне надання її копій або доступу до неї невизначеному колу осіб.

Під *збутом комп'ютерної інформації з обмеженим доступом* потрібно розуміти її оплатне або безоплатне відчуження.

Суб'єктивний бік даного злочину характеризується виною у формі прямого умислу. Особа усвідомлює, що комп'ютерна інформація, яку вона збуває або поширює, є інформацією з обмеженим доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій.

Суб'єкт злочину – загальний.

Кваліфікуючими ознаками злочину (ч. 2 ст. 361-2 ККУ) є дії, передбачені ч. 1 цієї статті, вчинені: 1) повторно; 2) за попередньою змовою групою осіб; 3) якщо вони заподіяли значну шкоду.

4.2.5. Незаконні дії з комп'ютерною інформацією, учинені особою, яка має право доступу до неї (ст. 362 ККУ)

Основним безпосереднім об'єктом цього злочину виступає встановлений порядок розділення доступу до інформації та її оброблення в ІТС. *Факультативним додатковим об'єктом* є відносини права власності на інформацію.

Предметом злочину відповідно до диспозиції є інформація, яка оброблюється в ІТС або зберігається на її носіях. *Оброблення інформації в системі* – 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 (ст. 1 Закону).

Об'єктивний бік злочину, передбаченого ч. 1 ст. 362 ККУ, відповідає формальному складу та характеризується наявністю декількох форм діянь: 1) несанкціонована зміна інформації; 2) несанкціоноване знищення інформації; 3) несанкціоноване блокування інформації.

Несанкціонована зміна інформації являє собою здійснену із порушенням порядку доступу до інформації в системі модифікацію змісту відомостей, які в ній зберігаються чи оброблюються.

Несанкціоноване знищення інформації – дії, що провадяться з порушенням порядку доступу до інформації в системі, в результаті яких вона зникає в системі або руйнується настільки, що втрачає зміст.

Несанкціоноване блокування інформації – дії, що провадяться з порушенням порядку доступу до інформації в системі, в результаті яких унеможливлюється доступ до інформації в системі за умови, що її не змінено та не знищено.

Об'єктивна сторона злочину, передбаченого ч. 2 ст. 362 ККУ, відповідає матеріальному складу та включає:

1) діяння у двох формах: несанкціоноване перехоплення інформації та несанкціоноване копіювання інформації;

2) наслідки – виток інформації;

3) причинно-наслідковий зв'язок.

Несанкціоноване копіювання інформації – це відтворення її зі збереженням вихідної інформації, що провадиться з порушенням порядку доступу до цієї інформації. Наприклад, особа має право лише на ознайомлення з певною базою даних, а вона створює її копію.

Несанкціоноване перехоплення – це отримання з порушенням порядку доступу до інформації її копії за допомогою специфічних технічних засобів під час передавання цієї інформації від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або через оброблення електромагнітних випромінювань під час роботи інформаційно-телекомунікаційної системи, у якій оброблюється така інформація.

Виток інформації – ознайомлення чи отримання доступу до неї фізичних та/або юридичних осіб, які не мають права доступу.

Суб'єктивний бік цього злочину характеризується виною у виді прямого або непрямого умислу. При цьому особа має усвідомлювати, що вчиняє несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства (ст. 1 Закону).

Суб'єкт злочину, передбаченого ст. 362 ККУ, спеціальний – особа, яка має право доступу до комп'ютерної інформації. Відповідно до ст. 4

Закону: «Порядок доступу до інформації, перелік користувачів та їх повноваження щодо цієї інформації визначаються власником інформації. Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження щодо цієї інформації визначаються законодавством». Згідно зі ст. 5 Закону: «Власник системи забезпечує захист інформації (*в тому числі й порядок доступу до інформації*) в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом».

Отже, вказаний спеціальний статус особи встановлюється із затвердженням порядку її доступу до інформації в системі, який встановлюється законодавством або відповідним нормативним актом (наказом, розпорядженням тощо), виданим власником системи відповідно до договору із власником інформації.

Кваліфікуючими ознаками злочину (ч. 3 ст. 362 ККУ) є дії, передбачені частиною першою або другою цієї статті, вчинені: 1) повторно; 2) за попередньою змовою групою осіб; 3) якщо вони заподіяли значну шкоду.

4.2.6. Порушення правил експлуатації інформаційно-телекомунікаційних систем та порушення порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 ККУ)

Кримінальну відповідальність за порушення правил експлуатації ІТС, а також порушення по-

рядку чи правил захисту інформації встановлено в ст. 363 ККУ «Порушення правил експлуатації ЕОМ (комп'ютери), АС, КМ, МЕ або порядку чи правил захисту інформації, яка в них обробляється».

Основний безпосередній об'єкт злочину, передбаченого цією статтею, складають суспільні відносини, у межах яких гарантується безпека використання ІТС, а також дотримання порядку та правил захисту КІ чи інформації в МЕ. *Факультативним додатковим об'єктом* є відносини права власності на ІТС та на інформацію.

Склад злочину є *безпредметним*, тобто предмет не є обов'язковою його ознакою.

Диспозиція цієї статті є бланкетною, тобто містить терміни, роз'яснення яких слід шукати в інших нормативно-правових актах. *Правила експлуатації* ІТС є вимогами, що ставляться власниками систем до їх використання або обслуговування їх технічних і програмних засобів. Вони, зазвичай, містяться в окремих підзаконних актах (наказах, розпорядженнях).

Порядок захисту інформації – це визначені нормативно-правовими актами вимоги щодо створення та організації роботи системи захисту інформації, які забезпечують запобігання несанкціонованим діям щодо інформації в системі. *Правила захисту інформації*, своєю чергою, є вимогами щодо використання системи захисту інформації певного виду, які забезпечують її правильну роботу.

Підзаконні нормативно-правові акти, в яких затверджуються ці порядок та правила, видаються власником конкретної ІТС на підставі положень

закону або договору із власником інформації (статті 4, 5 Закону).

Об'єктивна сторона складу злочину, передбаченого цією статтею, характеризується такими ознаками:

1) діяння – порушення правил експлуатації ІТС або порядку чи правил захисту КІ в системі чи інформації в мережах електрозв'язку;

2) суспільно небезпечні наслідки – значна шкода;

3) причинний зв'язок між діянням і суспільно небезпечними наслідками.

Аналіз диспозиції дає підстави зробити висновок про те, що діяння може виявлятися у трьох альтернативних формах:

– порушення правил експлуатації ІТС;

– порушення порядку захисту інформації;

– порушення правил захисту інформації.

Порушення правил експлуатації ІТС – недотримання вимог, що ставляться її власником до їх використання або обслуговування. Таке порушення може полягати, наприклад, у спробі відповідальної особи встановити нове програмне або апаратне забезпечення без повідомлення власника системи, якщо такий обов'язок передбачений правилами, порушенні порядку включення або відключення засобів комп'ютерної техніки тощо.

Порушення порядку захисту інформації – недотримання визначених нормативними актами вимог щодо створення системи захисту інформації та організації її роботи. Прикладом такого діяння може бути надання відповідальною особою можливості користувачам використовувати комп'ютерну техні-

ку для роботи з таємною інформацією за відсутності сертифікованої належним чином системи захисту.

Порушення правил захисту інформації – недотримання вимог щодо використання системи захисту інформації певного виду. Це може бути, наприклад, неналежне зберігання паролів для доступу до інформації, підключенні комп'ютерної техніки до мережі без фільтрів (антивірусів, мережевих екранів, брандмауерів тощо), невчинення вчасно обновлення антивірусних баз, нереагування на повідомлення системи захисту про загрози безпеці, відсутність відповідних дій із боку відповідальної особи тощо.

Оскільки аналізований склад злочину матеріальний, він буде вважатися закінченим від моменту настання суспільно небезпечних наслідків – *значної шкоди* (примітка до ст. 361 ККУ).

Суб'єктивний бік цього злочину характеризується тим, що діяння може бути вчинене і умисно, і з необережності, а щодо наслідків завжди має бути необережність. Якщо настання наслідків охоплюється умислом винної особи, то склад злочину, передбачений ст. 363 ККУ, відсутній. У таких випадках дії винної особи, за наявності відповідних ознак, потрібно кваліфікувати як умисне пошкодження майна (ст. 194 ККУ), або як пособництво в несанкціонованому втручанні в роботу ІТС (ч. 5 ст. 27, ст. 361 ККУ), або як несанкціоновані дії з комп'ютерною інформацією, вчинені особою, що має доступ до неї (ст. 362 ККУ).

Суб'єкт злочину, передбаченого ст. 363 ККУ, спеціальний – особа, яка відповідає за експлуатацію ІТС чи на яку покладається забезпечення

захисту інформації та контролю за ним. Такий статус особи встановлюється відповідним наказом або розпорядженням власника системи та закріпленими на підставі цього наказу функціональними обов'язками, згідно із законодавством (у разі оброблення в системі інформації, яка є власністю держави, або ІОД, вимога щодо захисту якої встановлена законом) або договором із власником інформації (в інших випадках).

4.2.7. Масове поширення повідомлень електрозв'язку (ст. 363-1 ККУ)

Безпосередній об'єкт цього злочину складає процес оброблення інформації в ІТС, який включає 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.

Предметом цього злочину є повідомлення електрозв'язку (т. зв. «спам») – електронні, текстові та/або мультимедійні повідомлення, які без попередньої згоди (замовлення) споживача умисно масово надсилаються на його адресу електронної пошти або кінцеве обладнання абонента, крім повідомлень оператора, провайдера щодо надання послуг.

Оскільки склад злочину, передбачений ст. 363-1 ККУ, є *матеріальним*, до ознак його *об'єктивного боку* належать: 1) діяння – масове поширення повідомлень електрозв'язку, здійснене без попередньої згоди адресатів; 2) суспільно небезпечні

наслідки – порушення або припинення роботи ІТС; 3) причинний зв'язок між діянням та наслідками.

Розповсюдження повідомлень електрозв'язку полягає в направленні певним адресатам копій даних повідомлень, яке, по-перше, є масовим і, по-друге, здійснюється без попередньої згоди адресатів.

Розповсюдження слід вважати *масовим* тоді, коли одне або кілька повідомлень отримує більше, ніж один адресат, адже в диспозиції аналізованої статті йдеться про множинність повідомлень електрозв'язку та їх адресатів. Зазначимо: поняття «масове» в цій нормі використовується як оцінне, тобто встановлення того, чи було певне розповсюдження повідомлень електрозв'язку масовим, залежить від аналізу багатьох обставин конкретного розповсюдження (кількість повідомлень або копій повідомлень, їх розмір; кількість адресатів; час, що було використано для розповсюдження; технічні характеристики обладнання, яке використовувалося для розповсюдження, тощо).

Відсутність попередньої згоди адресатів полягає в тому, що адресат ні в якій формі (письмово, усно, через використання електронної пошти або в інший спосіб) не давав згоди на надсилання йому повідомлень, що є предметом злочину.

Порушення роботи ІТС являє собою таку зміну режиму її роботи, яка створює загрозу для її функціонування, тобто погіршення роботи повністю або частково, тимчасове створення перешкод для використання за призначенням – для оброблення інформації. Може виражатися в уповільненні виконання стандартних операцій, затратах

часу для оброблення інформації, яка не є цільовою для даної системи тощо.

Припинення роботи ІТС полягає в тимчасовому або остаточному припиненні її функціонування, невиконанні її засобами завдань щодо оброблення інформації. Наприклад, відмова в обслуговуванні користувача поштовою програмою через переповнення об'єму поштової скриньки повідомленнями електрозв'язку.

Суб'єктивний бік характеризується виною у формі прямого умислу стосовно діяння й умисним або необережним ставленням до наслідків.

Суб'єкт даного злочину загальний.

Кваліфікуючими ознаками злочину (ч. 2 ст. 363-1 ККУ) є дії, передбачені частиною першою цієї статті, вчинені: 1) повторно; 2) за попередньою змовою групою осіб.

Основні поняття

Порушення порядку захисту інформації – недотримання визначених нормативними актами вимог щодо створення системи захисту інформації та організації її роботи.

Порушення правил захисту інформації – недотримання вимог щодо використання системи захисту інформації певного виду.

Контрольні завдання

1. Назвіть загальні питання кваліфікації кіберзлочинів, що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем.

2. Сформулюйте спеціальні питання кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

3. Назвіть загальні характеристики Розділу XVI ККУ.

Розділ 5

Кваліфікація злочинів, пов'язаних із комп'ютерами

5.1. Загальні особливості кваліфікації злочинів, пов'язаних із комп'ютерами

До цієї групи кіберзлочинів відповідно до Конвенції належать два правопорушення: підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8). При цьому шахрайство пов'язане із заволодінням чужим майном, підроблення – із незаконним здійсненням інших юридично значимих дій.

ККУ містить декілька статей, які передбачають відповідальність за підроблення різних предметів (зокрема, статті 199, 200, 358, 361, 362), а також за шахрайство (ст. 190). Проте за значенням підроблення відповідно до Конвенції вона стосується саме комп'ютерної інформації, яка є предметом лише двох статей із наведеного переліку – статті 361, 362. При вчиненні злочинів, передбачених в інших статтях, ІТТ використовуються як засіб вчинення злочину, а тому вони будуть розглянуті в наступній темі.

У такий спосіб слід відмежовувати злочини, пов'язані з комп'ютером. Фактично ці діяння вчиняються для посягання в іншій, ніж інформаційна, сфері, на інший об'єкт, інформаційні процеси в

якому забезпечено за допомогою ІТТ, а отже вплинувши на них, або використавши їх можливості, можна вчинити посягання на цей об'єкт, який будемо називати «основним», як і склад злочину, який його охороняє.

Отже, виділяються дві групи таких злочинів:

1. Діяння, в ході вчинення яких здійснювався протиправний вплив на ІТТ, що містить склад злочину, передбаченого статтями Розділу XVI ККУ, а тому постає питання про сукупність злочинів.

2. Діяння, в ході вчинення яких можливості комп'ютерної системи використовуються при вчиненні «основного» злочину без протиправного впливу на неї, тобто коли склад злочину Розділу XVI відсутній. Звичайно, питання про сукупність тут не повинне виникати – вчиняється один злочин.

За відсутності можливості розглянути всі варіанти «основних» злочинів, ми зупинимося лише на найбільш поширених – злочинах проти власності. До цієї групи злочинів належать найбільш актуальні зараз в діяльності підрозділів протидії кіберзлочинам злочини у сферах платіжних систем, економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж. Найчастіше такі правопорушення вчиняються з корисливим мотивом, тобто для заволодіння чужим майном. А отже такі злочини вчиняються в сукупності зі злочином проти власності, який є «основним» складом вчиненого діяння.

Оскільки ці злочини одночасно є найбільш складними у кваліфікації, на їх прикладі ми

з'ясуємо більшість особливостей та засвоїмо правила, які можна застосовувати при кваліфікації злочинів, пов'язаних із комп'ютерами.

5.2. Кваліфікація кіберзлочинів проти власності

Посягання проти власності, що належать до першої групи за наведеною вище класифікацією, неодноразово траплялися в практиці правоохоронних органів України, більше того, можна сказати, що саме з них почалася історія кіберзлочинності в Україні.

Приклад 1

Так, у 1995 році в Дніпропетровському регіональному управлінні «Промінвестбанку» України було викрадено близько 864 млн крб. Роком пізніше у відділенні АКБ «Україна» у м. Сімферополі з використанням комп'ютерної техніки було викрадено близько 450 млн крб, а у 1994-му в Черкаській обласній дирекції «Укрсоцбанку» вчинено розкрадання 990 млн крб. Правоохоронні органи України в 1996-му запобігли спробам незаконного переказу з рахунку Національного банку України в АКБ «Таврія» 10 млн гривень, спробам втручання в електронну систему Мелітопольского відділення АК АПБ «Україна» із метою крадіжки 448 тис. гривень, а також спробам крадіжки 182 тис. гривень із використанням електронних міжбанківських розрахунків у Закарпатському відділенні банку «Аваль». Восени 1998 року з використанням комп'ютерної системи електронних платежів близь-

ко 80 млн гривень було викрадено з рахунків Вінницької дирекції НБУ.

Механізм учинення таких злочинів, зазвичай, полягає в тому, що електронна система переказу платежів, яка використовується тією чи тією фінансовою установою, застосовується злочинцем для здійснення незаконного переказу коштів, для незаконного заволодіння чужою власністю, причому вчиняється діяння, яке містить ознаки комп'ютерного злочину, передбаченого Розділом XVI. Такі діяння можна кваліфікувати як шахрайство, вчинене через незаконні операції із використанням електронно-обчислювальної техніки (ч. 3 ст. 190 ККУ), але лише за наявності необхідних ознак.

Слід також мати на увазі, що за смислом обману чи зловживання довірою, як способів вчинення шахрайства, вони можуть бути спрямовані тільки на людину. Обманути чи зловжити довірою ЕОМ (комп'ютерів), АС та КМ і МЕ неможливо. А тому *випадки, у яких без безпосередньої участі людини, а лише через надання підробленої інформації технічному чи програмному засобу (банкомату, платіжній системі, терміналу тощо) відбувається заволодіння майном, слід розглядати як таємне викрадення майна – крадіжку (ст. 185). Вказані ж випадки, коли описаним шляхом спричиняється значна матеріальна шкода, слід кваліфікувати як спричинення значної матеріальної шкоди через обман без ознак шахрайства (ст. 192). Кваліфікація таких діянь як шахрайства (за ч. 3 ст. 190) буде неправильною.*

Для глибшого розуміння наведемо типові приклади використання для кваліфікації ч. 3 ст. 190 ККУ.

Засуджений, особа А., задля заволодіння грошовими коштами, через обман користувачів інтернету, зареєструвався на інтернет-ресурсі «Aukro.ua» (цей сайт є інтернет-аукціоном, на якому здійснюється продаж та придбання різноманітних товарів). У подальшому він пропонував до продажу телефони, камери та інші електронні товари. Усі товари виставлялися на лотах за заниженими цінами, щоб привабити якомога більше клієнтів. Після того, як покупець вигравав аукціон, йому надходило відповідне повідомлення з «Aukro.ua», а також указувалися контактний телефон, «E-mail» та адреса продавця. Коли покупець зв'язувався з А., то останній повідомляв, що він справді продає товар, який виставлений на інтернет-аукціоні «Aukro.ua», пропонував перерахувати вартість товару на один із його «Web-гаманців» платіжної системи «WebMoney», а після перерахування коштів товар буде надісланий покупцю. Але після перерахування коштів покупець свого товару так і не отримував. У подальшому А. відкрив платіжну картку «Миттєва» ЧФ ВАТ КБ «ПриватБанк», на яку переводив гроші, отримані шахрайським шляхом.

Також на сьогодні одним із поширених видів шахрайства, вчинюваного з використанням електронно-обчислювальної техніки, є так званий «фішинг». Він полягає в тому, що зловмисники масово надсилають електронні листи, у яких від

імені якогось відомого банку, інтернет-магазину, фінансової компанії чи під іншим приводом, наприклад виграш у лотереї, пропонують адресатам повідомити реквізити своєї пластикової картки або іншу важливу персональну інформацію, а потім використовують ці дані для заволодіння грошима адресатів або вчинення інших злочинів. Така злочинна діяльність здебільшого транснаціональна, до якої, на жаль, все частіше залучаються українські громадяни.

Наприклад, при розгляді клопотання про надання правової допомоги з Федеративної Республіки Німеччина з його матеріалів з'ясувалося, що у 2009 році, більш точна дата не встановлена, обвинувачені, з метою незаконного збагачення, зорганізувалися у стійке об'єднання для вчинення шахрайських дій та завдання шкоди в інтернеті. Їх компанія, що була зареєстрована на території Республіки Панама, діяла на всій території Європи та пропонувала послуги з надання простору для зберігання даних в інтернеті й анонімного розміщення в інтернеті нелегального контенту. Крім того, вказана мережа використовувалася для здійснення несанкціонованих втручань в роботу ЕОМ (комп'ютерів), АС та КМ – і в інтересах обвинувачених, і в інтересах сторонніх осіб за грошову винагороду. Також обвинувачені займалися так званим «фішингом», тобто вистежуванням та отриманням реквізитів банківських платіжних карт із подальшим незаконним зняттям грошових коштів із них. Так, у ході розслідування встановлено, що обвинувачені не менш як 325 разів надавали ком-

п'ютерні послуги операторам нелегальних шахрайських інтернет-магазинів. При цьому декілька серверів, орендовані обвинуваченим, знаходились на одному з підприємств м. Харкова.

Значного поширення набуло розкрадання матеріальних і фінансових коштів через цілеспрямоване перекручення змісту комп'ютерної інформації шляхом її зміни, особою, яка має право доступу до неї (ст. 362), або підробки шляхом несанкціонованого втручання (ст. 361). Відповідно утворюється сукупність злочину проти власності та одного із указаних в цих статтях.

Для прикладу можна навести такий випадок.

Приклад 2

З вересня до грудня 2009 року головний інженер-програміст одного з підприємств електрозв'язку розробив комп'ютерну програму, яка дозволяє відшукувати в масиві фіксованої структури телефонні розмови, проведені із заданих номерів телефонів, відбирати їх і стирати інформацію про них у даному масиві. Винний увійшов у змову з громадянином Пакистану, який залучав клієнтів. Спільно вони надавали їм за заниженими тарифами послуги міжнародного та міжміського телефонного зв'язку, а інформацію про переговори, що здійснювалися клієнтами, знищували за допомогою програми, розробленої інженером-програмістом. Унаслідок таких дій підприємству електрозв'язку було заподіяно збитки розміром близько 150 тис. гривень.

Кваліфікувати дії головного інженера, якби вони були вчинені після набрання чинності новим ККУ, потрібно було б за сукупністю злочинів, пе-

редбачених ст. 192 (спричинення значної матеріальної шкоди шляхом обману без ознак шахрайства), ст. 361 (несанкціоноване втручання в роботу АС обчислення плати за надання послуг міжміського та міжнародного зв'язку, яке спричинило підроблення комп'ютерної інформації) та ст. 361^1 (створення з метою використання шкідливої програми, призначеної для несанкціонованого втручання в роботу АС).

Приклад 3

Схожий випадок стався влітку 2012 року в Херсоні. Студент одного з вишів міста вчинив несанкціоноване втручання в роботу комп'ютерної мережі місцевого провайдера інтернет-послуг і перекрутив комп'ютерну інформацію про рахунки клієнтів та сплачений час роботи в мережі (створив фіктивний рахунок). Після цього протягом кількох місяців безкоштовно користувався інтернетом, чим заподіяв матеріальну шкоду провайдерові у розмірі 11 000 грн. За чинним ККУ подібні дії треба кваліфікувати як сукупність злочинів, передбачених статтями 192 і 361 ККУ.

Подібні випадки у світовій практиці одержали назву «крадіжка машинного часу». Такого роду злочини полягають у тому, що особа неправомірно використовує дороге комп'ютерне устаткування (наприклад суперкомп'ютери) або ресурси КМ, абонентом яких вона не є. Найбільш поширеним видом подібних посягань у вітчизняній практиці є отримання доступу до інтернету за рахунок законних абонентів через використання їх логінів та паролів. Видається, що правильною кваліфікацією

подібних дій, є оцінка їх як сукупності злочинів, передбачених статтями 192 та 361 ККУ. Однак відповідальність за злочин, передбачений ст. 192 ККУ, настає лише в разі заподіяння матеріальної шкоди, що перевищує 50 НМДГ. Оскільки шкода, що заподіюється внаслідок більшості фактів заволодіння чужим машинним часом, значно менша, подібні дії отримують правову оцінку як блокування комп'ютерної інформації законних користувачів у той час, коли за їх рахунок та під їхніми іменами порушники отримували доступ до інформації (ст. 361 ККУ), а також якщо отримання чужих логінів і паролів здійснювалося через несанкціоноване втручання або особою, яка має доступ до комп'ютерної інформації, відповідно як несанкціоноване втручання, що призвело до витоку комп'ютерної інформації (ст. 361 ККУ) або як злочин, передбачений ст. 362 ККУ.

Так, у вироку щодо обвинувачення Р. у вчиненні злочину, передбаченого ч. 1 ст. 361 ККУ України, зазначається: у січні 2018 року Р., перебуваючи в Голованівському відділенні Гайворонської МДПІ в кабінеті своєї дружини Р-вої при здійсненні уповноваженою особою Р-вою процедури під'єднання до інтернету, діючи умисно, незаконно дізнався про ІОД – логін та пароль доступу до мережі вказаного відділення Гайворонської МДПІ. Після цього, в період з 28 січня по 11 червня 2018 року Р., діючи умисно, без дозволу керівництва Голованівського відділення Гайворонської МДПІ, незаконно використовуючи логін та пароль доступу до інтернету Голованівського відділення

Гайворонської МДПІ з власного комп'ютера неодноразово здійснював несанкціоноване втручання в роботу комп'ютерної мережі, що призвело до блокування інформації Голованівського відділення Гайворонської МДПІ щодо звітності платників податків, оскільки одночасна робота двох користувачів з однаковими логінами та паролями неможлива.

Як приклад крадіжки, що кваліфікується за сукупністю з комп'ютерним злочином, розглянемо випадок кваліфікації за ч. 2 ст. 361 та ч. 2 ст. 185 ККУ.

Приклад 4

Так, 26 березня 2016 року близько 8 години, Ц. за попередньою змовою із Ч., з метою заволодіння чужим майном через підключення до інтернету в приміщенні Пункту колективного користування послугами інтернету, через підбір випадкових цифр логінів, паролів та трансферів, видавши себе за законного користувача, вчинили несанкціоноване втручання в роботу ЕОМ (комп'ютерів), АС та КМ для доступу до програмного комплексу віддаленого обслуговування клієнтів сайту, належного закритому акціонерному товариству комерційний банк (ЗАТ КБ) «ПриватБанк». Внаслідок несанкціонованого втручання зазнала витоку та блокування конфіденційна інформація про користувачів АС та інформація про банківський рахунок клієнта банка гр-на Т.

Отримавши доступ до конфіденційного рахунку за кредитною карткою клієнта банку Т., Ц. за попередньою змовою із Ч., продовжуючи свої злочинні дії, за рахунок кредитних коштів ЗАТ КБ

«ПриватБанк», у період з 10 год 08 хв до 10 год 43 хв через інтернет учинили шість фінансових операцій з придбання шести електронних ваучерів Закритого акціонерного товариства (ЗАТ) «Київстар GSM» на поповнення рахунку мобільного телефону на загальну суму 1525 грн. Отримавши з АС текстове повідомлення про авторизацію проведених операцій із зазначенням ідентифікаційного коду придбаних ваучерів, Ц. та Ч., у період з 11 год 22 хв до 11 год 26 хв через уведення кода ваучерів у свій мобільний телефон із абонентською скретч карткою «Київстар GSM» для мобільного зв'язку, вчинили фінансову операцію та поповнили рахунок своєї скретч картки на загальну суму 1525 грн.

Також у період із 26 березня по 13 квітня 2016 року подібні дії (несанкціоноване втручання та подальше викрадення грошей) Ц. та Ч. вчинили ще відносно 10 потерпілих, у зв'язку з чим суд при кваліфікації означених діянь врахував ознаку повторності.

Слід зауважити, що суд кваліфікував дії обох підсудних за сукупністю злочинів, передбачених ст. 361 ч. 2, ст. 190 ч. 3 ККУ. Проте така кваліфікація бачиться помилковою з наведених вище підстав – зловмисники не обманювали шляхом використання інформації, здобутої при несанкціонованому втручанні, безпосередньо працівника банку, який тільки і міг би бути об'єктом такого обману. Вони створили в АС видимість законного користувача й АС видала їм гроші, але це відбулося без участі людини, зокрема власника грошей, тобто

таємно, що і утворює спосіб крадіжки. Отже подібні діяння слід кваліфікувати за ч. 2 ст. 361 та частиною ст. 185, яка відповідає іншим ознакам злочину (в даному випадку ч. 2 – крадіжка, вчинена повторно і за попередньою змовою групою осіб).

На перший погляд, здається, що наведені приклади не мають суттєвої різниці й неможливо чітко визначити, коли при кваліфікації слід застосовувати статті 185, 190 або 192 ККУ. А тому слід знати відмінності між цими складами злочинів, які полягають у способі їх вчинення.

Крадіжка (ст. 185) вчиняється способом *таємного викрадення*, під яким слід вважати випадки, коли особа заволодіває чужим майном: у відсутності власника або інших осіб; у присутності власника або інших осіб, але непомітно для них; у присутності власника або інших осіб, які, однак, не усвідомлюють самого факту викрадення і не можуть дати таким діям належної оцінки внаслідок певних обставин (малолітства, фізичних і психічних недоліків, стану алкогольного сп'яніння, помилки); у присутності осіб, які схвалюють або ставляться байдуже до факту вчинення крадіжки винним, і останній це усвідомлює. Таємним судова практика визнає також випадки, коли особа, викрадаючи чуже майно, вважає, що робить це таємно, незалежно від того, чи спостерігав хто-небудь за його діями. Наприклад, за кишеньковим злодієм спостерігають працівники міліції та затримують його безпосередньо після скоєння злочину. Такі дії слід кваліфікувати як крадіжка.

У ст. 190 під обманом слід розуміти повідомлення неправдивих відомостей або приховування чи замовчування обставин, повідомлення про які є обов'язковим. Зловживання довірою полягає в завідомому використанні винним довірливих відносин із потерпілим, унаслідок яких винний і одержує майно або право на майно. Ключовим при шахрайстві є *добровільна передача майна* законним володільцем зловмиснику під впливом обману чи довіри до нього.

Відповідно до ст. 192 незаконні дії майнового характеру вчиняються особою, яка *вже володіє майном*, шляхом обману або зловживання довірою в таких формах: 1) протиправне використання особою чужого майна, що перебуває в його віданні або розпорядженні, для одержання особистої вигоди (наприклад самовільне використання транспортних засобів, механізмів, іншого майна); 2) звернення на свою користь платежів, які повинні надійти від окремих громадян за послуги, особою не уповноваженою на їхнє одержання (наприклад, провідник вагону незаконно приймає пасажира та одержує від нього платіж за проїзд, обертаючи кошти на свою користь); 3) неправомірне неповернення або несвоєчасне повернення майна або коштів, що позбавляє власника можливості їхнього використання за власним розсудом; 4) ухилення від сплати обов'язкових платежів (наприклад, за житло, телекомунікаційні послуги, проїзд тощо).

На продовження розгляду особливостей способів вчинення злочинів проти власності слід зауважити, що розповсюджені випадки блокування ро-

боти операційної системи програмою, яка повідомляє, що, якщо не буде переведена певна сума грошей на вказаний рахунок, вся інформація на носіях буде знищена, повинні кваліфікуватися як *вимагання* (ч. 1 ст. 189 ККУ) та несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 361 ККУ). Способом вчинення вимагання тут буде погроза знищення майна (інформації), і такі злочини вважаються закінченими вже з моменту висунення вимоги передати гроші чи інше майно.

Приклад 5

Прикладом такого злочину може бути вірус Petya, який 27.06.2017 р. спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Масштабна деструктивна атака різновидом вірусу Petya стала можливою завдяки компрометації системи оновлення програми M.E. DOC та встановлення прихованого бекдору. Отже, масштабною деструктивною атакою зловмисники закрили собі наявний в них завдяки бекдору доступ до комп'ютерів та комп'ютерних мереж у близько 80 % українських підприємств (у тому числі – представництв закордонних компаній). Є підстави вважати, що зловмисники пішли на такий крок, оскільки або здобули надійніший доступ до інформаційних систем важливих для них жертв, або ж вважають, що зможуть доволі просто відновити його.

До інших випадків, які мають особливості кваліфікації, слід віднести і діяння, пов'язані із:

– використанням пристроїв, призначених для отримання необхідної інформації (пін-коду, інформації з магнітної стрічки або чипу картки) або предмета (картки, грошей);

– перепрограмуванням технічних пристроїв платіжних чи банківських систем.

Перші можуть використовуватись через установлення на технічні пристрої платіжних чи банківських систем (так звані, «накладки») або окремо (найбільш зухвалим подібним пристроєм є фальшивий банкомат, термінал або поштомат). Другі вчиняються шляхом внесення необхідних змін в програму, яка виконується на ЕОМ (комп'ютері) в складі банкомату чи іншого технічного пристрою платіжної (банківської) системи та керує його роботою.

З другими, в принципі, питань при кваліфікації не виникає – це пряме втручання в роботу комп'ютерної системи, яке призводить до підроблення, знищення, витоку інформації.

З першими на практиці виникають труднощі при кваліфікації, оскільки вони вчиняються з використанням ІТТ, але більшість їх не підпадає під відповідні склади злочинів, оскільки фактично спрямовані лише на отримання інформації. У таких випадках слід шукати можливість застосувати «традиційні» статті ККУ. У цьому разі в практиці склалася тенденція до кваліфікації таких дій за ст. 359 ККУ (незаконне використання спеціальних технічних засобів отримання інформації), яку також застосовують при кваліфікації застосування інших пристроїв в подібних діяннях

(наприклад прихованих фото- чи відеокамер). Слід мати на увазі, що така кваліфікація повинна підкріплятися висновком спеціаліста, який визнає цей пристрій спеціальним технічним засобом негласного отримання інформації (визначення їх дано нижче при розгляді складу ст. 163). В іншому ж разі, за наявності в події сукупності інших необхідних ознак, можна кваліфікувати такі дії за ст. 14 ККУ як готування до злочину, зокрема, до передбаченого ст. 200 або ст. 361. Звичайно, останні злочини також можуть вчинятися для готування до іншого злочину, найчастіше – проти власності. Включати чи не включати в формулу кваліфікації статті, які передбачають відповідальність за ці злочини, залежить від обсягу обставин справи, які вказують на готування до них і які вдасться виявити та доказати.

Якщо ж такий пристрій буде призначений для отримання безпосередньо чужого майна (грошей – якщо це термінал, або майна, якщо це поштомат), то особа, яка його встановила, повинна понести відповідальність за закінчений злочин проти власності – шахрайство (ч. 3 ст. 190).

Достатньо відомим є спосіб незаконного заволодіння чужим майном із використанням засобів автоматизованого опрацювання інформації, який отримав назву «метод Салямі». Подібний спосіб використовується в банківських установах і полягає в такій зміні програмного забезпечення фінансового закладу, яка призводить до несанкціонованого перерахування на певний рахунок дуже невеликої кількості грошей при кожній транзакції, по-

в'язаній із перерахуванням великим сум та значними залишками на відповідних рахунках. Отже, на рахунку, який контролюється зловмисником через деякий час, залежно від кількості операцій на значні суми, накопичується певна сума, яка в подальшому незаконно привласнюється. Подібні випадки, з позицій відповідальності за злочини проти власності, не можна кваліфікувати як шахрайство, оскільки наявні ознаки саме таємного заволодіння чужим майном – крадіжки. Зловмисник бажає якнайдовше залишатися непоміченим, саме тому гроші «знімаються» при операціях на великі суми та з рахунків із великими залишками. Тому в подібній ситуації, знову ж таки, правильною буде кваліфікація вчиненого як крадіжки (ст. 185 ККУ) та несанкціонованого втручання, що призвело до спотворення процесу оброблення інформації (ст. 361 ККУ), але не шахрайства.

Викрадення, пошкодження чи знищення комп'ютерної техніки – це звичайні злочини проти власності, тому труднощів із кваліфікацією таких дій не виникає. Але іноді вказані *злочини проти власності можуть виступати як спосіб вчинення незаконного втручання*. Від незаконного втручання вони відрізняються за об'єктом (право власності на річ і право власності на комп'ютерну інформацію), предметом (комп'ютерна техніка й комп'ютерна інформація), об'єктивним боком (викрадення, пошкодження, знищення техніки та знищення, перекручення комп'ютерної інформації). Однак найголовнішою ознакою відмежування злочинів проти власності від незаконного втручання

є *спрямованість умислу*. Якщо дії особи є порушенням фізичної цілісності комп'ютерної техніки (ознака об'єктивного боку злочину проти власності), але мета, яку переслідує суб'єкт, полягає в заподіянні шкоди відносинам власності на інформацію, то дії цієї особи слід кваліфікувати як незаконне втручання в роботу ЕОМ, систем та КМ, оскільки знищення або пошкодження комп'ютерної техніки в цьому разі є способом вчинення незаконного втручання в роботу ЕОМ, систем або КМ. Кваліфікувати подібні дії потрібно як сукупність злочинів, передбачених ст. 361 «Незаконне втручання в роботу ЕОМ» і ст. 194 «Умисне знищення або пошкодження майна».

Цікавими є випадки вчинення злочинів проти власності за відсутності ознак злочинів, передбачених Розділом XVI ККУ. Цікавими вони є тому, що вчиняються з використанням іноді дивних можливостей ІТТ, які найчастіше не виявлені на етапах їх розроблення та впровадження, але помічаються злочинцем і використовуються. Але ці можливості є легальними властивостями системи, вони не виникають під впливом зловмисника, а тому перше бажання кваліфікувати такі діяння за статтями Розділу XVI слід відкидати та кваліфікувати його відповідно до основного об'єкта посягання та інших ознак складу злочину.

Отже, при вчиненні цих злочинів особа може використовувати недоліки технічних засобів або програм чи їх особливі можливості.

Прикладом першого є можливість, яка донедавна існувала в банкоматах деяких банків, отри-

мання з банкомату частини коштів із генерацією відміни операції. Полягала вона в тому, що при висуненні пачки купюр із пристрою видавання можливо було витягнути з неї центральну частину, не чіпляючи верхню та нижню. Після певного часу, який відведено для витягнення коштів, банкомат фіксував їх залишок у пристрої та генерував відміну операції зняття коштів, отже сума на рахунку залишалася незмінною. Як видно, основа вчинення цього злочину лежить в особливостях технічного засобу, який працює під керівництвом комп'ютера, але жодного втручання в його роботу чи змін в інформації не було вчинено. Отже, це буде банальна крадіжка (ст. 185).

Іншим прикладом є використання недоліку роботи касового термінала, який, якщо після друку чеку швидко висмикнути дріт живлення, відміняв платіжну операцію з нарахування грошей на телефонний рахунок.

Прикладом другого типу використання можливостей ІТТ при вчиненні злочину – врахування особливостей роботи програм – може слугувати наступний. Касир невеличкого супермаркету помітила, що отримана виручка повністю звіряється з інформацією в комп'ютерній системі лише наприкінці місяця, а кожен день перед здачею в банк вона просто підраховується і фіксується за фактом. Використовуючи такі результати своїх спостережень, вона частину коштів, які давали їй покупці, не клала до каси, а присвоювала і використовувала на власний розсуд. Знову ж таки, у цьому разі відсутній який-небудь незаконний вплив на ком-

п'ютерну систему чи інформацію в ній, хоча її можливості використовуються.

У цьому прикладі буде інша кваліфікація – за ч. 1 ст. 191 ККУ (привласнення чи розтрата чужого майна, яке було ввірене особі чи перебувало в її віданні). На цих двох прикладах, як в принципі й інших, наданих вище, потрібно усвідомити різницю в способах вчинення злочинів проти власності, які суттєво впливають на кваліфікацію.

5.3. Кваліфікація злочинів проти права на приватність у кіберсфері

Іншим найбільш поширеним видом «основного» злочину при вчиненні кіберзлочину є злочини проти права на приватність у кіберсфері.

Взагалі основні аспекти права на приватність передбачено у трьох статтях Конституції України. Зокрема, ст. 30 Основного Закону гарантує кожному недоторканність житла; ст. 31 – таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції; ст. 32 забороняє втручатися в особисте й сімейне життя людей. Кримінально-правова охорона цих прав забезпечується відповідними нормами ККУ (статті 162, 163, 182). Утім слід зауважити, що кримінально-правова охорона приватності в Україні не обмежується трьома названими вище нормами. Зокрема, це право безпосередньо захищається також ст. 132 «Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту лю-

дини чи іншої невиліковної інфекційної хвороби», ст. 145 «Незаконне розголошення лікарської таємниці» та ст. 168 «Розголошення таємниці усиновлення (удочеріння)». Проте якщо остання, як і статті 162, 163, 182 ККУ, міститься в розділі V ОЧ ККУ, то перші дві чомусь опинилися в розділі II «Злочини проти життя та здоров'я особи», не дивлячись на те, що об'єктом злочину в них є не життя або здоров'я людини, а право на повагу до приватного життя.

Звичайно, в кіберсфері неможливо вчинити порушення недоторканності житла (ст. 162 ККУ). Всі ж інші посягання на приватне життя в кіберсфері ми розглянемо на прикладі складів злочинів, передбачених статтями 163 та 182 ККУ.

Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 ККУ).

Відповідно до ст. 31 Конституції України кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції.

Безпосереднім об'єктом злочину є конституційне право на таємницю листування, телефонних розмов, телеграфної чи іншої кореспонденції, гарантоване ст. 31 Конституції України.

Об'єктивну сторону злочину становить порушення таємниці: 1) листування, 2) телефонних розмов, 3) телеграфної кореспонденції, 4) іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Порушення таємниці листування – це дії, пов'язані з ознайомленням особи, яка не мала не це права, зі змістом чужого листування, з незаконним розголошенням змісту такої кореспонденції без згоди громадянина, який написав чи отримав лист (повідомлення), або з розголошенням самого факту листування між певними громадянами чи між певним громадянином і організацією, підприємством чи установою. При цьому поняттям листування охоплюються будь-які види кореспонденції, що передається поштою: письмова кореспонденція (прості та рекомендовані листи, поштові картки, бандеролі, секограми, дрібні пакети) та інші поштові відправлення, передбачені Законом від 4 жовтня 2001 року «Про поштовий зв'язок».

Наприклад, порушенням таємниці листування буде розголошення володільцем сервісу електронної пошти сторонній особі (стороннім особам) факту листування між певними особами, відкриття та ознайомлення з тестом електронного листа, а так само передання цього листа для ознайомлення іншій особі. Проте знищення такого листа не містить ознак злочину, передбаченого ст. 163 ККУ, хоча за певних умов може утворювати склад злочину, передбаченого ст. 182 ККУ.

Порушення таємниці телефонних розмов, телеграфної кореспонденції чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, полягає у вчиненні дій, аналогічних порушенню таємниці листування, але з урахуванням специфіки відповідного виду комунікації.

Так, порушення таємниці телефонних розмов охоплює не тільки їх незаконне прослуховування чи фіксування, а й незаконне надання чи одержання інформації про телефонні розмови, які відбулися, про абонентів розмов, про час і тривалість розмов тощо.

Поняття «інша кореспонденція, що передаються засобами зв'язку або через комп'ютер» охоплює всі інші види повідомлень чи комунікацій, які можуть бути передані через будь-які технічні засоби (мобільні телефони, факси, телетайпи тощо) або через комп'ютер.

Це можуть бути факсимільні повідомлення, голосова пошта, повідомлення електронної пошти, повідомлення, відправлені через комп'ютерні програми миттєвого обміну повідомленнями, приватні повідомлення, відправлені через соціальні мережі чи інші інтернет-сайти або форуми тощо.

Слід зауважити, що кримінально караним є лише порушення, тобто незаконне обмеження права особи на таємницю кореспонденції. Відповідно до ст. 306 ЦК фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції. При цьому листи, телеграми тощо є власністю адресата.

Листи, телеграми й інші види кореспонденції можуть використовуватися, зокрема шляхом опублікування, лише за згодою особи, яка направила їх, та адресата. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її

використання, зокрема шляхом опублікування, потрібна згода цієї особи.

У разі смерті фізичної особи, яка надіслала кореспонденцію, і адресата використання кореспонденції, зокрема шляхом її опублікування, можливе лише за згодою їхніх дітей, вдови (вдівця), а якщо їх немає – батьків, братів і сестер. У разі смерті фізичної особи, яка направила кореспонденцію, і адресата, а також у разі смерті їхніх дітей, удови (вдівця), батьків, братів та сестер кореспонденція, яка має наукову, художню, історичну цінність, може бути опублікована в порядку, встановленому законом. Кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи лише в разі, якщо в ній містяться докази, що мають значення для вирішення справи. Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню.

Винятки із загальної заборони порушувати таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, як випливає з тексту ст. 31 Конституції України, можуть бути встановлені лише судом у випадках, передбачених законом, щоб запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Підстави і порядок здійснення заходів, пов'язаних із обмеженням цього права, визначено Кримінальним процесуальним кодексом України, Законами України «Про оперативно-розшукову діяльність»; «Про контррозвідувальну діяльність»; «Про

боротьбу з тероризмом»; «Про попереднє ув'язнення»; Кримінально-виконавчим кодексом України. Крім того, для з'ясуванні питання про законність обмеження права на таємницю кореспонденції слід ураховувати також прецеденти Європейського суду з прав людини, у яких тлумачаться відповідні положення ст. 8 Конвенції про захист прав людини та основоположних свобод.

У разі порушення таємниці кореспонденції, що передається через комп'ютер, що виникло внаслідок вчинення діяння, передбаченого статтею Розділу XVI ККУ, то кваліфікація відбувається в сукупності з відповідною статтею. Наприклад, якщо особа отримувала доступ до електронної кореспонденції через несанкціоноване втручання в роботу комп'ютерної мережі, потрібна додаткова кваліфікація за ст. 361 ККУ.

Кваліфікуючі ознаки передбачено в ч. 2 ст. 163 ККУ, яка встановлює відповідальність за «ті самі дії, вчинені щодо державних чи громадських діячів або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації».

Спеціальні засоби, призначені для негласного зняття інформації, – це будь-які технічні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, спеціально створені, розроблені, модернізовані, запрограмовані чи пристосовані для виконання завдань із негласного (таємного) отримання інформації (наприклад, через фіксацію аудіоінформації, візуального спостереження, прослуховування телефонних розмов, пере-

хоплення інформації з технічних каналів зв'язку тощо). Незаконне використання таких засобів, поєднане з порушенням таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, охоплюється ч. 2 ст. 163 і не потребує додаткової кваліфікації за ч. 1 ст. 359, але за наявності кваліфікуючих обставин, передбачених ч. 2 ст. 359, це діяння кваліфікується за сукупністю злочинів, передбачених ч. 2 ст. 163 і ч. 2 ст. 359.

Суб'єкт злочину є загальним, але вчинення його службовою особою, як було зазначено, утворює кваліфікований склад злочину. Суб'єктивний бік злочину характеризується прямим умислом.

Порушення недоторканності приватного життя (ст. 182 ККУ)

Основним безпосереднім об'єктом злочину є право особи на повагу до його приватного життя, гарантованого ст. 32 Конституції України.

Предметом злочину, передбаченого ст. 182 ККУ, є конфіденційна інформація про особу. При цьому конфіденційна інформація про особу має відповідати таким критеріям: вона має стосуватися реальних (невигаданих) фактів особистого чи сімейного життя конкретної особи, яка вже відома чи особистість якої можна визначити; особа не бажає розголошення цієї інформації; ця інформація є таємною (невідомою іншим особам з можливими винятками); ця інформація не становить суспільного інтересу (з'ясовувати чи становить певна інформація про особу публічний інтерес потрібно в кожному конкретному випадку окремо). Саме щодо такої інформації існує заборона збирання, зберігання,

використання та поширення без згоди особи, крім випадків коли ця інформація має бути розголошена на підставі закону в інтересах національної безпеки, економічного добробуту та захисту прав людини.

Об'єктивний бік злочину полягає в діях, спрямованих на порушення недоторканності приватного життя і знаходять свій вияв у незаконному втручанні в особисте чи сімейне життя громадянина шляхом: 1) незаконного збирання конфіденційної інформації про особу; 2) незаконного зберігання конфіденційної інформації про особу; 3) незаконного використання конфіденційної інформації про особу; 4) незаконного знищення конфіденційної інформації про особу; 5) незаконного поширення конфіденційної інформації про особу; 6) незаконної зміни конфіденційної інформації про особу.

Названі дії утворюють склад злочину, передбаченого ст. 182 ККУ, тільки якщо вони не охоплюються іншим складом злочину, наприклад передбаченого статтями 132, 145, 159 або 168 ККУ.

Збирання конфіденційної інформації про особу полягає в активних діях, спрямованих на отримання інформації відносно особистого чи сімейного життя людини особою, яка не має законних підстав для ознайомлення з відповідними відомостями. Обов'язковою ознакою цієї форми об'єктивної сторони злочину є цілеспрямований характер дій винної особи, адже випадкове отримання інформації про приватне життя іншої особи не охоплюється цією формою об'єктивного боку та не тягне кримінальної відповідальності, якщо лише така

особа не вчинила інших дій, що містять склад злочину.

Зберіганням є незаконні дії зі збереження відповідної інформації в певному місці на будь-яких носіях (на папері, пергаменті, тканині тощо, носіях аудіо-, фото-, відео-, електронної інформації, чи на будь-яких інших матеріальних носіях інформації, а так само на віддаленому сервері в інтернеті). Звичайно, не утворює складу злочину зберігання певної інформації в пам'яті людини.

Використання конфіденційної інформації про особу полягає в незаконному користуванні зазначеною інформацією на власний розсуд із будь-якою метою.

Знищення конфіденційної інформації про особу полягає у вчиненні незаконних дій, унаслідок яких відповідна інформації повністю або частково перестає існувати на матеріальних носіях. Це може виявитися і у знищенні чи істотному пошкодженні матеріальних носіїв інформації, і у видаленні електронних файлів програмними засобами, якщо йдеться про інформацію, яка зберігається в електронному вигляді. При цьому для кваліфікації принципово важливим є суб'єктивне ставлення винної особи до своїх діянь: вона має усвідомлювати, що своїми діями незаконно й безповоротно знищує певну приватну інформацію іншої особи. Тому, скажімо, якщо потім з'ясується, що потерпілий мав копію цієї інформації, у зв'язку з чим вона не була фактично знищена, то це не впливатиме на кваліфікацію дій винного.

Зміна конфіденційної інформації про особу як форма злочину, передбаченого ст. 182 ККУ, полягає у вчиненні будь-яких дій, унаслідок яких така інформація спотворюється, стає неправдивою, викривленою. Це може полягати, скажімо, у внесенні змін до особистих паперів чи комп'ютерних файлів людини, до певних офіційних документів тощо.

Поширення конфіденційної інформації про особу – це незаконні дії, метою яких є доведення змісту відповідних відомостей про особисте чи сімейне життя особи без її згоди до відома інших людей (одного, кількох чи багатьох). При цьому для кваліфікації не має значення, яким чином особа, котра поширила конфіденційні відомості, одержала їх – законно чи незаконно.

Збирання, зберігання, використання, знищення, зміна або поширення конфіденційної інформації про особу визнаються незаконними, якщо вони вчинені без згоди цієї особи чи її законних представників та/або вчиняються з порушенням встановленого законом порядку. Не є незаконними дії, передбачені ч. 1 ст. 182 ККУ, які здійснюються без згоди відповідної особи, але в інтересах національної безпеки, економічного добробуту, захисту прав людини та на підставі й у порядку, визначеному законом.

У разі вчинення перелічених діянь разом із діянням, передбаченим статтею Розділу XVI ККУ, кваліфікація відбувається в сукупності з відповідною статтею. Наприклад, якщо особа отримала до-

ступ до конфіденційної інформації через несанкціоноване втручання в роботу комп'ютерної мережі, потрібна додаткова кваліфікація за ст. 361 ККУ.

З іншого боку, ст. 361-2 ККУ (Несанкціоновані збут або розповсюдження ІОД, яка зберігається в ЕОМ (комп'ютерах), АС, КМ або на носіях такої інформації) перетинається зі ст. 182 ККУ за предметом та діянням:

– конфіденційна інформація про особу може бути частиною предмета ст. 361-2 – ІОД – в тому разі, якщо вона зберігається в ЕОМ (комп'ютерах), АС, КМ або на носіях інформації;

– збут чи розповсюдження, передбачені в ст. 361-2, можуть бути частиною використання чи поширення конфіденційної інформації про особу відповідно до ст. 182.

За збігом цих двох обставин (предметом злочину є конфіденційна інформація про особу, яка зберігається в ЕОМ (комп'ютерах), АС, КМ або на носіях інформації, а використання чи поширення конфіденційної інформації відбулося через її збут чи розповсюдження) ми повинні застосувати правила сукупності ст. 361-2 та 182.

У всіх інших випадках кваліфікація відбувається за однією статтею відповідно до обставин події.

Кваліфікуючі ознаки злочину передбачено в ч. 2 ст. 182 ККУ: «ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи».

Злочин, передбачений ст. 182 ККУ, вважається вчиненим повторно, якщо винна особа раніше вчи-

няла цей злочин. Проте повторність не виникає, якщо винна особа раніше вчиняла інші подібні злочини, у тому числі передбачені статтями 132, 145, 159, 168 ККУ тощо.

Наявність істотної шкоди слід з'ясовувати в кожному конкретному випадку залежно від обставин, оскільки це поняття є оціночним. Шкода, яка полягає в заподіянні матеріальних збитків, згідно з приміткою до ст. 182 ККУ, вважається істотною, якщо вона в сто і більше разів перевищує НМДГ.

Злочин, передбачений ч. 1 ст. 182 ККУ, за конструкцією є формальним. Моментом його закінчення визнається скоєння винним суспільно небезпечних дій.

Суб'єктивний бік злочину характеризується прямим умислом. Суб'єкт злочину загальний.

Приклади

Згадаймо політичне протистояння в жовтні 2013-го – лютому 2014 року довкола підписання/непідписання тодішньою владою Угоди про асоціацію між Україною та ЄС (події Євромайдану).

Це протистояння активно відбувалося в соціальних мережах, де спостерігався значний сплеск зацікавленості проблемою. З першого дня Євромайдану «невідомі особи» почали масово використовувати інструменти соцмереж із метою засмічення інформаційного поля, уведення людей в оману та поширення чуток. Наприклад, у Twitter, де можна відслідковувати всі події за хештегом #євромайдан, десятки нетботів вкидали різноманітне інфосміття.

Використовувалися також механізми ускладнення традиційних комунікацій, зокрема мобільного зв'язку (через автоматичні дзвінки на телефони певних активістів чи політиків, що унеможливило використання їхніх мобільних телефонів у роботі).

Було «зламано» електронні пошти, акаунти політиків у Twitter та Facebook. Зі «зламаних» сторінок масово розсилалися фейкові повідомлення, спрямовані на дезінформування суспільства. Загалом відбулася прицільна атака на ресурси та інструменти, які забезпечують комунікацію політиків із громадськістю та ЗМІ через інтернет.

Постраждали й електронні ЗМІ, які були головними інформаційними майданчиками, а заразом і рушійними силами акцій протесту. Кілька днів поспіль хакерських атак зазнавали сайти «Української правди», «Главкому» та інтернет-видання «Цензор.нет». Офіційні сайти Міністерства внутрішніх справ, Кабінету Міністрів і Президента України зазнали хакерських атак.

Останнє на часі кіберпротистояння стосується загострення українсько-російських відносин. Частково воно є наслідком тієї суспільно-політичної кризи, яка охопила українське суспільство протягом грудня 2013-го – лютого 2014 року. Внаслідок цього протистояння було сформовано загони хактивістів, які йменують себе «Кіберберкутом» (Cyberberkut – віртуальна структура, що не визнає української влади, яка сформувалася після лютого 2014 р. та «Кіберсотнею Майдану», «Анонімусами» з росій-

ською або українською «пропискою» тощо. Діяльність «кіберберкутівців» та інших інтернет-активістів (хактивістів) аналогічного ідеологічного спрямування зводиться переважно до DDos-атак на державні установи, мас-медіа й навіть комерційні структури.

Найбільш масовою атакою цієї групи на урядові інтернет ресурси була атака, організована 3 березня 2014 року. Складнощі в роботі відчули численні (понад 100) сайти – і урядові (зокрема Верховної Ради України, Кабінету Міністрів України, РНБОУ), і різноманітних інтернет-ЗМІ.

З боку лояльних до нової влади хакерських структур було проведено аналогічні кібератаки проти вебсайту «Кремлін.Ру», сайтів Центробанку Росії, Міністерства іноземних справ РФ, Russia Today (RT), «Російської газети».

Разом із явними проявами кіберзброї присутні й інші її виміри, це передовсім маніпулювання суспільною свідомістю, із використанням різних методів впливу на думки, вподобання людей у кіберпросторі.

Маніпуляцією свідомості розуміють як дії, направлені на зміну психологічних установок, ціннісних орієнтацій, поведінки індивідів і аудиторій незалежно від їхнього бажання. Мета маніпуляції – контроль над аудиторією, її керованість. Для досягнення мети використовуються різні маніпулятивні технології: цілеспрямоване спотворення інформації (замовчування, селекція, «перекручування» тощо).

Основні поняття

Порушення таємниці листування – це дії, пов'язані з ознайомленням особи, яка не мала не це права, зі змістом чужого листування, з незаконним розголошенням змісту такої кореспонденції без згоди громадянина, який написав чи отримав лист (повідомлення), або з розголошенням самого факту листування між певними громадянами чи між певним громадянином і організацією, підприємством чи установою.

Контрольні запитання та завдання

1. Назвіть зміст поняття та ознаки кіберзлочину.
2. У якому акті вказано міжнародні нормативні акти в сфері протидії кіберзлочинності?
3. Назвіть загальні особливості кваліфікації злочинів, пов'язаних з комп'ютерами.
4. Сформулюйте кваліфікацію кіберзлочинів проти власності.
5. Сформулюйте кваліфікацію злочинів проти приватності у кіберсфері.

Розділ 6

Кваліфікація кіберзлочинів, пов'язаних зі змістом даних або порушенням авторського права й суміжних прав, злочинів расистського та ксенофобного характеру, вчинених через комп'ютерні системи

До інших кіберзлочинів належать традиційні діяння, в яких елементи ІТТ утворюють специфічні факультативні ознаки об'єктивної сторони:

– обстановку вчинення злочину – кіберпростір;

– засіб вчинення злочину.

Найчастіше такі злочини пов'язані зі змістом інформації, розміщення якої в кіберпросторі є протиправним, оскільки вільний її обіг або заборонений, або обмежений, зокрема, це стосується порнографії, об'єктів інтелектуальної власності, расистського та ксенофобного матеріалів, матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або злочинами проти людства.

Щодо деяких видів традиційних злочинів слід зробити зауваження, що їх ознаки все частіше спостерігаються в діях різних осіб в кіберпросторі, проте не отримують належної юридичної оцінки з боку правоохоронних органів, оскільки чинний

кримінальний закон не пристосований до інформаційного суспільства. Хоча він містить можливості притягнення таких осіб до відповідальності, отже не слід їх відкидати та треба намагатися їх застосовувати на практиці.

Наприклад, важливими ознаками простого хуліганства (ч. 1 ст. 296 ККУ) є винятковий цинізм та особлива зухвалість, хоча б одна з яких повинна бути присутня в діях винної особи в кіберпросторі. Зокрема, це може виражатися в: знущанні над особою, яке тривалий час і вперто не припинялось (тролінг), тяжкій образі потерпілого, або в діях, які були пов'язані з пошкодженням чи знищенням інформації у великих обсягах, або навіть не великих, але критично важливої інформації, зриві масового заходу (наприклад телеконференції), тимчасовому припиненні нормальної діяльності установи, підприємства (зокрема інтернет-магазину, соціальної мережі та, в принципі, будь-якого сайту). Зі зростанням доступності відеоконференцзв'язку стає можливим прояв виняткового цинізму у вигляді непристойних неподобних рухів тіла, оголення статевих органів. Єдине питання, яке виникає завжди при оцінці таких діянь, – розповсюдження на кіберпростір поняття «громадський порядок», грубе порушення якого є необхідним наслідком хуліганства. Але якщо кіберпростір став невід'ємною частиною суспільного життя, то чому б ні? Крім того, не слід прив'язувати поняття «громадський порядок» до поняття «громадське місце», адже і при вчиненні традиційних злочинів це не є обов'язковим.

6.1. Кваліфікація кіберзлочинів, пов'язаних зі змістом даних

Правильність кваліфікації злочинів, пов'язаних із розповсюдженням дитячої порнографії через інтернет має неабияку актуальність. Про це свідчить і прийнятий Верховною Радою України Закон України «Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії», спрямований на імплементацію «Конвенції про кіберзлочинність» та Факультативного протоколу до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії (ратифікована Законом України від 3 квітня 2003 року).

Відповідно до п. «с» ст. 2 Факультативного протоколу до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії, дитячу порнографію розуміють як «будь-яке зображення будь-якими засобами дитини, яка здійснює реальні або змодельовані відверто сексуальні дії, або будь-яке зображення статевих органів дитини, головно в сексуальних цілях».

Дещо відмінне від указаного визначення пропонує нам Закон України «Про захист суспільної моралі», у ч. 1 ст. 1 якого дитяча порнографія визначається як «зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, задіяної в реальній або змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях». З одного боку, вітчизняний законодавець розширює перелік від-

повідних зображень (зображення особи, яка виглядає як дитина), з іншого – звужує (зображення статевих органів дитини можливе тільки в сексуальних цілях).

Указані положення слід ураховувати при кваліфікації злочинів, пов'язаних із розповсюдженням дитячої порнографії через інтернет, та одночасно враховувати наступне.

Виявлення порноресурсів на зарубіжних вебсайтах дає змогу застосовувати національне законодавство при доведенні хоча б одного випадку ознайомлення з цими інтернет-ресурсами особами, які знаходяться на території України. Оскільки, згідно із ч. 2 ст. 6 ККУ, злочин визнається вчиненим на території України, якщо його було почато, продовжено, закінчено або припинено на території України. Об'єктивний бік злочину, передбаченого ч. 1 ст. 301 ККУ, передбачає таку форму, як інше переміщення. Тому, наприклад, передача творів, зображень порнографічного характеру за допомогою світового інтернету цілком охоплюються іншим переміщенням, тобто такі дії слід кваліфікувати за ст. 301 ККУ.

Незаконне втручання в роботу ЕОМ (комп'ютерів), АС, КМ задля поширення творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру або незаконне розміщення цих творів на чужих вебсайтах, що призвело до витоку, втрати, підроблення, блокування інформації, спотворення процесу оброблення інформації або до порушення встановленого порядку

її маршрутизації, потребує кваліфікації за сукупністю злочинів за статтями 301 та 361 ККУ.

У слідчій практиці непоодинокі випадки, коли особа створює та поширює програмні віруси, які, заразивши комп'ютер, з'єднуються з порносайтами, і ставлять їх як стартові сторінки браузера, створюють ситуацію, коли браузер зберігає «заборонені» (як і будь-які інші) зображення на жорсткому диску.

Тому створення задля використання, поширення або збуту, а також розповсюдження або збут шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), АС, КМ чи МЕ, потребує кваліфікації за ст. 361^1 ККУ.

При цьому цілком можливі ситуації, коли особа, яка створює шкідливий програмний засіб, обізнана про його подальше використання (наприклад, створення на замовлення). У цій ситуації слід казати про співучасть такої особи (винний є пособником) у вчиненні злочинів, передбачених статтями 301 та 361 ККУ. При цьому слід застосовувати таку кваліфікуючу ознаку, як вчинення злочину за попередньою змовою групою осіб.

Судова та слідча практика свідчить про окремі проблеми встановлення саме факту демонстрації зображень порнографічного характеру та ознак суб'єктивної сторони злочину.

Приклад 1

Так, за фактом поширення порнографічної продукції ЗАТ «Воля-кабель» було порушено кримінальну справу прокуратурою Дніпровського району

м. Києва № 54-0731. У постанові про порушення кримінальної справи зазначено, що програми Private Gold, Private Blue та Spice Platinum є порнографією, і що такий висновок ґрунтується на висновках спеціаліста.

Але при цьому потрібно згадати, що ЗАТ «Воля-кабель» надає послуги кабельного телебачення та відповідно до Закону України «Про телекомунікації» є провайдером телекомунікацій. Послуга кабельного телебачення полягає в забезпеченні доступу до обраних абонентом пакетів телевізійних програм, які виготовляються та/чи розповсюджуються на території України вітчизняними та іноземними телеорганізаціями (правовласниками), про що укладається угода. Отже, з технічного погляду, підприємство забезпечує прийом і індивідуальний розподіл пакетів програм, які самостійно вибрав абонент. При цьому, відповідно до ст. 40 Закону України «Про телекомунікації», оператори, провайдери телекомунікацій не несуть відповідальності за зміст інформації, що передається їх мережами. Власного мовлення, тобто виробництва та розповсюдження телевізійних програм, ЗАТ «Воля-кабель» не здійснює, програми розподіляються без унесення змін та доповнень, на будь-які носії програми не записуються. Отже, відповідальність за змістову частину програм та передач (і іноземних, і вітчизняних) несуть телеорганізації, які здійснюють їх розповсюдження. Контроль за дотриманням законодавства при здійсненні мовлення вітчизняними телеорганізаціями здійснює Національна рада з питань телебачення та радіо-

мовлення. Що ж до програм та передач іноземних телеорганізацій, то в цьому разі слід керуватись положеннями Європейської конвенції про транскордонне телебачення від 5 травня 1989 року. Конвенція не допускає наявності в програмах телеорганізацій, що здійснюють транскордонне мовлення будь-яких проявів порнографії. Що ж до програм Private Gold, Private Blue та Spice Platinum, то ці програми розповсюджуються транскордонним способом їх країнами походження є Королівство Нідерланди та Сполучене Королівство Великобританії (які підписали Конвенцію) відповідно, а отже їх мовлення регулюється положеннями Європейської конвенції про транскордонне телебачення та не може містити порнографію. ЗАТ «Воля-кабель» має угоди з правовласниками цих програм, телеорганізації, що розповсюджують зазначені програми мають відповідні дозволи та ліцензії країни походження, сигнал, що несе ці програми легально присутній на міжнародному супутнику, а отже питання щодо відповідності програм Private Gold, Private Blue та Spice Platinum міжнародному законодавству в сфері телебачення та захисту суспільної моралі неможна поставати як таке. Зважаючи на еротичний характер програм, беручи до уваги положення ст. 13 Закону України «Про захист суспільної моралі», згідно з якою розповсюдження теле-, радіо-, аудіо- і відеопродукції сексуального чи еротичного характеру спеціалізованим засобом масової інформації можливе лише за умови спеціального оброблення сигналу, ЗАТ «Воля-кабель» було вжито заходів для забезпечення доступу до

програм Private Gold, Private Blue та Spice Platinum у кодованому вигляді, тобто таким чином, щоб прийом сигналу став неможливим без пристрою декодування. Більше того, враховуючи потребу певного обмеження обігу еротичної продукції, ЗАТ «Воля-кабель» пропонує абонентам для придбання декодуюче приладдя, яке додатково обладнане так званим «батьківським кодом», тобто абонент може самостійно обмежити доступ до програм за допомогою спеціального шифру, що є ще одним суттєвим додатковим обмеженням для перегляду програм неповнолітніми особами.

Тому за відсутністю принаймні ознак суб'єктивної сторони злочину (про порнографічний характер інформації питання повинно вирішуватися із застосуванням норм міжнародного права) справа підлягала закриттю, що і було здійснено.

Поширення зображень порнографічного характеру, що містять дитячу порнографію через створення вебресурсів, потребує кваліфікації за ч. 4 ст. 301 ККУ. Хоча в слідчій практиці трапляються випадки помилкової кваліфікації.

Приклад 2

Так, слідчим відділом Печерського РУ ГУМВС України в м. Києві 13 січня 2010 року порушено кримінальну справу № 06-10035 відносно винних осіб, дії яких кваліфіковано за ч. 3 ст. 301 ККУ. Хоча досудовим слідством встановлено, що винні особи в період часу з 2005-го до кінця 2007 року за попередньою змовою групою осіб на вебсайтах «Dark robbery», «Dark home pussy», «Dark video», «Dark collections» розміщували продукцію порно-

графічного характеру, виготовлену за участі дітей, а також рекламні сайти з картинками попереднього перегляду, після огляду яких користувач мав можливість придбати безпосередній доступ до сайтів, на яких розміщувались порнографічні матеріали. Під час спілкування між собою за допомогою інтернет-пейджеру ICC2 невстановлені особи використовували індивідуальні номери, псевдоніми. Задля отримання винагороди за збут в інтернеті порнографічних матеріалів, невстановлені особи використовували електронну платіжну систему, яка приймала грошові кошти за доступ користувачів до вебсайтів в інтернеті, на яких розміщувались порнографічні матеріали, виготовленої за участі дітей, а також рекламували та розповсюджували в інтернеті дитячу порнографію через створення таких вебсайтів та наповнення їх відповідними фотозображеннями.

Копіювання зображень порнографічного характеру, що містять дитячу порнографію, з інтернету без мети збуту не утворює складу злочину. Копіювання ж зображень порнографічного характеру, що містять дитячу порнографію, з мережі задля збуту слід кваліфікувати за ст. 301 ККУ.

Так, Л. визнана винною в тому, що, прагнучи швидкого особистого збагачення, через збут і поширення продукції порнографічного змісту, перебуваючи за місцем свого проживання, здійснюючи свій злочинний намір, на власному персональному комп'ютері, використовуючи доступ до всесвітньої інформаційної мережі, застосовуючи відповідні комп'ютерні програми, завантажила з невстанов-

лених слідством файлообмінників вказаної вище інформаційної системи на жорсткий диск свого комп'ютера файли, з відео- та фотопродукцією порнографічного змісту.

Переслідуючи мету незаконного збагачення, а саме одержання постійного прибутку як основного джерела доходу від збуту й розповсюдження продукції порнографічного характеру, Л., діючи умисно та усвідомлюючи протиправність своїх дій, використовуючи персональний комп'ютер, в інтернеті за електронною адресою: http://www/ucoz.ru/terms/, який є вільним в доступі та безкоштовним для користування, з 16.02.2010 власноруч створювала сайти, на які завантажила з жорсткого диску свого комп'ютера, попередньо завантажені нею файли порнографічного змісту. Для надходження коштів, отриманих унаслідок розповсюдження файлів з відео та фото продукцією порнографічного змісту, Л. зареєструвалась в системі електронних платежів «Web money», де створила електронний рахунок.

У Додатковому протоколі до Конвенції про кіберзлочинність Україна зробила застереження щодо заперечення, значної мінімізації, схвалення або виправдання геноциду чи злочинів проти людства: ці заперечення чи значна мінімізація, повинні бути вчинені з наміром підбурити до ненависті, дискримінації чи насильства проти будь-якої особи чи групи осіб на підставі ознак раси, кольору шкіри, національного чи етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій.

А тому дії расистського або ксенофобського характеру з використанням комп'ютерних систем (поширення матеріалів, погроза, образа тощо), кваліфікуються за статтями 161 або 300 ККУ.

Особливості кваліфікації цих діянь, пов'язані з їх учиненням із використанням ІТТ, подібні до злочинів, пов'язаних із порнографією.

Комп'ютерні технології призвели до появи нових об'єктів інтелектуальної власності: програмного забезпечення, баз даних, топографії інтегральних мікросхем тощо, – які стали новими видами предметів злочинів проти інтелектуальної власності (статті 176, 177 ККУ).

При кваліфікації окремих злочинів проти прав інтелектуальної власності, пов'язаних з використанням комп'ютерної техніки, слід відмежовувати несанкціоноване розповсюдження або збут комп'ютерної ІОД (ст. 361^2 ККУ) від цих злочинів.

Відмінність цих злочинів полягає в ознаках об'єкта і предмета. Безпосередніми об'єктами злочину, передбаченого ст. 176 ККУ, виступають авторські права (особисті немайнові та майнові права авторів, їх правонаступників, пов'язані зі створенням і використанням творів науки, літератури, мистецтва) і суміжні права (права виконавців, виробників фонограм, організаторів мовлення, пов'язані з використанням творів). Безпосередній об'єкт порушення прав на об'єкти промислової власності (ст. 177 ККУ) складають відносини володіння, розпоряджання, користування результатом своєї творчості в будь-якій сфері промисловості чи господарської діяльності. Ці норми охороняють інтереси

автора, особи, яка створила певні об'єкти інтелектуальної власності. У свою чергу, незаконні розповсюдження або збут комп'ютерної інформації (ст. 361^2 ККУ) посягають на інший об'єкт – відносини володіння, користування та розпоряджання комп'ютерною ІОД як її авторів, так і осіб, котрі такими не є.

Із цього положення випливає другий критерій, який дає змогу відмежувати згаданий комп'ютерний злочин від порушення авторського права, а саме предмет посягання.

Предметом першого з названих злочинів є комп'ютерна ІОД, предметом останнього – тільки об'єкти авторського права, до яких чинне законодавство України відносить, зокрема, програми для ЕОМ і бази даних. Правильне визначення предмета вказаних злочинів безпосередньо впливає на кваліфікацію посягань проти прав інтелектуальної власності, пов'язаних із використанням комп'ютерної техніки.

Особливості визначення вказаних предметів при кваліфікації злочинів полягають у наступному. Ознакою комп'ютерної ІОД є те, що вона повинна бути створена та захищена відповідно до положень чинного законодавства, зокрема положень відповідних законів чи підзаконних нормативно-правових актів, у яких регламентується порядок її створення і захисту.

Комп'ютерна ІОД може бути конфіденційною і таємною, зокрема такою, що містить банківську чи комерційну таємницю.

Приклад 3

Наприклад, підсудний Д., займаючи посаду інженера конструктора 3-ї категорії розрахунково-дослідницького відділу, перебуваючи на своєму робочому місці,умисно з метою несанкціонованих дій з інформацією, яка обробляється в ЕОМ (комп'ютерах), КМ та зберігається на носіях такої інформації, увійшовши до інформаційно-комп'ютерного комплексу ДП «Антонов» на своєму робочому комп'ютері, використовуючи зареєстрований за ним у відділі обчислювальної техніки ДП «Антонов» логін із паролем та маючи право доступу до інформації, несанкціоновано, не маючи відповідного дозволу, скопіював з файл-сервера з відкритим доступом на власний USB-носій» файл, який містив ІОД про креслення літака АН-178, а саме конструкторську схему фюзеляжу з прорахованими даними, що має регламентований доступ, який полягає в ідентифікації користувача такого доступу після правильного введення паролю доступу. Надалі, використовуючи комп'ютер, підключений до інтернету, підсудний розповсюдив з USB носія в мережі на сайті під своїм ніком ІОД про креслення літака АН-178, внаслідок чого означена інформація стала доступною особам, які не мали права доступу до неї. Такі дії були кваліфіковані за статтями 362 ч. 2 та 361^2 ч. 1 ККУ.

Комп'ютерна програма, яка є одним з об'єктів авторського права, може бути визнана, за певних обставин, винаходом. Саме тому низка вітчизняних спеціалістів у галузі цивільного права вважають за можливе захист комп'ютерної програми як

об'єкта права промислової власності. Комп'ютерні програми бажано охороняти патентним правом, насамперед тому, що в цьому випадку виняткове право виникло б безпосередньо на алгоритм (ідею), а не на одну з окремих форм його зовнішнього прояву у вигляді програми. Проте з правового погляду дотепер не одержали повного вирішення проблеми, пов'язані, зокрема, з пошуком аналогів заявленого алгоритму, виявленням його прототипу, складанням опису й формули, визначенням новизни, а також установленням факту його протиправного використання. Пояснюється це тим, що алгоритм не є матеріальним об'єктом, і тому важко встановити і подібність, і розходження між ними, й тим самим прирівняти його до технічного рішення. Але й твердження про те, що об'єкти цього типу взагалі неможливо зрівняти, виявити, пізнати, скласти для них патентну формулу й т. п. спростовуються більшою кількістю виданих патентів й авторських свідоцтв на об'єкти програмного забезпечення ЕОМ (США, ФРН, СРСР, Японія, Великобританія та ін.), практикою проведення експертизи щодо них, цілою серією рішень патентних судів і публікаціями. Усе це фактично зроблено для тисяч об'єктів, на які видані патенти. Це дає підстави говорити, що проблеми патентоспроможності комп'ютерних програм можна звести до проблем експертизи і юридичної техніки.

З викладеного вище можна визначити такі правила кваліфікації:

1) порушення майнових прав автора комп'ютерної програми слід кваліфікувати за ст. 176 ККУ;

2) у разі визнання комп'ютерної програми винаходом та видачі відповідного патенту до вчинення злочину порушник виключного права на використання винаходу може бути притягнутий до відповідальності за ст. 177 ККУ.

Слід також відзначити, що потерпілим від злочину, передбаченого ст. 361^2 ККУ, може бути будь-яка фізична чи юридична особа або держава, якщо їй належить право власності на комп'ютерну інформацію, а потерпілим від порушення авторського права та суміжних прав визнається тільки автор того чи того об'єкта авторського права або особа, якій на законних підставах належить виключне чи невиключне авторське право.

Із цього можна визначити такі правила кваліфікації:

1) якщо особа поширює за допомогою комп'ютерної мережі, наприклад електронний варіант популярного художнього твору без згоди автора, наявним є склад злочину, передбачений ст. 176 ККУ (за умови настання вказаних у статті наслідків); склад злочину, передбачений ст. 361^2 ККУ, у цій ситуації відсутній через відсутність предмета: електронний варіант художнього твору не є комп'ютерною ІОД;

2) якщо предметом розповсюдження буде комп'ютерна ІОД, яка одночасно є й об'єктом авторського права, наприклад електронний варіант підручника з грифом «таємно», матиме місце сукупність злочинів, передбачених статтями 176 та 361^2 ККУ.

Злочин, передбачений ст. 232 ККУ «Розголошення комерційної або банківської таємниці» (якщо його предметом є відповідна комп'ютерна інформація), потрібно відмежовувати від несанкціонованого збуту або поширення комп'ютерної інформації (ст. 361^2 ККУ) за ознаками суб'єкта. Розголошення комерційної або банківської таємниці характеризується наявністю спеціального суб'єкта, тому поширення або збут комп'ютерної інформації, що є предметом вказаного злочину, загальним суб'єктом потрібно кваліфікувати за ст. 361^2 ККУ.

Крім того, обов'язковою ознакою об'єктивного боку розголошення комерційної або банківської таємниці (ст. 232 ККУ) є наявність істотної шкоди, тому поширення комп'ютерної інформації, яка містить лікарську, банківську або комерційну таємницю, що не призвело до названих наслідків, слід кваліфікувати за ст. 361^2 ККУ.

6.2. Кваліфікація кіберзлочинів, при вчиненні яких ІТТ використовуються як засоби вчинення

Виготовлення, зберігання, придбання, перевезення, пересилання, ввезення в Україну задля використання при продажу товарів, збуту або збут підроблених грошей, державних цінних паперів, білетів державної лотереї, марок акцизного збору чи голографічних захисних елементів (ст. 199 ККУ).

Основний безпосередній об'єкт злочину – фінансово-кредитна система України в частині встановленого законодавством порядку випуску та

обігу грошей, державних цінних паперів і білетів державної лотереї, порядку сплати акцизного збору, а також авторське та суміжні права, *додаткові об'єкти* – право власності, права і законні інтереси споживачів. У разі вчинення дій із підробленою іноземною валютою об'єктом злочину слід визнавати також установлений порядок виконання Україною міжнародно-правових зобов'язань. Розглядуваний злочин належить до числа конвенційних.

Предмет злочину: 1) національна валюта України у виді банкнот чи металевої монети; 2) іноземна валюта – іноземні грошові знаки у виді банкнот, казначейських білетів і монет; 3) державні цінні папери; 4) білети державної лотереї; 5) марки акцизного збору; 6) голографічні захисні елементи. Ці предмети можуть бути: *підроблені* – виготовлені будь-яким способом, включаючи промисловий, усупереч установленому законодавством України порядку та імітують (фальсифікують) справжні або перероблені в будь-який спосіб (наклеювання, малювання, друкування тощо), зокрема через зміну зображення, що визначають номінал, рік затвердження зразка (виготовлення), банк-емітент, інші реквізити та елементи дизайну, і за зовнішнім виглядом можуть бути сприйняті як справжні.

Для наявності складу злочину, передбаченого ст. 199 ККУ, треба встановити, що вказані підроблені предмети мають *істотну схожість* із відповідними оригіналами за формою, розміром, кольором, основними реквізитами тощо. У тих випадках, коли очевидна їх невідповідність відповідному оригіналу виключає участь підробки в обігу,

а інші обставини справи свідчать про те, що умисел винної особи був спрямований лише на обман окремих громадян задля заволодіння їх майном, такі предмети можуть входити до складу шахрайства (ст. 190 ККУ).

Крім підроблення, марки акцизного збору та голографічні захисні елементи як предмети цього злочину можуть бути *незаконно виготовлені чи одержані* внаслідок подання особою сфальсифікованих документів (наприклад, документи містять неправдиві відомості про те, що контрольні марки нібито призначені для маркування примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних, а насправді суб'єкт планує їх продати виробникам контрафактної продукції; у пакет документів, який подається до Державного департаменту інтелектуальної власності, входять підроблені копії договору про передачу майнових прав автора та/або державного посвідчення на право поширення і демонстрування фільмів). Законодавство забороняє будь-яку посередницьку діяльність з одержання та розповсюдження контрольних марок.

Незаконним одержанням також є повторне використання на іншій продукції законно придбаних акцизних марок або їх викрадення зі спеціалізованих підприємств під час перевезення чи зберігання або внаслідок зловживання службовою особою своїм службовим становищем чи в результаті її службової недбалості під час реалізації марок.

Об'єктивна сторона злочину може виражатися в таких діях: 1) виготовлення; 2) зберігання; 3) при-

дбання; 4) перевезення; 5) пересилання; 6) увезення в Україну або 7) збут підробленої національної валюти України у вигляді банкнот чи металевої монети, іноземної валюти, державних цінних паперів чи білетів державної лотереї, марок акцизного збору, голографічних захисних елементів.

Поняття «*виготовлення* підроблених грошових знаків, державних цінних паперів і білетів державної лотереї, марок акцизного збору, голографічних захисних елементів» охоплює і *повне підроблення* – імітацію вказаних предметів цілком, і *часткове підроблення* – істотну фальсифікацію окремих частин справжніх грошей, цінних паперів і лотерейних білетів, марок акцизного збору, голографічних захисних елементів, що може полягати, наприклад, у переробці цифрового та буквеного номіналу справжньої банкноти, зміні номера або серії облігації, підробленні підпису або відбитку печатки на цінному папері.

Злочин у формі виготовлення підроблених грошових знаків, державних цінних паперів і білетів державної лотереї, марок акцизного збору, голографічних захисних елементів визнається *закінченим* із моменту виготовлення хоча б одного вказаного предмета незалежно від того, чи вдалося винному здійснити збут фальшивки.

Зберігання підроблених грошей, державних цінних паперів і білетів державної лотереї марок акцизного збору, голографічних захисних елементів (триваючий злочин) розуміють як умисні дії, пов'язані з перебуванням указаних предметів у володінні винного (він може тримати їх при собі, в

будь-якому приміщенні, сховищі тощо, але у будь-якому разі під своїм контролем).

Придбання – це отримання винним підроблених грошей, цінних паперів або лотерейних білетів, марок акцизного збору, голографічних захисних елементів будь-яким способом (купівля, отримання в обмін на інші предмети, одержання як оплати за виконання роботи тощо).

Перевезення полягає в переміщенні їх транспортом (наземним, водним, повітряним) з одного місця в інше і в межах території України, і за цими межами.

Пересилання – це переміщення означених предметів шляхом відправлення поштою, багажем, посильним або іншим способом з одного місця в інше без супроводження особи, котра здійснює пересилання.

Ввезенням в Україну треба визнавати переміщення підробок через Державний кордон України на її територію з використанням будь-яких транспортних засобів.

Збут – це оплатне або безоплатне умисне відчуження підроблених грошей, державних цінних паперів і білетів державної лотереї, марок акцизного збору, голографічних захисних елементів незалежно від способу (продаж, обмін, дарування, передача в борг, у рахунок погашення боргу тощо). Вважається *закінченим* із моменту збуту хоча б одного предмета злочину.

Суб'єктивна сторона злочину характеризується прямим умислом. Обов'язковою суб'єктивною ознакою виготовлення, зберігання, придбання, пере-

силання, ввезення в Україну підроблених грошей, державних цінних паперів і білетів державної лотереї, марок акцизного збору, голографічних захисних елементів є *мета їх збуту або використання при продажу товарів*.

Суб'єкт злочину – загальний.

Ч. 2 ст. 199 ККУ передбачено відповідальність за «ті самі дії, вчинені повторно або за попередньою змовою групою осіб чи у великому розмірі».

Ч. 3 ст. 199 ККУ передбачено відповідальність за «дії, передбачені частинами першою або другою цієї статті, вчинені організованою групою чи в особливо великому розмірі».

Розмір визнається *великим*, якщо сума підробки у двісті й більше разів перевищує НМДГ, а *особливо великим* – якщо сума підробки у чотириста та більше разів перевищує такий мінімум (примітка до ст. 199 ККУ).

Стаття 200. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення

Об'єктом злочину є встановлений порядок виготовлення, використання та обігу документів на переказ, платіжних карток та інших засобів доступу до банківських рахунків, який забезпечує нормальне функціонування банківської системи України.

Предметом злочину. При розгляді ст. 200 ККУ потрібно звернути особливу увагу на те, що в ній не сформульоване визначення всіх предметів злочи-

нів, які в ній застосовуються. Так, диспозицією вказаної статті предметом даного злочину названі: документи на переказ, платіжні картки, інші засоби доступу до банківських рахунків, електронні гроші. Однак у статті дається тлумачення лише поняття документа на переказ. Законом України «Про платіжні системи та переказ коштів в Україні» документи на переказ і платіжні картки віднесено до платіжних інструментів, тому потрібно розглянути дані поняття, сформульовані в профільному Законі, для встановлення правильного їх тлумачення, з'ясування їхнього місця в кримінальному праві.

З набранням чинності Закону України «Про платіжні системи та переказ коштів в Україні» від 5 квітня 2001 р., було сформоване таке визначення платіжної системи: «це платіжна організація, учасники платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів». Проведення переказу коштів, тобто забезпечення руху певної суми коштів задля зарахування на рахунок отримувача або видачі йому в готівковій формі, є обов'язковою функцією, що має виконувати платіжна система.

Платіжна система також розглядається як набір платіжних інструментів, банківських процедур і, зазвичай, міжбанківських систем переказу коштів, поєднання яких забезпечує грошовий обіг разом з інституційними та організаційними правилами та процедурами, що регламентують використання цих інструментів і механізмів. Таке поняття

охоплює всю процедуру здійснення безготівкових розрахунків та механізм їх реалізації.

Одне з основних завдань, яке розв'язується при створенні платіжної системи, полягає у виробленні та дотриманні загальних правил обслуговування карток, які входять у систему емітентів, проведення взаєморозрахунків і платежів. Ці правила охоплюють і суто технічні аспекти операцій із картками – стандарти даних, процедури авторизації, специфікації на устаткування, яке використовується, і фінансові сторони обслуговування карток – процедури розрахунків із підприємствами торгівлі та сервісу, що входять до складу прийомної мережі, правила взаєморозрахунків між банками, тарифи і т. д.

Отже, з організаційного погляду, ядром платіжної системи є заснована на договірних зобов'язаннях асоціація банків. До складу платіжної системи також уходять підприємства торгівлі й сервісу, що утворюють мережу точок обслуговування. Для успішного функціонування платіжної системи необхідні й спеціалізовані нефінансові організації, що здійснюють технічну підтримку обслуговування карток: процесингові та комунікаційні центри, центри технічного обслуговування тощо.

Платіжні системи певним чином є замінником розрахунків готівкою при здійсненні платежів. Відтак платіжну систему можна розглядати і як систему, за допомогою якої здійснюються електронні розрахунки між організаціями та користувачами задля купівлі-продажу товарів і послуг, у

тому числі й через інтернет. Якщо вивчати платіжну систему з цього боку, то здійснення незаконних дій із різними засобами доступу до банківських рахунків можливе через використання самої платіжної системи.

В умовах формування ринкової економіки найбільш поширеною формою розрахунків є переказ, який реалізується за допомогою різних платіжних інструментів. У ст. 1.31 озазначеного вище Закону термін «платіжний інструмент» визначено так: це засіб певної форми на паперовому, електронному чи іншому носії інформації, який використовується для ініціювання переказів. До платіжних інструментів належать документи на переказ та електронні платіжні засоби.

Статтею 200 ККУ установлено, що одним із предметів цього злочину є документ на переказ, який у кримінальному праві слід розуміти як документ у паперовому або електронному вигляді, що використовується банками чи їх клієнтами для передачі доручень або інформації на переказ грошових коштів між суб'єктами переказу грошових коштів (розрахункові документи, документи на переказ готівкових коштів, а також ті, що використовуються при проведенні міжбанківського переказу та платіжного повідомлення, інші). Документ на переказ, згідно зі ст. 1.6 Закону «Про платіжні системи та переказ коштів в Україні» – це електронний або паперовий документ, що використовується суб'єктами переказу, їх клієнтами, кліринговими, еквайринговими установами або іншими

установами – учасниками платіжної системи для передачі доручень на переказ коштів. У ст. 16.1 Закону вказано, що до документів на переказ належать розрахункові документи, документи на переказ готівки, міжбанківські розрахункові документи, клірингові вимоги та інші документи, що використовуються в платіжних системах для ініціювання переказу.

Стаття 1.14 Закону «Про платіжні системи та переказ коштів в Україні» визначає термін «електронний платіжний засіб» як платіжний інструмент, який надає його держателю можливість за допомогою платіжного пристрою отримати інформацію про належні держателю кошти та ініціювати їх переказ. Стаття 14.1 встановлює, що електронний платіжний засіб може існувати в будь-якій формі, на будь-якому носії, що дає змогу зберігати інформацію, необхідну для ініціювання електронного переказу.

З контексту статей 1.19-3 та 1.27 Закону випливає, що до електронних платіжних засобів законодавець відносить мобільний платіжний інструмент (електронний платіжний засіб, реалізований в апаратно-програмному середовищі мобільного телефону або іншого бездротового пристрою користувача) та платіжну картку (електронний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу коштів із рахунка платника або з відповідного рахунка банку з метою оплати вартості

товарів і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором). Платіжна картка також є предметом злочину, зазначеним у ст. 200 ККУ, поняття якої в кримінальному праві не має.

Статтею 200 ККУ до предметів злочину віднесено також і електронні гроші. Однак роз'яснення цього терміна в кодексі також відсутнє. У ст. 15.1 Закону України «Про платіжні системи та переказ коштів в Україні» визначено термін електронні гроші – одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі.

Обладнання для виготовлення платіжних карток, документів на переказ, інших засобів доступу до банківських рахунків, згадане в назві ст. 200, не є предметом коментованого злочину, оскільки згадка про таке обладнання в тексті статті відсутня. Проте придбання або приготування означеного обладнання для виготовлення підроблених предметів даного злочину слід кваліфікувати як готування до його вчинення.

Об'єктивний бік злочину полягає в: 1) підробці; 2) придбанні; 3) зберіганні; 4) перевезенні; 5) пересиланні; 6) використанні чи 7) збуті означених вище предметів.

Підробкою предметів даного злочину є будь-які дії, внаслідок яких створюються підроблені документи на переказ, платіжні картки чи інші засоби доступу до банківських рахунків, у т. ч. і фальсифікація відповідних справжніх предметів, якщо після вчинення цих дій із застосуванням підроблених предметів можуть бути проведені незаконні (ініційовані не власником рахунку або не забезпечені наявністю грошей на банківському рахунку) перекази грошових коштів або ж доступ до інформації щодо певного банківського рахунку отримує неуповноважена на це особа. Підроблення може бути здійснене за допомогою спеціального технічного обладнання, комп'ютерних програмних засобів або в будь-який інший спосіб (дописка, підчистка, виправлення у паперових документах тощо).

Виготовлення предмета, який лише своїми зовнішніми ознаками нагадує розрахункову картку й реально не може бути використаний для одержання доступу до певного банківського рахунку чи до інформації про такий рахунок (наприклад, унаслідок відсутності необхідного для цього електронного пристрою), не містить складу злочину, передбаченого ст. 200.

Деякі з документів на переказ, що є предметом даного злочину, можуть існувати не лише в паперовій, а й в електронній формі. Оскільки такі електронні документи мають певні індивідуальні реквізити, за якими вони розпізнаються адресатом, цілком можливою є їх підроблення через утручання в роботу відповідних комп'ютерних систем чи мереж.

У цих випадках дії винної особи треба визнавати сукупністю злочинів і кваліфікувати за статтями 200 та 361.

Поняття придбання, зберігання, перевезення, пересилання, збуту, вжиті у цій статті, за своїм змістом збігаються з аналогічними поняттями, застосованими у ст. 199. Під використанням підроблених документів на переказ чи платіжних карток слід розуміти пред'явлення їх як справжніх задля здійснення незаконного переказу грошових коштів, незаконного доступу до інформації щодо відповідного банківського рахунка тощо. Використанням підробленої платіжної картки слід вважати також спробу отримання з її допомогою грошових коштів через банківський автомат, здійснення з її застосуванням оплати товарів чи послуг.

Якщо внаслідок використання зазначених у цій статті підроблених предметів особа, яка їх використала, заволодіває чужими грошовими коштами, вчинене слід кваліфікувати як сукупність злочинів за відповідними частинами статей 190 і 200.

Про поняття збуту див. ст. 199.

Злочин, залежно від способу, є закінченим з моменту вчинення однієї із перелічених у ч. 1 ст. 200 дій.

Суб'єкт злочину загальний.

Суб'єктивний бік злочину характеризується прямим умислом. У випадках придбання, зберігання, перевезення, пересилання відповідних предметів злочину обов'язковою ознакою суб'єктивного боку злочину є мета їх збуту.

Кваліфікуючими ознаками злочину є вчинення його: 1) повторно; 2) за попередньою змовою групою осіб.

Підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів (ст. 358 ККУ)

Безпосереднім об'єктом злочину є суспільні відносини, що регулюють виготовлення, збут та використання документів у різних сферах діяльності людини, а саме документообіг у державі.

Предметом злочину може бути підроблення посвідчення, офіційного документа, печаток, штампів чи бланків.

Посвідчення розуміють як документ, що містить відомості про володільця і офіційно посвідчує його особу та (або) правовий статус. Необхідними реквізитами посвідчення, зазвичай, є фотографія, підпис керівника відповідної установи, підприємства чи організації, який скріплюється їхньою печаткою, а також особистий підпис володільця документа (посвідчення: тимчасове посвідчення громадянина України, особи моряка, інваліда, водія, учасника ліквідації аварії на ЧАЕС, пенсійне, судді або працівника правоохоронного органу, біженця, ветерана війни).

Бланк – макет документа у вигляді паперового листа, що містить елементи фірмового стилю або інформацію постійного характеру (накладні, акти, листи тощо); призначений для подальшого заповнення та внесення записів у відведені місця від руки або машинним способом.

Об'єктивний бік цього злочину характеризується наявністю обов'язкової ознаки, а саме: суспільно небезпечного діяння. При цьому це діяння проявляється у формі активної дії. У диспозиції норми ця дія закріплена як підроблення посвідчення або іншого офіційного документа або збут такого документа, а також виготовлення підроблених печаток, штампів чи бланків або їх збут.

Під *підробленням* розуміють: а) повне виготовлення фальшивого документа, схожого на справжній (відтворення і матеріальної форми, і змісту носія інформації); б) часткова фальсифікація: внесення у справжній із точки зору форми документ неправдивих відомостей (наприклад бездоганно оформлений листок тимчасової непрацездатності, виданий завідомо здоровій людині); в) зміна змісту або характеру документа через механічні маніпуляції (дописування, підтирання, підчистка, витравлення тексту тощо); г) підроблення відбитків штампу, печатки як необхідного реквізиту документа. Часткова фальсифікація (т. зв. переробка) перекручування істини відбувається через унесення в документ неправдивих відомостей (виправлення, внесення фіктивних записів, знищення частини тексту, витравлення, підчистка, змивання, підроблення підпису, переклеювання фотографії, проставлення на документі відбитка підробленої печатки тощо).

Збут розуміють як будь-яке сплатне чи безоплатне відчуження цих предметів та запускання їх в обіг (продаж, обмін, дарування, передача в рахунок погашення боргу тощо).

Виготовлення підроблених штампів, бланків або печаток розуміють як повне виготовлення сфальсифікованих форм-кліше і бланків, а також внесення змін у справжні штампи, печатки або бланки, що спотворює належний зміст їх реквізитів. Способом такого виготовлення може бути вирізання на гумі, лінолеумі, шкірі, дереві або гравіювання на м'яких металах.

Злочин уважається закінченим із моменту вчинення суспільно небезпечної дії і носить при цьому формальний характер.

Суб'єктом злочину є фізична осудна особа, яка досягла 16-річного віку.

Суб'єктивний бік цього злочину характеризується виною у формі прямого умислу. Законодавець чітко окреслив *обов'язкову мету* ч. 1 ст. 358 ККУ – подальше використання цього документа або його збут.

Мета *використання* підробленого документа означає прагнення винного отримати певні права або звільнитись від обов'язків і має конкретний характер (приховати шлюб або судимість, збільшити стаж роботи за спеціальністю, влаштуватись на певну посаду, вступити до вузу тощо).

Мету *збуту* слід розуміти як бажання досягти будь-якої форми реалізації (оплатної чи безоплатної) підробленого документа (продаж, дарування, обмін, сплата боргу, позика тощо).

Об'єктивний бік ч. 2 ст. 358 ККУ характеризується наявністю обов'язкової ознаки, а саме: суспільно небезпечного діяння – складання чи видача завідомо підроблених офіційних документів, виго-

товлення підроблених офіційних печаток, штампів чи бланків або їх збут чи збут завідомо підроблених офіційних документів, у тому числі особистих документів особи.

При цьому суспільно небезпечне діяння виступає у формі активної дії.

Суспільно небезпечна дія проявляється в таких формах:

– виготовлення підроблених печаток, штампів чи бланків;

– збут підроблених печаток, штампів чи бланків;

– складання завідомо підроблених офіційних документів;

– видача завідомо підроблених офіційних документів.

Складання розуміють як унесення до документа, який зовні оформлено правильно, відомостей, що не відповідають дійсності повністю або частково (наприклад запис у дійсний бланк, який має відтиск печатки і підпис, неправдивих відомостей про фактичне використання сировини та матеріалів).

Видачу розуміють як надання або випуск документів, зміст яких повністю або частково не відповідає дійсності та які були складені цією ж або іншою особою (наприклад надання певним суб'єктам підприємницької діяльності завідомо фіктивних документів задля приховування їх діяльності, або випуск фіктивних ліцензій, патентів з метою їх подальшого продажу тощо).

Злочин вважається закінченим із моменту вчинення суспільно небезпечної дії і носить при цьому формальний характер.

Суб'єкт ч. 2 ст. 358 ККУ – спеціальний, норма передбачає складання чи видачу завідомо підроблених офіційних документів *працівником юридичної особи* будь-якої форми власності, який не є службовою особою, приватним підприємцем, аудитором, експертом, оцінювачем, адвокатом або іншою особою, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг.

Працівником юридичної особи будь-якої форми власності, який не є службовою особою, вважається особа, що є членом трудового колективу та бере участь у трудовому процесі, тобто працює за певним фахом і при цьому не наділена повноваженнями службової особи. Юридичну особу Цивільний кодекс України розуміє як організацію, що створена і зареєстрована у встановленому законом порядку (ст. 80 ЦК України).

Приватний підприємець – це громадянин України або іншої країни, який має законодавчо встановлене право на здійснення підприємницької діяльності. Тобто підприємцем вважається громадянин України, або іншої країни, який законодавчо не обмежений у правоздатності або дієздатності та зареєстрований належним чином в органах державної влади.

Аудитором може бути фізична особа, яка має сертифікат, що визначає її кваліфікаційну придатність на заняття аудиторською діяльністю на території України (ст. 4 Закону України «Про аудиторську діяльність»).

При цьому аудиторську діяльність розуміють як підприємницьку діяльність, яка включає в себе

організаційне й методичне забезпечення аудиту, практичне виконання аудиторських перевірок (аудит) та надання інших аудиторських послуг. Що ж до аудиту, то це перевірка даних бухгалтерського обліку й показників фінансової звітності суб'єкта господарювання задля висловлення незалежної думки аудитора про її достовірність в усіх суттєвих аспектах та відповідність вимогам законів України, положень (стандартів) бухгалтерського обліку або інших правил (внутрішніх положень суб'єктів господарювання) згідно з вимогами користувачів.

Експерт – компетентна особа, яка має відповідну освіту, кваліфікацію, науковий або практичний досвід, володіє спеціальними знаннями тощо.

Водночас, положення ч. 1 ст. 66 Кодексу адміністративного судочинства України визначають, що експертом є особа, яка має необхідні знання та якій у порядку, встановленому цим кодексом, доручається дати висновок із питань, що виникають під час розгляду справи і стосуються спеціальних знань цієї особи, через дослідження матеріальних об'єктів, явищ і процесів, що містять інформацію про обставини у справі.

Оцінювач – це громадяни України, іноземці та особи без громадянства, які склали кваліфікаційний іспит, одержали кваліфікаційне свідоцтво оцінювача та здійснюють оціночну діяльність, що полягає в організаційному, методичному та практичному забезпеченні проведення оцінки майна, розгляді та підготовці висновків щодо вартості майна (Закону України «Про оцінку майна, май-

нових прав та професійну оціночну діяльність в Україні»).

Адвокат – це фізична особа, яка здійснює адвокатську діяльність на підставах та в порядку, що передбачені Закону України «Про адвокатуру та адвокатську діяльність». При цьому адвокатську діяльність розуміють як незалежну професійну діяльність адвоката щодо здійснення захисту, представництва та надання інших видів правової допомоги клієнту.

Положення зазначеного вище закону наголошують на тому, що адвокатом може бути фізична особа, яка має повну вищу юридичну освіту, володіє державною мовою, має стаж роботи в галузі права не менше двох років, склала кваліфікаційний іспит, пройшла стажування (крім випадків, встановлених законом), склала присягу адвоката України та отримала свідоцтво про право на заняття адвокатською діяльністю (ст. 6 Закону України «Про адвокатуру та адвокатську діяльність»).

Інша особа, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг. Для того, щоб визначити зміст цього суб'єкта злочину, потрібно спочатку усвідомити що законодавець має на увазі під професійною діяльністю, пов'язаною з наданням публічних послуг.

Відповідно до положень Концепції розвитку системи надання адміністративних послуг органами виконавчої влади, послуги, що надаються органами державної влади, органами місцевого самоврядування, підприємствами, установами, органі-

заціями, які перебувають в їх управлінні, становлять сферу публічних послуг.

Частина 3 ст. 358 ККУ передбачено відповідальність за «дії, передбачені частинами першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб».

Об'єктивна сторона ч. 4 ст. 358 ККУ цього злочину характеризується наявністю обов'язкової ознаки, а саме: суспільно небезпечного діяння. При цьому дане діяння проявляється у формі активної дії. У диспозиції норми ця дія закріплена використання завідомо підробленого документа.

Використання завідомо підробленого документа, може бути вчинене одним із двох способів: 1) пред'явлення документа; 2) подання документа.

При пред'явленні документа суб'єкт, видаючи підробку за справжній документ, ознайомлює із його змістом інших осіб. При цьому підроблений документ залишається у володінні винного (наприклад пред'явлення підробленого посвідчення водія працівникові ДАІ).

Подання документа також передбачає, що певне коло осіб ознайомлюється зі змістом підробленого документа. Але підробка не залишається у винного, а передається уповноваженим особам для посвідчення тих чи тих фактів задля отримання прав або звільнення від обов'язків (наприклад особа подає на підприємство підроблений документ про закінчення вищого закладу освіти для того, щоб зайняти певну посаду).

Злочин уважається закінченим із моменту вчинення суспільно небезпечної дії.

6.3. Питання кваліфікації легалізації (відмивання) доходів, одержаних злочинним шляхом (ст. 209 ККУ)

У результаті вчинення кіберзлочинів часто отримуються великі суми грошей та отримується інше майно, а тому слід знати особливості кваліфікації цього злочину.

Основний безпосередній об'єкт злочину – встановлений задля протидії залученню в економіку «брудних» коштів порядок здійснення господарської діяльності, а також порядок учинення цивільно-правових угод в частині особистого та іншого подібного використання майна, не пов'язаного з господарською діяльністю. Додатковий об'єкт – інтереси правосуддя, нормальне функціонування фінансово-кредитної системи, засади добросовісної конкуренції.

Предмет злочину – кошти та інше майно, одержане внаслідок учинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів, а також права на кошти та майно.

Кошти та інше майно виступають предметом легалізації за умови, що вони раніше були одержані через учинення суспільно небезпечного діяння, що передувало легалізації (відмиванню) доходів, тобто предикатного діяння. Останнім може бути: діяння, за яке Кримінальним кодексом України передбачено основне покарання у вигляді позбавлення волі або штрафу понад три тисячі неоподат-

ковуваних мінімумів доходів громадян; та/або діяння, вчинене за межами України, якщо воно визнається суспільно небезпечним протиправним діянням, що передувало легалізації (відмиванню) доходів, за кримінальним законом держави, де воно було вчинене, і є злочином за Кримінальним кодексом України та внаслідок вчинення якого незаконно одержані доходи.

Об'єктивна сторона злочину може виражатися в одній із чотирьох альтернативних форм: 1) учинення фінансової операції з коштами або іншим майном, одержаними внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів; 2) вчинення правочину з коштами або іншим майном, одержаними внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів; 3) учинення дій, спрямованих на приховання чи маскування незаконного походження таких коштів або іншого майна, володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження або переміщення; 4) набуття, володіння або використання коштів чи іншого майна, одержаних унаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів.

Фінансова операція – будь-яка операція, пов'язана зі здійсненням або забезпеченням здійснення платежу за допомогою суб'єкта первинного фінансового моніторингу. До вчинення фінансової операції з коштами або іншим майном, одержаними

внаслідок учинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів належать: унесення або зняття депозиту (внеску, вкладу); переказ грошей із рахунку на рахунок; обмін валюти; надання послуг із випуску, купівлі або продажу цінних паперів та інших видів фінансових активів; надання або отримання позики або кредиту; страхування (перестрахування); надання фінансових гарантій та зобов'язань; довірче управління портфелем цінних паперів; фінансовий лізинг; здійснення випуску, обігу, погашення державної та іншої грошової лотереї; надання послуг із випуску, купівлі, продажу й обслуговування чеків, векселів, платіжних карток та інших платіжних інструментів; відкриття рахунку. Фінансова операція може здійснюватися за допомогою будь-якого суб'єкта господарювання.

Поняття «*правочин*» охоплює дії фізичних і юридичних осіб, спрямовані на набуття, зміну або припинення цивільних прав та обов'язків (ст. 202 ЦК України). Це різноманітні договори: купівлі-продажу, позики, доручення, комісії, страхування, схову, перевезення, про сумісну діяльність тощо.

Учинення дій, спрямованих на приховання чи маскування незаконного походження таких коштів або іншого майна, володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження або переміщення – це активні дії, спрямовані на те, щоб унеможливити або ускладнити встановлення факту одержання коштів або іншого майна внаслідок вчинення предикат-

ного діяння, приховати чи замаскувати «справжній характер» майна. Вони можуть полягати у: зміні правового статусу коштів або іншого майна через підроблення документів, що засвідчують право власності; отриманні фіктивних документів на придбання майна; вчиненні цивільно-правових угод (удавана купівля у комісійному магазині, ломбарді тощо); оформленні права власності на підставних осіб; укладенні фіктивних угод про надання кредитів або різноманітних послуг (юридичних, аудиторських, маркетингових); унесенні коштів на банківські рахунки юридичних і фізичних осіб, у т. ч. в офшорних зонах; переміщенні коштів з одного рахунку на інший (за умови, що всі зазначені дії не були способом вчинення предикатного діяння).

Набуття коштів чи іншого майна, одержаних внаслідок вчинення злочину, що передував легалізації доходів – це отримання такого майна винною особою, яка усвідомлює його відповідне походження, тим чи тим оплатним або безоплатним способом (купівля, отримання в обмін на інші предмети, прийняття як оплати за надані послуги або виконану роботу, одержання як подарунка або як оплати боргу тощо).

Володіння коштами чи іншим майном, одержаним внаслідок учинення злочину, що передував легалізації доходів означає фактичне перебування такого майна в особи, яка має можливість впливати на нього. Володіти майном може і його власник, і інші особи. На відміну від укладання угоди, набуття і володіння таким майном здійснюється за

недійсними правочинами, якими одержанню такого майна або володінню ним надається правомірний вигляд.

Використання коштів чи іншого майна, одержаних унаслідок учинення злочину, що передував легалізації (відмиванню) доходів – це вилучення в будь-якій формі корисних властивостей таких коштів чи майна для задоволення потреб власника або інших осіб. Наприклад: унесення коштів як внеску у статутний фонд підприємства, створення фіктивних господарюючих суб'єктів, купівля підприємств із великими обсягами готівкових надходжень, де складно встановити фактичний обсяг проданих товарів, наданих послуг, виконаних робіт (роздрібна торгівля, сфера обслуговування, громадське харчування, гральні й розважальні заклади тощо), придбання підприємств за кордоном із використанням громадянина іноземної держави як фіктивного власника, виплата дивідендів і заробітної плати, поповнення обігових коштів суб'єкта господарювання, використання під час здійснення виробничої діяльності викраденого обладнання.

Суб'єкт злочину – фізична осудна особа, яка досягла 16 років. Особа, яка вчинила предикатне діяння, може бути суб'єктом цього злочину в різних його формах, крім набуття та володіння, а за використання коштів чи іншого майна відповідає лише в разі, якщо воно полягало у вчиненні фінансової операції чи укладенні угоди. За ст. 209 ККУ також може нести відповідальність особа, яка не вчиняла предикатного діяння, але вчинила одне з альтернативних, указаних у ч. 1 цієї статті.

Суб'єктивний бік злочину – прямий умисел, який характеризується усвідомленням винним злочинного походження предмета легалізації. Обов'язковою ознакою суб'єктивної сторони злочину є *мета легалізації* – надання правомірного вигляду володінню, користуванню і розпорядженню предметами, зазначеними у ст. 209 ККУ, або приховання чи маскування їх незаконного походження, володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження, переміщення.

Частиною 2 ст. 209 ККУ передбачено відповідальність за «дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або у великому розмірі».

Легалізація (відмивання) доходів, одержаних злочинним шляхом, визнається вчиненою в *великому розмірі*, якщо предметом злочину були кошти або інше майно на суму, що перевищує шість тисяч НМДГ.

Частиною 3 ст. 209 ККУ передбачено відповідальність за «дії, передбачені частинами першою або другою цієї статті, вчинені організованою групою або в особливо великому розмірі».

Легалізація (відмивання) доходів, одержаних злочинним шляхом, визнається вчиненою у *особливо великому розмірі*, якщо предметом злочину були кошти або інше майно на суму, що перевищує вісімнадцять тисяч НМДГ.

У багатьох випадках перед органами розслідування постає завдання доказування факту використання конкретного комп'ютера для доступу до

інтернет-ресурсів. Така потреба, зокрема, виникає, коли для з'єднання із глобальною мережею використовувалася динамічна IP-адреса, яка могла бути надана необмеженому колу осіб (наприклад, при використанні безпровідного з'єднання Wi-Fi або при підключенні до мережі через засоби стільникового зв'язку тощо). У таких випадках слід відстежувати MAC-адресу комп'ютера зловмисника. MAC-адреса або фізична адреса комп'ютера – це незмінний ідентифікаційний номер пристрою, за допомогою якого здійснюється з'єднання з мережею.

Слід відзначити, що при вчиненні злочинів означеної категорії для зашифровки схеми руху коштів зловмисниками використовуються віртуальні трансферні системи, такі як «Webmoney», «E-passport», «Yandex-деньги» та інші. Для цього злочинці відкривають власні інтернет-гаманці через створення облікових записів в адміністраторів систем. Номер інтернет-гаманця, зазвичай, не приховується. Він може міститися в рекламному оголошенні, на сайті інтернет-крамниці або повідомлятися в ході спілкування з покупцями.

Номер гаманця дає змогу отримати деяку інформацію про його власника і відомості, які в подальшому можна використати в суді як докази діяльності підозрюваного.

Оператор трансферної системи, зазвичай, має відомості про програмне забезпечення, яким клієнт користується для здійснення операцій із гаманців.

Такі клієнтські програми є специфічними та можуть завантажуватися на комп'ютер користу-

вача зі сайтів оператора. Відповідна інформація також може бути надана оператором за запитом і матиме доказове значення після вилучення комп'ютерної техніки, яка використовувалася для вчинення злочину, та проведення комп'ютерно-технічної експертизи.

Отримана інформація в подальшому дасть змогу з'ясувати додаткові відомості про фігуранта: встановити його особу та місце проживання, номер мобільного телефону, комп'ютер, який використовується для з'єднання з інтернетом. У деяких випадках для підтвердження сертифікатів представники трансферних систем вимагають від клієнтів надання копій документів, які підтверджують особу (найчастіше паспорта), отже є вірогідність отримання за запитом повних паспортних даних власника інтернет-гаманця.

Як уже зазначалося, відомості про осіб, які представляють оперативний інтерес, можливо отримати через елементарне використання пошукових систем. У поле пошуку рекомендується вводити будь-які ідентифікуючі дані об'єкта: номери телефонів, гаманців, облікових записів інтернет-пейджерів, електронні та поштові адреси, прізвища або вигадані для спілкування в мережі імена, назви суб'єктів підприємницької діяльності тощо.

Серед інтернет-ресурсів, на яких може міститися інформація, що становить оперативний інтерес, слід визначити такі: сайти, які відкрито пропонують послуги сексуального характеру за гроші або роблять це завуальовано: під виглядом масажних салонів, VIP-відпочинку, ескорт-послуг тощо;

вебсторінки з дошками оголошень незалежно від спеціалізації («куплю», «продам», «пропоную роботу» і т. д.) або регіональної спрямованості; форуми різноманітної тематики; соціальні мережі; сайти знайомств, на яких розміщуються анкети користувачів.

Щоб закріпити процесуальне значення інформації, здобутої під час проведення розшукових заходів, потрібно належним чином оформити документи про отримання та фіксацію інформації. За наявності відкритого доступу до змісту сайту, слід оформити протокол огляду в присутності понятих із застосуванням відеозапису або програм, які фіксують зображення, що виводиться на екран. У разі використання програм «SnagIt», «Camtasia» отримані відомості потрібно записати на оптичний носій без можливості перезапису (CD-R) та долучити диск до протоколу як додаток.

У сучасних умовах фінансовим компаніям потрібно використовувати комплекс програмних і апаратних засобів, які б дали змогу забезпечити високий рівень захищеності інфраструктури зі збереженням достатньої ефективності бізнес-процесів. Для запобігання атакам ефективними є методи соціальної інженерії – це регулярне інструктування всіх співробітників компанії безпечній роботі в інтернет-мережі та інформування їх про наявні види загроз. Користування послугами сторонніх компаній, які спеціалізуються на захисті даних від DDoS-атак, підключившись до хмарних сервісів організації. Сайтам, яким найбільше загрожують

кібератаки, варто піклуватися про рівень захищеності своїх систем. Варто згадати, що найнебезпечніші сайти розроблені на мові PHP, оскільки 75 % із них містять критичні вразливості. Більш захищеними виявилися вебресурси на ASP.NET (55 %) та Java (70 %) (згідно з інформацією компанії Positive Technologies).

Адміністратори корпоративної мережі організації мають контролювати, які вебсайти їх співробітники відвідують і якими програмними забезпеченнями користуються. Зовнішні ресурси повинні мати дійсні SSL сертифікати.

На цьому етапі розвитку сфери інтернет-банкінгу в Україні системи захисту не досить розвинуті та захищені від кібератак. Для забезпечення уникнення усіляких ризиків, службам безпеки банків потрібно захистити не тільки бази даних і робоче обладнання персоналу, а також і комп'ютерні мережі, термінали працівників фронт-офісу та банкомати від дій кіберзлочинців. Основною ціллю українських спеціалістів із кібербезпеки має стати захист своїх клієнтів, адже зарубіжні конкуренти у XXI ст. задають високу планку у цій сфері.

Основні поняття

Перевезення полягає в переміщенні їх транспортом (наземним, водним, повітряним) з одного місця в інше і в межах території України, і за цими межами.

Пересилання – переміщення зазначених предметів через відправлення поштою, багажем, посильним або іншим способом з одного місця в інше без супроводження особи, котра здійснює пересилання.

Ввезенням в Україну треба визнавати переміщення підробок через державний кордон України на її територію з використанням будь-яких транспортних засобів.

Збут – оплатне або безоплатне умисне відчуження підроблених грошей, державних цінних паперів і білетів державної лотереї, марок акцизного збору, голографічних захисних елементів незалежно від способу (продаж, обмін, дарування, передача в борг, у рахунок погашення боргу тощо). Вважається *закінченим* з моменту збуту хоча б одного предмету злочину.

Контрольні завдання

1. Сформулюйте кваліфікацію кіберзлочинів пов'язаних зі змістом.

2. Назвіть кваліфікацію кіберзлочинів при вчиненні яких ІТТ використовуються як засоби вчинення злочинів.

3. Сформулюйте питання кваліфікації легалізації (відмивання) доходів, одержаних злочинним шляхом (ст. 209 ККУ).

Підсумкові тестові завдання

1. Назвіть родовий об'єкт несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України).

A) суспільні відносини щодо охорони інших особистих прав і свобод людини і громадянина;

B) суспільні відносини щодо охорони прав на об'єкти права інтелектуальної власності;

C) суспільні відносини у сфері здійснення господарської діяльності та іншої діяльності, пов'язаної з наданням інформаційних послуг;

D) суспільні відносини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку.

Відповідь: D

2. Що слід розуміти під значною шкодою як кваліфікуючою ознакою несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України)?

A) матеріальні збитки, що в десять і більше разів перевищують установлений законодавством розмір мінімальної заробітної плати;

B) матеріальні збитки, що в сто і більше разів перевищують неоподаткованих мінімумів доходів громадян;

C) матеріальні збитки, що у двісті п'ятдесят і більше разів перевищують установлений законодавством розмір мінімальної заробітної плати;

D) такої кваліфікуючої ознаки, як значна шкода, для злочину, про який йдеться в питанні, законом не передбачено.

Відповідь: B

3. Якою є форма вини в порушенні правил експлуатації електроннообчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України)?

A) умисна форма вини;

B) необережна форма вини;

C) умисна або необережна форма вини;

D) складна (подвійна) форма вини.

Відповідь: B

4. Хто є суб'єктом створення задля використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збуту (ст. 361-1 КК України)?

A) фізична осудна особа, яка досягла шістнадцяти років;

B) громадянин України, який постійно не проживає в Україні;

C) працівник підприємства, установи, організації незалежно від форми власності;

D) службова особа підприємства, установи, організації або громадянин – суб'єкт підприємницької діяльності.

Відповідь: A

5. Якою є суб'єктивний бік перешкоджання роботі електроннообчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку через масове розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України)?

A) умисна форма вини, мотиви й цілі для кваліфікації злочину значення не мають;

B) необережна форма вини, корисливий мотив, цілі для кваліфікації злочину значення не мають;

C) умисна форма вини, корисливий мотив, цілі для кваліфікації злочину значення не мають;

D) необережна форма вини, мотиви для кваліфікації злочину значення не мають, ціль наживи.

Відповідь: A

6. Метою, яка передбачена в КК України як ознака суб'єктивного боку зловживання владою або службовим становищем (ст. 364 КК України), є:

A) одержання будь-якої неправомірної вигоди;

B) уникнення відповідальності за вчинення правопорушення;

C) розтрата державних коштів в особливо великих розмірах;

D) зайняття незаконними видами підприємницької діяльності.

Відповідь: A

7. Службовими особами слід вважати таких, які тимчасово чи за спеціальним повноваженням здійснюють наступні функції:

A) інформаційні;

B) організаційно-розпорядчі;

C) технічні;
D) інноваційні.
Відповідь: B

8. Відповідно до цілей, зазначених у статтях 364, 368, 368-2 та 369 КК України до державних та комунальних підприємств прирівнюються юридичні особи, у статутному фонді яких державна чи комунальна частка перевищує:

A) п'ятдесят відсотків;
B) двадцять п'ять відсотків;
C) сімдесят п'ять відсотків;
D) тридцять три відсотки.
Відповідь: A

9. Ознакою об'єктивного боку перевищення влади або службових повноважень працівником правоохоронного органу (ст. 365 КК України) є:

A) неправильне застосування норм матеріального права;
B) неправильне застосування норм процесуального права;
C) завдання істотної шкоди охоронюваним інтересам;
D) несумлінне виконання службових обов'язків.
Відповідь: C

10. До об'єктивного боку службового підроблення (ст. 366 КК України) належить:

A) незаконний випуск банкнот в обіг;
B) незаконні операції з цінними паперами;
C) унесення до документації неправдивих даних;
D) шахрайство з фінансовими ресурсами.
Відповідь: C

11. Відповідно до ст. 366-1 КК України («Декларування недостовірної інформації») суб'єктами цього злочину є:

A) будь-які посадовці юридичних осіб приватного права;

B) політичні та громадські діячі в Україні та за її межами;

C) особи, уповноважені на виконання функцій місцевого самоврядування;

D) діячі науки, культури та спорту.

Відповідь: С Д

12. Службовими особами слід уважати таких, які тимчасово чи за спеціальним повноваженням здійснюють такі функції:

A) інформаційні;

B) організаційно-розпорядчі;

C) технічні;

D) інноваційні.

Відповідь: B

13. Відповідно до цілей, які зазначені в статтях 364, 368, 368-2 та 369 КК України до державних та комунальних підприємств прирівнюються юридичні особи, у статутному фонді яких державна чи комунальна частка перевищує:

A) п'ятдесят відсотків;

B) двадцять п'ять відсотків;

C) сімдесят п'ять відсотків;

D) тридцять три відсотки.

Відповідь: A

14. До чого за кримінально-правовим змістом близька сукупність злочинів?

A) повторності однорідних злочинів;

B) повторності різнорідних злочинів;

C) повторності тотожних злочинів;

D) рецидиву злочинів.

Відповідь: B

15. Як мають кваліфікуватися злочини, що утворюють сукупність?

A) усі злочини кваліфікуються з посиланням на статтю Загальної частини КК України, якою передбачене поняття сукупності злочинів (ст. 33);

B) усі злочини, що входять до сукупності, кваліфікуються один раз за відповідною статтею (частиною статті) Особливої частини КК України;

C) кожен злочин, що входить до сукупності, кваліфікується окремо за відповідною статтею (частиною статті) Особливої частини КК України;

D) усі закінчені злочини кваліфікуються один раз за відповідною статтею (частиною статті) Особливої частини КК України, усі незакінчені злочини самостійно не кваліфікуються;

Відповідь: C

16. Що є видами множинності злочинів?

A) продовжувані злочини, триваючі, складні;

B) рецидив, загальний рецидив, спеціальний рецидив;

C) повторність, сукупність, рецидив;

D) неоднократність, систематичність, злочинний промисел.

Відповідь: C

17. Який злочин не є видом складного одиничного злочину?

A) матеріальний;

B) продовжуваний;

C) триваючий;

D) складений.

Відповідь: A

18. Чим визнається злочин, який складається з двох або більше тотожних діянь, об'єднаних єдиним злочинним наміром?

A) повторюваним злочином;

B) складеним злочином;

C) триваючим злочином;

D) продовжуваним злочином.

Відповідь: D

19. У якому випадку має місце одиничний злочин?

A) він учинений однією особою;

B) він передбачений КК України як самостійний склад злочину;

C) склад такого злочину містить лише одну кваліфікуючу ознаку;

D) у санкції статті Особливої частини КК України за нього передбачено один вид покарання.

Відповідь: B

20. Що є множинністю злочинів?

A) учинення особою двох або більше злочинів, за які вона не була засуджена;

B) скоєння особою двох або більше одиничних злочинів, якщо хоч два з них мають юридичне значення;

C) учинення двома особами двох або більше злочинів за умови засудження за попередній злочин;

D) учинення двома особами двох або більше злочинів за умови відсутності засудження за попередній злочин.

Відповідь: B

21. У якому випадку ідеальна сукупність має місце?

A) злочин вчинено спільними зусиллями декількох осіб;

B) одним діянням учинено два або більше злочинів;

C) різними діяннями вчинено два або більше злочинів;

D) учинено декілька тотожних злочинних діянь, об'єднаних єдиним злочинним наміром.

Відповідь: B

22. Що є рецидивом злочинів?

A) учинення нового злочину особою, яка має судимість за тяжкий або особливо тяжкий злочин;

B) учинення нового злочину особою, яка визнана рецидивістом;

C) учинення нового злочину особою, яка раніше вчиняла злочин;

D) учинення нового умисного злочину особою, яка має судимість за умисний злочин.

Відповідь: D

23. Чим визнається вчинення особою двох або більше злочинів, передбачених різними статтями або різними частинами однієї статті Особливої частини КК України, за жоден із яких її не було засуджено?

A) повторністю злочинів;

B) сукупністю злочинів;

C) рецидивом злочинів;

D) складеним злочином.

Відповідь: B

24. У якому випадку повторність має місце?

A) якщо особу звільнили від кримінальної відповідальності за попередній злочин;

B) якщо особа в різний час скоїла такі злочини, як крадіжка (ст. 185 КК) та грабіж (ст. 186 КК);

C) якщо особа вчиняє злочин і адміністративне правопорушення;

D) якщо особа у різний час скоїла такі злочини, як крадіжка (ст. 185 КК) та умисне вбивство (ст. 115 КК).

Відповідь: B

25. У якому випадку має місце ідеальна сукупність?

A) якщо в кожному діянні, що утворює сукупність, є всі необхідні ознаки складу злочину;

B) якщо в одному діянні є ознаки двох або більше складів злочинів, передбачених різними частинами однієї і тієї ж статті;

C) якщо в одному діянні є ознаки двох або більше складів злочину, передбачених різними статтями КК України;

D) якщо в одному діянні, що утворює сукупність, є ознаки злочину та ознаки адміністративного проступку.

Відповідь: C

26. У якому випадку множинність злочинів має кримінально-правове значення?

A) при законодавчій дефініції складу злочину;

B) при кваліфікації вчинених злочинів кількома суб'єктами;

C) при призначенні покарання особі, яка вчинила декілька злочинів;

D) при звільненні від покарання.

Відповідь: C

27. Які із зазначених злочинів відносять до простих одиничних?

A) продовжувані;

B) триваючі;

C) злочини з альтернативними діями;

D) злочини з похідними наслідками.

Відповідь: C

28. Коли продовжуваний злочин слід вважати закінченим?

A) з моменту явки особи з повинною;

B) з моменту припинення злочинної діяльності;

C) з моменту здійснення останнього злочинного діяння, що становить продовжуваний злочин;

D) з моменту вчинення першого злочинного діяння, що становить продовжуваний злочин.

Відповідь: C

29. Коли відповідно до чинного Кримінального кодексу України замах на вчинення злочину вважається незакінченим?

A) якщо особа не довела до кінця суспільно небезпечне діяння (дію чи бездіяльність) із причин, які залежали від її волі;

B) якщо особа, яка вчинила суспільно небезпечне діяння (дію чи бездіяльність), фактично не

заподіяла істотної шкоди фізичній чи юридичній особі, суспільству або державі;

C) якщо особа виконала дії, що характеризують об'єктивну сторону злочину, а злочинні наслідки не настали, з причин, які були невідомі.

D) якщо особа з причин, що не залежали від її волі, не вчинила усіх дій, які вважала необхідними для доведення злочину до кінця.

Відповідь: D

30. Чим характеризується суб'єктивний бік готування до злочину або замаху на злочин?

A) умисною виною у вигляді прямого і непрямого умислу;

B) умисною виною;

C) умисною або необережною виною;

D) умисною виною у вигляді прямого умислу.

Відповідь: D

31. Що визнається відповідно до чинного Кримінального кодексу України закінченим злочином?

A) підшукання або пристосування засобів чи знарядь для вчинення злочину;

B) умисні дії, спрямовані на заподіяння шкоди потерпілому;

C) діяння, яке містить усі ознаки складу злочину, передбаченого відповідною статтею Особливої частини Кримінального кодексу України;

D) діяння, яке містить всі об'єктивні ознаки складу злочину.

Відповідь: C

32. Що є добровільною відмовою при незакінченому злочині?

A) припинення злочину за власною волею;

B) добровільне припинення особою злочинних дій;

C) остаточне припинення особою за своєю волею готування до злочину або замаху на злочин, якщо при цьому вона усвідомлювала можливість доведення злочину до кінця;

D) остаточне припинення особою суспільно небезпечних дій, передбачених Кримінальним кодексом України.

Відповідь: C

33. За яких умов можлива добровільна відмова на стадії закінченого замаху?

A) особа добровільно з'явилася із зізнанням до правоохоронних органів і повідомила про вчинений нею злочин;

B) між діянням і наслідком є певний проміжок часу, протягом якого особа може втрутитися в розвиток причинного зв'язку і перешкодити настанню суспільно небезпечних наслідків;

C) особа відмовилася від повторення спроби вчинити злочин;

D) наслідки не настали з причин, що не залежать від волі винного.

Відповідь: B

34. Що відповідно до чинного Кримінального кодексу України визнається замахом на злочин?

A) учинення особою з прямим умислом діяння (дії або бездіяльності), безпосередньо спрямованого на вчинення злочину, передбаченого відповідною статтею Особливої частини Кримінального кодексу України, якщо при цьому злочин не було доведено до кінця з причин, що не залежали від її волі;

B) умисна дія, безпосередньо спрямована на вчинення злочину, якщо при цьому злочин не було доведено до кінця з причин, що залежали від волі суб'єкта;

C) приведення предметів (засобів) у такий стан, щоб їх можна було використати для успішного виконання злочину в майбутньому;

D) пристосування знарядь чи засобів для вчинення злочину.

Відповідь: A

35. За готування до вчинення якого злочину особа не підлягає кримінальній відповідальності?

A) за готування до вчинення необережних злочинів;

B) за готування до злочинів, вчинених через злочинну недбалість;

C) за готування до вчинення злочинів невеликої тяжкості.

D) за готування до злочинів невеликої та середньої тяжкості.

Відповідь: C

36. Що є підставою виключення кримінальної відповідальності при добровільній відмові від злочину?

A) відмова від подальшої спроби вчинити злочин;

B) не доведення злочину до кінця;

C) остаточне припинення особою за своєю волею готування до злочину або замаху на злочин, якщо при цьому вона усвідомлювала можливість доведення злочину до кінця;

D) осуд особою вчиненого злочину.

Відповідь: C

37. Що є співучастю у злочині?

A) умисна спільна участь декількох осіб у вчиненні будь-якого злочину;

B) спільна участь декількох суб'єктів злочину у вчиненні злочину;

C) умисна спільна участь декількох суб'єктів злочину у вчиненні умисного злочину;

D) умисна спільна участь декількох суб'єктів злочину у вчиненні будь-якого злочину.

Відповідь: C

38. Чи можлива співучасть у вчиненні необережного злочину?

A) можлива завжди;

B) можлива, якщо цей злочин є тяжким чи особливо тяжким;

C) можлива, якщо хоча б один із співучасників злочину діє умисно;

D) неможлива.

Відповідь: D

39. Хто є співучасником злочину за Кримінальним кодексом України?

A) потурач;

B) фінансист;

C) змовник;

D) підбурювач.

Відповідь: D

40. Який вид співучасника є найбільш суспільно небезпечним відповідно до Кримінального кодексу України?

A) підбурювач;

B) організатор;

C) виконавець;

D) пособник.

Відповідь: C

41. Як кваліфікується злочин, учинений виконавцем?

A) за статтею Особливої частини КК України з посиланням на ст. 26 КК, у якій дається поняття «співучасть»;

B) за статтею Особливої частини КК України з посиланням на ч. 1 ст. 27 КК України, в якій називаються види співучасників;

C) за статтею Особливої частини КК України з посиланням на ч. 2 ст. 27 КК України, в якій дається поняття «виконавець (співвиконавець)»;

D) за статтею Особливої частини КК України.

Відповідь: D

42. Що визнається посереднім заподіянням?

A) використання для вчинення злочину інших осіб, які відповідно до закону не підлягають кримінальній відповідальності за вчинене;

B) використання для вчинення злочину інших осіб;

C) використання для вчинення злочину тварин чи комах;

D) використання для вчинення злочину спеціальних технічних пристроїв чи знарядь.

Відповідь: A

43. Що є формою співучасті?

A) організована злочинність;

B) група осіб без попередньої змови;

C) злочинне співтовариство;

D) злочинне угруповання.

Відповідь: B

44. У яких випадках має місце проста співучасть у злочині?

A) усі співучасники є співвиконавцями злочину;

B) для вчинення злочину створено організовану групу;

C) для вчинення злочину створено злочинну організацію;

D) у вчиненні злочину поряд із виконавцем бере участь інший співучасник злочину (організатор, підбурювач або пособник).

Відповідь: A

45. У якому випадку складна співучасть має місце?

A) всі співучасники є співвиконавцями злочину;

B) у вчиненні злочину беруть участь три і більше співучасників, які є співвиконавцями;

C) у вчиненні злочину беруть участь три і більше співвиконавців, які виконують різні за своїм характером функції;

D) злочин вчинюється виконавцем у співучасті з організатором, підбурювачем чи пособником.

Відповідь: D

46. Що є кримінальним законом?

A) кодифікований законодавчий акт;

B) звичайний закон;

C) конституційний закон;

D) основний закон.

Відповідь: A

47. Якою галуззю права є Кримінальне право?

A) галузь публічного права України;

B) галузь приватного права України;

C) галузь світового права;

D) галузь відновлювального права.

Відповідь: A

48. Що є предметом кримінального права?

A) матеріальні цінності, що охороняються кримінальним законодавством;

B) суспільні відносини, що виникають у зв'язку призначенням особі покарання; C) суспільні відносини, що виникають у зв'язку з учиненням правопорушення;

D) суспільні відносини, що виникають у зв'язку з дією кримінального закону.

Відповідь: D

49. Що є завданням кримінального права відповідно до КК України?

A) визначення суспільно небезпечних діянь, які є кримінальними проступками;

B) визначення видів злочинців;

C) правове забезпечення охорони найбільш важливих суспільних відносин;

D) визначення підстав кримінальної відповідальності.

Відповідь: C

50. У які дві підсистеми об'єднуються норми права, з яких складається Кримінальне право?

A) загальна й унікальна частини;

B) Загальна й Особлива частини;

C) проста і складна частини;

D) основна й особлива частини.

Відповідь: B

51. Які із означених функцій є основними функціями кримінального права?

A) охоронна і регулятивна;

B) правовідновлювальна та фундаментальна;

C) охоронна та виховна;

D) регулятивна і гарантійна.

Відповідь: A

52. Як називається структурний елемент статті Особливої частини КК України, у якому визначається вид і розмір покарання за злочин?

A) гіпотеза;

B) диспозиція;

C) санкція;

D) примітка.

Відповідь: C

53. Які принципи чинності закону про кримінальну відповідальність у просторі передбачає Кримінальний кодекс України (вкажіть повний перелік)?

A) територіальний, реальний, міжнародний;

B) громадянства та універсальний;

C) універсальний, громадянства, реальний;

D) територіальний, громадянства, універсальний, реальний.

Відповідь: D

54. Що є часом вчинення злочину?

A) час початку готування до злочину;

B) час вчинення суспільно небезпечного діяння;

C) час настання суспільно небезпечних наслідків;

D) час повідомлення про підозру у вчиненні кримінального правопорушення.

Відповідь: B

55. Що є місцем вчинення злочину?

A) приміщення, у якому було приховано злочинця або предмети, здобуті злочинним шляхом;

B) певна територія або інше місце, де вчиняється суспільно небезпечне діяння і настають його суспільно небезпечні наслідки;

C) територія, на якій було затримано злочинця;

D) територія України.

Відповідь: B

56. Між якими суб'єктами виникають суспільні відносини при вчиненні кримінального правопорушення?

A) державою і правоохоронними органами;

B) між особами за фактом порушення прав одного з них;

C) державою в особі правоохоронних органів і особою, яка вчинила кримінальне правопорушення;

D) правоохоронними органами.

Відповідь: C

57. Назвіть, які кримінальні закони мають зворотну силу?

A) всі кримінальні закони мають зворотну силу;

B) жоден кримінальний закон не має зворотної сили;

C) такий, що встановлює злочинність діяння та посилює покарання;

D) такий, що пом'якшує покарання чи скасовує злочинність діяння.

Відповідь: D

Словник

Атака на відмову в обслуговуванні (англ. *DoS attack*) – дестабілізація віддаленої системи, приведення її в неробочий стан.

Атака «людина посередині» (англ. *Man in the middle*) – ситуація, коли криптоаналітик (атакувальник) здатний читати та видозмінювати на свій розсуд повідомлення, якими обмінюються кореспонденти, причому жоден з останніх не може здогадатися про його присутність в каналі.

Атака сторонніми каналами (англ. *side channel attack*) – використання будь-якої інформації про фізичні процеси у пристрої, такі як диференційній аналіз енерговикористання.

Атака на цілісність даних – спотворення, зміна або знищення даних.

База даних (БД) – комплекс програмно-апаратних рішень для збору, розміщення, реєстрації і надання доступу засобами інтернет.

Банкоматне шахрайство – використання «білого пластику» для «копіювання» (підробки) платіжної картки та в подальшому зняття готівки в банкоматах.

Відладники. Дозволяють переривати виконання програми при досягненні заздалегідь заданих умов, виробляти покрокове виконання програми, змінювати вміст пам'яті і регістрів тощо.

Дизасемблери. Проводять дизасемблювання програми для подальшого вивчення отриманого коду.

Динамічна IP-адреса, може бути надана необмеженому колу осіб (наприклад при використанні

безпровідного з'єднання Wi-Fi або при підключенні до мережі через засоби стільникового зв'язку тощо).

Єкосистема *FinTech* – сукупність традиційних фінансових посередників, їх об'єднань, *FinTech*-компаній, компаній інфраструктури, стартапів, регуляторів, акселераторів, інкубаторів та споживачів, які взаємодіють між собою в кіберпросторі, завдяки чому зростає ефективність задоволення потреб споживачів, безпека здійснення фінансових операцій, відбувається оптимізація діяльності постачальників послуг та регуляторів.

Витік інформації – несанкціоноване зняття чи доступ до конфіденційної інформації з каналів зв'язку.

Грінмейл – «корпоративний шантаж, який полягає в начебто законній діяльності міноритарного акціонера (подання численних скарг, позовів проти товариства, ініціювання перевірок діяльності товариства), направленої на спонукання менеджменту або мажоритарних акціонерів товариства придбати акції в цього міноритарного акціонера за ціною, яка багаторазово перевищує їхню ринкову вартість, або отримання відступних у грошовій або іншій формі». Цей вид загрози пов'язаний на перший погляд із рейдерством, але з іншого боку саме завдяки інтернет-мережі та розвитку сучасних інформаційних мереж стає можливим досягати поставленої мети в короткі проміжки часу.

FinTech – інноваційні технології, які використовуються фінансовими інститутами, органами державного управління, торговельними організаціями для задоволення потреб споживачів фінансо-

вих, адміністративних послуг та товарів в умовах розвитку економіки споживання. Іншими словами *FinTech* передбачає використання технологій для фінансових рішень.

ROMAD™ Endpoint Defense – програмне забезпечення наступного покоління (Next Generation) класу Endpoint Detection and Response (NG EDR); захист кінцевої точки від кібератак, які використовують шкідливе програмне забезпечення (ШПЗ); технологічні інновації, які дозволяють проводити поведінковий аналіз 100 % системних викликів у реальному часі з мінімальним навантаженням обчислювальних ресурсів; за результатом аналізу детектується та блокується деструктивна активність ШПЗ до того, як заподіяна будь-яка шкода кінцевій точці; виявлення та блокування сімейств ШПЗ, а не окремих штамів вірусів.

Smart city **(розумне місто)** – місто, яке об'єднує сучасні методи керування процесами комплексного функціонування міста, метою яких є покращення рівня життя пересічних громадян. Збільшення міського населення призводить до необхідності використання сучасних підходів управління, використання новітніх інформаційних технологій – платформ та методів для інтелектуального розвитку міста, але є і зворотна сторона такого розвитку.

SQL-ін'єкція – один з поширених способів злому сайтів та програм, що працюють із базами даних, заснований на впровадженні в запит довільного SQL-коду.

Інформаційна безпека – безпека інформації (організації та/або особистої), у тому числі в IT-системах.

IP-адреса – (адреса інтернет-протоколу). При реєстрації мережі в інтернеті їй виділяється мережний ідентифікатор залежно від класу. Ідентифікація ж вузлів у підмережах мережі здійснюється організацією-власником. Коли особа підключається до інтернет-мережі, її комп'ютер стає частиною мережі і йому надається унікальна IP-адреса.

Кардерство – це вид шахрайства, при якому проводиться операція з використанням платіжної картки або її реквізитів, що не ініційована або не підтверджені її власником. Реквізити платіжних карт, зазвичай, беруть зі зламаних серверів інтернет-магазинів, платіжних та розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «троянці», «боти» з функцією формграббер). Така загроза актуальна і для фізичних осіб, і юридичних. Кібербезпека є частиною **інформаційної безпеки** будь-якої організації.

Кібербезпека – безпека IT-систем (обладнання та програм). Наприклад, наскільки захищений ваш комп'ютер чи ваш вебсайт від зламу хакерами – це питання кібербезпеки.

Кібервійна – військові дії, що здійснюються в електронному просторі в електронному вигляді. Зброя в кібервійні – це інформація, інструменти – комп'ютери, театр військових дій – інтернет, який стає потужною зброєю, яка суттєво підсилюється технологіями штучного інтелекту.

Кіберзброя представляє собою широкий спектр технічних і програмних інструментів, які найчас-

тіше спрямовані саме на використання вразливих місць у системах передачі даних.

Кібертероризм – використання комп'ютерних та телекомунікаційних технологій (насамперед інтернету) в терористичних цілях. Головну тактику кібертероризму можна охарактеризувати так: кіберзлочин повинен мати досить небезпечні наслідки, стати широко відомим, отримати великий суспільний резонанс і створити атмосферу загрози повторення акту без вказівки конкретного об'єкта. Що ж до природи кібертероризму, то він якісно відрізняється від загальноприйнятого поняття тероризму, зберігаючи лише стержень цього явища і ознаки.

Комп'ютерний хакер – будь-який досвідчений комп'ютерний експерт, який використовує свої технічні знання для подолання проблеми.

MAC-адреса або фізична адреса комп'ютера – незмінний ідентифікаційний номер пристрою, за допомогою якого здійснюється з'єднання з мережею.

Отримання IP-адреси здійснюється при кожному підключенні, але ця адреса кожного разу має нове значення з діапазону динамічних IP-адрес провайдера, через якого здійснюється підключення.

Підміна (англ. *spoofing*) – змушення жертви відправляти трафік не легітимному одержувачу безпосередньо, а атакуючому, який потім вже ретранслює трафік далі. При цьому останній отримує можливість модифікації трафіку або, як мінімум, перегляду.

Скіминг – крадіжка даних карти за допомогою спеціального пристрою, що зчитує (скімера).

Статичні IP-адреси, зазвичай, закріплені за тими вузлами інтернету, що повинні бути присутніми в мережі постійно. Це сервери, призначення яких полягає в тому, щоб обробляти запити користувачів інтернету.

Махінації в торговельно-сервісних мережах:

– «клонування» реквізитів платіжних карток із застосуванням технічних засобів;

– транзакції без проведення авторизації на суму меншу встановленого ліміту;

Махінації в онлайн-просторі:

– підробка даних платіжних карток;

– здійснення транзакцій, використовуючи викрадені дані платіжних карток;

– написання програмного забезпечення для крадіжки реквізитів платіжних карток (перехоплення трафіку, створення підробних WEB-сайтів, поширення троянських програм та вірусів).

Махінації в системах дистанційного банківського обслуговування (надалі – ДБО):

– написання троянських програм та комп'ютерних вірусів для прихованого перехоплення контролю над комп'ютером клієнта з установленим програмним забезпеченням ДБО;

– отримання платежів через міжнародну систему SWIFT від закордонних відправників унаслідок втручання в роботу комп'ютерів та систем ДБО клієнтів закордонних банківських установ.

Основні методи тестування безпеки:

Code review – перегляд вихідного коду програми. Зазвичай, перегляд виконує кваліфікований

розробник. Тестувальник, своєю чергою, може використовувати утиліти для статичного й динамічного аналізу: RATS, cppcheck та ін. Цей метод дає змогу виявити уразливості в коді ще на етапі реалізації проекту.

Fuzz – тестування – ще один метод тестування безпеки, суть якого полягає в тому, що на вхід програми подаються свідомо неправильні, непередбачені або випадкові дані. Отже, ми вивчаємо поведінку програми при використанні самих різних вхідних даних. При застосуванні фаззінга – тестування можна виявити помилки обробки вхідних даних, витоку пам'яті, невірні коди помилок. Існує ряд програмних засобів для проведення фаззінга тестування – *Skyfish, SPIKE Proxy, OWASP WSFuzzer (Soap)*.

Тестування на проникнення (*penetration testing*). Цей метод дає змогу проводити тестування, взаємодіючи з додатком лише з користувацької сторони. Тестувальник може використовувати і автоматичні сканери безпеки, такі як skipfish або wapiti, і аналізатори мережі. Важливим аспектом при тестуванні на проникненні є ручне (дослідне) тестування, адже програмні засоби не завжди можуть виявити всі уразливості в безпеці.

Обфускація, або заплутування коду – приведення початкового коду або виконуваного програмного коду до вигляду, який зберігає його функціональність, але ускладнює аналіз, розуміння алгоритму роботи й модифікації при декомпіляції. Обфускація – це безпека через приховування.

Основні утиліти для злому, їх можна класифікувати так:

– **засоби моніторингу** – набір утиліт, які відстежують операції з файлами, реєстром, портами й мережею;

– **засоби пасивного аналізу програми** показують різну інформацію про програму: витягують ресурси, показують зв'язок, що використовуються бібліотеки;

– **інші утиліти** – різноманітні редактори, аналізатори тощо.

Стеганографія – наука про передачу секретного повідомлення через збереження в таємниці самого факту передачі такого повідомлення.

Криптографічний захист інформації – вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних задля приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Криптографічні методи захисту інформації – спеціальні методи захисту інформації, а саме: шифрування, кодування та ін., в результаті дії яких прочитання її стає недоступним без наявності ключа криптограми і зворотного перетворення.

Криптографія поділяється на такі розділи:

криптосистеми з відкритим ключем, або асиметричний шифр – система, у якій використовується відкритий і закритий ключі, пов'язані математичним способом між собою. Шифрується інфор-

мація відкритим, доступним для всіх ключем, а розшифровується за допомогою закритого, який відомий лише отримувачу.

Симетричні криптосистеми. Відповідно до їх назви, у таких криптосистемах використовується один ключ і для алгоритму шифрування, і для дешифрування. Сам ключ повинен зберігатися в секреті, оскільки симетричні криптоалгоритми виконують перетворення невеликого блоку даних таким способом, що прочитання інформації можливе лише за наявності секретного ключа. Ця система має чотири класи перетворень, а саме: підстановка, перестановка, аналітичне перетворення, комбіноване перетворення.

Електронний підпис. Системою електронного цифрового підпису називається криптографічне перетворення його електронних даних, до яких додається сам підпис або логічне їх поєднання, яке дає змогу перевірити його цілісність та ідентифікувати користувача (передплатника) та достовірність повідомлення.

Управління ключами. Ця система відіграє найважливішу роль і криптографії, вона є основою забезпечення конфіденційності, цілісності та ідентифікації інформації. Процес полягає у складанні та розподілі ключів поміж користувачами. Цей інформаційний процес включає в себе три елементи: накопичення ключів, їх генерацію та розподіл.

Фішинг (англ. *Phishing*) – 1) отримання конфіденційної інформації (паролі, номери банківських карток тощо) обманним шляхом;

2) схема, за якої хакери змушують користувачів передавати конфіденційну інформацію. Цей вид шахрайства заснований на довірі та заволодінні злочинцем аккаунтом іншого користувача. Він зазвичай передбачає надсилання користувачу соціальної мережі повідомлення, яке ніби походить із довіреного джерела, наприклад від знайомого з проханням позичити електронних грошей, скачати контент або перейти за посиланням. Людина не може точно знати, хто відправив їй повідомлення – друг чи шахрай, який заволодів його сторінкою, і, зазвичай, вона, не замислюючись про це, виконує прохання;

3) вид шахрайства, мета якого – виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів.

Фармінг – перенаправлення жертви за помилковою адресою, наприклад це імітація сторінки авторизації в соціальну мережу задля заволодіння логіном та паролем від облікового запису. Аби не потрапити у цю пастку, потрібно уважно дивитися, за якими посиланнями та сторінками здійснюється перехід та використовувати механізм двофакторної аутентифікації в соцмережі.

Хакер (з англомовного сектора вікіпедії):

– людина, що захоплюється дослідженням подробиць програмованих систем, вивченням питання підвищення їх можливостей, на противагу більшості користувачів, які вважають за краще обмежуватися вивченням необхідного мінімуму.

– той, хто програмує з ентузіазмом, або люблячий програмувати, а не просто теоретизувати про програмування;

– експерт щодо певної комп'ютерної програми або той, хто часто працює з нею (приклад: «хакер Unix»);

– експерт або ентузіаст будь-якого роду. Той, хто може вважатися «хакером астрономії», наприклад хто любить інтелектуальні випробування, які полягають у творчому подоланні або обході обмежень. Хакер – це оцінка кваліфікації користувача інформаційної системи.

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403)
{Із змінами, внесеними згідно із Законом
№ 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст. 241}

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз – показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4) кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

5) кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і

потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

8) кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність – сукупність кіберзлочинів;

10) кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням інтернету та/або інших глобальних мереж передачі даних;

12) кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм – терористична діяльність, що здійснюється в кіберпросторі або з його використанням;

14) кібершпигунство – шпигунство, що здійснюється в кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури;

16) критично важливі об'єкти інфраструктури (далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

17) Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та

яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

18) національні електронні інформаційні ресурси (далі – національні інформаційні ресурси) – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

19) об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

20) система управління технологічними процесами (далі – технологічна система) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

21) системи електронних комунікацій (далі – комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (вклю-

чаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Терміни «національна безпека», «національні інтереси», «загрози національній безпеці» вживаються в цьому Законі у значенні, визначеному Законом України «Про основи національної безпеки України».

Стаття 2. Принципи застосування Закону

1. Цей Закон не поширюється на:

1) відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші вебресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;

4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

2. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

6) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:

відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону.

Стаття 3. Правові основи забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

2. Якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.

Стаття 4. Об'єкти кібербезпеки та кіберзахисту

1. Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

2. Об'єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, перелік таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.

Стаття 5. Суб'єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

5. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Стаття 6. Об'єкти критичної інфраструктури

1. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

2. Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України – Національним банком України.

3. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

4. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне

інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України «Про захист персональних даних».

Стаття 7. Принципи забезпечення кібербезпеки

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Стаття 8. Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

2. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, ви-

мога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важли-

вим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

4) Міністерство оборони України, Генеральний штаб Збройних сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

5) залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

8) розвитку мережі команд реагування на комп'ютерні надзвичайні події;

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

12) обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

16) встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

17) державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

23) обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також

обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

4. Порядок функціонування Національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

5. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким

загрозам, програми та методики проведення кібернавчань.

Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA

1. Завданнями CERT-UA є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також

громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.

Стаття 11. Сприяння суб'єктам забезпечення кібербезпеки України

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та

захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

Стаття 13. Фінансове забезпечення заходів кібербезпеки

Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України «Про порядок направлення підрозділів Збройних сил України до інших держав» та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України».

3. Відповідно до законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

2. Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України.

3. Незалежний аудит діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту.

Звіти про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього

Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап'ятиденний строк після закінчення календарного року.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб'єктів національної кібербезпеки Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, може порушити питання про розгляд цих питань Верховною Радою України.

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.

2. Внести зміни до таких законів України:

1) статтю 7 Закону України «Про Національний банк України» (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами) доповнити пунктами 32 і 33 такого змісту:

«32) визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; утворює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;

33) забезпечує формування та ведення переліку об'єктів критичної інфраструктури, а також реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України, визначає критерії та порядок віднесення об'єктів у банківській системі України до об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України»;

2) у Законі України «Про оборону України» (Відомості Верховної Ради України, 2000 р., № 49, ст. 420; 2011 р., № 4, ст. 27; 2015 р., № 16, ст. 110; 2016 р., № 33, ст. 564):

а) статтю 3 після абзацу дев'ятнадцятого доповнити новим абзацом такого змісту:

«здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії».

У зв'язку з цим абзац двадцятий вважати абзацом двадцять першим;

б) друге речення частини другої статті 4 доповнити словами «у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі»;

3) у Законі України «Про розвідувальні органи України» (Відомості Верховної Ради України, 2001 р., № 19, ст. 94; 2006 р., № 14, ст. 116; 2016 р., № 33, ст. 564 із наступними змінами):

а) абзац другий статті 1 після слів «за межами України» доповнити словами «у тому числі у кіберпросторі»;

б) абзац шостий статті 4 після слів «національній безпеці України» доповнити словами «у тому числі у кіберпросторі»;

{Підпункт 4 пункту 2 розділу втратив чинність на підставі Закону № 2469-VIII від 21.06.2018}

5) абзац шостий статті 3 Закону України «Про Службу зовнішньої розвідки України» (Відомості Верховної Ради України, 2006 р., № 8, ст. 94) після слів «національній безпеці України» доповнити словами «у тому числі у кіберпросторі»;

6) у Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» (Відомості Верховної Ради України, 2014 р., № 25, ст. 890, № 29, ст. 946):

а) частину першу статті 2 та абзац другий частини першої статті 3 після слів «криптографічного та технічного захисту інформації» доповнити словом «кіберзахисту»;

б) у частині першій статті 14:

пункт 39 після слів «забезпечення функціонування» доповнити словом «урядової»;

доповнити пунктами 85–92 такого змісту:

«85) формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах;

86) координація діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту;

87) забезпечення створення та функціонування Національної телекомунікаційної мережі;

88) впровадження організаційно-технічної моделі кіберзахисту, здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

89) інформування про кіберзагрози та відповідні методи захисту від них;

90) забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації);

91) координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

92) забезпечення функціонування Державного центру кіберзахисту».

3. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:

забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону;

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

Президент України П. Порошенко

м. Київ
5 жовтня 2017 року
№ 2163-VIII

Список використаної літератури

1. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: дис. … канд. юрид. наук: 12.00.08/Ін-т держави і права ім. В. М. Корецького НАН України. Київ, 2003. 246 с.
2. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія / Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з пробл. боротьби з організ. злочинністю. Київ: КИТ, 2010. 408 с.
3. Бутузов В. М., Кузьмін С. А., Шеломцев В. П. Науково-практичний коментар до Кримінального кодексу України. Особлива частина. Розділ XVI. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Київ: Вид-во Паливода А. В., 2010. 152 с.
4. Бутузов В. М., Остапець С. Л., Шеломенцев В. П. Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: наук.-практ. коментар. Київ: Друкарня МВС України, 2005. 86 с.
5. Дешко Л. М., Бондарєва К. Д. Кібербезпека в Україні: національна стратегія та міжнародне співробітництво. *Електронне наукове фахове видання «Порівняльно-аналітичне право»*. 2018. № 2. С. 379–382. URL: http://www.pap.in.ua/2_2018/112.pdf
6. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р. *Верховна Рада України: Законодавство.* 10.05.2016 р. URL: http://zakon1.rada.gov.ua/laws/show/994_687
7. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. *Голос України*. 27.06.2003. № 119.

8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради*. 2005. № 26. Ст. 347.
9. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
10. Закон України «Про Національну поліцію» від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.
11. Закон України «Про основні засади забезпечення кібербезпеки України», зі змінами, внесеними від 21.06.2018 р. № 2469-VIII.
12. Зінченко І. О. Кримінальне право України. Загальна та Особлива частина у питаннях і відповідях: наук.-практ. посіб. Київ: Атіка, 2013. 240 с.
13. Карчевський М. В. Злочини у сфері використання комп'ютерної техніки: навч. посіб./Луган. держ. ун-т внутр. справ. Луганськ: РВВ ЛДУВС, 2006. 192 с.
14. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія/Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 526 с.
15. Кваліфікація злочинів: навч. посіб./Г. М. Анісімов, О. О. Володіна, І. О. Зінченко та ін.; за ред. М. І. Панова. Харків: Право, 2016. 356 с.
16. Кваліфікація злочинів: навч. посіб./за ред. О. О. Дудорова, Є. О. Письменського. Київ: Істина, 2010. 430 с.
17. Кодекс України про адміністративні правопорушення від 07.12.1984 р. *Відомості Верховної Ради УРСР*. 1984. № 51. С. 1122.
18. Комп'ютерний тероризм: практика запобігання, протидії, розслідування: кримінолого-криміналістичний аналіз та правові, управлінські і тактико-технологічні засади запобігання, протидії, розслідування комп'ютерних терористичних актів: навч. посіб. / П. Д. Біленчук [та ін.]; заг. ред. П. Д. Біленчук; Хмельн. держ. центр наук.-техн. і екон. інфор-

мації, Київ. нац. ун-т внутр. справ. Хмельницький: Хм. ЦНТЕІ, 2008. 258 с.
19. Компьютерные террористы: новейшие технологии на службе преступного мира/[авт.-сост. Татьяна Ивановна Ревяко]. Минск: Литература, 1997. 639 с. (Энциклопедия преступлений и катастроф).
20. Конвенція про кіберзлочинність від 23.11.2001 р. *Верховна Рада України: Законодавство.* 10.05.2016 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575
21. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
22. Копотун І. М., Боровик А. В. Кримінально-правова характеристика кіберзлочинів в україні: академ. курс. Київ: ФОП Кандиба, 2018. 164 с.
23. Копотун І. М. Актуальність викликів та потенціальних загроз, спричинених міжнародним тероризмом//Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності: матеріали 2-ї Всеукр. наук.-практ. конф. (Хмельницьк, 2 берез. 2018 р.)/Нац. акад. держ. прикорд. служби України ім. Богдана Хмельницького. Харків: Нац. акад. держ. прик. служби, 2018. С. 57–61.
24. Копотун І. М. Терористичні напади екстремістського характеру//Актуальні питання протидії злочинності в сучасних умовах: вітчизняний та зарубіжний досвід*:* матеріали 2-ї Міжнар. наук.-практ. конф. (Дніпро, 15 берез. 2018 р.). Дніпропетровськ: Дніпр. держ. ун-т. внутр. справ, 2018. С. 79–81.
25. Корченко О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Безпека інформації*. 2013. Т. 19, № 1.
26. Кримінальне право України (у питаннях та відповідях): навч. посіб./[Литвинов О. М., Житний О. О., Клемпарський М. М. та ін.]; за заг. ред. О. М. Литвинова; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2016. 328 с.

27. Кримінальне право України. (Особлива частина): підручник/кол. авторів А. В. Байлов, О. А. Васильєв, О. О. Житний та ін.; за заг. ред. О. М. Литвинова; наук. ред. серії О. М. Бандурка. Харків: ХНУВС, 2011. 572 с.
28. Кримінальне право України. Особлива частина. Альбом схем: навч. посіб.: рекомендовано МОН України/В. Я. Горбачевський, І. А. Вартилецька, О. В. Микитчик та ін. Київ: Правова єдність: Алерта, 2015. 576 с.
29. Кримінальне право України: Особлива частина: підручник: затверджено МОН України/А. О. Байда, Ю. В. Баулін, В. І. Борисов та ін. Харків: Право, 2015. 680 с.
30. Кримінальне право. Особлива частина: підручник: затверджено МОН України/А. С. Беніцький, В. П. Бодаєвський, Г. Є. Болдарь та ін. Київ: Дакор, 2015. 786 с.
31. Кримінальний кодекс України від 05.04.2001 р. *Відомості Верховної Ради України*. 2001. № 25. Ст. 131.
32. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI. *Голос України*. 19.05.2012. № 90–91.
33. Кримінально-правова характеристика та розслідування незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом: навч.-практ. посіб./Васильєв В. В., Пашнєв Д. В., Рудик М. В., Воронцов Д. В. Сімферополь: КрЮІ ОДУВС, 2010. 170 с.
34. Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Зб. наук. пр. Військового ін-ту КНУ ім. Тараса Шевченка*. Київ: ВІКНУ, 2011. Вип. 30.
35. Навроцький В. О. Основи кримінально-правової кваліфікації: навч. посіб. 2-ге вид. Київ: Юрінком Інтер, 2009. 512 с.

36. Пашнев Д. В. Компьютерные технологии как средство совершения преступлений, связанных с терроризмом//Противодействие ксенофобии, экстремизму и терроризму в современном обществе: науч. тр. Междунар. науч.-практ. конф./под общ. ред. А. Н. Игнатова; Ин-т экономики и права (филиал) ОУП ВПО «Академия труда и социальных отношений» в г. Севастополе. Симферополь: КРП «Изд-во "Крымучпедгиз"», 2012. 578 с. С. 174–177.
37. Пашнєв Д. В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України: зб. наук. пр.* [ред-кол. Л. М. Давиденко, Т. А. Денисова, О. М. Джужа та ін.]. Харків: Золота миля, 2013. 252 с. С. 34–42.
38. Постанова Кабінету Міністрів України від 11.04.2012 р. № 295 «Про затвердження Правил надання та отримання телекомунікаційних послуг». *Урядовий кур'єр*. 20.06.2012. № 109.
39. Постанова Кабінету Міністрів України від 29.03.2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». *Урядовий кур'єр*. 18.04.2006. № 73 /73–74/.
40. Про затвердження Стратегії національної безпеки: Указ Президента України від 26 травня 2015 р. № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070
41. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 407.
42. Про Стратегію кібербезпеки України: Указ Президента України від 27 січня 2016 р. № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836
43. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / [О. Є. Користін,

В. М. Бутузов, В. В. Василевич та ін.]. Київ: Вид. дім «Скіф», 2012. 728 с.
44. Словник термінів із кібербезпеки/за заг. ред. О. В. Копана, Є. Д. Скулиша. Київ: ВБ «Аванпост-Прим», 2012.
45. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 р. № 96/2016.
46. Шульга А. М., Павликівський В. І., Вапсва Ю. А. Кримінальне право України: основні питання та відповіді: посіб. для підгот. до форм контролю з навч. дисципліни «Кримінальне право України». Харків: Майдан, 2014. 276 с.

Навчальне видання

А. В. БОРОВИК, І. М. КОПОТУН

КІБЕРЗЛОЧИНИ В УКРАЇНІ

(кримінально-правова характеристика)

Навчальний посібник

Редактор *В. С. Голюк*
Технічний редактор *М. Б. Філіпович*

Формат 60×84$^{1}/_{16}$. 17,67 ум. друк. арк., 17,5 обл.-вид. арк.
Наклад 500 пр. Зам. СФ-2569. СПД Гадяк Ж. В. друкарня
«Волиньполіграф»™ (43021, м. Луцьк, вул. Привокзальна, 12).
Тел.: (0332) 77-07-14, 77-05-02.
Ел. адреса: vpdruk@gmail.com
Свідоцтво Держ. комітету телебачення та радіомовлення
України ДК № 3585 від 22.09.2009 р.