Додаток 1
до Порядку

ТАБЛИЦЯ

відповідності законодавства України акту права Європейського Союзу (acquis ЄС)

Переговорний розділ ***Розділ 24: Правосуддя, свобода та безпека, Розділ 10: Цифровізація та медіа***

Підрозділ/сфера ***19.30.10 Співробітництво поліції***

Найменування акта права Європейського Союзу (acquis ЄС) ***Директива (ЄС) 2013/40/ЄС Європейського Парламенту та Ради від 12 серпня 2013 року про атаки на інформаційні системи та заміну Рамкового рішення Ради 2005/222/ЮВС***

Положення акта права ЄС (у розрізі статей)	Норми законодавства України, що імплементують відповідне положення акта права ЄС	Ступінь врахування (відповідає, частково відповідає, не відповідає) відповідного положення акта права ЄС у зак-тві України	Примітка: основні заходи, строки, виконавці тощо (якщо частково відповідає, не відповідає)
1	2	3	4
Стаття 1 **Тематика** Ця Директива встановлює мінімальні правила, що стосуються визначення кримінальних злочинів та санкцій	**Кримінальний кодекс України** Розділ XVI КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ	**Відповідає**	-

1	2	3	4
у сфері атак на інформаційні системи. Вона також спрямована на сприяння запобіганню таким правопорушенням та покращення співпраці між судовими та іншими компетентними органами.	**Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж** 1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. **Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут** 1. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років. **Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації** 1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах,		

1	2	3	4
	комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. **Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк. **Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється** Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк. **Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку** 1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -		

1	2	3	4
	карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. **ЗУ «Про основні засади забезпечення кібербезпеки»** **Стаття 8 Національна система кібербезпеки** 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, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, 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 та Центру активної протидії агресії у кіберпросторі, 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 кримінально протиправних 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 кримінальних правопорушень 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 важливим інтересам держави; розслідує кіберінциденти	**Відповідає**	

1	2	3	4
	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; 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		

1	2	3	4
	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 кримінальних правопорушень 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		

1	2	3	4
	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. **Стаття 5.** Суб'єкти забезпечення кібербезпеки 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 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;		

1	2	3	4
	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. **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;		

1	2	3	4
	11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі. **ЗУ «Про Національну поліцію України»** Стаття 23. Основні повноваження поліції 1. Поліція відповідно до покладених на неї завдань: 1) здійснює превентивну та профілактичну діяльність, спрямовану на запобігання вчиненню правопорушень; 2) виявляє причини та умови, що сприяють вчиненню кримінальних та адміністративних правопорушень, вживає у межах своєї компетенції заходів для їх усунення; 3) вживає заходів з метою виявлення кримінальних, адміністративних правопорушень; припиняє виявлені кримінальні та адміністративні правопорушення; 4) вживає заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення кримінального, адміністративного правопорушення; 24-1) здійснює у визначеному законом порядку протидію злочинним посяганням на об'єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; захист об'єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об'єктів критичної інфраструктури; Стаття 26. Формування інформаційних ресурсів поліцією 1. Поліція засобами інформаційно-комунікаційної системи наповнює та підтримує в актуальному стані реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно: 1) осіб, щодо яких поліцейські здійснюють профілактичну роботу; У структурі НПУ відповідно ч.3 ст. 13 ЗУ «Про Національну поліцію» функціонує кримінальна поліція. ДКП у складі кримінальної поліції здійснює оперативно-розшукову діяльність та відповідно до **Положення про Департамент кіберполіції Національної поліції України**, затвердженого наказом Національної поліції України від 10.11.2015 № 85 (в редакції наказу Національної поліції України від 07.11.2019 № 1136), забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із протидії кіберзлочинам, підвищення поінформованості громадян про безпеку в кіберпросторі, зокрема: проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті.		

1	2	3	4
Стаття 2 **Визначення** Для цілей цієї Директиви застосовуються такі визначення: - «інформаційна система» означає пристрій або групу взаємопов'язаних або пов'язаних пристроїв, один або декілька з яких відповідно до програми автоматично обробляють комп'ютерні дані, а також комп'ютерні дані, що зберігаються, обробляються, отримуються або передаються цим пристроєм або групою пристроїв для цілей його або їх функціонування, використання, захисту та обслуговування;	**Закон України «Про ратифікацію Конвенції про кіберзлочинність»** від 7 вересня 2005 р. відповідно відповідно до підпункту 7.a статті 24: в Україні органами, на які покладаються повноваження згідно з пунктом 7 статті 24 Конвенції, є Міністерство юстиції України (щодо запитів судів) і Генеральна прокуратура України (щодо запитів органів досудового слідства); відповідно до підпункту 2.c статті 27: в Україні органами, відповідальними за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам, є Міністерство юстиції України (щодо доручень судів) та Генеральна прокуратура України (щодо доручень органів досудового слідства). **Закон України «Про захист інформації в інформаційно-комунікаційних системах»** **Стаття 1.** Визначення термінів інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів; інформаційно-комунікаційна система - сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле; електронна комунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб; **ЗУ «Про електронні комунікації»** **Стаття 2. Визначення термінів** автоматизована інформаційна система управління радіочастотним спектром - система надання, збирання, накопичення, захисту, обліку, обробки та використання інформації, що дає змогу здійснювати заходи щодо радіочастотного планування, оцінки електромагнітної сумісності, здійснення присвоєнь радіочастот та радіочастотного моніторингу. віртуальна електронна комунікаційна мережа - електронна комунікаційна мережа оператора, призначена для надання власних електронних комунікаційних послуг, що функціонує на умовах договору користування електронною комунікаційною мережею або її окремими складовими іншого оператора; електронна комунікаційна мережа - комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг; електронна комунікаційна мережа загального користування - електронна комунікаційна мережа, доступ до якої відкритий для всіх кінцевих користувачів послуг;		

1	2	3	4
- «комп'ютерні дані» означає представлення фактів, інформації або концепцій у формі, придатній для обробки в інформаційній системі, включаючи програму, придатну для виконання інформаційною системою певної функції;	**Кримінальний процесуальний кодекс України** **Стаття 99.** Документи 1. Документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. 2. До документів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані); 4. Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. **ЗУ «Про електронні комунікації»** **Стаття 2. Визначення термінів** дані - інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки, технічними та програмними засобами		
- "юридична особа" означає суб'єкт, що має статус юридичної особи відповідно до застосовного законодавства, але не включає держави або публічні органи, що діють при здійсненні державних повноважень, або публічні міжнародні організації;	**Цивільний кодекс України** **Стаття 80. Поняття юридичної особи** 1. Юридичною особою є організація, створена і зареєстрована у встановленому законом порядку. Юридична особа наділяється цивільною правоздатністю і дієздатністю, може бути позивачем та відповідачем у суді. **Кримінальний кодекс України** **Стаття 96-4 . Юридичні особи, до яких застосовуються заходи кримінально-правового характеру** 1. Заходи кримінально-правового характеру, у випадках, передбачених пунктами 1 і 2 частини першої статті 96-3 цього Кодексу, можуть бути застосовані судом до підприємства, установи чи організації, крім державних органів, органів влади Автономної Республіки Крим, органів місцевого самоврядування, організацій, створених ними у встановленому порядку, що повністю утримуються за рахунок відповідно державного чи місцевого бюджетів, фондів		

1	2	3	4
- "без права" означає поведінку, зазначену в цій Директиві, включаючи доступ, втручання або перехоплення, яка не дозволена власником або іншим правовласником системи або її частини, або не дозволена національним законодавством.	загальнообов'язкового державного соціального страхування, Фонду гарантування вкладів фізичних осіб, а також міжнародних організацій. 2. Заходи кримінально-правового характеру, у випадках, передбачених пунктами 3-6 частини першої статті 96-3 цього Кодексу, можуть бути застосовані судом до суб'єктів приватного та публічного права резидентів та нерезидентів України, включаючи підприємства, установи чи організації, державні органи, органи влади Автономної Республіки Крим, органи місцевого самоврядування, організації, створені ними у встановленому порядку, фонди, а також міжнародні організації, інші юридичні особи, що створені у відповідності до вимог національного чи міжнародного права. Якщо держава або суб'єкт державної власності володіє часткою більше 25 відсотків в юридичній особі або юридична особа знаходиться під ефективним контролем держави чи суб'єкта державної власності, то дана юридична особа несе цивільну відповідальність у повному обсязі за неправомірно отриману вигоду та шкоду, заподіяну кримінальним правопорушенням, що вчинене державою, суб'єктами державної власності або державного управління. 3. У разі реорганізації юридичних осіб, зазначених у частинах першій та другій цієї статті, заходи кримінально-правового характеру можуть бути застосовані до їх правонаступників, до яких перейшли майно, права та обов'язки, пов'язані з вчиненням кримінальних правопорушень, зазначених пунктами 1-6 частини першої статті 96-3 цього Кодексу. **Закон України «Про захист інформації в інформаційно-комунікаційних системах»** **Стаття 1.** Визначення термінів доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі; виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї; захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі; знищення інформації в системі - дії, внаслідок яких інформація в системі зникає; порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;		

1	2	3	4
Стаття 3 **Незаконний доступ до інформаційних систем** Держави-члени вживають необхідних заходів для забезпечення того, щоб, якщо його вчинено навмисно, доступ без права до всієї або до будь-якої частини інформаційної системи карався як кримінальний злочин, якщо він вчинений з порушенням заходів безпеки, принаймні у випадках, які не є незначними.	**Кримінальний кодекс України** Розділ XVI КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ **Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж** 1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. **Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут** 1. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, -	**Відповідає**	-

1	2	3	4
	караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років. **Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації** 1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. **Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк. **Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється** Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, -	**Відповідає**	

1	2	3	4
Стаття 4 **Незаконне втручання в систему** Держави-члени вживають необхідних заходів для забезпечення того, щоб серйозне перешкоджання або переривання функціонування інформаційної системи шляхом введення комп'ютерних даних, шляхом передачі, пошкодження, видалення, погіршення, зміни або приховування таких даних або надання таких даних недоступним, навмисно і без права, каралося як кримінальний злочин, принаймні для випадків, які не є незначними.	караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк. **Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку** 1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. **Кримінальний кодекс України** **Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж** 1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.	**Відповідає**	

1	2	3	4
Стаття 5 **Незаконне втручання в роботу з даними** Держави-члени вживають необхідних заходів для забезпечення того, щоб видалення, пошкодження, погіршення, зміна або приховування комп'ютерних даних в інформаційній системі або надання таких даних недоступних, навмисно і без права, каралося як кримінальний злочин, принаймні для випадків, які не є незначними.	**Кримінальний кодекс України** **Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк. **Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю** Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, - караються штрафом від трьох тисяч до восьми тисяч неоподатковуваних мінімумів доходів громадян. **Стаття 232. Розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках** Умисне розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.	**Відповідає**	

1	2	3	4
Стаття 6 **Незаконне перехоплення** Держави-члени вживають необхідних заходів для забезпечення того, щоб перехоплення за допомогою технічних засобів непублічних передач комп'ютерних даних до, з або всередині інформаційної системи, включаючи електромагнітне випромінювання інформаційної системи, що містить такі комп'ютерні дані, навмисно і без права каралося як кримінальний злочин, принаймні для випадків, які не є незначними.	**Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації** 1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. **Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк.	**Відповідає**	

1	2	3	4
Стаття 7 **Інструменти, що використовуються для вчинення правопорушень** Держави-члени вживають необхідних заходів для забезпечення того, щоб умисне виробництво, продаж, закупівля для використання, імпорт, розповсюдження або інше надання одного з наступних інструментів без права та з наміром його використання для вчинення будь-якого зі злочинів, зазначених у статтях 3-6, каралося як кримінальний злочин: принаймні для випадків, які не є незначними: - комп'ютерну програму, розроблену або адаптовану головним чином для вчинення будь-якого зі злочинів, зазначених у статтях 3 - 6; - комп'ютерний пароль, код доступу або подібні дані, за допомогою яких можна отримати доступ до всієї або будь-якої частини інформаційної системи.	**Кримінальний кодекс України** Розділ XVI КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ **Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж** 1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. **Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут** 1. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років.	**Відповідає**	

1	2	3	4
	Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації 1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. **Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк. **Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється** Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.	Відповідає	

1	2	3	4
	Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку 1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.		
Стаття 8 **Підбурювання, пособництво, підбурювання та замахи** 1. Держави-члени забезпечують, щоб підбурювання, пособництво та підбурювання до вчинення злочину, зазначеного у статтях 3-7, каралося як кримінальний злочин. 2. Держави-члени забезпечують, щоб замах на вчинення злочину, зазначеного у статтях 4 та 5, карався як кримінальний злочин.	**Кримінальний кодекс України** **Стаття 15. Замах на кримінальне правопорушення** 1. Замахом на кримінальне правопорушення є вчинення особою з прямим умислом діяння (дії або бездіяльності), безпосередньо спрямованого на вчинення кримінального правопорушення, передбаченого відповідною статтею Особливої частини Кримінального Кодексу України, якщо при цьому кримінальне правопорушення не було доведено до кінця з причин, що не залежали від її волі. 2. Замах на вчинення кримінального правопорушення є закінченим, якщо особа виконала усі дії, які вважала необхідними для доведення кримінального правопорушення до кінця, але кримінальне правопорушення не було закінчено з причин, які не залежали від її волі. 3. Замах на вчинення кримінального правопорушення є незакінченим, якщо особа з причин, що не залежали від її волі, не вчинила усіх дій, які вважала необхідними для доведення кримінального правопорушення до кінця. **Стаття 16. Кримінальна відповідальність за незакінчене кримінальне правопорушення** Кримінальна відповідальність за готування до кримінального правопорушення і замах на кримінальне правопорушення настає за статтею 14 або 15 і за тією статтею Особливої частини Кримінального Кодексу України, яка передбачає відповідальність за закінчене кримінальне правопорушення. **Стаття 27. Види співучасників** Співучасниками кримінального правопорушення, поряд із виконавцем, є організатор, підбурювач та пособник. 4. Підбурювачем є особа, яка умовлянням, підкупом, погрозою, примусом або іншим чином схилила іншого співучасника до вчинення кримінального правопорушення. 5. Пособником є особа, яка порадами, вказівками, наданням засобів чи знарядь або усуненням перешкод сприяла вчиненню кримінального правопорушення іншими співучасниками, а також	**Відповідає**	

1	2	3	4
	особа, яка заздалегідь обіцяла переховати особу, яка вчинила кримінальне правопорушення, знаряддя чи засоби вчинення кримінального правопорушення, сліди кримінального правопорушення чи предмети, здобуті кримінально протиправним шляхом, придбати чи збути такі предмети або іншим чином сприяти приховуванню кримінального правопорушення. **Стаття 29. Кримінальна відповідальність співучасників** 2. Організатор, підбурювач та пособник підлягають кримінальній відповідальності за відповідною частиною статті 27 і тією статтею (частиною статті) Особливої частини Кримінального кодексу України, яка передбачає кримінальне правопорушення, вчинене виконавцем. **Кримінальний кодекс України** **Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж** 1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. **Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут**		

1	2	3	4
	1. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років. **Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації** 1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. **Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк. **Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється**		

1	2	3	4
	Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк. **Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку** 1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. **Стаття 255. Створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній** 1. Створення злочинної організації, керівництво такою організацією або її структурними частинами - караються позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна. 2. Участь у злочинній організації - карається позбавленням волі на строк від п’яти до дванадцяти років з конфіскацією майна.		

1	2	3	4
Стаття 9 **Покарання** 1. Держави-члени вживають необхідних заходів для забезпечення того, щоб злочини, зазначені у статтях 3-8, каралися ефективними, пропорційними та переконливими кримінальними покараннями. 2. Держави-члени вживають необхідних заходів для забезпечення того, щоб злочини, зазначені у статтях 3-7, каралися максимальним строком позбавлення волі щонайменше на два роки, принаймні у випадках, які не є незначними. 3. Держави-члени вживають необхідних заходів для забезпечення того, щоб злочини, зазначені у статтях 4 та 5, якщо вони вчинені умисно, каралися максимальним строком позбавлення волі щонайменше на три роки, якщо значна кількість інформаційних систем постраждала внаслідок використання інструменту, зазначеного у статті 7, розроблені або адаптовані в першу чергу для цієї мети. 4. Держави-члени вживають необхідних заходів для забезпечення того, щоб злочини, зазначені у статтях 4 та 5,	**Кримінальний кодекс України** **Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж** 1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. **Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут** 1. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років. **Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації**	**Відповідає**	

1	2	3	4
каралися максимальним строком позбавлення волі щонайменше на п'ять років, якщо: - вони вчинені в рамках злочинної організації, як визначено в Рамковому рішенні 2008/841/ЮВС, незалежно від передбаченого в них покарання; - вони завдають серйозної шкоди; або - вони вчинені проти інформаційної системи критичної інфраструктури. 5. Держави-члени вживають необхідних заходів для забезпечення того, щоб, якщо злочини, зазначені у статтях 4 та 5, вчинено шляхом неправомірного використання персональних даних іншої особи з метою завоювання довіри третьої сторони, тим самим завдаючи шкоди законному власнику особистих даних, це може, відповідно до національного законодавства, вважатися обтяжуючими обставинами, якщо тільки ці обставини вже не охоплені іншим злочином, караним національним законодавством.	1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. **Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк. **Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється** Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк. **Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку**		

1	2	3	4
	1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. **Стаття 255. Створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній** 1. Створення злочинної організації, керівництво такою організацією або її структурними частинами - караються позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна. 2. Участь у злочинній організації - карається позбавленням волі на строк від п’яти до дванадцяти років з конфіскацією майна. Стаття 28. Вчинення кримінального правопорушення групою осіб, групою осіб за попередньою змовою, організованою групою або злочинною організацією 3. Кримінальне правопорушення визнається вчиненим організованою групою, якщо в його готуванні або вчиненні брали участь декілька осіб (три і більше), які попередньо зорганізувалися у стійке об'єднання для вчинення цього та іншого (інших) кримінальних правопорушень, об'єднаних єдиним планом з розподілом функцій учасників групи, спрямованих на досягнення цього плану, відомого всім учасникам групи. **Стаття 357.** Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження 1. Викрадення, привласнення, вимагання офіційних документів, штампів чи печаток або заволодіння ними шляхом шахрайства чи зловживання особи своїм службовим становищем, а так само їх умисне знищення, пошкодження чи приховування, а також здійснення таких самих дій відносно приватних документів, що знаходяться на підприємствах, в установах чи організаціях незалежно від форми власності, вчинене з корисливих мотивів або в інших особистих інтересах, - караються штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. **Стаття 185.** Крадіжка 1. Таємне викрадення чужого майна (крадіжка) - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від вісімдесяти до двохсот сорока годин, або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до п’яти років.		

1	2	3	4
	Стаття 190. Шахрайство 1. Заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (шахрайство) - карається штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від двохсот до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років.		
Стаття 10 **Відповідальність юридичних осіб** 1. Держави-члени вживають необхідних заходів для забезпечення того, щоб юридичні особи могли бути притягнуті до відповідальності за злочини, зазначені у статтях 3-8, вчинені в їхніх інтересах будь-якою особою, яка діє індивідуально або як частина тіла юридичної особи та займає провідне становище в юридичній особі, виходячи з одного з наступного: - повноваження на представництво юридичної особи; - повноваження приймати рішення від імені юридичної особи; - повноваження здійснювати контроль всередині юридичної особи. 2. Держави-члени вживають необхідних заходів для забезпечення притягнення	**Кримінальний кодекс України** **Стаття 96-4. Юридичні особи, до яких застосовуються заходи кримінально-правового характеру** 1. Заходи кримінально-правового характеру, у випадках, передбачених пунктами 1 і 2 частини першої статті 96-3 цього Кодексу, можуть бути застосовані судом до підприємства, установи чи організації, крім державних органів, органів влади Автономної Республіки Крим, органів місцевого самоврядування, організацій, створених ними у встановленому порядку, що повністю утримуються за рахунок відповідно державного чи місцевого бюджетів, фондів загальнообов'язкового державного соціального страхування, Фонду гарантування вкладів фізичних осіб, а також міжнародних організацій. 2. Заходи кримінально-правового характеру, у випадках, передбачених пунктами 3-6 частини першої статті 96-3 цього Кодексу, можуть бути застосовані судом до суб'єктів приватного та публічного права резидентів та нерезидентів України, включаючи підприємства, установи чи організації, державні органи, органи влади Автономної Республіки Крим, органи місцевого самоврядування, організації, створені ними у встановленому порядку, фонди, а також міжнародні організації, інші юридичні особи, що створені у відповідності до вимог національного чи міжнародного права. Якщо держава або суб'єкт державної власності володіє часткою більше 25 відсотків в юридичній особі або юридична особа знаходиться під ефективним контролем держави чи суб'єкта державної власності, то дана юридична особа несе цивільну відповідальність у повному обсязі за неправомірно отриману вигоду та шкоду, заподіяну кримінальним правопорушенням, що вчинене державою, суб'єктами державної власності або державного управління. 3. У разі реорганізації юридичних осіб, зазначених у частинах першій та другій цієї статті, заходи кримінально-правового характеру можуть бути застосовані до їх правонаступників, до яких перейшли майно, права та обов'язки, пов'язані з вчиненням кримінальних правопорушень, зазначених пунктами 1-6 частини першої статті 96-3 цього Кодексу.	**Відповідає**	

1	2	3	4
юридичних осіб до відповідальності, якщо відсутність нагляду або контролю з боку особи, зазначеної в частині 1, дозволила вчиненню особою, що перебуває під її керівництвом, будь-якого зі злочинів, зазначених у статтях 3-8, на користь такої юридичної особи. 3. Відповідальність юридичних осіб за пунктами 1 і 2 не виключає кримінального провадження проти фізичних осіб, які є виконавцями або підбурювачами до будь-якого зі злочинів, зазначених у статтях 3 - 8, або співучасниками будь-якого зі злочинів.	**Стаття 209. Легалізація (відмивання) майна, одержаного злочинним шляхом** 1. Набуття, володіння, використання, розпорядження майном, щодо якого фактичні обставини свідчать про його одержання злочинним шляхом, у тому числі здійснення фінансової операції, вчинення правочину з таким майном, або переміщення, зміна форми (перетворення) такого майна, або вчинення дій, спрямованих на приховування, маскування походження такого майна або володіння ним, права на таке майно, джерела його походження, місцезнаходження, якщо ці діяння вчинені особою, яка знала або повинна була знати, що таке майно прямо чи опосередковано, повністю чи частково одержано злочинним шляхом, - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до двох років та з конфіскацією майна. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або у великому розмірі, - караються позбавленням волі на строк від п’яти до восьми років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією майна. 3. Дії, передбачені частиною першою або другою цієї статті, вчинені організованою групою або в особливо великому розмірі, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією майна. **Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю** Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, - караються штрафом від трьох тисяч до восьми тисяч неоподатковуваних мінімумів доходів громадян. **Примітка.** Публічне, у тому числі через засоби масової інформації, журналістів, громадські об’єднання, професійні спілки, повідомлення особою інформації про вчинення кримінального або іншого правопорушення, здійснене з дотриманням вимог закону, не є діями, передбаченими цією статтею, і не тягне за собою кримінальну відповідальність. **Стаття 232. Розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках** Умисне розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках без згоди її власника особою, якій ця таємниця		

1	2	3	4
	відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років. **Стаття 255. Створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній** 1. Створення злочинної організації, керівництво такою організацією або її структурними частинами - караються позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна. 2. Участь у злочинній організації - карається позбавленням волі на строк від п’яти до дванадцяти років з конфіскацією майна. **Стаття 27.** Види співучасників 1. Співучасниками кримінального правопорушення, поряд із виконавцем, є організатор, підбурювач та пособник. 2. Виконавцем (співвиконавцем) є особа, яка у співучасті з іншими суб'єктами кримінального правопорушення безпосередньо чи шляхом використання інших осіб, що відповідно до закону не підлягають кримінальній відповідальності за скоєне, вчинила кримінальне правопорушення, передбачене цим Кодексом. 3. Організатором є особа, яка організувала вчинення кримінального правопорушення (кримінальних правопорушень) або керувала його (їх) підготовкою чи вчиненням. Організатором також є особа, яка утворила організовану групу чи злочинну організацію або керувала нею, або особа, яка забезпечувала фінансування чи організовувала приховування кримінально протиправної діяльності організованої групи або злочинної організації. 4. Підбурювачем є особа, яка умовлянням, підкупом, погрозою, примусом або іншим чином схилила іншого співучасника до вчинення кримінального правопорушення. 5. Пособником є особа, яка порадами, вказівками, наданням засобів чи знарядь або усуненням перешкод сприяла вчиненню кримінального правопорушення іншими співучасниками, а також особа, яка заздалегідь обіцяла переховати особу, яка вчинила кримінальне правопорушення, знаряддя чи засоби вчинення кримінального правопорушення, сліди кримінального правопорушення чи предмети, здобуті кримінально протиправним шляхом, придбати чи збути такі предмети або іншим чином сприяти приховуванню кримінального правопорушення. **Стаття 28.** Вчинення кримінального правопорушення групою осіб, групою осіб за попередньою змовою, організованою групою або злочинною організацією		

1	2	3	4
	1. Кримінальне правопорушення визнається таким, що вчинене групою осіб, якщо у ньому брали участь декілька (два або більше) виконавців без попередньої змови між собою. 2. Кримінальне правопорушення визнається вчиненим за попередньою змовою групою осіб, якщо його спільно вчинили декілька осіб (дві або більше), які заздалегідь, тобто до початку кримінального правопорушення, домовилися про спільне його вчинення. 3. Кримінальне правопорушення визнається вчиненим організованою групою, якщо в його готуванні або вчиненні брали участь декілька осіб (три і більше), які попередньо зорганізувалися у стійке об'єднання для вчинення цього та іншого (інших) кримінальних правопорушень, об'єднаних єдиним планом з розподілом функцій учасників групи, спрямованих на досягнення цього плану, відомого всім учасникам групи. 4. Кримінальне правопорушення визнається вчиненим злочинною організацією, якщо він скоєний стійким ієрархічним об'єднанням декількох осіб (п'ять і більше), члени якого або структурні частини якого за попередньою змовою зорганізувалися для спільної діяльності з метою безпосереднього вчинення тяжких або особливо тяжких злочинів учасниками цієї організації, або керівництва чи координації кримінально протиправної діяльності інших осіб, або забезпечення функціонування як самої злочинної організації, так і інших кримінально протиправних груп. **Стаття 29.** Кримінальна відповідальність співучасників 1. Виконавець (співвиконавець) підлягає кримінальній відповідальності за статтею Особливої частини Кримінального Кодексу України, яка передбачає вчинене ним кримінальне правопорушення. 2. Організатор, підбурювач та пособник підлягають кримінальній відповідальності за відповідною частиною статті 27 і тією статтею (частиною статті) Особливої частини цього Кодексу, яка передбачає кримінальне правопорушення, вчинене виконавцем. 3. Ознаки, що характеризують особу окремого співучасника кримінального правопорушення, ставляться в вину лише цьому співучасникові. Інші обставини, що обтяжують відповідальність і передбачені у статтях Особливої частини цього Кодексу як ознаки кримінального правопорушення, що впливають на кваліфікацію дій виконавця, ставляться в вину лише співучаснику, який усвідомлював ці обставини. 4. У разі вчинення виконавцем незакінченого кримінального правопорушення інші співучасники підлягають кримінальній відповідальності за співучасть у незакінченому кримінальному правопорушенні. 5. Співучасники не підлягають кримінальній відповідальності за діяння, вчинене виконавцем, якщо воно не охоплювалося їхнім умислом.		

1	2	3	4
	Стаття 30. Кримінальна відповідальність організаторів та учасників організованої групи чи злочинної організації 1. Організатор організованої групи чи злочинної організації підлягає кримінальній відповідальності за всі кримінальні правопорушення, вчинені організованою групою чи злочинною організацією, якщо вони охоплювалися його умислом. 2. Інші учасники організованої групи чи злочинної організації підлягають кримінальній відповідальності за кримінальні правопорушення, у підготовці або вчиненні яких вони брали участь, незалежно від тієї ролі, яку виконував у кримінальному правопорушенні кожен із них. **Стаття 364^{-1}.** Зловживання повноваженнями службовою особою юридичної особи приватного права незалежно від організаційно-правової форми 1. Зловживання повноваженнями, тобто умисне, з метою одержання неправомірної вигоди для себе чи інших осіб використання всупереч інтересам юридичної особи приватного права незалежно від організаційно-правової форми службовою особою такої юридичної особи своїх повноважень, якщо це завдало істотної шкоди охоронюваним законом правам або інтересам окремих громадян, або державним чи громадським інтересам, або інтересам юридичних осіб, - карається штрафом від однієї тисячі до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або арештом на строк до трьох місяців, або обмеженням волі на строк до двох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років. 2. Те саме діяння, якщо воно спричинило тяжкі наслідки, - карається штрафом від чотирьох тисяч до шести тисяч неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або позбавленням волі на строк від трьох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років. **Стаття 367.** Службова недбалість 1. Службова недбалість, тобто невиконання або неналежне виконання службовою особою своїх службових обов'язків через несумлінне ставлення до них, що завдало істотної шкоди охоронюваним законом правам, свободам та інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, - карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років. 2. Те саме діяння, якщо воно спричинило тяжкі наслідки, -		

1	2	3	4
	карається позбавленням волі на строк від двох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та зі штрафом від двохсот п'ятдесяти до семисот п'ятдесяти неоподатковуваних мінімумів доходів громадян або без такого. **Стаття 368[-3].** Підкуп службової особи юридичної особи приватного права незалежно від організаційно-правової форми 1. Пропозиція чи обіцянка службовій особі юридичної особи приватного права незалежно від організаційно-правової форми надати їй або третій особі неправомірну вигоду, а так само надання такої вигоди або прохання її надати за вчинення зазначеною службовою особою дій чи її бездіяльність з використанням наданих їй повноважень в інтересах того, хто пропонує, обіцяє чи надає таку вигоду, або в інтересах третьої особи - караються штрафом від однієї тисячі до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від ста до двохсот годин, або обмеженням волі на строк до двох років, або позбавленням волі на той самий строк. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб чи організованою групою, - караються штрафом від двох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк. 3. Прийняття пропозиції, обіцянки або одержання службовою особою юридичної особи приватного права незалежно від організаційно-правової форми неправомірної вигоди для себе чи третьої особи за вчинення дій або бездіяльність з використанням наданих їй повноважень в інтересах того, хто пропонує, обіцяє чи надає таку вигоду, або в інтересах третьої особи - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років. 4. Дії, передбачені частиною третьою цієї статті, вчинені повторно або за попередньою змовою групою осіб чи поєднані з вимаганням неправомірної вигоди, - караються позбавленням волі на строк від трьох до семи років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, з конфіскацією майна. **Стаття 368[-4].** Підкуп особи, яка надає публічні послуги 1. Пропозиція чи обіцянка аудитору, нотаріусу, оцінювачу, іншій особі, яка не є державним службовцем, посадовою особою місцевого самоврядування, але провадить професійну діяльність, пов’язану з наданням публічних послуг, у тому числі послуг експерта, арбітражного		

1	2	3	4
	керуючого, приватного виконавця, незалежного посередника, члена трудового арбітражу, третейського судді (під час виконання цих функцій), надати йому/їй або третій особі неправомірну вигоду, а так само надання такої вигоди або прохання її надати за вчинення особою, яка надає публічні послуги, дій або її бездіяльність з використанням наданих їй повноважень в інтересах того, хто пропонує, обіцяє чи надає таку вигоду, або в інтересах третьої особи - караються штрафом від однієї тисячі до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від ста до двохсот годин, або обмеженням волі на строк до двох років, або позбавленням волі на той самий строк. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб чи організованою групою, - караються штрафом від двох тисяч до п'яти тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк. 3. Прийняття пропозиції, обіцянки або одержання аудитором, нотаріусом, приватним виконавцем, експертом, оцінювачем, третейським суддею або іншою особою, яка провадить професійну діяльність, пов'язану з наданням публічних послуг, а також незалежним посередником чи арбітром під час розгляду колективних трудових спорів неправомірної вигоди для себе чи третьої особи за вчинення дій або бездіяльність з використанням наданих їй повноважень в інтересах того, хто пропонує, обіцяє чи надає таку вигоду, або в інтересах третьої особи - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк від одного до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років. 4. Дії, передбачені частиною третьою цієї статті, вчинені повторно або за попередньою змовою групою осіб чи поєднані з вимаганням неправомірної вигоди, - караються позбавленням волі на строк від чотирьох до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, з конфіскацією майна. **Стаття 354.** Підкуп працівника підприємства, установи чи організації 1. Пропозиція чи обіцянка працівникові підприємства, установи чи організації, який не є службовою особою, або особі, яка працює на користь підприємства, установи чи організації, надати йому (їй) або третій особі неправомірну вигоду, а так само надання такої вигоди за		

1	2	3	4
	вчинення чи невчинення працівником будь-яких дій з використанням становища, яке він займає, або особою, яка працює на користь підприємства, установи чи організації, в інтересах того, хто пропонує, обіцяє чи надає таку вигоду, або в інтересах третьої особи - караються штрафом від ста до двохсот п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до ста годин, або виправними роботами на строк до одного року, або обмеженням волі на строк до двох років, або позбавленням волі на той самий строк. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від двохсот п'ятдесяти до п'ятисот неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від ста до двохсот годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк. 3. Прийняття пропозиції, обіцянки або одержання працівником підприємства, установи чи організації, який не є службовою особою, або особою, яка працює на користь підприємства, установи чи організації, неправомірної вигоди, а так само прохання надати таку вигоду для себе чи третьої особи за вчинення чи невчинення будь-яких дій з використанням становища, яке займає працівник на підприємстві, в установі чи організації, або у зв'язку з діяльністю особи на користь підприємства, установи чи організації, в інтересах того, хто пропонує, обіцяє чи надає таку вигоду, або в інтересах третьої особи - караються штрафом від двохсот п'ятдесяти до п'ятисот неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від ста до двохсот годин, або обмеженням волі на строк до двох років, або позбавленням волі на той самий строк. 4. Дії, передбачені частиною третьою цієї статті, вчинені повторно або за попередньою змовою групою осіб чи поєднані з вимаганням неправомірної вигоди, - караються штрафом від п'ятисот до семисот п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від ста шістдесяти до двохсот сорока годин, або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк. 5. У статтях 354, 368, 368^{-3} і 368^{-4} цього Кодексу під вимаганням неправомірної вигоди слід розуміти вимогу щодо надання неправомірної вигоди з погрозою вчинення дій або бездіяльності з використанням свого становища, наданих повноважень, влади, службового становища стосовно особи, яка надає неправомірну вигоду, або умисне створення умов, за яких особа вимушена надати неправомірну вигоду з метою запобігання шкідливим наслідкам щодо своїх прав і законних інтересів.		

1	2	3	4
Стаття 11 **Санкції проти юридичних осіб** 1. Держави-члени вживають необхідних заходів для забезпечення того, щоб юридична особа, притягнута до відповідальності згідно зі Статтею 10(1), була покарана ефективними, пропорційними та переконливими санкціями, які включають кримінальні або некримінальні штрафи та які можуть включати інші санкції, такі як: - виключення з права на суспільні блага або допомогу; - тимчасова або постійна дискваліфікація з практики комерційної діяльності; - Приміщення (поміщення) під судовий нагляд; - судова ліквідація; - тимчасове або постійне закриття закладів, які використовувалися для вчинення правопорушення. 2. Держави-члени вживають необхідних заходів для забезпечення того, щоб юридична особа, притягнута до відповідальності згідно зі Статтею 10(2), була покарана ефективними, пропорційними та стримуючими санкціями або іншими заходами.	**Санкції статей 27-30, 209, 255, 354, 364-1, 367, 368-3, 368-4 Кримінального кодексу України.** **Стаття 96-6. Види заходів кримінально-правового характеру, що застосовуються до юридичних осіб** 1. До юридичних осіб судом можуть бути застосовані такі заходи кримінально-правового характеру: 1) штраф; 2) конфіскація майна; 3) ліквідація. 2. До юридичних осіб штраф та ліквідація можуть застосовуватися лише як основні заходи кримінально-правового характеру, а конфіскація майна - лише як додатковий. При застосуванні заходів кримінально-правового характеру юридична особа зобов'язана відшкодувати нанесені збитки та шкоду в повному обсязі, а також розмір отриманої неправомірної вигоди, яка отримана або могла бути отримана юридичною особою.	**Відповідає**	

1	2	3	4
Стаття 12 **Юрисдикції** 1. Держави-члени встановлюють свою юрисдикцію стосовно злочинів, зазначених у статтях 3 - 8, якщо злочин було вчинено: 1 повністю або частково в межах своєї території; або 2 одним із їхніх громадян, принаймні у випадках, коли діяння є злочином, у якому воно було вчинене. 2. При встановленні юрисдикції відповідно до пункту (1) частини 1 держава-член забезпечує, щоб вона мала юрисдикцію, якщо: - злочинець вчиняє правопорушення, фізично перебуваючи на його території, незалежно від того, чи є злочин проти інформаційної системи на його території; або - Злочин скоєно проти інформаційної системи на її території, незалежно від того, чи вчиняє злочинець правопорушення, перебуваючи фізично на її території. 3. Держава-член інформує Комісію, якщо вона вирішує встановити юрисдикцію щодо злочину, зазначеного у статтях 3-8, вчиненого за межами її території, у тому числі, якщо:	**Кримінальний кодекс України** **Стаття 6. Чинність закону про кримінальну відповідальність щодо кримінального правопорушення, вчиненого на території України** 1. Особи, які вчинили кримінальні правопорушення на території України, підлягають кримінальній відповідальності за цим Кодексом. 2. Кримінальне правопорушення визнається вчиненим на території України, якщо його було почато, продовжено, закінчено або припинено на території України. 3. Кримінальне правопорушення визнається вчиненим на території України, якщо його виконавець або хоча б один із співучасників діяв на території України. 4. Питання про кримінальну відповідальність дипломатичних представників іноземних держав та інших громадян, які за законами України і міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, не є підсудні у кримінальних справах судам України, в разі вчинення ними кримінального правопорушення на території України вирішується дипломатичним шляхом. **Стаття 7. Чинність закону про кримінальну відповідальність щодо кримінальних правопорушень, вчинених громадянами України або особами без громадянства за межами України** 1. Громадяни України та особи без громадянства, що постійно проживають в Україні, які вчинили кримінальні правопорушення за її межами, підлягають кримінальній відповідальності за цим Кодексом, якщо інше не передбачено міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України. 2. Якщо особи, зазначені у частині першій цієї статті, за вчинені кримінальні правопорушення зазнали кримінального покарання за межами України, вони не можуть бути притягнені в Україні до кримінальної відповідальності за ці кримінальні правопорушення. **Стаття 8. Чинність закону про кримінальну відповідальність щодо кримінальних правопорушень, вчинених іноземцями або особами без громадянства за межами України** 1. Іноземці або особи без громадянства, що не проживають постійно в Україні, які вчинили кримінальні правопорушення за її межами, підлягають в Україні відповідальності за цим Кодексом у випадках, передбачених міжнародними договорами або якщо вони вчинили передбачені цим Кодексом тяжкі або особливо тяжкі злочини проти прав і свобод громадян України або інтересів України. 2. Іноземці або особи без громадянства, що не проживають постійно в Україні, також підлягають в Україні відповідальності згідно з цим Кодексом, якщо вони за межами України вчинили у співучасті із службовими особами, які є громадянами України, будь-яке кримінальне правопорушення, передбачене у статтях 368, 368-3, 368-4, 369 і 369-2 цього Кодексу, або якщо	**Відповідає**	

1	2	3	4
- злочинець має своє звичайне місце проживання на її території; або - злочин вчинено в інтересах юридичної особи, заснованого на його території.	вони пропонували, обіцяли, надали неправомірну вигоду таким службовим особам, або прийняли пропозицію, обіцянку неправомірної вигоди чи одержали від них таку вигоду. **Стаття 10. Вирішення питання про кримінальну відповідальність осіб, які підлягають кримінальній відповідальності за законодавством іноземної держави і перебувають на території України, та виконання вироків, винесених іноземними судами чи міжнародними судовими установами** 1. Громадяни України, які вчинили злочини поза межами України, не можуть бути видані іноземній державі для притягнення до кримінальної відповідальності та віддання до суду. 2. Іноземці та особи без громадянства, які вчинили злочини поза межами України і перебувають на території України, можуть бути видані іноземній державі для притягнення до кримінальної відповідальності і віддання до суду. 3. Україна може перейняти кримінальне провадження, в якому судовими органами іноземної держави не ухвалено вирок, щодо громадян України та іноземців, які вчинили злочини за межами України і перебувають на території України, але які не можуть бути видані іноземній державі або у видачі яких відмовлено, якщо діяння, у зв'язку з яким запитується передача кримінального провадження, згідно з цим Кодексом визнається злочином. 4. Виконання в Україні вироку іноземного суду чи міжнародної судової установи можливо, якщо діяння, внаслідок вчинення якого було ухвалено вирок, згідно з цим Кодексом визнається кримінальним правопорушенням або було б кримінальним правопорушенням у разі його вчинення на території України. Кримінальний процесуальний кодекс України **Кримінальний процесуальний кодекс України** **Стаття 4. Дія Кодексу в просторі** 1. Кримінальне провадження на території України здійснюється з підстав та в порядку, передбачених цим Кодексом, незалежно від місця вчинення кримінального правопорушення. 2. Кримінальне процесуальне законодавство України застосовується також при здійсненні провадження щодо кримінальних правопорушень, вчинених на території дипломатичного представництва чи консульської установи України за кордоном, на повітряному, морському чи річковому судні, що перебуває за межами України під прапором або з розпізнавальним знаком України, якщо це судно приписано до порту, розташованого в Україні. 3. Якщо міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, передбачено поширення юрисдикції України на особовий склад Збройних Сил України, який перебуває на території іншої держави, то провадження щодо кримінальних правопорушень, вчинених на території іншої держави стосовно особи з такого особового складу, здійснюється в порядку, передбаченому цим Кодексом.		

1	2	3	4
	Розділ IX МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ Глава 42. Загальні засади міжнародного співробітництва **Стаття 542. Обсяг міжнародного співробітництва під час кримінального провадження** 1. Міжнародне співробітництво під час кримінального провадження полягає у вжитті необхідних заходів з метою надання міжнародної правової допомоги шляхом вручення документів, виконання окремих процесуальних дій, видачі осіб, які вчинили кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування, передачі засуджених осіб та виконання вироків. Міжнародним договором України можуть бути передбачені інші, ніж у цьому Кодексі, форми співробітництва під час кримінального провадження. **Стаття 543. Законодавство, що регулює міжнародне співробітництво під час кримінального провадження** 1. Порядок направлення запиту до іншої держави, порядок розгляду уповноваженим (центральним) органом України запиту іншої держави або міжнародної судової установи про таку допомогу і порядок виконання такого запиту визначаються цим Кодексом і чинними міжнародними договорами України. **Стаття 544. Надання та отримання міжнародної правової допомоги чи іншого міжнародного співробітництва без договору** 1. За відсутності міжнародного договору України міжнародна правова допомога чи інше співробітництво може бути надано на підставі запиту іншої держави чи запитано на засадах взаємності. 2. Уповноважений (центральний) орган України, направляючи до такої держави запит, письмово гарантує запитуваній стороні розглянути в майбутньому її запит про надання такого самого виду міжнародної правової допомоги. 3. Згідно з умовами частини першої цієї статті уповноважений (центральний) орган України розглядає запит іноземної держави лише за наявності письмової гарантії запитуючої сторони прийняти і розглянути в майбутньому запит України на засадах взаємності. 4. Уповноважений (центральний) орган України при зверненні за міжнародною правовою допомогою до такої держави та наданні такій державі міжнародної правової допомоги керується цим Кодексом. 5. За відсутності міжнародного договору з відповідною державою уповноважений (центральний) орган України надсилає запит про надання міжнародної правової допомоги до Міністерства закордонних справ України для подальшого передання його компетентному органу запитуваної сторони дипломатичним шляхом.		

1	2	3	4
	Стаття 545. Центральний орган України 1. Офіс Генерального прокурора звертається із запитами про міжнародну правову допомогу у кримінальному провадженні під час досудового розслідування та розглядає відповідні запити іноземних компетентних органів, крім досудового розслідування кримінальних правопорушень, віднесених до підслідності Національного антикорупційного бюро України, яке у таких випадках здійснює функції центрального органу України. 2. Міністерство юстиції України звертається із запитами судів про міжнародну правову допомогу у кримінальному провадженні під час судового провадження та розглядає відповідні запити судів іноземних держав. 3. Офіс Генерального прокурора та Міністерство юстиції України у триденний строк надсилають до Національного антикорупційного бюро України отримані (надані) у рамках надання міжнародної правової допомоги матеріали, які стосуються фінансових та корупційних кримінальних правопорушень, у вигляді довідки. 4. Якщо цим Кодексом або чинним міжнародним договором України передбачено інший порядок зносин, на визначений цими законодавчими актами орган поширюються повноваження, передбачені частинами першою, другою цієї статті. **Стаття 548. Запит про міжнародне співробітництво** 1. Запит (доручення, клопотання) про міжнародне співробітництво складається органом, який здійснює кримінальне провадження, або уповноваженим ним органом згідно з вимогами цього Кодексу та відповідного міжнародного договору України, а за його відсутності - згідно з цим Кодексом. 2. Запит і долучені до нього документи складаються у письмовій формі, засвідчуються підписом уповноваженої особи та печаткою відповідного органу. 3. Запит і долучені до нього документи супроводжуються засвідченим у встановленому порядку перекладом мовою, визначеною відповідним міжнародним договором України, а за відсутності такого договору - офіційною мовою запитуваної сторони або іншою прийнятною для цієї сторони мовою. 4. Запит надсилається за кордон поштою, а в невідкладних випадках електронним, факсимільним або іншим засобом зв’язку. У такому разі оригінал запиту надсилається поштою не пізніше трьох днів з моменту його передання електронною поштою, факсимільним або іншим засобом зв’язку. 5. Уповноважений (центральний) орган України може прийняти до розгляду запит, який надійшов від запитуючої сторони електронним, факсимільним або іншим засобом зв’язку. Виконання такого запиту здійснюється виключно за умови підтвердження надіслання або		

1	2	3	4
	передачі його оригіналу. Направлення компетентному органу іноземної держави матеріалів виконання запиту можливе тільки після отримання українською стороною оригіналу запиту. Глава 43. Міжнародна правова допомога при проведенні процесуальних дій **Стаття 551. Запит про міжнародну правову допомогу** 1. Суд, прокурор або слідчий за погодженням з прокурором надсилає до уповноваженого (центрального) органу України запит про міжнародну правову допомогу у кримінальному провадженні, яке він здійснює. 2. Уповноважений (центральний) орган України розглядає запит на предмет обґрунтованості і відповідності вимогам законів та міжнародних договорів України. 3. У разі прийняття рішення про направлення запиту уповноважений (центральний) орган України протягом десяти днів надсилає запит уповноваженому (центральному) органу запитуваної сторони безпосередньо або дипломатичним шляхом. 4. У разі відмови у направленні запиту всі матеріали протягом десяти днів повертаються відповідному органу України з викладом недоліків, які потрібно усунути, або з поясненням причин неможливості направлення запиту. **Стаття 561. Процесуальні дії, які можуть бути проведені в порядку надання міжнародної правової допомоги** 1. На території України з метою виконання запиту про надання міжнародної правової допомоги можуть бути проведені будь-які процесуальні дії, передбачені цим Кодексом або міжнародним договором. **Стаття 562. Процесуальні дії, які потребують спеціального дозволу** 1. Якщо для виконання запиту компетентного органу іноземної держави необхідно провести процесуальну дію, виконання якої в Україні можливе лише з дозволу прокурора або суду, така дія здійснюється лише за умови отримання відповідного дозволу в порядку, передбаченому цим Кодексом, навіть якщо законодавство запитуючої сторони цього не передбачає. Підставою для вирішення питання щодо надання такого дозволу є матеріали звернення компетентного органу іноземної держави. 2. У разі якщо при зверненні за допомогою в іноземній державі необхідно виконати процесуальну дію, для проведення якої в Україні потрібен дозвіл прокурора або суду, така процесуальна дія потребує надання відповідного дозволу прокурором або судом у порядку, встановленому цим Кодексом, лише у разі, якщо це передбачено міжнародним договором або є обов'язковою умовою надання такого виду допомоги за законодавством запитуваної сторони. При цьому строк дії такого дозволу не обмежується, а належно засвідчена копія дозволу долучається до матеріалів запиту. Глава 45. Кримінальне провадження у порядку перейняття		

1	2	3	4
	Стаття 595. Порядок і умови перейняття кримінального провадження від іноземних держав 1. Клопотання компетентних органів інших держав про перейняття Україною кримінального провадження розглядається центральним органом України щодо міжнародної правової допомоги або органом, уповноваженим здійснювати зносини відповідно до частини третьої статті 545 цього Кодексу, протягом двадцяти днів з дня його надходження. 2. Кримінальне провадження, в якому судовими органами іноземної держави не було ухвалено вирок, може бути перейняте Україною за таких умов: 1) особа, яка притягається до кримінальної відповідальності, є громадянином України і перебуває на її території; 2) особа, яка притягається до кримінальної відповідальності, є іноземцем або особою без громадянства і перебуває на території України, а її видача згідно із цим Кодексом або міжнародним договором України неможлива або у видачі відмовлено; 3) запитуюча держава надала гарантії, що у разі ухвалення вироку в Україні особа, яка притягається до кримінальної відповідальності, не піддаватиметься у запитуючій державі державному обвинуваченню за те ж кримінальне правопорушення; 4) діяння, якого стосується запит, є кримінальним правопорушенням за законом України про кримінальну відповідальність. 3. У разі перейняття кримінального провадження Офіс Генерального прокурора в порядку, передбаченому цим Кодексом, доручає здійснення досудового розслідування відповідному прокурору, про що повідомляє державу, яка надіслала запит. 4. При відмові перейняти кримінальне провадження Офіс Генерального прокурора повертає матеріали відповідним органам іноземної держави з обґрунтуванням підстав відмови. **Закон України «Про ратифікацію Конвенції про кіберзлочинність»** від 7 вересня 2005 р. відповідно відповідно до підпункту 7.a статті 24: в Україні органами, на які покладаються повноваження згідно з пунктом 7 статті 24 Конвенції, є Міністерство юстиції України (щодо запитів судів) і Генеральна прокуратура України (щодо запитів органів досудового слідства); відповідно до підпункту 2.c статті 27: в Україні органами, відповідальними за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам, є Міністерство юстиції України (щодо доручень судів) та Генеральна прокуратура України (щодо доручень органів досудового слідства).		

1	2	3	4
Стаття 13 **Обмін інформацією** 1. З метою обміну інформацією стосовно злочинів, зазначених у статтях 3-8, держави-члени забезпечують, щоб вони мали оперативний національний контактний пункт і використовували існуючу мережу оперативних контактних пунктів, доступних 24 години на добу та сім днів на тиждень. Держави-члени також забезпечують, щоб у них були передбачені процедури таким чином, щоб у разі термінових запитів про допомогу компетентний орган міг протягом восьми годин з моменту отримання принаймні визначити, чи буде відповідь на запит, а також форму та орієнтовний час такої відповіді. 2. Держави-члени інформують Комісію про призначену ними контактну особу, зазначену в параграфі 1. Комісія надсилає таку інформацію іншим державам-членам та компетентним спеціалізованим установам та органам Союзу. 3. Держави-члени вживають необхідних заходів для забезпечення надання належних каналів звітування з метою	**Закон України «Про ратифікацію Конвенції про кіберзлочинність»** від 7 вересня 2005 р. відповідно до пункту 1 статті 35: в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. (Закон доповнено абзацом згідно із Законом від 21.09.2010) **ЗУ «Про Національну поліцію»** Розділ IV Стаття 23. Основні повноваження поліції 42) здійснює представництво та забезпечує виконання зобов’язань України в Міжнародній організації кримінальної поліції - Інтерполі та виступає як Національне центральне бюро Інтерполу; 43) здійснює співробітництво з Європейським поліцейським офісом (Європолом) та діє як Національний контактний пункт між компетентними органами України та Європолом; 44) організовує взаємодію правоохоронних та інших державних органів України з Міжнародною організацією кримінальної поліції - Інтерполом, Європейським поліцейським офісом (Європолом), а також компетентними органами інших держав з питань, що належать до сфери діяльності Інтерполу та Європолу. Відповідно до Положення про Департамент кіберполіції Національної поліції України затвердженого наказом Національної поліції України 10.11.2015 № 85 (в редакції від 07.11.2019 № 1136) Департамент кіберполіції НПУ відповідно до законодавства створює та забезпечує функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні кримінальних правопорушень, пов’язаних з комп’ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких кримінальних правопорушень, а також збирання доказів в електронній формі.	**Відповідає**	

1	2	3	4
полегшення повідомлення компетентних національних органів про злочини, зазначені у статтях 3-6.			
Стаття 14 **Моніторинг та статистика** 1. Держави-члени забезпечують наявність системи обліку, виготовлення та надання статистичних даних про злочини, зазначені у статтях 3-7. 2. Статистичні дані, зазначені в частині 1, повинні, як мінімум, охоплювати існуючі дані про кількість злочинів, зазначених у статтях 3-7, зареєстрованих державами-членами, та кількість осіб, притягнутих до кримінальної відповідальності та засуджених за злочини, зазначені у статтях 3-7. 3. Держави-члени передають дані, зібрані відповідно до цієї статті, Комісії. Комісія забезпечує публікацію та подання консолідованого огляду статистичних звітів компетентним спеціалізованим агенціям та органам Союзу.	Відповідно до частини другої статті 214 КПК України та Положення про порядок ведення Єдиного реєстру досудових розслідувань, затвердженого наказом Генеральної прокуратури України від 06.04.2016 № 139, зареєстрованого в Міністерстві юстиції України 05.05.2016 за № 680/28810, з метою забезпечення єдиного обліку, аналізу стану та структури кримінальних правопорушень, вчинених у державі, ведеться Єдиний реєстр досудових розслідувань (далі – Реєстр), держателем якого є Генеральна прокуратура України. Відомості з Реєстру надаються у вигляді «Витягу з Єдиного реєстру досудових розслідувань» в порядку, встановленому КПК України. Відповідно до Положення право доступу до відомостей, які внесені до Реєстру має Держатель Реєстру – у повному обсязі з урахуванням повноважень, якими наділені прокурори та керівники підрозділів Генеральної прокуратури України. Статистичну інформацію, яка відображає публічну інформацію про стан громадської безпеки та дає можливість на базі геоінформаційної системи вести моніторинг в режимі реального часу здійснених правопорушень розміщено на веб-ресурсі https://old.gp.gov.ua/ua/statinfo.html.	**Виходить за межі компетенції НПУ**	

1	2	3	4
Стаття 15 **Заміна рамкового рішення 2005/222/ЮВС** Рамкове рішення 2005/222/ЮВС цим замінюється щодо держав-членів, які беруть участь в ухваленні цієї Директиви, без шкоди для зобов'язань держав-членів щодо строку транспонування Рамкового рішення в національне законодавство. Стосовно держав-членів, які беруть участь в ухваленні цієї Директиви, посилання на Рамкове рішення 2005/222/ЮВС слід тлумачити як покликання на цю Директиву.	-	**Виходить за межі компетенції НПУ**	
Стаття 16 **Транспозиція** 1. Держави-члени повинні ввести в дію закони, підзаконні нормативно-правові акти та адміністративні положення, необхідні для виконання цієї Директиви, до 4 вересня 2015 року. 2. Держави-члени передають Комісії текст заходів, що транспонують у їхнє національне законодавство зобов'язання, покладені на них згідно з цією Директивою.	-	**Виходить за межі компетенції НПУ**	

1	2	3	4
3. Коли держави-члени ухвалюють такі заходи, вони повинні містити посилання на цю Директиву або супроводжуватися таким посиланням з нагоди їх офіційного опублікування. Методи здійснення такого посилання встановлюються державами-членами.			
Стаття 17 **Звітності** Комісія до 4 вересня 2017 року подає звіт Європейському Парламенту та Раді, в якому оцінюється, якою мірою держави-члени вжили необхідних заходів для виконання цієї Директиви, супроводжуваний, у разі необхідності, законодавчими пропозиціями. Комісія також враховує технічні та правові розробки у сфері кіберзлочинності, особливо стосовно сфери застосування цієї Директиви.	- -	**Виходить за межі компетенції НПУ**	

1	2	3	4
Стаття 18 **Набуття чинності** Ця Директива набуває чинності на двадцятий день після її публікації в *Офіційному віснику Європейського Союзу*.		**Виходить за межі компетенції НПУ**	
Стаття 19 **Адресатів** Ця Директива адресована державам-членам відповідно до Договорів. Вчинено в Брюсселі, 12 серпня 2013 року.	-	**Виходить за межі компетенції НПУ**	