Міністерство освіти і науки України
Національний університет «Одеська політехніка»

Д.Д. Татакі

НОРМАТИВНО-ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Конспект лекцій
для здобувачів вищої освіти спеціальності 125 Кібербезпека

Одеса НУ «Одеська політехніка» 2022

Нормативно-правове та організаційне забезпечення захисту інформації: Конспект лекцій / Укладач Д.Д. Татакі. Одеса: НУ «Одеська політехніка», 2022. 158 с.

ЗМІСТ

Лекція 1. ПОНЯТТЯ ІНФОРМАЦІЇ. ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЇ

Питання для опрацювання:

1.1. Інформація: поняття, види

1.2. Правовий захист інформації

Джерела:

1. Цивільний кодекс України від 16.01.2003 року № 435-IV 2341 / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/435-15
2. Про інформацію: ЗУ від 02.10.1992 року № 2657-XII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2657-12
3. Про державну таємницю: ЗУ від 21.01.1994 року № 3855-XII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/3855-12
4. Про звернення громадян: ЗУ від 02.10.1996 року № 393/96-ВР / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/393/96-вр
5. Про захист економічної конкуренції: ЗУ від 11.01.2001 року № 2210-III / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2210-14
6. Про захист персональних даних: ЗУ від 01.06.2010 року № 2297-VI / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/2297-17
7. Про доступ до публічної інформації: ЗУ від 13.01.2011 року № 2939-VI / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2939-17
8. Про критичну інфраструктуру: ЗУ від 16.11.2021 року № 1882-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#n409
9. Про медіа: ЗУ від 13.12.2022 року № 2849-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text
10. Порядок функціонування веб-сайтів органів виконавчої влади, затверджений наказом Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України 25.11.2002 року № 327/225 / Держкомінформ України, Держкомзв'язку та інформатизації. URL: http://zakon2.rada.gov.ua/laws/show/z1022-02

1.1. Інформація: поняття, види

Поняття «інформація» визначено у деяких нормативних актах України, основним з яких є Закон України «Про інформацію». Під інформацією розуміють будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені

в електронному вигляді (ст. 1 Закону). Таке ж визначення міститься і у Цивільному кодексі України (ст. 200 ЦКУ).

Дещо по-іншому охарактеризовано зазначене поняття у Законі України «Про захист економічної конкуренції», а саме: відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості (ст. 1). Отже, поняття «інформація» містить:

1) відомості про події і явища, що відбуваються у суспільстві, державі, навколишньому природному середовищі;

2) дані, які можна зберігати в будь-якій формі й вигляді.

Однак для набуття певного правового статусу ці дані мають відповідати вимогам й ознакам, передбаченим правовими нормами:

1) документовані або публічно оголошені відомості;

2) повідомлення як об'єкт цивільних прав і які відносяться до категорії нематеріальних благ;

3) передбачені або встановлені законом носії інформації як джерела відомостей, які являють собою матеріальні об'єкти, що зберігають інформацію, повідомлення засобів масової інформації, публічні виступи.

У Законі України «Про інформацію» наведено такі основні види інформації за змістом (ст. 10):

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- критична технологічна інформація;

Розглянемо характеристики кожного виду інформації.

Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Основними даними про фізичну особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата й місце народження. Джерелами документованої інформації про особу є видані на її ім'я, підписані нею документи, а також відомості про особу, зібрані державними органами влади і органами місцевого самоврядування в межах своїх повноважень.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, за винятком випадків, передбачених законом. Кожна особа має право на ознайомлення з інформацією, зібраною про неї. Інформація про особу охороняється Законом України «Про захист персональних даних», Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Додатковим протоколом до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних, ратифікованими Україною 6 липня 2010 року.

Інформація довідково-енциклопедичного характеру – це систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя й навколишнє природне середовище. Основними джерелами цієї інформації є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних інформаційних служб, мереж та систем, а також довідки, що даються уповноваженими на те державними органами і органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками і автоматизованими інформаційними системами. Система цієї інформації, доступ до неї регулюються багатьма нормативними актами, серед яких закони України «Про бібліотеки і бібліотечну справу», «Про Національний архівний фонд та архівні установи», «Про рекламу», «Про звернення громадян» та ін. Багато уваги приділяється забезпеченню доступу до інформації через мережу Інтернет (зокрема через веб-сайти органів державної влади та місцевого самоврядування) «Порядок функціонування веб-сайтів органів виконавчої влади» затверджений спільним наказом Державного комітету інформаційної політики, телебачення і радіомовлення України та Державного комітету зв'язку та інформатизації України від 25.11.2002 р. № 327/225 та багато інших.

Інформація про стан довкілля (екологічна інформація) становить відомості та /або дані про:

- стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;

- фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи

адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);

- стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля; також до екологічної може бути віднесено й іншу інформацію.

Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом. Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України «Про інформацію», «Про державну таємницю», та іншими нормативними актами.

Інформація про товар (роботу, послугу) складається з відомостей та / або даних, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

Правовий режим інформації про товар (роботу, послугу) визначається законами України «Про рекламу», «Про захист прав споживачів» та іншими нормативними актами.

Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України. Правовий режим науково-технічної інформації визначається Законом України «Про науково-технічну інформацію» та іншими нормативними актами.

Податкова інформація - сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення й боротьбу з ними і їх профілактику тощо.

Джерелами правової інформації є Конституція України, інші законодавчі й підзаконні нормативні правові акти, міжнародні договори і угоди, норми й принципи

міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

Серед нормативних актів, що регулюють доступ до правової інформації особливо слід відзначити Закон України «Про медіа» та «Про доступ до публічної інформації

З метою забезпечення всім громадянам доступу до законодавчих та інших нормативних актів держава забезпечує видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Статистична інформація – документована інформація, що дає кількісну характеристику масових явищ і процесів, що відбуваються в економічній, соціальній, культурній та інших сферах життя.

Офіційна державна статистична інформація підлягає систематичному оприлюдненню. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежено згідно із законом. Система статистичної інформації, її джерела й режим визначаються Законом України «Про офіційну статистику» й іншими правовими актами в цій галузі.

Соціологічна інформація – будь-які документовані відомості про ставлення окремих громадян і соціальних груп до суспільних подій та явищ, процесів, фактів тощо. Основними джерелами соціологічної інформації є документовані або публічно оголошені відомості, в яких відображено результати соціологічних опитувань, спостережень та інших соціологічних досліджень. Соціологічні дослідження здійснюються державними органами, об'єднаннями громадян, зареєстрованими у встановленому порядку.

Критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів критичної інфраструктури. Правовий режим критичної технологічної інформації визначається Законом України «Про критичну інфраструктуру» та іншими нормативними актами. Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.

Однак закріплені в Законі види інформації не є вичерпними. Науковці виділяють ще декілька її видів, які отримали окреме правове регулювання. Так, наприклад, іноді визначають *комп'ютерну інформацію*: «відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну».

За способом поширення інформації можна визначити *масову інформацію* – тобто інформацію, що поширюється з метою її доведення до необмеженого кола осіб.

Друкованими засобами масової інформації є періодичні друковані видання (преса) – газети, журнали, бюлетені тощо й разові видання з визначеним тиражем.

Аудіовізуальними засобами масової інформації є: радіомовлення, телебачення, кіно, звукозапис, відеозапис тощо.

Порядок створення (заснування) і організації діяльності окремих засобів масової інформації визначається законами України «Про медіа».

1.2. Правовий захист інформації

Основним напрямком в системі захисту інформації є правовий захист інформації, актуальність якого зростає в умовах побудови інформаційного суспільства.

Правова форма захисту інформації - це захист інформації, який «базується на використанні статей Конституції і законів держави, положень цивільного і кримінального кодексів та інших нормативно-правових документів в галузі інформатики, інформаційних відносин та захисту інформації. Вона регламентує права і обов'язки суб'єктів інформаційних відносин, правовий статус органів, технічних засобів і способів захисту інформації і є базою для створення морально-етичних норм в області захисту інформації».

Правовий захист інформації визнаний як на міжнародному (міжнародні договори, угоди, конвенції, декларації тощо), так і на державному рівні. На державному рівні правовий захист регулюється державними та відомчими нормативно-правовими актами *(рис. 1.1)*.

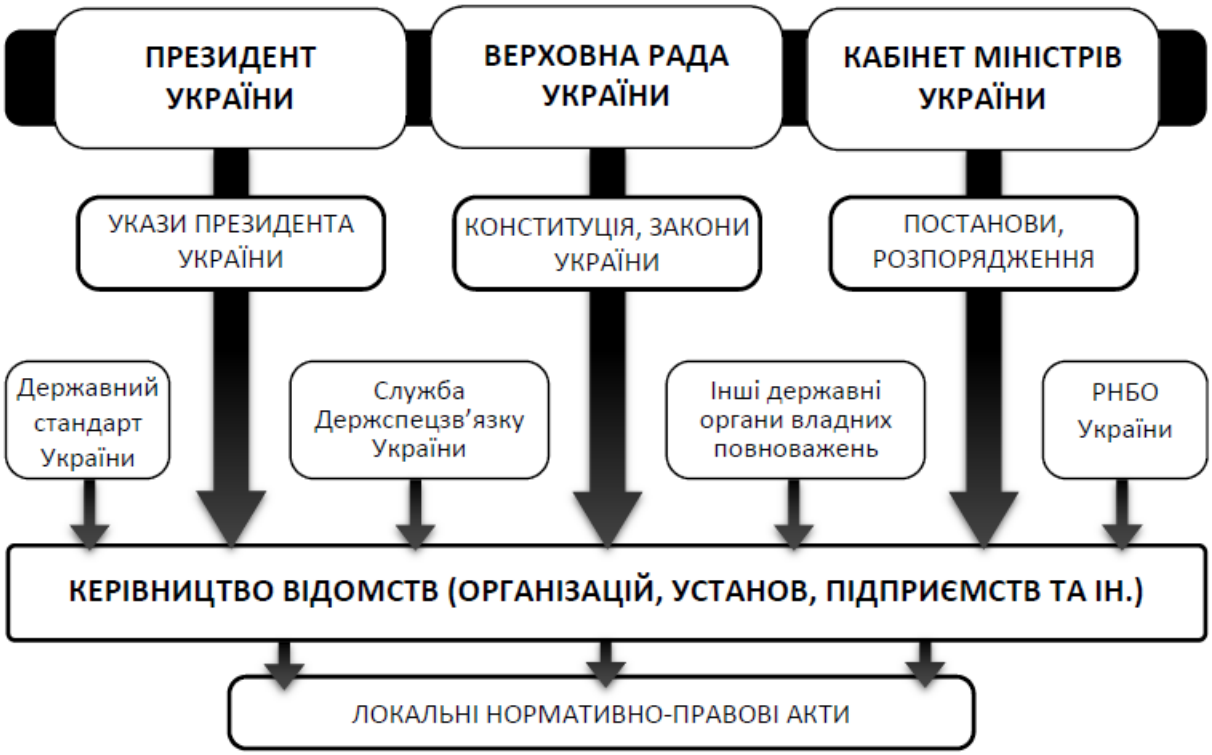

Рис. 1.1. Джерела нормативних вимог у сфері захисту інформації

Система законодавчих актів та розроблених на їх базі нормативних та організаційно-розпорядчих документів повинна забезпечувати організацію ефективного нагляду за їх виконанням з боку правоохоронних органів та реалізацію засобів судового захисту та відповідальності суб'єктів інформаційних відносин. Отже, на державному рівні правовий захист інформації передбачає, перш за все, організацію ефективної нормотворчої, правоохоронної та правозастосовної діяльності. Тому дуже часто правовий напрямок захисту інформації на рівні держави об'єднують з організаційним напрямком.

При розгляді організаційно-правового захисту, як самостійного напрямку захисту інформації, слід сказати, що він охоплює досить велику кількість відносно окремих напрямків *(рис. 1.2),* кожен з яких вимагає відповідного законодавчого врегулювання.

Рис. 1.2. Основні напрямки організаційно-правового захисту інформації в Україні

У широкому сенсі правовим фундаментом для правового захисту інформації виступає національне інформаційне право, предметом *якого саме і є* суспільні відносини, що виникають з приводу встановлення режимів та форм обігу інформації, реалізації інформаційних прав і правового статусу суб'єктів інформаційних процесів і формування їх правомірної поведінки і зв'язків.

В рамках інформаційного права в основному діють два правових способи регулювання, які створюють два можливих види правового обігу інформації *(рис. 1.3)*:

- *відкритий* - врегульований диспозитивним методом (виключно цивільно-правовими нормами);

- *закритий* - регулюється імперативним методом (адміністративно-правові норми).

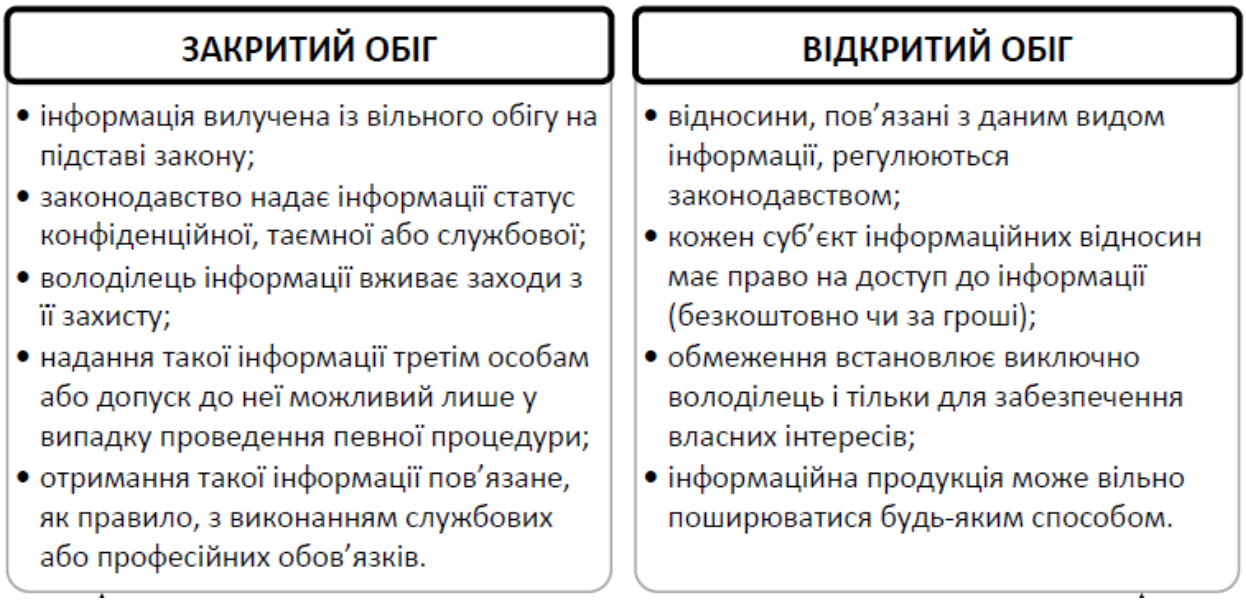

Рис. 1.3. Види обігу інформації та їх правові ознаки

До цих методів також долучається вільний обіг інформації, який безпосередньо правом не врегульований, але щодо якого можуть виникати охоронні правовідносини в разі порушення визначених заборон або обмежень.

У вузькому сенсі мова йде про необхідність створення підсистеми організаційно-правового захисту інформації, яка ґрунтується на базі різних документів *(рис. 1.4)*.

Рис. 1.4. Документальне забезпечення підсистеми організаційно-правового захисту інформації

До першої групи (*нормативно-правової*) відносяться документи, що становлять законодавчу базу щодо захисту інформації. Це закони та підзаконні

акти, що визначають юридичну відповідальність.

До другої групи (*довідково-інформаційної*) належать документи, які містять повну інформацію про всі аспекти проблеми захисту і визнані фахівцями в цій галузі (словники, довідники); державні стандарти щодо захисту інформації; технічні описи засобів захисту інформації та ін.

Керуючі методичні матеріали (третя група документів) - це сукупність таких документів, які містять повний і систематизований опис порядку і принципу проведення робіт із захисту інформації, методики вимірювання зон витоку інформації технічними каналами, проектування системи захисту інформації тощо.

До четвертої групи належать *систематизовані набори інструкцій* для різних підрозділів і посадових осіб відповідно до їх повноважень.

До реєстраційних документів (п’ята група) належать облікові документи, що дозволяють контролювати наявність закритої інформації на об’єкті захисту і обмежувати доступ до неї, а також експлуатаційно-технічна документація, що дозволяє реєструвати всі факти і події, що загрожують безпеці інформації.

Отже, сукупність перерахованих вище документів становить правову базу, що забезпечує нормативне регулювання процесів щодо захисту інформації.

Лекція 2. ПОНЯТТЯ ТА ЗМІСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Питання для опрацювання:

2.1. Правовий режим інформації

2.2. Правові основи доступу до інформації

Джерела:

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 року / Рада Європи. URL: http://zakon2.rada.gov.ua/laws/show/994_326/ed20100706
2. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 року / Рада Європи. URL: http://zakon1.rada.gov.ua/laws/show/994_363
3. Про державну таємницю: ЗУ від 21.01.1994 року № 3855-XII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/3855-12
4. Про доступ до публічної інформації: ЗУ 13.01.2011 року № 2939-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text
5. Про звернення громадян: ЗУ 02.10.1996 року № 393/96-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text
6. Про інформацію: ЗУ від 02.10.1992 року № 2657-XII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2657-12

2.1. Правовий режим інформації

У науковій літературі правовий режим визначається, як порядок регулювання, виражений у комплексі правових засобів, що характеризують поєднання взаємодіючих дозволів, заборон, а також позитивних зобов'язань, які створюють особливе спрямування регулювання. Механізм правового режиму пов'язаний, насамперед, із орієнтацією на суб'єкт.

Правовий режим інформації включає:

- право використання інформації в якості об'єкта правових відносин;
- право володіння інформацією;
- право доступу до інформації;
- право власності та інші майнові права на різні носії, що містять документовану інформацію;

- право поширення та надання інформації.

Право використання інформації в якості об'єкта правових відносин полягає в можливості встановлення публічних, цивільних та інших правових відносин, об'єктом яких є інформація.

Право володіння інформацією полягає в можливості розпорядження нею (дозвіл або обмеження доступу; використання; поширення; передача іншим особам; правовий захист та інші дії) на розсуд правовласника.

Право доступу до інформації полягає у можливості її вільного отримання та використання, якщо законодавством не встановлені обмеження доступу до інформації, або інші вимоги до порядку її надання або розповсюдження.

Право власності та інші майнові права на матеріальні носії, що містять документовану інформацію, встановлюється цивільним законодавством. Це значить, що носії інформації є об'єктами цивільних прав поряд з іншими речами.

Інформація, є предметом власності і підлягає захисту відповідно до вимог правових документів або вимогами, встановлюваними власником інформації. Власником інформації може бути: фізична або юридична особа, а також держава.

Право поширення і надання інформації полягає у можливості вільного здійснення дій, спрямованих на отримання інформації невизначеним колом осіб або на передачу інформації невизначеному колу осіб (поширення), і дій, спрямованих на отримання або передачу інформації визначеному колу осіб, при дотриманні вимог, встановлених законодавством України.

Отже, правовий режим інформації створює умови для забезпечення інформаційної безпеки.

2.2. Правові основи доступу до інформації

Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення й зберігання інформації.

Відповідно до Закону України «Про інформацію» за режимом доступу інформація поділяється на *відкриту інформацію* та *інформацію з обмеженим доступом* (ст. 20).

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини і громадянина;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, ратифікованих Верховною Радою України (ст. 21 ЗУ «Про інформацію», ст. 8 ЗУ «Про державну таємницю»).

Інформацією з обмеженим доступом становить *конфіденційна*, *таємна* та *службова інформація* (ст. 6 ЗУ «Про доступ до публічної інформації»).

Для визначення критерію, який був покладений в основу даного поділу, необхідно висвітлити поняття конфіденційної, таємної та службової інформації.

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом. (ст. 21 ЗУ «Про інформацію»). Таким чином, можна зробити висновок, що конфіденційна інформація це інформація, яка є перебуває у володінні окремих фізичних та юридичних осіб.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, приховування якої являє загрозу життю і здоров'ю людей. При порівнянні таких категорій інформації як конфіденційна, таємна та службова видно, що законодавцем в основу їх поділу були покладені різні критерії. В першому випадку це право володіння, а в другому та третьому це шкода особі, суспільству і державі.

До видів таємної інформації, які передбачені чинним законодавством відносимо:

- *державну таємницю;*
- *військову таємницю;*
- *професійну таємницю;*

- комерційну таємницю;

- банківську таємницю;

- інсайдерську інформацію;

- адвокатську таємницю;

- таємницю нотаріальних дій;

- лікарську таємницю;

- таємницю страхування;

- таємницю усиновлення;

- таємницю голосування;

- таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції.

Відповідно до статті 9 Законом України «Про доступ до публічної інформації» до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування». Доступ до таких документів надається відповідно до частини другої статті 6 Закону України «Про доступ до публічної інформації».

Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

Постановою Кабінету Міністрів від 19 жовтня 2016 р. № 736 затверджено Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію.

Державні органи і організації, органи місцевого самоврядування, інформаційні системи яких вміщують інформацію про громадян, зобов'язані надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом, а також вживати заходів щодо запобігання несанкціонованому

доступу до неї. У разі порушень цих вимог Закон гарантує захист громадян від заподіяної їм шкоди використанням такої інформації.

Забороняється доступ сторонніх осіб до відомостей про іншу особу, зібраних відповідно до чинного законодавства державними органами, організаціями й посадовими особами.

Інформацію про громадян не слід зберігати довше, ніж це необхідно для досягнення законно встановленої мети.

Всім організаціям, які збирають інформацію про громадян, необхідно до початку роботи з нею здійснити у встановленому Кабінетом Міністрів України порядку державну реєстрацію відповідних баз даних. Необхідна кількість даних про громадян, яку можна одержати законним шляхом, має бути максимально обмеженою й може використовуватися лише для досягнення законно встановленої мети.

Відмова в доступі до такої інформації або приховування її, або незаконне збирання, використання, зберігання або поширення можуть бути оскаржені в суді.

Під *інформаційним запитом* (далі – запитом) стосовно доступу до офіційних документів у законі розуміється звернення з вимогою про надання можливості ознайомлення з офіційними документами. Запит може бути індивідуальним або колективним. Він подається у письмовій формі.

Громадянин має право звернутися до державних органів і вимагати надання будь-якого офіційного документа незалежно від того, стосується цей документ його особисто чи ні, крім випадків обмеження доступу, передбачених Законом.

Під запитом щодо надання письмової або усної інформації у Законі розуміється звернення з вимогою надати такі відомості з окремих питань про діяльність органів законодавчої, виконавчої або судової влади України, їх посадових осіб.

Громадяни України, державні органи, організації і об'єднання громадян подають запит відповідному органу законодавчої, виконавчої або судової влади, його посадовим особам. У запиті має бути зазначено прізвище, ім'я та по батькові запитувача, документ, письмова або усна інформація, що його цікавить, та адреса, за якою він бажає одержати відповідь.

Органи законодавчої, виконавчої або судової влади України, їх посадові особи зобов'язані надавати інформацію, що стосується їхньої діяльності, письмово, усно, по телефону або використовуючи публічні виступи своїх посадових осіб.

Строк вивчення запиту щодо можливості його задоволення не має перевищувати десяти календарних днів. Протягом указаного строку державна установа письмово доводить до відома запитувача, що його запит буде задоволено або що запитуваний документ не підлягає наданню для ознайомлення.

Задоволення запиту здійснюється протягом місяця, якщо інше не передбачено законом. Відмова в задоволенні запиту доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

У відмові має бути зазначено:

1) посадову особу державної установи, яка відмовляє у задоволенні запиту;

2) дату відмови;

3) мотивовану підставу відмови.

Відстрочення задоволення запиту допускається в разі, якщо запитуваний документ не може бути надано для ознайомлення у місячний строк. Повідомлення про це доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

У повідомленні про відстрочення має бути зазначено:

1) посадову особу державної установи, яка відмовляє у задоволенні запиту в установлений місячний строк;

2) дату надсилання або видачі повідомлення про відстрочення;

3) причини, з яких запитуваний документ не може бути видано у встановлений Законом строк;

4) термін, у який буде задоволено запит.

Відмову або відстрочення задоволення запиту може бути оскаржено. У разі відмови в наданні документа для ознайомлення або відстрочення задоволення запиту запитувач має право оскаржити ці дії в органах вищого рівня. Якщо на таку скаргу дається негативна відповідь, запитувач має право оскаржити цю відмову в суді.

У разі, коли запитувач звернувся до суду, обов'язок доводити законність відмови або відстрочення задоволення запиту покладається на відповідача – державну установу. Суд має право для забезпечення повноти і об'єктивності розгляду справи запитати офіційні документи, у можливості ознайомлення з якими було відмовлено, і, вивчивши їх, прийняти рішення про обґрунтованість (або необґрунтованість) дій посадових осіб державної установи. Якщо відмову або відстрочення визнано необґрунтованою, суд зобов'язує державну установу надати запитувачеві змогу ознайомитися з офіційним документом і виносить окрему ухвалу щодо посадових осіб, які йому відмовили.

Необґрунтована відмова у наданні змоги для ознайомлення з офіційними документами або порушення визначеного строку її надання без поважних причин тягнуть за собою дисциплінарну або іншу відповідальність посадових осіб державних установ у порядку, встановленому законами України.

Запитувачі мають право робити виписки з наданих їм для ознайомлення офіційних документів, фотографувати їх, записувати текст на магнітну плівку тощо.

Власник документів має право за відповідну плату виготовляти за бажанням запитувачів копії цих документів. Не підлягає оплаті робота щодо пошуку офіційних документів. Порядок оплати копій запитуваних документів встановлюється державними установами.

Кабінет Міністрів України або інші державні установи визначають порядок і розмір оплати робіт щодо пошуку, збирання, підготовки, створення й надання запитуваної письмової інформації. Ця оплата не має перевищувати реальних витрат, пов'язаних з виконанням запитів.

Не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять:

- інформацію, визнану у встановленому порядку державною таємницею;
- конфіденційну інформацію;
- відомості про оперативну й слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання й суду у тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню або дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;
- інформацію, що стосується особистого життя громадян;
- документи, що становлять внутрішньовідомчу службову кореспонденцію (доповідні записки, переписка між підрозділами й ін.), якщо вони пов'язані з розробленням напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю;
- відомості, що не підлягають розголошенню згідно з іншими нормативними актами. Установа, до якої звернуто запит, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акту

Лекція 3. ВИДИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Питання для опрацювання:

3.1. Правовий порядок доступу до інформації

3.2. Поняття правових інститутів таємниць

Джерела:

1. Господарський кодекс України від 16 січня 2003 року № 436-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/436-15#n276
2. Цивільний кодекс України від 16 січня 2003 року № 435-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/435-15#n4141
3. Про банки і банківську діяльність: ЗУ від 07.12.2000 року № 2121-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2121-14#n983
4. Про інформацію: ЗУ від 02.10.1992 року № 2657-XII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2657-12
5. Про доступ до публічної інформації: ЗУ від 13.01.2011 року № 2939-VI / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2939-17
6. Про захист персональних даних: ЗУ від 01.06.2010 року № 2297-VI / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/2297-17
7. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена постановою Кабінету Міністрів від 19.10.2016 р. № 736 /Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/736-2016-вр#Text

3.1. Правовий порядок доступу до інформації

Розвиток сучасного інформаційного суспільства визначається стрімким зростанням ролі інформації в багатьох сферах суспільних відносин. В рамках інформаційних відносин відбувається реалізація прав суб'єктів на інформацію. У ст. 34 Конституції України закріплено право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово чи будь-яким іншим способом і на свій вибір. Однак на законодавчому рівні встановлено обмеження доступу до певних видів інформації, яке зумовлене необхідністю правового забезпечення захисту окремих видів інформації.

Доступ фактично є певною дозвільною процедурою, яка полягає в отриманні згоди компетентного органу (особи) на одержання документа або

інформації, отримання якої безпосередньо пов’язане з реалізацією права на інформацію, і, відповідно, обмежує це право.

Відповідно до ЗУ «Про інформацію», вчинення права на отримання інформації пов’язане з поняттям доступу до інформації.

Доступ до інформації - це передбачений правовими нормами порядок отримання, використання, поширення та зберігання інформації.

Головними *характеристиками порядку доступу до інформації* є:

- суб’єкт визначення доступності цієї інформації;
- коло суб’єктів, які мають доступ до цієї інформації;
- особливі вимоги і правила збереження та поширення цієї інформації;
- термін дії порядку.

Суб’єктом визначення доступності інформації є особа, в компетенцію якої входить вирішення питань щодо встановлення обмежень на доступ до інформації та її матеріальних носіїв, а також надання права доступу до такої інформації.

Суб’єкт, який має доступ до інформації - це особа, якій надано право ознайомлення з матеріальними носіями інформації або їх використання. Надання особі права доступу до інформації, зазвичай пов’язане з взяттям нею на себе зобов’язань з нерозголошення отриманої інформації.

Порядок доступу до інформації означає певну сукупність правил, якими позначені особливі вимоги і правила зберігання та поширення інформації. Ці правила визначають діяльність осіб, на яких покладено відповідальність за зберігання матеріальних носіїв інформації, встановлюють необхідність застосування певних правових, організаційних, технічних та криптографічних засобів захисту інформації. Ці правила також визначають порядок надання доступу до такої інформації.

Більшість видів ІзОД мають визначений законодавством або власником інформації термін дії режиму обмеження доступу до інформації. Цей термін визначають, як правило, при ухваленні рішення про обмеження доступу до інформації або її матеріальних носіїв. Після закінчення цього терміну може бути ухвалено рішення або про його відновлення, або про надання інформації статусу відкритої.

Згідно зі п. 1 ст. 20 ЗУ «Про інформацію», в залежності від *порядку доступу* інформація поділяється на *відкриту* та *інформацію з обмеженим доступом* (ІзОД) *(рис. 3.1).*

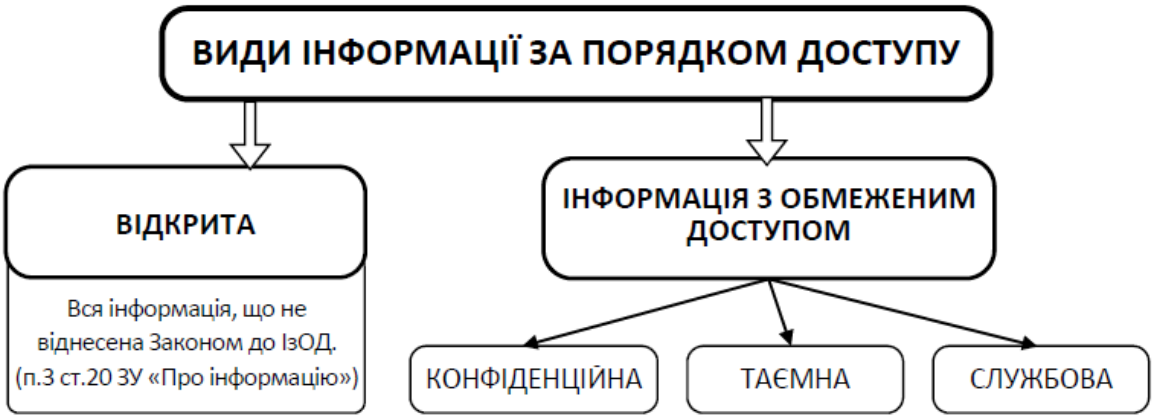

Рис. 3.1. Види інформації за порядком доступу

Будь-яка інформація є *відкритою,* крім тієї, яка відноситься законом до ІзОД.

Питання *обмеження доступу до інформації* регулюються різними нормативно-правовими актами України, серед яких:

Конституція України, Закони України «Про інформацію», «Про доступ до публічної інформації» та ін.

Так, відповідно до п. 2 ст. 6 ЗУ «Про доступ до публічної інформації» обмеження доступу до інформації здійснюється при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

ІзОД може бути поширена, якщо вона є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення (ст. 29 ЗУ «Про інформацію»).

Предметом суспільного інтересу вважається інформація, яка:

- свідчить про загрозу державному суверенітету, територіальної цілісності України;

- забезпечує реалізацію конституційних прав, свобод і обов'язків;

- свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Відповідно до ч. 7 ст. 6 ЗУ «Про доступ до публічної інформації» обмеженню доступу підлягає інформація, а не документ. Якщо документ містить ІзОД, для ознайомлення надається інформація, доступ до якої необмежений.

Отже, на законодавчому рівні проведено поділ інформації на ІзОД та інформації, яка є строго відкритою і не може належати ІзОД.

Згідно з п. 1 ст. 21 ЗУ «Про інформацію» ІзОД поділяється на *конфіденційну, таємну* та *службову* інформацію.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку, відповідно до передбачених нею умов, а також в інших випадках, визначених законом (п. 2 ст. 21 ЗУ «Про інформацію»).

Конфіденційна інформація - це інформація виключно приватних суб'єктів, яка може бути різною. До конфіденційної інформації може належати як інформація про її власника, так і інша інформація, що потрапила у володіння приватного суб'єкта (відомості про непублічну подію, властивості природних об'єктів, місце їх знаходження та ін.).

Отже, будь-яка інформація може бути віднесена до конфіденційної, якщо це не заборонено законом.

До конфіденційної інформації належать персональні дані (п. 2 ст. 5 ЗУ «Про захист персональних даних»).

Особливим видом конфіденційної інформації є комерційна таємниця: згідно зі ст. 36 ГКУ юридична або фізична особа-підприємець (суб'єкт господарювання) самостійно визначають склад і обсяг відомостей, що становлять комерційну таємницю. Це і є головна ознака, яка відрізняє «комерційну таємницю» від таємної інформації, склад і режим захисту якої визначається законом.

Також, конфіденційною інформацією є інформація про споживачів телекомунікаційних послуг. Відповідно до ст. 119 ЗУ «Про електронні телекомунікації» оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі

отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

До конфіденційної інформації у сфері господарської (підприємницької) діяльності відноситься інформація, яка визначається ст. 862 ЦКУ та «ноу-хау» (таємниці виробництва) (ст. 1 ЗУ «Про інвестиційну діяльність»).

Згідно зі ст. ст. 60-61 ЗУ «Про банки і банківську діяльність» банківська таємниця також відноситься до конфіденційної інформації.

Таким чином, конфіденційна інформація включає в себе наступні види, що не мають ознак державної таємниці: таємниця особистого життя, комерційна, банківська та професійні таємниці.

Винятком є інформація, для якої встановлені правові обмеження щодо можливості ‘її віднесення до категорії конфіденційної. Це окремі відомості комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо).

Розпорядники, що володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди - «*лише в інтересах національної безпеки, економічного добробуту та прав людини»* (ст. 7 ЗУ «Про доступ до публічної інформації»).

На підставі вище викладеного, можна виділити правові ознаки конфіденційної інформації:

- визнана конфіденційною законом;

- по об’єкту - це інформація про фізичному особу (персональні дані), інформація, доступ до якої обмежено правовласником;

- за суб’єктом - фізична або юридична особа, яка не є суб’єктом владних повноважень;

- поширюється за власним бажанням і розсуд суб’єктів незалежно від правовласників.

Другим видом ІзОД є *таємна інформація.*

Відповідно до ст. ст. 6 і 8 ЗУ «Про доступ до публічної інформації» *таємна інформація* - це інформація, розголошення якої може завдати шкоди особі, суспільству і державі, доступ до якої обмежується виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку для запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. її розголошення може завдати істотної шкоди цим

інтересам. Шкода від оприлюднення такої інформації переважає над суспільним інтересом в її отриманні. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Крім ЗУ «Про доступ до публічної інформації» поняття «таємна інформація» розкривається в багатьох нормативно-правових актах.

Положення про роботу із засобами обчислювальної техніки і телекомунікаційною мережею Міністерства економіки України визначають таємну інформацію, як «*інформацію, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю*».

Основними характеристиками таємної інформації є те, що: відношення її до категорії таємних відомостей, доступ до неї громадян, порядок обігу та захисту, порядок і строки її опублікування визначаються законодавчо.

Обмеження доступу до таємної інформації встановлюється законодавством у разі відповідності інформації певним критеріям. Засекречується інформація незалежно від бажання чи небажання її власника, більш того власник інформації зобов'язаний реалізувати своє право власності на інформацію з урахуванням встановлених законом обмежень. А у випадку їх порушення, може бути позбавлений права власності на інформацію та її матеріальні носії. Рішення про засекречування інформації приймають уповноважені органи державної влади, а вміст режиму доступу до інформації, засоби її захисту та юридичну відповідальність за порушення режиму визначаються законодавчо.

Таємна інформація не є однорідною та відрізняється по предмету інформації, що захищається; по суб'єктам, на яких поширюються обов'язки не порушувати таємницю у зв'язку з професійною або службовою діяльністю.

Порядок доступу до таємної інформації та її правові ознаки визначені ЗУ «Про доступ до публічної інформації».

Між таємною інформацією та конфіденційною інформацією існують відмінності. Полягають вони в тому, що обмеження доступу до таємної інформації встановлюється законом і не вимагає волевиявлення особи, якого така інформація стосується. Тоді як підставою для визнання інформації конфіденційною є, насамперед, бажання фізичної або юридичної особи вважати певну інформацію про нього або інформацію, яка знаходиться в його володінні, конфіденційною. Друга відмінність - режим доступу до таємної інформації визначається законом, а доступ до конфіденційної - особою, яка цей доступ і обмежила.

Третій вид ІзОД - *службова інформація.*

До *службової інформації* може належати така інформація (ст. 9 ЗУ «Про доступ до публічної інформації»), яка:

1) міститься в документах суб'єктів владних повноважень, що становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установ або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та / або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яка не відноситься до державної таємниці. Документам, які містять інформацію, що становить службову інформацію, присвоюється гриф «для службового користування» (ДСК).

Обов'язковість присвоєння грифу пояснюється необхідністю особливого обліку та зберігання таких документів, зокрема, для забезпечення відповідної реєстрації таких документів в систему обліку публічної інформації, передбаченої в ст. 18 ЗУ «Про доступ до публічної інформації». Гриф представляється як матеріальним носіям службової інформації, так і документам в електронній формі.

Робота з такими документами здійснюється відповідно до Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженої постановою Кабінету Міністрів від 19 жовтня 2016 р. № 736. Тому віднесення до службової інформації повинно бути дійсно необхідним і не повинно бути автоматичним (не треба в кожній службової записки застосовувати гриф ДСК).

Перелік відомостей, що становлять службову інформацію, складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмежений у доступі.

Відомості, що становлять службову інформацію, містяться в внутрішньовідомчої службової кореспонденції, доповідних записках, рекомендаціях. Ці відомості визначаються не через зміст інформації, а через документи, в яких вони містяться. При цьому мова йде тільки про документи суб'єктів владних повноважень, визначених у ст. 13 ЗУ «Про доступ до публічної інформації». Такі документи повинні бути пов'язані з розробкою напряму діяльності існуючого органу або із здійсненням його контрольних або наглядових

функцій.

До службової інформації не відноситься інформація, що міститься в міжвідомчій кореспонденції.

В п. 2 ст. 6 ЗУ «Про доступ до публічної інформації» визначено три загальних умови обмеження доступу до інформації. При наявності одночасно всіх цих умов суб'єкт владних повноважень може обмежити доступ до певної інформації і надати документів, що містять її гриф ДСК.

П. 3 ст. 21 ЗУ «Про інформацію» встановлює, що *«порядок віднесення до... службової інформації, а також порядок доступу до неї регулюється законом».* Порядок віднесення інформації до службової інформації визначається різними нормативно-правовими актами, які можна об'єднати в кілька груп:

- відомчі положення та інструкції про забезпечення доступу до публічної інформації;
- нормативно-правові акти, що визначають обов'язок не розголошувати службову інформацію;
- відомчі переліки відомостей, що становлять службову інформацію;
- відомчі інструкції і положення про порядок використання службової інформації в окремих службах і органах;
- акти про ведення загального діловодства за зверненням службових листів, службових документів, записок;
- нормативно-правові акти, що передбачають проведення службових розслідувань за порушення правил використання службової інформації та дисциплінарну відповідальність.

Підсумовуючи можна зробити висновок, що правовими ознаками службової інформації є:

- визнана службовою законом;
- міститься в документах суб'єктів владних повноважень;
- зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності або в сфері оборони;
- не є державною таємницею;
- є власністю держави (створена на державні кошти).

Отже, до службової інформації можуть відноситися такі види таємниць: податкова, нарадчої кімнати, а також інформація військового характеру, що не є державною таємницею.

Слід зауважити, що наведена класифікація видів ІзОД за порядком доступу залишається дещо складною та заплутаною і має певні недоліки.

3.2. Поняття правових інститутів таємниць

Інститут таємниці - один з найважливіших інститутів, що визначають співвідношення інтересів особистості, суспільства і держави, приватного і публічного права, підстави та межі втручання держави в недержавну сферу, ступінь інформаційної захищеності. Він охоплює широке коло досить різнорідних суспільних відносин, що виникають у різних сферах діяльності особистості, суспільства і держави.

Зміст будь-якої таємниці, незалежно від специфіки її різновидів, полягає в тому, що предмет таємниці утворюють відомості, не призначені для широкого кола осіб, їх розголошення може спричинити небажані наслідки для зберігачів і носіїв таємниці.

У правовому відношенні інститут таємниці становить інтерес з позиції обмеження гласності та визначення меж втручання в сферу його дії, розробки гарантій його захисту.

Правовий інститут будь-якої таємниці можна умовно представити у вигляді трьох складових *(рис. 3.2):*

- *загальна частина* - визначення таємниці, принципи і критерії віднесення інформації до таємниці, обмеження по включенню певної інформації до таємниці, правові ознаки таємниці тощо;

- *режим таємниці* - правовий механізм обмеження доступу до інформації, що становить таємницю;

- *санкції* - юридична відповідальність за протиправні дії з інформацією, що складає таємницю.

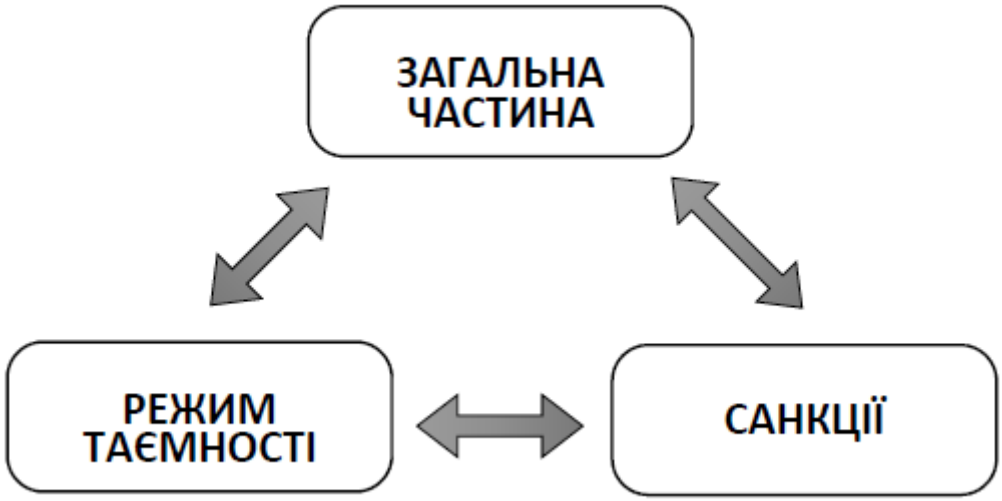

Рис. 3.2. Склад правового інституту таємниці

Сукупність правових норм, яка регламентує інформаційні відносини в сфері обігу інформації, що становить таємницю, і утворює *окремий правовий інститут,* оскільки їй притаманні однорідність фактичного змісту, єдність правових норм.

Відзначимо, що до правових інститутів, які регулюють сукупність однорідних суспільних відносин, пов'язаних з обігом ІзОД і мають всі зазначені складові зараз відносять правові інститути таємниць: державної, банківської, комерційної, професійної, особистого життя, нарадчої кімнати тощо.

- іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення;

- інформацію фінансових установ, підготовлену для контрольно-фінансових відомств.

Лекція 4. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

Питання для опрацювання:

4.1. Поняття і правовий режим державної таємниці

4.2. Організаційно-правові методи охорони державної таємниці

Джерела:

1. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 23.12.2020 № 383 / Служба безпеки України. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text
2. Кодекс України про адміністративні правопорушення від 07.12.1984 року № 8073-X / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text
3. Кримінальний кодекс України від 05.04.2001 року № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
4. Про Службу безпеки України: ЗУ 25.03.1992 року № 2229-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text
5. Про державну таємницю: ЗУ від 21.01.1994 року № 3855-XII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/3855-12

4.1. Поняття і правовий режим державної таємниці

В системі правовідносин, що виникають при обігу інформації, особливе місце займає *інститут державної таємниці* (ДТ). Важливість і значимість цього інституту під час розвитку інформаційного суспільства, коли інформація стає основним і цінним ресурсом, зростає на багато разів. Інститут ДТ існує в усіх країнах світу і сьогодні є основною складовою системи інформаційної безпеки, яка займає провідне місце в системі національної безпеки держави.

Сьогодні в Україні сформована досить чітка система охорони ДТ, яка включає в себе *комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів,* спрямованих на запобігання розголошенню таємної інформації та втрати її матеріальних носіїв.

Правовий інститут ДТ в Україні представлений трьома складовими:

- загальна частина: визначення таємниці, принципи і критерії віднесення інформації до ДТ, правові ознаки ДТ;

- режим ДТ: механізм обмеження доступу до зазначених відомостей, тобто механізм їх організаційно-правового захисту;

- санкції за неправомірне поводження з відомостями, що становлять ДТ.

Базовим законом, що регулює *перші дві складові* (загальну частину та режим ДТ), є ЗУ «Про державну таємницю». Також одним з основних, є ЗУ «Про службу безпеки України», оскільки Служба безпеки України (СБУ) виступає основною спеціальною службою, що здійснює охорону ДТ. Третя складова (санкції) прописана в ККУ, в КУпАП і в інших нормативно-правових актах.

Відповідно до ст. 1 ЗУ «Про державну таємницю»: «*державна таємниця (далі також - секретна інформація)* - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою». З цього визначення випливають найважливіші *правові ознаки* ДТ:

1) ДТ - це вид таємної інформації, який регулюється ЗУ «Про державну таємницю»;

2) ДТ становлять лише відомості в чітко зазначених сферах;

3) розголошення ДТ може завдати шкоди національній безпеці України;

4) існує організаційно-правовий механізм віднесення інформації до ДТ;

5) охорона ДТ здійснюється державою.

Інформація, яка може бути віднесена до ДТ, визначається відповідно до норм ст. 8 ЗУ «Про державну таємницю» та викладена в Зводі відомостей, що становлять державну таємницю в Україні (ЗВДТ). ЗВДТ «визначає відомості, що згідно із рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених законодавством сферах».

ДТ становлять:

1. У сфері оборони:

- інформація, що стосується безпосередньо Збройних Сил України;

- інформація військово-технічного характеру;

- інформація про заходи захисту населення в умовах можливих конфліктів;

- відомості географічно-топологічного характеру, які мають значення для оборони країни;

2. У сфері економіки, науки і техніки:

- інформація військово-економічного характеру;

- стратегічна економічна інформація;

- фінансово-економічна інформація;

- науково-технічна інформація;

3. У сфері зовнішніх відносин:

- окремі аспекти зовнішньополітичної і зовнішньоекономічної діяльності;

- окремі аспекти міждержавного військово-економічного співробітництва;

- відомості про експорт та імпорт озброєння, військової та спеціальної техніки, окремих стратегічних видів сировини і продукції;

4. У сфері державної безпеки та охорони правопорядку:

- окремі аспекти негласної правоохоронної діяльності;

- заходи щодо захисту різного роду режимних об'єктів;

- відомості щодо безпосереднього здійснення заходів з захисту інформації.

Отже, до ДТ відноситься інформація в різних сферах діяльності, а саме: оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

В останні роки були внесені зміни в національне законодавство з метою впорядкування та попередження зловживань в засекречування інформації. Так, згідно зі ст. 8 ЗУ «Про державну таємницю» забороняється відносити до ДТ будь-які відомості, якщо цим будуть обмежуватися конституційні права і свободи людини і громадянина, буде наноситися шкода здоров'ю та безпеці населення.

Не відноситься до ДТ наступна інформація:

- про стан довкілля, про якість харчових продуктів і предметів побуту, про впливі товару (роботи, послуги) на життя і здоров'я людини;

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують безпеці громадян;

- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також соціально-демографічні показники, стан правопорядку, освіти і культури населення;

- про факти порушень прав і свобод людини і громадянина;

- про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових і службових осіб;

- інша інформація, доступ до якої, відповідно до законів і міжнародних договорів, згода на обов'язковість яких надається Верховною Радою України, не може бути обмежений.

Віднесення відомостей до ДТ здійснюється відповідно до їх галузевої, відомчої або цільової приналежності, а також відповідно до законодавства.

Обґрунтування необхідності віднесення відомостей до ДТ покладається на органи державної влади, підприємства, установи та організації, які ці відомості отримано і розроблені.

4.2. Організаційно-правові методи охорони державної таємниці

Національна система охорони ДТ створювалася з урахуванням досвіду розвинених демократичних країн і перевірених на практиці традиційних засобів і методів. Значною мірою сучасна Україна є спадкоємицею системи захисту секретної інформації, яка існувала ще під час Радянського Союзу. Більшість елементів цієї структури було збережено, а внаслідок - розвинуто і вдосконалено.

Заходи, які вживає держава, охороняючи свої таємниці, повинні бути адекватні існуючим в даний момент загрозам (як зовнішнім, так і внутрішнім). Ефективне вирішення цього питання можливе лише за умови комплексного підходу, який включає дослідження виникнення потреби в охороні ДТ взагалі, та особливостей формування цієї системи на території України, зокрема.

Формування системи охорони ДТ передбачає введення системи взаємодіючих адміністративно-правових режимів, функції яких, в тій чи іншій мірі, спрямовані на охорону ДТ. Введення відповідних режимів передбачає нормативно-правове регулювання відносин у цій сфері та створення державних органів, діяльність яких спрямована на вирішення конкретних задач з забезпечення зазначених режимів.

Щодо *другої складової правового інституту ДТ* (режиму ДТ) відзначимо, що в цілях захисту ДТ використовуються наступні основні *організаційно-правові методи* (ст. 18 ЗУ «Про державну таємницю»):

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

- дозвільний порядок здійснюється органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов’язаної з ДТ;

- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до ДТ, а також розташування і переміщення об’єктів і технічних засобів, що їм належать;

- особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з ДТ;

- режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з ДТ;

- спеціальний порядок допуску та доступу громадян до ДТ;

- технічний та криптографічний захист секретної інформації.

Відомості ДТ можуть мати різну *ступінь секретності,* яка є категорією, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її захисту державою. За ступенем секретності виділяють три категорії: Т - *таємно;* ЦТ - *цілком таємно;* ОВ - *особливої важливості.*

Конкретні дані можуть відноситися до певної категорії відомостей, які містять ДТ тільки за умови, що їх розголошення завдасть шкоди інтересам національній безпеці України. При цьому обов'язково враховується ступінь секретності інформації, критерії визначення якої встановлюються СБУ. Термін, протягом якого діє рішення про віднесення інформації до ДТ, не може перевищувати для інформації із ступенем секретності «Т» - 5 років, для інформації «ЦТ» - 10 років і для інформації «ОВ» - 30 років (ч. 1 ст. 13 ЗУ «Про державну таємницю»).

Після закінчення передбаченого терміну дії рішення про віднесення інформації до ДТ, приймається рішення про скасування рішення про віднесення її до ДТ або приймається рішення про продовження терміну дії певного рішення в рамках вище зазначених строків.

Президент України з власної ініціативи або за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до ДТ, ніж строки, встановлені ч. 1 ст. 13.

Встановлення терміну дії рішення про віднесення інформації до ДТ, прийняття рішення про його продовження здійснюються з дотриманням вимог ст. 6 ЗУ «Про доступ до публічної інформації».

Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до ДТ здійснюється на основі рішення державного експерта з питань таємниць або на підставі рішення суду у випадках, передбачених ст. 12 ЗУ «Про державну таємницю», і оформляються СБУ шляхом внесення відповідних змін до ЗВДТ. Інформація вважається ДТ з вищою або нижчою ступенем секретності або не складає ДТ, з моменту опублікування

відповідних змін до СС ДТ.

Інформація, включена в ЗВДТ, подається за формою *(рис. 4.1):*

Номер статті ЗВДТ	Зміст відомостей, що становлять державну таємницю	Ступінь секретності	Суб'єктирежимно-секретної діяльності, держекспертами яких прийняті рішення
1	2	3	4
1. Сфера оборони			
1.1.1	Відомості про стратегічне розгортання військ (сил)		ДПС ДССЗЗІ ЗС НГУ СБ СЗР УДО
	за сукупністю всіх складових показників у цілому щодо: виду, окремого роду військ (сил) ЗС; ДПС; ДССТ; ДССЗЗІ; СБ	ОВ	
	за окремими складовими показниками у цілому щодо: виду, окремого роду військ (сил) ЗС; ДПС; ДССТ; ДССЗЗІ; СБ;	ЦТ	

Рис. 4.1. Форма подачі відомостей, що становлять ДТ

Рішення про віднесення інформації до ДТ приймається державним експертом з питань таємниць не пізніше одного місяця з дня отримання звернення відповідного органу державної влади, органу місцевого самоврядування, підприємств, установ, організацій чи громадянина, після чого воно підлягає реєстрації СБУ в ЗВДТ.

Інформація також може бути вилучена з ЗВДТ. Підставою для цього є висновок державного експерта з питань таємниць про скасування рішення про віднесення інформації до ДТ. Цей висновок набирає чинності з моменту внесення СБУ змін до ЗВДТ, які згідно зі ст. 12 ЗУ «Про державну таємницю» формуються та публікуються в офіційних виданнях СБУ на підставі рішень державних експертів з питань таємниць.

Важливою справою є *засекречування та розсекречування матеріальних носіїв,* які містять ДТ.

Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі ЗВДТ (розгорнутих переліків відомостей, що становлять ДТ), відповідному документу, виробу або іншому матеріальному носію інформації грифу секретності посадовою особою, який готує або створює їх. Засекречування

документів здійснюється тільки в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується до незасекреченої частини.

Гриф секретності кожного матеріального носія таємної інформації повинен відповідати ступеню секретності міститься інформації, відповідно до ЗВДТ, - «ОВ», «ЦТ» або «Т». Реквізити кожного матеріального носія секретної інформації складаються з:

- грифу секретності;
- номера примірника;
- статті ЗВДТ, на підставі якої здійснюється засекречення;
- найменування посади та підпису особи, яка надала гриф секретності.

Якщо перераховані реквізити неможливо нанести безпосередньо на матеріальний носій секретної інформації, то вони повинні бути визначені в супровідних документах.

Забороняється надавати гриф секретності, матеріальним носіям іншої таємної інформації, яка не складає ДТ.

Перелік посад, перебування на яких дає посадовим особам право надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником державного органу, органу місцевого самоврядування, підприємства, установи, організації, здійснює діяльність, пов’язану з ДТ.

Ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт, виконуваних в інтересах забезпечення національної безпеки та оборони держави, встановлюються шляхом винесення відповідного висновку державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації, а також в разі підвищення або зниження ступеня секретності такої інформації або скасування рішення про віднесення її до ДТ, керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов’язані протягом шести місяців забезпечити зміну грифу секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників державних органів, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі

матеріальні носії секретної інформації.

Термін засекречування матеріальних носіїв інформації має відповідати терміну дії рішення про віднесення інформації до ДТ, встановленого рішенням державного експерта.

Термін дії засекречування матеріальних носіїв інформації починається з моменту надання їм грифу секретності.

Громадяни та юридичні особи мають право внести посадовим особам, які надали гриф секретності матеріальному носію таємної інформації, обов'язкову для розгляду мотивовану пропозицію про розсекречування цього носія інформації. Зазначені посадові особи повинні протягом одного місяця надати письмову відповідь з цього приводу.

Рішення про засекречування матеріального носія інформації може бути оскаржено громадянином чи юридичною особою в порядку підлеглості вищому органу або посадовій особі, а також у суді. У разі незадоволення скарги, поданої в порядку підлеглості, громадянин або юридична особа мають право оскаржити рішення вищого органу або посадової особи в суді.

Питання віднесення інформації у зазначених вище сферах, зміни ступеня секретності інформації та її розсекречування, покладено на *державних експертів з питань таємниць.* Ці експерти призначаються у Верховній Раді - Головою Верховної Ради, в інших органах державної влади - Президентом України за поданням керівника відповідного державного органу.

Державний експерт з питань таємниць відповідно до покладених на нього завдань визначає підстави, за якими інформація може бути віднесена до ДТ, ступінь секретності інформації та державні органи, яким надається право приймати рішення про доступ осіб до таємної інформації, що становить ДТ та виконує інші функції, передбачені законодавством.

Державний експерт з питань таємниць при виконанні покладених на нього функцій *зобов'язаний:*

- погоджувати з представником СБУ свої висновки про скасування рішень про віднесення інформації до міждержавних таємниць з відповідними посадовими особами держав-учасників міжнародних договорів України;

- представляти СБУ не пізніше ніж через десять днів з моменту підписання рішення про віднесення відомостей до ДТ або про скасування цих рішень, а розгорнуті переліки відомостей, що становлять державну таємницю, - в той же термін з моменту їх затвердження;

- розглядати протягом одного місяця пропозиції СБУ про віднесення

інформації до державної таємниці, скасування чи продовження терміну дії раніше прийнятого рішення про віднесення інформації до ДТ;

- надавати відповідний гриф секретності рішенням про віднесення інформації до ДТ і про скасування цих рішень в залежності від важливості їх отримання;

- брати участь в засіданнях державних експертів з питань таємниць;

- ініціювати питання про притягнення до відповідальності посадових осіб, які порушують законодавство України про ДТ.

Державний експерт з питань таємниць *має право:*

- безперешкодно проводити перевірку виконання державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями, що перебувають у сфері його діяльності, рішень про віднесення інформації до ДТ, скасування цих рішень, додержання порядку засекречення інформації та у разі виявлення порушень давати обов'язкові для виконання приписи про їх усунення;

- створювати експертні комісії з фахівців і вчених, що мають допуск до ДТ, для підготовки проектів рішень про віднесення інформації до ДТ, зниження ступеня її секретності та скасування зазначених рішень, висновків по обізнаності про ДТ громадян, котрі мають або мали допуск до ДТ, а також для підготовки відповідних висновків в випадку розголошення секретної інформації або втрати матеріальних носіїв такої інформації;

- скасовувати безпідставні рішення про надання носію інформації грифу секретності, зміну або скасування цього грифу;

- клопотати про притягнення до відповідальності посадових осіб, які порушують законодавство України про ДТ;

- отримувати в установленому порядку від державних органів, органів місцевого самоврядування, підприємств, установ та організацій дані, необхідні для виконання своїх функцій.

Державний експерт з питань таємниць несе персональну відповідальність за законність і обґрунтованість свого рішення про віднесення інформації до ДТ або про зниження її ступеня секретності, або скасування рішення про віднесення її до ДТ, а також за умисне невжиття рішення про віднесення до ДТ інформації, розголошення якої може нанести шкоду інтересам національної безпеки України.

Для віднесення інформації до ДТ державним експертом з питань таємниць видається мотивоване рішення, яке може бути видано як за його ініціативою, так і за зверненнями громадян, керівників відповідних органів і організацій. У цьому

рішенні зазначаються:

- інформація, яка повинна становити ДТ та її відповідність категоріям і вимогам, передбачених законодавством;

- підстави для віднесення інформації до ДТ і обґрунтування збитку, котрий може бути завдано національній безпеці країни у разі її розголошення;

- ступінь секретності зазначеної інформації;

- орган державної влади, орган місцевого самоврядування, підприємство, установа, організація або громадянин, який зробив пропозиції про віднесення цієї інформації до ДТ, і орган державної влади, який має право визначати коло суб'єктів, що мають доступ до цієї інформації;

- термін дії рішення про віднесення інформації до ДТ.

Рішення про віднесення інформації до ДТ, продовження терміну дії раніше прийнятого рішення про віднесення інформації до ДТ, зміна ступеня секретності інформації, скасування раніше прийнятого рішення про віднесення інформації до ДТ приймаються державним експертом з питань таємниць протягом одного місяця з моменту надходження звернення державного органу, органу місцевого самоврядування, підприємства, установи, організації чи громадянина. Такі рішення підлягають реєстрації СБУ і є підставою для формування ЗВДТ, та внесення змін до зазначеного Зводу, галузевих або відомчих розгорнутих переліків відомостей, що становлять ДТ. Порядок реєстрації рішень державних експертів з питань таємниць визначається Кабінетом Міністрів України.

У державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що здійснюють діяльність, пов'язану з ДТ, з метою розробки і здійснення заходів щодо забезпечення режиму секретності, постійного контролю над їх виконанням, створюються на правах окремих структурних підрозділів *режимно-секретні органи* (РСО), які підпорядковуються безпосередньо керівникові цих установ.

Створення, реорганізація або ліквідація РСО здійснюються за погодженням із СБУ.

До складу РСО входять підрозділи режиму, криптографічного, технічного захисту інформації, таємного діловодства та інші підрозділи, що безпосередньо забезпечують охорону ДТ, в залежності від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

РСО комплектуються спеціалістами, яким надано допуск до ДТ зі ступенем секретності «ЦТ», якщо характер робіт не потребує іншого. Прийняття в ці структурні підрозділи тимчасових працівників не допускається.

Основними завданнями РСО є:

- недопущення необґрунтованого допуску та доступу осіб до таємної інформації;

- своєчасна розробка і реалізація заходів, що забезпечують охорону ДТ, спільно з іншими структурними підрозділами державних органів, органів місцевого самоврядування, підприємств і організацій;

- запобігання розголошенню секретної інформації, випадків втрат матеріальних носіїв цієї інформації, заволодіння секретною інформацією іноземними державами та громадянами України, яким надано допуску та доступу до неї;

- виявлення та закриття каналів витоку секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;

- забезпечення впровадження заходів режиму таємності при виконанні всіх видів робіт, пов'язаних з ДТ, і при здійсненні зовнішніх відносин;

- організація та ведення таємного діловодства;

- здійснення контролю над станом режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

РСО *має право:*

- вимагати від усіх безпосередніх учасників роботи з ДТ неухильного виконання вимог законодавства щодо забезпечення захисту ДТ;

- здійснювати перевірку стану та організації роботи з питань захисту ДТ і забезпечення режимів секретності;

- брати участь в службових розслідуваннях;

- отримувати від громадян, яким оформляються документи на допуск до секретної інформації, анкетні дані;

- використовувати засоби зв'язку та вести в установленому порядку поштово-телеграфне листування з питань забезпечення режиму таємності та ін.

Передача функцій РСО будь-яким іншим підрозділам державного органу, органів місцевого самоврядування, підприємств, установ та організацією не допускається.

Залежно від ступеня секретності інформації встановлено такі *форми допуску* до ДТ:

форма 1 - для роботи з таємною інформацією, що має ступінь секретності «ОВ», «ЦТ» і «Т», термін дії - 5 років;

форма 2 - для роботи з таємною інформацією, що має ступінь секретності «ЦТ» і «Т», термін дії - 7 років;

форма 3 - для роботи з таємною інформацією, що має ступінь секретності «Т», термін дії - 10 років.

Органами СБУ надається допуск до ДТ дієздатним громадянам України віком від 18 років, яким він необхідний при виконанні службової, виробничої, наукової чи науково-дослідної діяльності або навчанні.

Надання допуску до роботи з документами, що містять ДТ, здійснюється відповідно до Положення з питань державної таємниці, затвердженого постановою КМУ від 29 листопада 2001 р. № 1601. При цьому заповнюється облікова карта громадянина про надання допуску до ДТ форма, якої затверджена СБУ.

Всі облікові картки громадянина про надання допуску до ДТ реєструються в журналі реєстрації облікових карток.

Згідно зі ст. 23 ЗУ «Про державну таємницю» надання допуску передбачає:

- визначення необхідності роботи громадянина із секретною інформацією;
- перевірку громадянина у зв'язку з допуском до ДТ;
- взяття громадянином письмового зобов'язання щодо збереження довіреної йому ДТ;
- отримання в письмовій формі згоди громадянина на передбачене законом обмеження прав у зв'язку з його допуском до ДТ;
- ознайомлення громадянина з мірою відповідальності за порушення законодавства про ДТ.

Безпосередньо перелік відомостей, які надає громадянин для оформлення допуску до ДТ, а також текст зобов'язання, яке він дає, затверджено Указом Голови СБУ «Про затвердження зобов'язання громадянина України у зв'язку з допуском до ДТ і анкети для оформлення допуску до ДТ».

Доступ до ДТ надається вищим державним посадовим особам за фактом вступу на посаду: Президенту, Голові Верховної Ради України, Прем'єр-міністру, Голові Верховного Суду, Голові Конституційного Суду, Генеральному прокурору, Голові СБУ (з письмовим зобов'язанням про нерозголошення ДТ).

Громадяни, які мають допуск до ДТ обмежуються частково в своїх правах: це стосується виїзду за кордон на ПМП, свободи інформаційної діяльності.

Секретна інформація може передаватися за кордон іноземній державі чи організації тільки за міжнародними угодами, за згодою Верховної Ради України, Президента, за пропозицією Ради національної безпеки і оборони (РНБО).

Ст. 23 ЗУ «Про державну таємницю» визначає перелік, на підставі якого громадянину може бути відмовлено в наданні допуску до ДТ:

- відсутності у громадянина обґрунтованої необхідності в роботі із секретною інформацією;
- сприяння громадянином діяльності іноземної держави, іноземної організації або їх представників, а також окремих іноземців або осіб без громадянства, що наносить збиток інтересам національної безпеці України, або участь громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;
- відмова громадянина взяти на себе письмове зобов'язання по збереженню ДТ, яка буде йому довірено, а також при відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до ДТ;
- наявність у громадянина судимості за тяжкі або особливо тяжкі злочини, чи не погашеної або не знятої в установленому порядку;
- наявність у громадянина психічних розладів, які можуть нанести шкоду охороні ДТ, у відповідності з переліком, затвердженого Міністерством охорони здоров'я України та СБУ.

Крім того, в наданні допуску також може бути відмовлено в разі:

- повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;
- постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;
- невиконання громадянином обов'язків щодо збереження ДТ, яка йому довірена або довірялася раніше.

Лекція 5. ТАЄМНИЦЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА СУДОЧИНСТВА

Питання для опрацювання:

5.1. Поняття та правові ознаки таємниці досудового розслідування

5.2. Види таємної інформації в кримінальному провадженні

Джерела:

1. Кримінальний кодекс України від 05.04.2001 року № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
2. Кримінальний процесуальний кодекс України 13.04.2012 року № 4651-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n1239
3. Про доступ до судових рішень: ЗУ від 22 грудня 2005 року N 3262-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3262-15#Text
4. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: ЗУ від 23 грудня 1993 року № 3782-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3782-12#Text
5. Про судоустрій і статус суддів: ЗУ від 2 червня 2016 року № 1402-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text
6. Єдиний державний реєстр судових рішень / Державна судова адміністрація України. URL: http://reyestr.court.gov.ua

5.1. Поняття та правові ознаки таємниці досудового розслідування

Одним з видів таємниць, прямо зазначених у ч. 1 ст. 8 ЗУ «Про доступ до публічної інформації» є *таємниця досудового розслідування* (ТДР).

ТДР є різновидом професійної таємниці та однією з умов, що сприяє успішному розкриттю злочинів і викриттю обвинуваченого. Передчасне її розголошення може негативно вплинути на хід розслідування, надасть можливість обвинуваченому приховати або знищити сліди злочину, предмети і документи, які можуть стати доказами, ухилитися від слідчого та судді, іноді також заподіяти шкоду обвинуваченому, потерпілому та іншим особам.

Правовий інститут ТДР містить:

- *загальну частину:* визначення, принципи і критерії відносини інформації до ТДР, правові ознаки ТДР;
- *режим ТДР:* механізм обмежень доступу до даних, що становить ТДР;
- *санкції* за неправомірне використання відомостей, що становлять ТДР.

Розглянемо першу складову правового інституту ТДР.

ТДР - службова інформація, що створюється та збирається в системі діяльності з виявлення та розкриття злочинів, і використовується співробітниками правоохоронних органів, що здійснюють зазначену діяльність з метою попереднього розслідування подій злочину та протидії їм.

Також необхідно зазначити, що до складу правового інституту ТДР входять два типи правових норм - *норми матеріального права* (матеріальні норми) та *норми процесуального права* (процесуальні норми).

В свою чергу сукупність норм матеріального права, що входять до правового інституту ТДР можна розділити на *загальні,* які регулюють порядок захисту та/або забезпечення доступу до інформації, що може відноситися до ТДР (персональні дані, комерційна таємниця, банківська таємниця) та *спеціальні*, які регулюють порядок захисту та/або забезпечення доступу до інформації, що безпосередньо становить ТДР.

До *загальних матеріальних норм* правового інституту ТДР відносяться деякі норми Законів України «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги» та ін.

До спеціальних норм матеріального права, що входять до правового інституту ТДР можна віднести деякі норми Законів України «Про судоустрій та статус суддів» і «Про доступ до судових рішень».

Специфіка *процесуальних норм,* що входять до правового інституту ТДР, визначається поширенням їх дії лише процесуальні правовідносини, що виникають в процесі судочинства або досудового розслідування. Такі норми містяться, насамперед, у Кримінальному процесуальному кодексі України, Цивільному процесуальному кодексі України, Кодексі України про адміністративні правопорушення.

ТДР (таємницю слідства) складають всі відомості, отримані в процесі здійснення слідчих і оперативно-розшукових дій. Тому вмістом кримінального провадження є інформація певного роду, що формалізована відповідно до вимог кримінального процесуального закону з певним доступом до неї. Так, у кримінальному провадженні може знаходитися інформація, що не підлягає розголошенню ні за яких умов. До неї належать форми, методи та результати оперативно- розшукових заходів, утримання та матеріали оперативно-розшукової справи, інформація яких відноситься до державної таємниці, відповідно до ст. 8 ЗУ «Про державну таємницю». Також, відповідно до ч. 4 ст. 6

ЗУ «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» і ч. 4 ст. 18 ЗУ «Про державний захист працівників суду і правоохоронних органів» до ІзОД відносяться відомості про заходи безпеки та осіб, взятих під варту.

З усього розглянутого слідують *правові ознаки ТДР:*

1) ТДР - це вид ІзОД, який регулюється КПКУ та іншими законодавчими актами;

2) ТДР складають всі відомості, отримані в процесі здійснення слідчих і оперативно-розшукових дій, а також інформація, що не підлягає розголошенню (форми, методи та результати оперативно-розшукових заходів, утримання та матеріали оперативно-розшукової справи, інформація яких відноситься до ДТ);

3) розголошення ТДР може негативно вплинути на розкриття злочину і викриття винних.

5.2. Види таємної інформації в кримінальному провадженні

Щодо *другої складової правового інституту ТДР* (режиму ТДР) необхідно зазначити, що особливість правового регулювання даного виду таємниці полягає в тому, що в юридичній науковій літературі існує дискусія з приводу загальної назви та вмісту ТДР.

Досудове розслідування (дізнання) є однією із стадій кримінального провадження, яке починається з моменту внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань і закінчується закриттям кримінального провадження, або направленням до суду обвинувального акту, клопотанням про застосування примусових заходів медичного або виховного характеру, клопотанням про звільнення особи від кримінальної відповідальності.

Тобто разом з ТДР використовується багато інших видів таємної інформації: в процесі кримінального провадження в суді першої інстанції, яке включає підготовче судове провадження, судовий розгляд і ухвалення судового рішення, провадження з перегляду судового рішення в апеляційному або касаційному порядку, Верховним Судом України, а також за ново виявленими обставинами. Тому в науковій літературі крім поняття *«ТДР»* використовується поняття *«таємниця слідства і судочинства», яка включає в себе професійну таємницю суддів.*

Основним міжнародно-правовим актом, що встановлює стандарти діяльності судових органів і який закріплює цей вид таємної інформації, є

«Основні принципи незалежності судових органів», схвалені ООН. Згідно з п. 15 цих принципів «судді зобов'язані зберігати професійну таємницю щодо своєї роботи та конфіденційної інформації, отриманої в ході виконання ними своїх обов'язків, за винятком відкритих судових розглядів, і їх не можна змушувати давати показання з таких питань».

Згідно зі ст. 12 Кодексу професійної етики судді «суддя не може робити публічні заяви, коментувати в засобах масової інформації справи, які перебувають у провадженні суду, і піддавати сумніву судові рішення, що набрали законної сили. Суддя не має права розголошувати інформацію, яка стала йому відомою у зв'язку з розглядом справи».

Ст. 7 ЗУ «Про доступ до судових рішень» визначені відомості, які не можуть бути розголошені в текстах судових рішень, відкритих для загального доступу, а саме:

- імена (ім'я, по батькові, прізвище) фізичних осіб;
- адреса місць проживання або перебування фізичних осіб, номери телефонів або інших засобів зв'язку, адреси електронної пошти, ідентифікаційні номери (коди);
- реєстраційні номери транспортних засобів;
- інша інформація, що дозволяє ідентифікувати фізичну особу.

До зазначених відомостей *не належать:*

- прізвища та ініціали суддів, які прийняли судове рішення;
- імена посадових чи службових осіб, які, виконуючи свої повноваження, беруть участь в цивільному, господарському, адміністративному або кримінальному провадженнях, справах про адміністративні правопорушення (проступки);
- імена сторін у справі, яка розглядалася міжнародною судовою чи іншою міжнародною організацією, на вирішення якої в тексті судового рішення містяться посилання.

Однак поняття *«таємниця слідства і судочинства»* є досить суперечливим, оскільки воно порушує одну з основ судочинства - принципу гласності та відкритості, гарантованого ст. 129 Конституції України та п. 20 ст. 7 КПКУ.

Нормами ст. 27 КПКУ та ст. 11 ЗУ «Про судоустрій і статус суддів» гарантується гласність і відкритість судового провадження та його повне фіксування технічними засобами.

Ніхто не може бути обмежений у праві на отримання в суді усної або письмової інформації про результати розгляду його судової справи. Кожен, хто

не є стороною у справі, має право на вільний доступ до судового рішення.

Для забезпечення прозорості діяльності судової влади та створення механізму для реалізації гласності судового процесу в Україні був прийнятий ЗУ «Про доступ до судових рішень». На виконання зазначеного закону з 1.06.2006 р. доступ до судових актів судів загальної юрисдикції здійснюється через Єдиний державний реєстр судових рішень, роботу якого забезпечує Державна судова адміністрація України. Доступ до реєстру здійснюється через офіційний веб-портал судової влади України за адресою: http://reyestr.court.gov.ua.

Розгляд справ у судах відбувається відкрито, крім випадків, встановлених процесуальним законом. Будь-який присутній в залі судового засідання, може вести стенограму, робити нотатки, використовувати портативні аудіозаписувальні пристрої. Проведення в залі судового засідання фотозйомки, відеозапису, транслювання судового засідання по радіо і телебаченню, а також проведення звукозапису із застосуванням стаціонарної апаратури допускаються на підставі ухвали суду, що приймається з урахуванням думки сторін та можливості проведення таких дій без шкоди для судового розгляду.

Учасники судового провадження та особи, які не брали участі у кримінальному провадженні, але щодо яких суд вирішив питання про їх права, свободи, інтереси чи обов'язки, не можуть бути обмежені у праві на отримання в суді як усної, так і письмової інформації про результати судового розгляду і в праві на ознайомлення з процесуальними рішеннями, а також отримання їх копій.

Ніхто не може бути обмежений у праві на отримання в суді інформації про дату, час і місце судового розгляду та про вжиті в ньому судові рішення, крім випадків, встановлених законом.

Розгляд справи в закритому судовому засіданні допускається за вмотивованим рішенням суду у випадках, передбачених процесуальним законом. Слідчий суддя або суд може прийняти рішення про здійснення кримінального провадження у *закритому судовому засіданні* впродовж усього судового розгляду або його окремої частини лише у наступних випадках:

1) якщо обвинуваченим є неповнолітній;

2) розгляду справи про злочин проти статевої свободи та статевої недоторканості особи;

3) необхідності запобігти розголошенню відомостей про особисте та сімейне життя чи обставин, які принижують гідність особи;

4) якщо здійснення провадження у відкритому судовому засіданні може призвести до розголошення таємниці, що охороняється законом;

5) необхідності забезпечення безпеки осіб, що беруть участь у кримінальному провадженні.

Особисті записи, листи, зміст особистих телефонних розмов, телеграфних та електронних повідомлень можуть бути розглянуті у відкритому судовому засіданні тільки в тому випадку, якщо слідчий суддя або суд не прийме рішення про їх розгляд в закритому судовому засіданні, на підставі зазначеного п. 3.

Судове рішення, ухвалене у відкритому судовому засіданні, проголошується публічно. Для закритого судового засідання, судове рішення проголошується публічно з пропуском закритої інформації, і яка на момент проголошення судового рішення підлягає подальшої захисту від розголошення.

При розгляді справ перебіг судового процесу фіксується технічними засобами в порядку, встановленому процесуальним законом. Офіційним записом судового засідання є лише технічний запис, здійснений судом у порядку, передбаченому п. 4 ст. 107 КПКУ. Фіксування судового засідання за допомогою технічних в є обов'язковим. У разі неприбуття в судове засідання всіх осіб, які беруть участь у провадженні, або в разі, якщо судочинство здійснюється судом за відсутності осіб, фіксування за допомогою технічних засобів кримінального провадження в суді не здійснюється.

Учасники судового провадження мають право отримати копію запису судового засідання, зробленого за допомогою технічних засобів.

Незастосування технічних засобів фіксування кримінального провадження у випадках, якщо воно є обов'язковим, тягне недійсність відповідної процесуальної дії та отриманих в результаті її здійснення результатів, за винятком випадків, якщо сторони не заперечують проти визнання такої дії та результатів її здійснення чинними.

В процесі прийняття судового рішення виникає *«таємниця нарадчої кімнати»* (ст. 82^1 Закону України «Про судоустрій і статус суддів») або *«таємниця наради суддів»* (ст. 367 КПКУ). Згідно з нормами цих законодавчих актів при ухваленні судового рішення ніхто не має права перебувати в нарадчій кімнаті, крім складу суду, який розглядає справу. Суд може перервати нараду лише для відпочинку з настанням нічного часу. Під час перерви судді не можуть спілкуватися з особами, які брали участь у кримінальному провадженні. Під час перебування в нарадчій кімнаті суддя не має права розглядати інші судові справи. Судді не мають права розголошувати хід обговорення та ухвалення рішення у нарадчій кімнаті. Єдиною інформацією, яка публікується за результатами наради суддів, є рішення, постанова чи вирок суду.

Таємниця нарадчої кімнати є однією з гарантій виконання конституційної вимоги незалежності суддів і підпорядкування їх тільки закону. Таємниця наради дозволяє суддям вільно висловлювати свою думку з будь-якого питання, яке розглядається, відстоювати її, наводити аргументи, голосувати за те рішення, яке суддя вважає правильним і справедливим.

Таємниця наради суддів забезпечується також відсутністю протоколу і розголошенням тільки результатів голосування, а не його ходом.

В нарадчій кімнаті судді обговорюють і вирішують питання, перелічені в ст. 368 КПКУ. Ці питання головуючий послідовно ставить на голосування, причому кожне питання в такій формі, щоб на нього можна було дати тільки позитивну або негативну відповідь. Нарада суддів проводиться з кожного питання, при цьому ніхто із суддів не має права утримуватися від голосування при винесенні рішення. Щоб усунути вплив особливого становища головуючого на інших суддів, особливо на народних засідателів, закон зобов'язує його голосувати останнім (ст. 375 КПКУ). Дотримання цього порядку в нарадчій кімнаті не фіксується в будь-якому процесуальному документі і в силу таємниці наради суддів не може бути перевірено при перегляді справи в апеляційному чи касаційному порядку. Ніяких винятків з правила про таємницю наради суддів у КПКУ не передбачено.

Відповідно до ст. 54 Закону України «Про судоустрій і статус суддів» суддя зобов'язаний «не розголошувати відомості, які становлять таємницю, що охороняється законом, в тому числі і таємницю нарадчої кімнати і закритого судового засідання».

Також, в процесі кримінального провадження може розглядатися інформація, що складає одну із законодавчо визначених таємниць *(ст. 162 КПКУ):*

В процесі здійснення кримінального судочинства може виникати *«таємниця особи, щодо якої здійснюються заходи безпеки»,* передбаченої Законом України «Про забезпечення безпеки осіб, що беруть участь в кримінальному судочинстві».

Зокрема, особи, які беруть участь у кримінальному судочинстві, за наявності реальної загрози їх життю, здоров'ю, житлу чи майну мають право на забезпечення безпеки. Відомості про заходи безпеки та осіб, взятих під захист, є *ІзОД.*

Також в КПКУ введено поняття *«таємниця спілкування»* (п. 7 ст. 7). Згідно зі ст. 14 даного Кодексу та ст. 31 Конституції України «таємниця спілкування» -

правове положення, відповідно до якого, в ході кримінального провадження кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Втручання в приватне спілкування захисника, священнослужителя з підозрюваним, обвинуваченим, засудженим, виправданим - заборонено.

Втручання в таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених КПКУ, з метою виявлення та запобігання тяжкому чи особливо тяжкого злочину, встановлення його обставин, особи, яка вчинила злочин, якщо іншим способом неможливо досягти цієї мети. Інформація, отримана в результаті втручання у спілкування, не може бути використана інакше як для вирішення завдань кримінального судочинства.

Нормами ст. 258 КПКУ гарантується невтручання в приватне спілкування. Зокрема, ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді. Прокурор, слідчий за погодженням з прокурором зобов'язаний звернутися до слідчого судді з клопотанням про дозвіл на втручання в приватне спілкування в порядку, передбаченому ст. 246, 248, 249 КПКУ, якщо будь-яка слідча дія передбачає таке втручання. Ч. 4 ст. 258 КПКУ передбачено, що втручанням в приватне спілкування є отримання доступу до змісту спілкування за умови, що учасники спілкування мають достатні підстави вважати спілкування приватним.

Різновидом втручання в приватне спілкування є:

1) аудіо-, відеоконтроль особи;
2) арешт, огляд і виїмка кореспонденції;
3) зняття інформації з транспортних телекомунікаційних мереж;
4) зняття інформації з електронних інформаційних систем.

В разі втручання в таємницю спілкування існує загроза порушення конституційних прав особи, оскільки відсутній контроль над припиненням подальшого втручання в приватне спілкування в кримінальному провадженні - фактичні дані про злочин або особу вже отримані, а термін дії постанови слідчого судді ще не закінчився. В такому випадку, прокурор повинен прийняти процесуальне рішення у вигляді постанови про припинення негласної слідчої дії і повідомити про це слідчому судді письмово.

Відповідно до чинного законодавства кримінальне провадження складається з кількох частин, сукупність яких становить систему стадій кримінального процесу, в яких відбувається обіг інформації, що становить ТДР і розглянуті вище таємниці. На підставі цього можна окремо виділити види

таємної інформації в кримінальному провадженні *(рис. 5.1).*

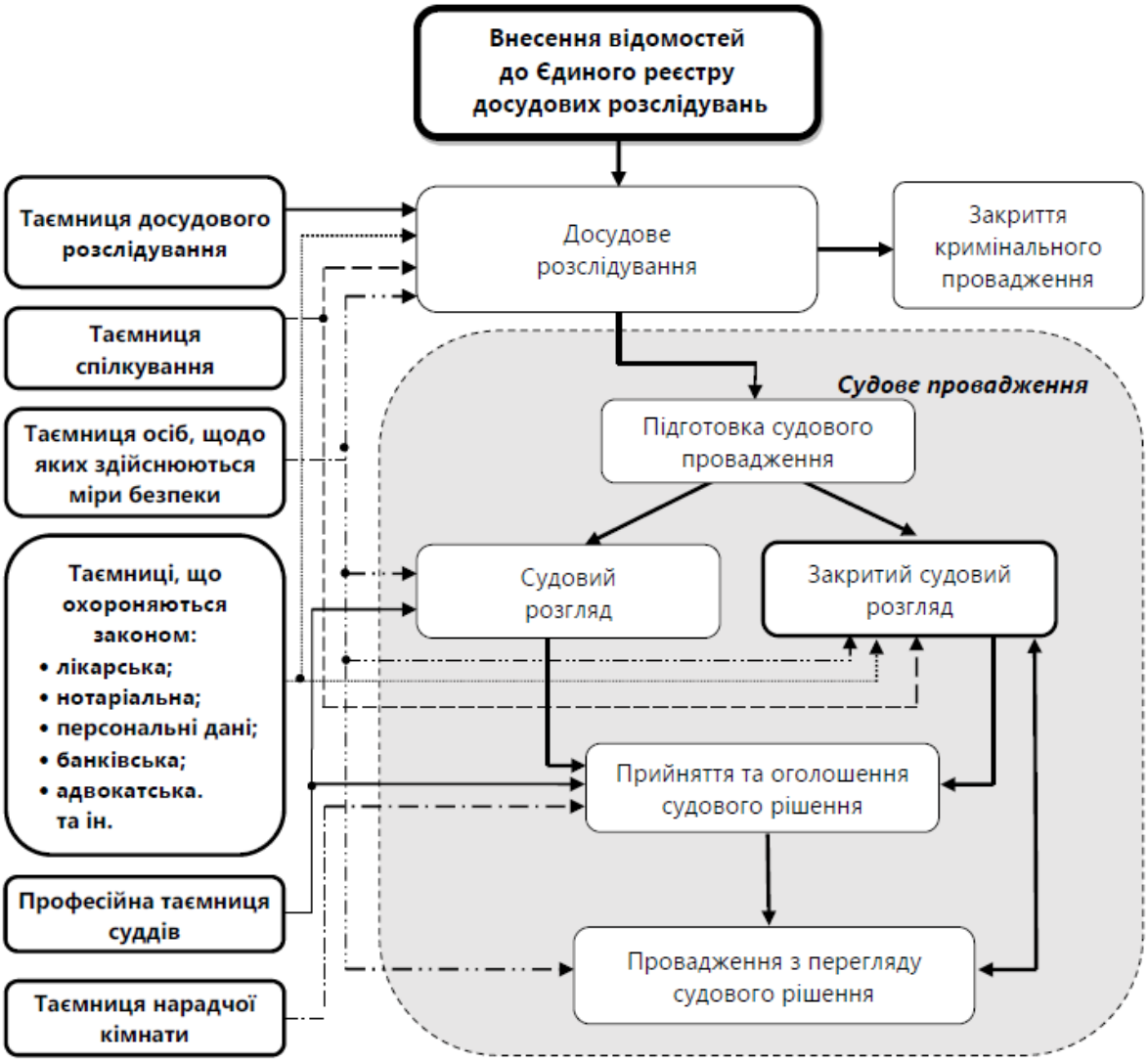

Рис. 5.1. Види таємної інформації в кримінальному судочинстві

Таким чином, зараз обсяг інформації, доступ до якої обмежено у процесі досудового розслідування та судочинства чинним законодавством, значно ширше, ніж поняття *таємниця досудового розслідування, таємниця слідства, таємниця нарадчої кімнати, таємниця осіб, щодо яких здійснюються міри безпеки, таємниця спілкування* тощо.

В результатах досудового розслідування особами з метою перешкоджання проведення розслідування, здатності вплинути на хід розслідування, нанести шкоду в об'єктивності встановлення обставин кримінальної правопорушення. Існування цієї заборони також обумовлено тим, що передчасне розголошення даних слідства третім особам у приватній бесіді, публічному виступі, в ЗМІ може

скомпрометувати учасників провадження, негативно вплинути на розкриття злочину, викриття винних, оскільки інформованість окремих зацікавлених осіб або організованих злочинних угрупувань про направлення розслідування і про конкретні слідчі та інші процесуальні дії, дозволить їм активно протидіяти зусиллям слідчого або оперативників.

Дані досудового розслідування можна оголосити лише з дозволу слідчого або прокурора та тільки в тому обсязі, в якому вони представляють можливим. У необхідних випадках слідчий попереджає всіх учасників досудового розслідування (свідків, потерпілого, захисника, експерта, спеціаліста, перекладача, понятих та інших осіб, присутніх при проведенні досудового розслідування) про обов'язок не розголошувати без його дозволу даних досудового розслідування.

Необґрунтоване оприлюднення даних досудового розслідування серйозно ускладнює провадження по кримінальній справі, спричиняє порушення прав і законних інтересів громадян, ускладнення здійснення правосуддя, може спричинити втрату доказів, порушити права та інтереси учасників процесу тощо. Відомості, які має слідство і дізнання, об'єктивно представляють інтерес для сторони, яка надає протидію розслідуванню.

Основними способами необґрунтованого (злочинного) оприлюднення відомостей, що входять до ТДР є:

1) отримання інформації через корумпованих працівників правоохоронних органів;

2) безпосереднє спостереження і аналіз дій працівників правоохоронних органів; аналіз виступів працівників правоохоронних органів в засобах масової інформації, а також журналістів, які проводять «журналістське розслідування»;

3) встановлення прослуховуючої апаратури і апаратури прихованої відео-та фотозйомки;

4) знімання інформації з технічних каналів зв'язку;

5) проникнення в комп'ютерні мережі правоохоронних органів;

6) отримання інформації через спеціально впроваджених в ряди працівників правоохоронних органів суб'єктів;

7) провокації працівників правоохоронних органів на необережне розголошення слідчої таємниці;

8) отримання інформації від родичів та інших близьких працівників правоохоронних органів, яким ТДР була розголошена цими працівниками з

необережності;

9) отримання інформації через підозрюваних, обвинувачених, які брали участь у проведенні слідчих дій у справі;

10) отримання інформації через потерпілих і свідків, які беруть участь у розслідуванні;

11) отримання інформації через адвокатів, які захищають підозрюваних і обвинувачуваних;

12) отримання інформації через експертів, фахівців, а також інших учасників кримінального процесу - перекладачів, законних представників.

У чинному законодавстві України представлені кримінально- правові засоби забезпечення неприпустимості розголошення інформації, що становить ТДР та інших видів таємниць.

Зокрема, за розголошення *даних досудового слідства* або *дізнання,* вчинене суддею, прокурором, слідчим, працівником органу дізнання, оперативно-розшукового органу незалежно від того, чи брала ця особа безпосередньо участь у досудовому слідстві чи дізнанні, якщо розголошені дані ганьблять людину, принижують її честь і гідність встановлена кримінальна відповідальність ст. 387 ККУ.

Також, відповідно до ч. 1 ст. 381 ККУ розголошення відомостей про заходи безпеки щодо особи, взятої під захист, службовою особою, яка прийняла рішення про ці заходи, особою, яка її здійснює, або службовою особою, якій ці рішення стали відомі у зв'язку з її службовим становищем, а так ж особою, взятою під захист, якщо ці дії заподіяли шкоду здоров'ю особи, взятої під захист - карається штрафом від ста до трьохсот неоподатковуваних податком мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеження волі на строк до трьох років.

Відповідальність за розголошення відомостей, що становлять *«таємницю особи, щодо якої здійснюються заходи безпеки»,* передбачена ст. 25 ЗУ «Про забезпечення безпеки осіб, що беруть участь в кримінальному судочинстві»:

Частиною 1 передбачена дисциплінарна відповідальність за розголошення відомостей про заходи безпеки особами, які прийняли рішення про ці заходи, або особами, які їх здійснюють. А у випадках, коли розголошення цих відомостей спричинило тяжкі наслідки - передбачена кримінальна відповідальність.

Частиною 2 вказаної статті передбачена адміністративна відповідальність передбачена за розголошення таких відомостей особою, взятою під захист. А в разі, якщо це призвело або могло призвести до тяжких наслідків, - кримінальну

відповідальність.

За розголошення охоронюваної законом таємниці, у тому числі *таємниці нарадчої кімнати* або *таємниці* , яка стала відома судді під час розгляду справи в *закритому судовому засіданні* згідно зі ст. 83 ЗУ «Про судоустрій і статус суддів» передбачено дисциплінарну відповідальність судді.

Відсутність в законодавстві чіткого поняття ТДР та відомостей, які її складають, дає підставу деяким учасникам досудового розслідування зневажливо ставитися до збереження розглянутих видів таємниць. Це вимагає розробки та прийняття окремого нормативно-правового акту щодо правового регулювання обігу таємної інформації в процесі досудового розслідування та судочинства.

Лекція 6. ПОНЯТТЯ ТА ЗМІСТ БАНКІВСЬКОЇ ТАЄМНИЦІ

Питання для опрацювання:

6.1. Поняття і правовий режим банківської таємниці

6.2. Організаційно-правовий захист банківської таємниці

Джерела:

1. Кримінальний кодекс України від 05.04.2001 року № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
2. Цивільний кодекс України від 16.01.2003 року № 435-IV 2341 / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/435-15
3. Про банки і банківську діяльність: ЗУ від 07.12.2000 року № 2121-III2341 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text

6.1. Поняття і правовий режим банківської таємниці

Банківська система в будь-якій країні є важливою складовою економіко-господарського механізму. З метою забезпечення її стабільного та ефективного функціонування держава створює ряд гарантій банківської діяльності, чинне місце серед яких займає *банківська таємниця* (БТ).

Інститут БТ є складовою частиною правової системи будь-якої розвиненої країни світу, зміст якої обумовлено особливостями економіко-правової доктрини держави та формування нормативної бази, що забезпечує правовий захист інформації з обмеженим доступом.

Правовий інститут БТ, як і будь-який інший таємниці, можна умовно представити трьома складовими:

- загальна частина: визначення БТ, принципи і критерії інформації, котра відноситься до БТ, правові ознаки БТ;
- режим БТ: правовий механізм обмеження доступу до інформації, складової БТ;
- санкції: юридична відповідальність за протиправні дії з інформацією, що складає БТ.

Щодо *першої складової правового інституту БТ* відзначимо, що в юридичній науці та в чинному законодавстві досі немає єдиного розуміння поняття, правової природи і змісту БТ, її співвідношення з іншими видами таємниць (комерційної, службової, професійної тощо).

Ряд авторів вважають, що БТ є різновидом комерційної таємниці (КТ), оскільки склад БТ утворює КТ клієнта, що стала відомою банку в силу наявності договірних відносин між ним і банком, і КТ самого банку як самостійного суб'єкта господарювання. Інші автори розглядають БТ як різновид службової таємниці: *«БТ визначається як інформація про операції, рахунки і вклади клієнтів і кореспондентів банку. Носії такої інформації мають гриф секретності, оскільки вона є різновидом службової таємниці».*

Треті визначають БТ, як «встановлену законом і гарантовану банком систему правових та спеціальних технічних засобів, що забезпечують правовий режим обмеженого доступу до інформації про банківський рахунок, операції за рахунком і відомості про клієнта».

Не додає ясності й норма ст. 1076 ЦКУ, згідно з якою *«банк гарантує таємницю банківського рахунку, операцій за рахунком і відомостей про клієнта».* Ця норма носить загальний характер, адже в ній не наводиться перелік відомостей про клієнта, які можуть становити БТ.

Якщо клієнт - *фізична особа,* то БТ є його паспортні дані, відомості про внесення третіми особами грошей на рахунок вкладника, номер рахунку тощо. А також будь-які відомості, які стали відомі банку в процесі обслуговування клієнта.

Якщо клієнт - *юридична особа,* то БТ складають всі відомості, які зберігаються в справі клієнта, в тому числі довідки та свідоцтва державних органів про реєстрацію та облік, установчі документи, інформація, що міститься в документах, що дають право займатися підприємницькою діяльністю (ліцензії та ін.), в різних формах бухгалтерської звітності та в інших документах, відомості про кредитну історію клієнта, про зміст і умови кредитного договору та договору про забезпечення виконання зобов'язань тощо.

Безумовно таємниця вкладів, рахунків та операцій по ним і персональні дані клієнтів є елементом таємниці особистого (сімейної) життя і відносяться до персональної інформації про особу, поширення якої без згоди її власника заборонено законодавством. Але поняття *«відомості про клієнта»* є необмеженим і вимагає, законодавчого уточнення.

Обсяг інформації, що становить БТ (не обмежуючи її обсягу, визначеного ЦКУ), конкретизують норми ч. 1 ст. 60 ЗУ «Про банки і банківську діяльність», який є основоположним документом, що визначає правовий режим БТ в Україні. Тут визначено, що *«інформація щодо діяльності та фінансового стану клієнта,*

яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку, є БТ».

Повний перелік цієї інформації наступний:

- відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;
- операції, проведені на користь чи за дорученням клієнта, здійснені ним угоди;
- фінансово-економічний стан клієнтів;
- системи охорони банку та клієнтів;
- інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;
- відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша інформація;
- інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;
- коди, що використовуються банками для захисту інформації.

До цього списку не входить інформація, що підлягає розголосу, а саме: дата реєстрації, кількість балансових філій, кількість працюючих на кінець року, кількість рахунків, валюта балансу, обсяг кредитного портфеля, обсяг вкладів громадян, капітал банку згідно з інструкцією про порядок регулювання та аналіз діяльності комерційних банків, оплачений статутний фонд, сума доходів, сума витрат, прибуток, рентабельність власного капіталу в процентах та інші відомості, що визначаються Державним комітетом статистики України, Національним банком України і самим банком (на власний розсуд) відповідно до законодавства України.

Інформація про банки чи клієнтів, яка збирається під час проведення банківського нагляду, також становить БТ. Можна стверджувати, що до БТ певного банку також належить інформація про клієнтів інших банків, яка стала відома з документів, угод та операцій клієнта банку.

З теоретичної точки зору неоднозначним є визначення місця БТ серед видів ІзОД.

Зміст глави 10 ЗУ «Про банки і банківську діяльність» недостатньо точно розподіляє співвідношення БТ з категорією конфіденційної інформації. Аналіз положень ч. 2 і 3 ст. 61 цього Закону дає підстави вважати, що конфіденційна інформація співвідноситься з БТ як загальне і окреме. Так, назва ст. 61 говорить: *«зобов'язання щодо збереження банківської таємниці",* а в ч. 4 даної статті

наголошується, що *«приватні особи та організації, які при виконанні своїх функцій або наданні послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб».*

Отже, можна зробити висновок, що законодавець розглядає БТ не як окремий вид ІзОД, а як підвид конфіденційної інформації.

Також й вчені відносять БТ до конфіденційної інформації: «БТ є специфічним видом конфіденційної інформації, яка пов'язана з виконанням юридичними особами банківської діяльності та приналежністю фізичних осіб до відповідної професії - банківських службовців».

Однак, відповідно до ст. 8 ЗУ «Про доступ до публічної інформації», БТ належить до категорії таємної інформації, в силу своєї назви - таємниця.

Поширення конфіденційної інформації здійснюється за бажанням юридичних і фізичних осіб у володінні, користуванні або розпорядженні яких така інформація знаходиться. А поширення (або розголошення) БТ здійснюється в чітко встановлених законодавством межах, порядку та за оформленим запитом належних суб'єктів.

Володілець (власник) конфіденційної інформації самостійно визначає режим доступу до неї. У той же час порядок доступу та зобов'язання щодо збереження БТ чітко визначені законодавством.

Різниця між цими поняттями проводить і сам законодавець. Так, глава 10 ЗУ «Про банки і банківську діяльність» називається «Банківська таємниця та конфіденційність інформації». Тобто, БТ відноситься не тільки до конфіденційної категорії, але й до таємної.

З вище сказаного випливають *правові ознаки БТ:*

- це конфіденційна інформація, отримана банком від його клієнтів у зв'язку з наданням банківських послуг;

- розголошення інформації, що становить БТ, заборонено законом;

- ця інформація не відноситься до державної таємниці, але є таємною.

Практичний інтерес представляє також *порівняння БТ* з іншого різновидом таємної інформації - *комерційною таємницею* (КТ).

Правовий режим КТ регламентується ГКУ, ЦКУ, ЗУ «Про господарські товариства» та деякими підзаконними нормативними актами. Незважаючи на загальну правову природу БТ і КТ, з практичної точки зору досить важливим є проведення чіткого розмежування цих двох категорій в чинному законодавстві та в науковій літературі, і виділення принципових відмінностей:

- на відміну від КТ, зміст і обсяг якої встановлюється керівником підприємства на свій розсуд, перелік відомостей, що складають БТ, встановлений ЗУ «Про банки і банківську діяльність». Це, до речі, і об'єднує банківську і державну таємницю, оскільки склад і обсяг останньої, також визначений на рівні закону;

- БТ складають чужі відомості, тобто відомості про клієнтів і кореспондентів банку, що знаходяться в банку на правовому титулі володіння. Тому банк не має права використовувати і розпоряджатися такими відомостями без спеціальної згоди клієнта. У той самий час відомості, що становлять КТ банку, знаходяться у власності банку;

- правовий режим КТ визначається ГКУ та ЦКУ, а правовий режим БТ визначається ЗУ «Про банки і банківську діяльність».

Отже, БТ є окремим самостійним видом таємниці, що належить до ІзОД.

6.2. Організаційно-правовий захист банківської таємниці

Режим БТ - це правовий механізм її захисту, який ґрунтується на законодавчих підставах обмеження доступу до інформації, що становить таємницю, чіткої регламентації процесу обороту цієї інформації (отримання, засекречування, збереження, передачі, розсекречення та ін.). Саме ця складова БТ та її практична реалізація має багато спільного з режимами комерційної, службової та професійної таємниць.

Специфічні риси правового режиму БТ полягають у тому, що його встановлення не вимагає додаткового оформлення локальними актами.

Конкретні шляхи реалізації *організаційно-правового захисту БТ* згідно зі ст. 61 ЗУ «Про банки і банківську діяльність» полягають у наступному:

- обмеження кола осіб, що мають доступ до інформації, що становить БТ;

- організація спеціального діловодства з документами, що містять БТ;

- застосування технічних засобів щодо запобігання несанкціонованого доступу до електронних та інших носіїв інформації;

- застосування застережень щодо збереження БТ та відповідальності за її порушення в договорах і угодах між банком і клієнтом.

З метою *запобігання несанкціонованому доступу* до інформації, що містить БТ, суб'єкти, які мають доступ до такої інформації, у власних інструкціях з діловодства встановлюють особливий порядок реєстрації, використання, зберігання та доступу до документів, що містить БТ.

При обробці вихідних документів виконавець документа визначає потребу проставляння на ньому *грифу «Банківська таємниця»,* з урахуванням вимог ст. 1076 ЦКУ та ст. 60 ЗУ «Про банки і банківську діяльність».

Гриф «Банківська таємниця» не проставляється на документах, які банки надають клієнтам - власникам інформації, яка містить БТ. Забороняється відправлення документів з грифом «Банківська таємниця» з використанням факсимільного зв'язку або іншими каналами зв'язку, що не забезпечують захист інформації.

Роздруківка документів з грифом «Банківська таємниця» у технологічних автоматизованих робочих місцях (АРМ) здійснюється згідно з технологічними схемами роботи відповідних АРМ банку. На роздрукованих документах проставляється гриф «Банківська таємниця», і вони обліковуються відповідно до вимог з обліку паперових документів.

Важливим елементом правового режиму БТ є законодавчо визначений *порядок розкриття банкам* БТ, який встановлений ст. 62 ЗУ «Про банки і банківську діяльність».

Коло осіб або перелік суб'єктів, які мають право вимагати безпосередньо від банку в тому чи іншому обсязі розкриття інформації, що містить БТ, є вичерпним і певним ст. 62 ЗУ «Про банки і банківську діяльність», а саме:

- власник такої інформації;
- суд (на його рішенню);
- органи прокуратури України, СБУ, Міністерства внутрішніх справ України, Національне антикорупційне бюро України, Антимонопольний комітет України;
- центральний орган виконавчої влади, що реалізує державну податкову політику;
- центральний орган виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму;
- органи державної виконавчої служби;
- Національна комісія з цінних паперів та фондового ринку;
- Національне агентство з питань запобігання корупції;
- інші банки;
- інші особи, зазначені власником рахунку (вкладу) в заповідальному розпорядженні банку;
- Фонд гарантування вкладів фізичних осіб;

- державні нотаріальні контори чи приватні нотаріуси, іноземні консульські установи по справах спадщини за рахунками (вкладами) померлих власників рахунків (вкладів);

- службовці Нацбанку України або уповноважені ними особи;

особа (у тому числі, уповноважена діяти від імені держави), на користь якої відчужуються активи та зобов'язання, банку при виконанні заходів, передбачених програмою фінансового оздоровлення банку, або під час здійснення процедури ліквідації.

Цей перелік суб'єктів БТ є повним і вичерпним, що свідчить про те, що інші фізичні та юридичні особи, в тому числі і державні органи, мають право отримувати відповідну інформацію виключно за рішенням суду, а не безпосередньо в банку.

Іншою проблемою в порядку розкриття БТ стосується визначення *обсягу надання інформації,* яка містить БТ. Аналіз норм чинного законодавства показує, що розкриття інформації, яка містить БТ, зазначеним вище суб'єктам може здійснюватися:

1. *в повному обсязі* БТ розкривається банком:

a) за письмовим запитом або з письмового дозволу власника такої інформації;

b) на письмову вимогу суду або за рішенням суду;

c) спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу (в тому числі без їх письмового запиту щодо фінансових операцій, що стали об'єктами фінансового моніторингу);

d) на вимогу службовців Національного банку України або уповноважених ними осіб, в рамках, наданих ЗУ «Про Національний банк України» повноважень, які здійснюють функції банківського нагляду або валютного контролю.

2. *в обмеженому обсязі* (в межах повноважень кожного з суб'єктів звернення, за конкретний проміжок часу і тільки щодо операцій за рахунками конкретної юридичної особи або фізичної особи - суб'єктів незалежно від підприємницької діяльності) на письмову вимогу органів, визначених ст. 62 ЗУ «Про банки та банківську діяльності».

Інформація, яка містить БТ в відношенні фізичної особи - громадянина, який не є суб'єктом підприємницької діяльності, може бути розкрита банком виключно на письмову вимогу суду або за рішенням суду. Отже, законом не

передбачається, щоб зазначені вище суб'єкти на їх письмову вимогу, отримували від банків таку інформацію в повному об'ємі.

Щодо третього елементу в процедурі розкриття БТ - встановлення вимог до запитів державних органів на отримання інформації, яка містить БТ, то вони викладені в ч. 2 ст. 62 ЗУ «Про банки і банківську діяльність». Так, вимога відповідного державного органу на отримання інформації, яка містить БТ, повинна:

- бути викладена на бланку державного органу встановленої форми;
- бути подана за підписом керівника державного органу (або його заступника), скріпленим гербовою печаткою;
- містити передбачені законом підстави для отримання цієї інформації;
- містити посилання на норми спеціальних законів, відповідно до яких державний орган має право на отримання такої інформації.

Певні суперечності в цьому елементі полягають в тому, що відповідні державні органи зобов'язані використовувати тільки паперову форму запиту інформації від банку, але останнім дозволяється надавати цю інформацію, як в паперовому вигляді, так і в електронному. Хоча «передача інформації, яка містить БТ, електронною поштою або в режимі on-line здійснюється лише в захищеному (зашифрованому) вигляді з контролем цілісності та з обов'язковим наданням підтвердження про її надходження з електронним підписом одержувача з використанням засобів захисту».

Слід також зазначити, що режим таємності певного обсягу банківської інформації, що входить до складу БТ, має кінцевий, а не абсолютний характер. Припинення режиму конфіденційності даної інформації пов'язується з настанням певної події в часі, а саме: на стадії ліквідації банку, призначення ліквідатора, відомості про фінансове становище банку перестають бути конфіденційними чи становити БТ. Проте решта відомостей, що становлять БТ, зберігають режим таємниці, навіть після завершення угоди про банківське обслуговування клієнта.

Щодо *третьої складової правового інституту БТ - санкцій,* зазначимо таке: основними видами відповідальності за розголошення БТ є дисциплінарна, цивільно-правова і кримінальна.

До посадових і службових осіб банків можуть бути застосовані заходи *дисциплінарної відповідальності,* згідно із загальним трудовим законодавством, або спеціальним законодавством, яке визначає правовий статус тих чи інших категорій осіб, наприклад, державних службовців.

Застосування одного з видів відповідальності (наприклад, дисциплінарної") не виключає можливості застосування та інших її видів (цивільно-правової, кримінальної).

У разі розголошення банком відомостей, що становлять БТ, клієнт має право вимагати від банку відшкодування завданих збитків та моральної шкоди. Положення ч. 1 ст. 22 ЦКУ встановлюють загальне правило про право особи на відшкодування збитків, завданих порушенням її цивільного права.

В ч. 2 ст. 22 ЦКУ законодавець розділяє збитки на два види:

- *реальний збиток* - втрати, які особа понесла в зв'язку з знищенням або пошкодженням речі, а також витрати, які особа зробила або мусить зробити для відновлення свого порушеного права;

- *втрачена вигода* - доходи, які особа могла отримати при звичайних обставинах, якби її право не було порушене.

Відповідно до ч. 4 ст. 61 ЗУ «Про банки і банківську діяльність», у разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, уповноважених здійснювати банківський нагляд, збитки відшкодовуються винними органами.

Що стосується *кримінальної відповідальності,* то вона настає відповідно до чинного ККУ за вчинення таких злочинів, як «незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» (ст. 231) та «розголошення комерційної або банківської таємниці» (ст. 232).

Слід зауважити, що притягнення особи до кримінальної відповідальності за ст. ст. 231, 232 ККУ можливо тільки у випадку, якщо використання чи розголошення відомостей, що становлять БТ, завдало істотної шкоди суб'єкту господарювання. Під *«істотною»* слід розуміти шкоду, яка в 100 і більше разів перевищує неоподатковуваний мінімум доходів громадян. Максимальне покарання, передбачене ст. 231 ККУ, - позбавлення волі на строк до трьох років, а за ст. 232 - позбавлення волі на строк до двох років.

Отже, БТ є самостійним видом ІзОД і має свій специфічний режим захисту, не тотожний ніякому іншому правовому режиму конфіденційності.

Лекція 7. ПРАВОВІ ОСНОВИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Питання для опрацювання:

7.1. Поняття і ознаки комерційної таємниці

7.2. Захист комерційної таємниці

Джерела:

1. Господарський кодекс України від 16 січня 2003 року № 436-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/436-15#n276
2. Цивільний кодекс України від 16.01.2003 року № 435-IV 2341 / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/435-15
3. Кодекс України про адміністративні правопорушення від 07.12.1984 року № 8073-X / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text
4. Кримінальний кодекс України від 05.04.2001 року № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
5. Про захист економічної конкуренції: ЗУ від 11.01.2001 року № 2210-III / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2210-14

7.1. Поняття і ознаки комерційної таємниці

Аналогічно розглянутим двом таємницям, правовий інститут комерційної таємниці (КТ) в Україні також представлений трьома складовими.

Щодо *першої складової* слід відзначити, що в світі не існує єдиного підходу до визначення поняття КТ. Застосовуються різні визначення інформації, що містить КТ: «*ділові таємниці*», «*виробничі таємниці», «торговельні таємниці», «ноу - хау»* та інші. В Україні всі вищевказані види таємниць об'єднані в один узагальнюючий термін - КТ, який знайшов своє відображення у чинному законодавстві, хоча й неоднозначне.

В ст. 505 ЦКУ КТ - «це інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію».

У наведеному визначенні КТ викликає сумнів термін «секретна інформація», який не вписується в традиційну класифікацію інформації в

українському законодавстві (ст. 8 ЗУ «Про доступ до публічної інформації»). Секретною (таємною) інформацією є інформація, яка становить державну, професійну, БТ та ін. КТ являє собою вид конфіденційної інформації.

Нормами ст. 506 ЦКУ передбачено виключне право власника інформації, що становить КТ на встановлення режиму доступу до цієї інформації, надання права на використання та перешкоджання розголошенню, збиранню та використання.

Тобто суб'єктом визначення доступу до інформації, яка містить КТ, є власник відповідної інформації або особа, якій надано права розпоряджатися цією інформацією.

Глава 46 ЦКУ встановлює майнові права інтелектуальної власності на КТ, охорону КТ органами державної влади, а також термін дії права інтелектуальної власності на КТ.

Ст. 162 ГКУ трохи дає дещо інакше визначення КТ: «технічна, організаційна або інша комерційна інформація ... за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів з охорони її конфіденційності».

На рівні окремого закону визначення конкретних сфер або видів господарської діяльності і категорій (перелік) відомостей, які можуть становити КТ, в Україні досі не існує. Згідно зі ст. 36 ГКУ склад і обсяг відомостей, що становлять КТ і спосіб їх захисту, самостійно визначаються суб'єктом господарської діяльності.

У той же час, відповідно до ч. 2 ст. 505 ЦКУ, певні відомості «технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих з них, які відповідно до закону не можуть бути віднесені до КТ, можуть становити КТ».

Не може бути віднесена до КТ інформація, що відповідно до ЗУ «Про інформацію» підпадає під режим ДТ або, навпаки, відкрита інформація, наприклад, правила страхування, розроблені страховиком (ЗУ «Про страхування»).

Так само не можуть становити КТ відомості, які підлягають обов'язковому опублікуванню, наданню на запит необмеженого кола зацікавлених осіб, а також відомості, про які в законодавстві міститься пряма заборона на поширення на них режиму обмеженого доступу. Наприклад, ЗУ «Про бухгалтерський облік та фінансову звітність в Україні» передбачає, що фінансова звітність підприємств

не становить КТ, крім випадків, передбачених законодавством. В ЗУ «Про сертифіковані товарні склади та прості і подвійні складські свідоцтва» закріплена норма про те, що регламент сертифікованого складу не може становити КТ.

Щодо принципів та критеріїв віднесення інформації до КТ також існують певні труднощі, тому однією з ознак КТ є *комерційна цінність,* тобто цінова визначеність (вартість) такої інформації, методику підрахунку якої в кількісному вимірі досі не розроблено.

Інформація, складова КТ, повинна бути предметом адекватних існуючим обставинам заходів щодо збереження її конфіденційності, вжитих особою, яка законно контролює цю інформацію.

Як форму КТ можна розглядати *комерційні таємниці,* які є інформацією у вигляді документів, схем, виробів. Вони підлягають захисту від можливого посягання через викрадення, вивідування, витік інформації.

Їх розрізняють за такими ознаками:

- за природою КТ (технологічні, виробничі, організаційні, маркетингові, інтелектуальні, рекламні);

- за власністю (власність підприємства, групи підприємств, окремої особи, групи осіб тощо);

- за колом осіб, які мають до них доступ;

- за призначенням.

Інформація, яку можна віднести до КТ, повинна містити наступні ознаки: не бути державною таємницею (секретними даними); стосуватися торгово-виробничої діяльності підприємства; не завдавати шкоди інтересам суспільства; мати комерційну цінність та створювати переваги в конкурентній боротьбі; мати встановлені власником інформації обмеження в доступі.

До числа основних об’єктів правовідносин КТ відносяться:

- *володілець КТ:* фізична або юридична особа, що володіє на законній підставі інформацією, що становить КТ;

- *конфідент КТ:* фізична або юридична особа, якій в силу службового становища, договору або на іншій законній підставі відома КТ іншої особи;

- *носії КТ:* матеріальні об’єкти, в тому числі і фізичні поля, в яких інформація, складова КТ, знаходить відображення у вигляді символів, сигналів, технічних рішень і процесів.

Отже, до правових ознак *КТ* можна віднести:

- конфіденційність інформації, що є КТ, яка полягає в тому, що вона є невідомою та не є легкодоступною;

- інформація, складова КТ, має комерційну цінність (цінову визначеність);

- склад і обсяг відомостей, що становлять КТ, визначені суб'єктом господарювання або уповноваженим на це органом;

- власник КТ повинен застосовувати відповідні засоби для охорони цієї інформації.

7.2. Захист комерційної таємниці

Щодо другої складової правового інституту КТ (режиму таємності) слід зазначити, що згідно зі ст. 20 редакції ЗУ «Про інформацію» КТ відноситься до ІзОД. При цьому конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюється за їх бажанням відповідно до передбачених ними умов.

КТ постійно піддається різним загрозам, під якими розуміється окремі явища, події, процеси, настання яких може вплинути на захищеність КТ і призвести до негативних наслідків (прямих збитків, неотримання прибутку, підриву іміджу, зміни в планах, тимчасових втрат та ін.).

Класифікація загроз КТ представлена різними ознаками і критеріями *(таблиця 7.1).*

Таблиця 7.1 Класифікація загроз КТ

Критерії	**Різновиди**
За джерелами загрози	Зовнішні (промислове шпигунство, незаконні дії конкурентів, крадіжка матеріальних цінностей); внутрішні (розголошення працівниками конфіденційної інформації, низька мотивація персоналу, низька ефективність діяльності служби безпеки).
За ступенем тяжкості наслідків	Загрози з високою тяжкістю наслідків призводять до різкого погіршення всіх фінансово-економічних показників та припинення діяльності фірми; середньої - подолання наслідків вимагає великих витрат, але не вимагає тривалого часу; низькою - не завдають значної деструктивного впливу.
За ступенем імовірності загрози	Малоймовірні небезпеки (потенційні), які потенційно не мають реальної можливості наступити; реальні.

За стадії функціонування підприємства	На стадії створення підприємства; на стадії функціонування.
За ступенем імовірності загрози	Малоймовірні небезпеки (потенційні), які потенційно не мають реальної можливості наступити; реальні.
За стадії функціонування підприємства	На стадії створення підприємства; на стадії функціонування.
За об’єктом посягань	Інформаційні; фінансові; матеріальні; загрози престижу, авторитету, іміджу підприємства.
По суб’єкту загроз	Загрози з боку організованих злочинних угруповань; недобросовісних конкурентів; власних працівників; державних структур.
За характером напрямку	Прямі; непрямі.
По об’єкту напрямку	Виробничі таємниці; відомості про фінансову діяльність; відомості про управління; відомості про клієнтів і т. д.
За тривалістю дії	Тимчасові; постійні.
За рівнем суб’єктивного сприйняття	Неусвідомлені; із завищеним (заниженим) рівнем сприйняття; мнимі; адекватні.
При наявності людського фактору	Пов’язані з діяльністю людини; не пов’язані з діяльністю людини
За характером відповідальності суб’єктів загроз щодо їх наслідки	Дисциплінарна, цивільно-правова, адміністративна, кримінально-правова.
По виду збитків	Прямі; упущена вигода

Система захисту повинна комплексно поєднувати правові, організаційні, технічні та інші заходи, які приймає власник КТ з охорони її конфіденційності *(рис. 7.1)*.

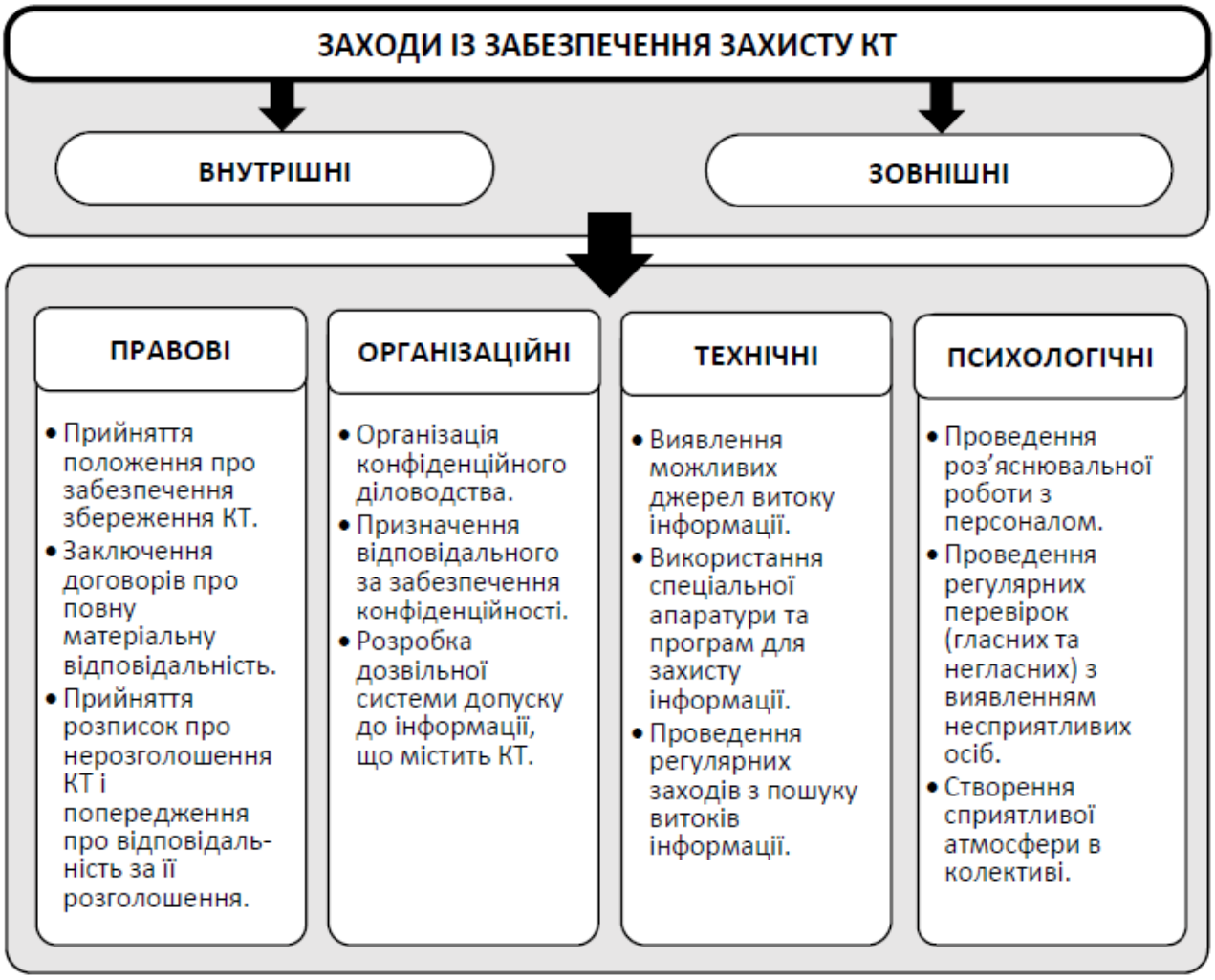

Рис. 7.1. Заходи по забезпеченню захисту КТ

Слід зазначити, що в умовах недосконалості чинного законодавства щодо КТ і з урахуванням останніх тенденцій світового досвіду багато фахівців вважають, що основних в реалізації правового *механізму захисту КТ доцільно перенести* в сферу локальних нормативно-правових актів і правового регулювання відносин в сфері «роботодавець-працівник».

Зокрема, в якості таких актів можуть розглядатися: Статут підприємства; Установчий договір; Колективний договір; Правила внутрішнього розпорядку, посадові інструкції тощо. На підставі вище викладеного можна побудувати концептуальну модель захисту КТ *(рис. 7.2).*

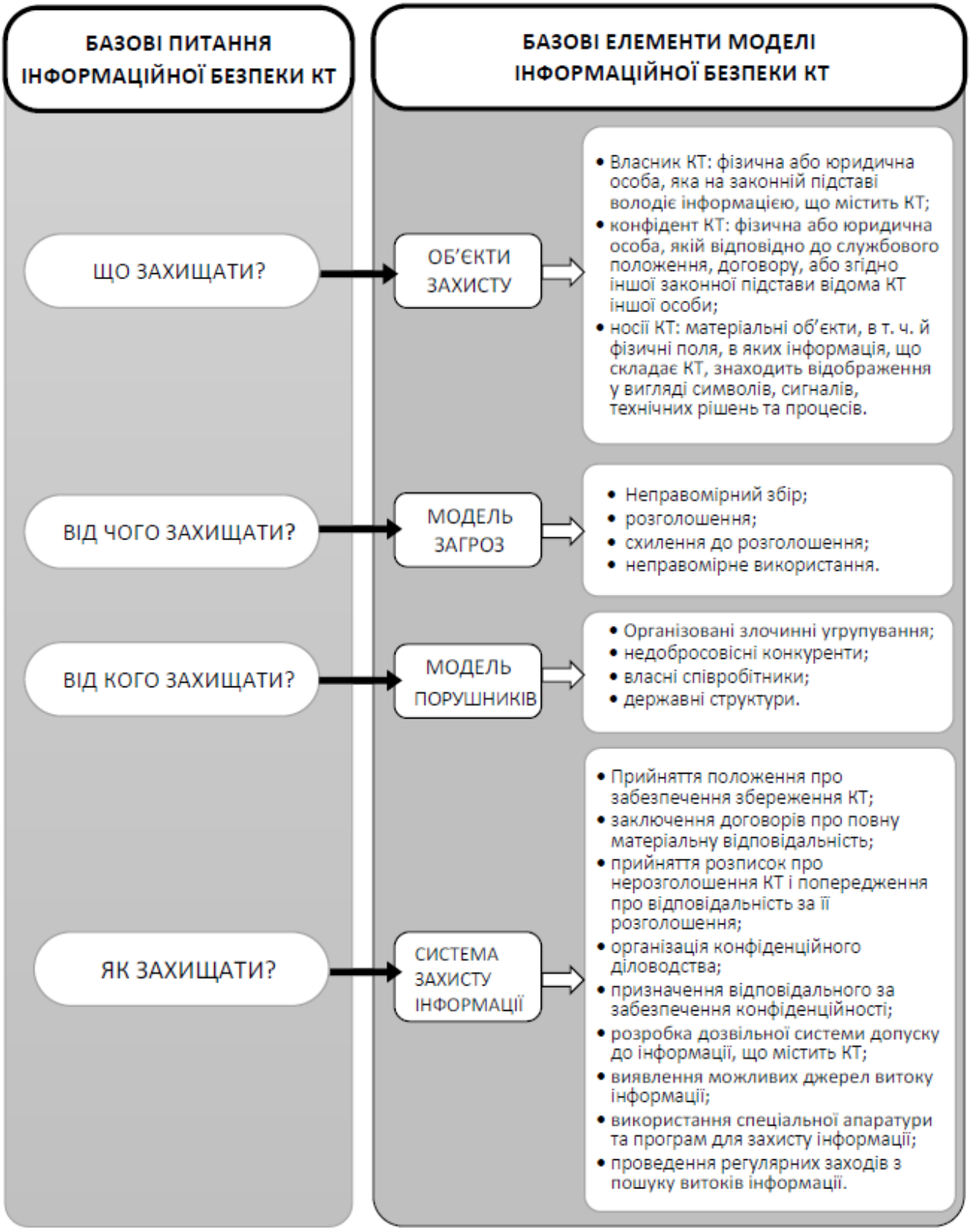

Рис. 7.2. Концептуальна модель захисту КТ

Щодо третьої складової інституту КТ зазначимо, що за порушення права

суб'єкта господарської діяльності на КТ до винної особи може бути застосована юридична відповідальність різної приналежності:

- цивільно-правова відповідальність в вигляді відшкодування збитків, заподіяних суб'єкту, на підставі ЦКУ;

- дисциплінарна і матеріальна відповідальність, передбачена КЗпПУ;

- адміністративна відповідальність, встановлена ч. 3 ст. 164-3 КУпАП;

- кримінальна відповідальність в Згідно зі ст. ст. 231, 232 ККУ.

Крім цього, адміністративно-господарські штрафи передбачені за недобросовісну конкуренцію у вигляді неправомірного збору, розголошення, схилення до розголошення та використання КТ (Глава 4 ЗУ «Про захист від недобросовісної конкуренції»).

Адміністративна відповідальність юридичних і фізичних осіб за отримання, використання, розголошення КТ передбачена, по-перше, ст. 164-3 «Недобросовісна конкуренція» КУпАП, а також ст. 16 «Неправомірне збирання КТ», ст. 17 «Розголошення КТ», ст. 18 «Схиляння до розголошення КТ» і ст. 19 «Неправомірне використання КТ» ЗУ «Про захист від недобросовісної конкуренції».

Неправомірним збиранням КТ вважається добування протиправним способом відомостей, відповідно до законодавства України КТ, якщо це завдало чи могло завдати шкоди суб'єкту господарської діяльності.

Розголошенням КТ є ознайомлення іншої особи без дозволу особи, уповноваженої на те, з відомостями, які відповідно до законодавства України КТ складають КТ, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням відповідних обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

Схиляннам до розголошення КТ являється примус особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням відповідних обов'язків відомості, які відповідно до законодавства України становлять КТ, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

Неправомірним використанням КТ є впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу уповноваженої на те особи відомостей, що становлять відповідно до законодавства України КТ.

Кримінальна відповідальність за порушення законодавства про захист КТ передбачена в розділі VII ККУ - «Злочини у сфері господарської діяльності». Так,

ст. 231 ККУ передбачає притягнення до відповідальності за такі злочинні дії як незаконне збирання з метою використання або використання відомостей, що становлять КТ. Злочином у сфері посягань на КТ є її розголошення (ст. 232 ККУ).

Зазначені злочинні дії відбуваються у відношенні предмета злочину і для отримання переваг в конкурентній боротьбі всупереч волі власника КТ і наносять останньому істотну шкоду, тим самим посягаючи на відносини добросовісної конкуренції.

Отже, в Україні створено основні елементи правового інституту КТ, але відсутній єдиний правовий механізм захисту КТ, хоча тенденції його розвитку цілком позитивні та відповідають світовим стандартам.

Лекція 8-9. ПРОФЕСІЙНА ТАЄМНИЦЯ ТА ІНШІ ВИДИ ТАЄМНИЦЬ, ПЕРЕДБАЧЕНИХ ЗАКОНОДАВСТВОМ УКРАЇНИ

Питання для опрацювання:

8.1. Поняття, ознаки та види професійної таємниці
8.2. Лікарська таємниця
8.3. Нотаріальна таємниця
8.4. Адвокатська таємниця
9.1. Податкова таємниця
9.2. Аудиторська таємниця
9.3. Журналістська таємниця
9.4. Інсайдерська таємниця
9.5. Таємниця страхування
9.6. Таємниця сповіді
9.7. Таємниця усиновлення
9.8. Таємниця голосування
9.9. Таємниця зв'язку (листування)

Джерела:

1. Кодекс України про адміністративні правопорушення від 07.12.1984 року № 8073-X / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text
2. Кримінальний кодекс України від 05.04.2001 року № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

8.1. Поняття, ознаки та види професійної таємниці

У сучасному законодавстві України чіткого визначення *професійної таємниці* (ПТ) немає. На сьогоднішній день єдиним законом, в якому згадується ПТ, є ЗУ «Про доступ до публічної інформації». В ст. 8 ПТ відноситься до таємної інформації: *«Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю».*

Згідно зі ст. 21 ЗУ «Про інформацію» таємна інформація відноситься до ІзОД, тобто ПТ є ІзОД і повинна мати власний *правовий інститут,* розглянутий раніше.

Щодо *першої складової правового інституту (загальної частини) ПТ*

зазначимо те, що не тільки в чинному законодавстві, але й в юридичній науці немає єдиного розуміння щодо поняття, правової природи та змісту ПТ, її співвідношення з іншими видами таємниць, зокрема службової (СТ).

ПТ умовно розподіляють на два види:

- ПТ в чистому вигляді, обумовлена самим родом діяльності (комерційна, службова та ін.);

- ПТ складовою частиною якої є довірена особиста таємниця.

ПТ - інформація, що захищається законом, яка довірена або стала відомою особі (держателю) виключно в силу виконання ним своїх професійних обов'язків, не пов'язаних з державною або муніципальною службою, поширення якої може завдати шкоди правам і законним інтересам іншої особи (довірителя), яка довірила ці відомості, і яка не є державною або комерційною таємницею.

До основних *суб'єктів правовідносин* в області ПТ відносяться довірителі (власники), утримувачі і користувачі ПТ.

Довіритель - фізична особа (незалежно від громадянства), що довірила відомості іншій особі, а також його правонаступники (у тому числі спадкоємці).

Утримувач - фізична або юридична особа, якій виключно в силу його професійної діяльності (професійних обов'язків) були довірені або стали відомі відомості, що становлять ПТ.

Користувач - особа, якій відомості, що становлять ПТ, стали відомі на законних підставах у зв'язку з виконанням ним своїх службових обов'язків у випадках і порядку, встановлених законом.

Поширеною ознакою ПТ є і те, що вона може належати особі, яка у зв'язку зі своїм професійним статусом отримала доступ до конфіденційних відомостей і не перебуває на державній або муніципальній службі. В цьому випадку інформація буде мати характер СТ.

Однак, ПТ і СТ суттєво відрізняються за суб'єктним і об'єктним складом, умовами виникнення та режимами правового захисту. Держателем ПТ є особа, яка не перебуває на державній або муніципальній службі, якій певна інформація надана клієнтом - довірителем таємниці. І навпаки, СТ - це конфіденційна інформація, яка стала відома в державних органах та органах місцевого самоврядування тільки на законних підставах і при виконанні їх представниками службових обов'язків. На відміну від ПТ, яку становить тільки «чужа» інформація, СТ крім таємниці довірителя може містити службову інформацію, що є власністю держави.

Але варто враховувати й те, що на практиці трапляються випадки, коли

певна ПТ (на законних підставах) надається органам державної влади, і коли одна і та ж інформація захищається одночасно і ПТ, і СТ.

Тому, не заперечуючи теоретичної самостійності ПТ і СТ, необхідно констатувати їх тісний взаємозв'язок в практичному аспекті збереження інформації, що є предметом ПТ. Розмежування цих таємниць є умовним, що не дозволяє сформувати комплексний підхід до вирішення практичних проблем розкриття та розслідування розголошення ПТ.

Встановлення правового режиму ПТ є правомірним тільки у випадках, коли отримання доступу до інформації, що відноситься до ПТ, обумовлено специфікою професії і є невід'ємним її елементом.

Заборона на поширення довіреної інформації не має абсолютного характеру, оскільки нормативно-правовими актами передбачено цілий ряд випадків, які зобов'язують носіїв відповідної інформації надати її в розпорядження уповноважених органів (наприклад, правоохоронних) та їх посадовим особам.

Таким чином, можна виділити *правові ознаки ПТ:*

1) довірена добровільно довірителем або стала відома особі у силу виконання ним своїх професійних обов'язків;

2) особа, якій довірено інформацію, не перебуває на державній або муніципальній службі (інакше інформація буде вважатися СТ);

3) заборона на поширення довіреної або інформації, що стала відомою, яка може завдати шкоди правам і законним інтересам довірителя, встановлений чинним законодавством;

4) інформація не відноситься до відомостей, що становлять державну або комерційну таємницю.

Щодо *другої складової правового інституту ПТ (режиму ПТ)* відзначимо, що особливості правового регулювання ПТ полягають в тому, що відповідні правила поведінки своїм виникненням зобов'язані не загальнолюдським моральним нормам, а нормам корпоративної моралі або професійної етики.

Ці норми виникли в процесі здійснення того чи іншого виду професійної діяльності, і для людини, що не відноситься до даної професії, можуть бути не прийнятними.

До ПТ відноситься інформація, з якою мають справу представники так званих «саморегульованих» професій та інші особи, яким ці відомості були довірені у зв'язку з їх професійним становищем. До ПТ слід віднести наступні таємниці: *лікарську, нотаріальну, адвокатську, аудиторську, журналістську,*

інсайдерську, страхування, сповіді, усиновлення, голосування, зв'язку (листування).

Обов'язок не розголошувати довірену їм інформацію належить до професійних обов'язків та є складовою частиною внутрішніх правил певної професії. Важливим у цьому відношенні є питання довіри - особа, яка потребує певної професійної допомоги, погоджується надати про себе інформацію, очікуючи збереження її у таємниці. Надана нею інформація може бути розголошена лише за його згодою. При цьому така інформація надається при реалізації (захисту) особою своїх прав і свобод (наприклад, право на здоров'я, на правову допомогу, на свободу віросповідання). Тому розголошення довіреної інформації спричинить обмеження прав особам, які не зможуть вільно користуватися послугами відповідних професій, без впевненості в захищеності переданої інформації.

Обов'язок зберігати інформацію виникає у представника професії, яким її було довірено; обов'язок не порушувати цю таємницю виникає і в інших осіб, зокрема, державних органів, які повинні поважати і не порушувати ПТ.

Щодо *третьої складової правового інституту ПТ - санкцій,* зазначимо таке, що правовий режим ПТ, як виду ІзОД, полягає в законодавчій забороні доступу до цих відомостей третіх осіб та встановленні санкцій за їх розголошення.

Таким чином, ПТ є самостійним видом ІзОД і повинна мати свій власний правовий інститут. Але сьогодні в нашій країні створені тільки певні елементи правового інституту ПТ. Окремі види інформації, складові ПТ, регулюються правовими нормами різних галузей законодавства. Ці норми не завжди взаємоузгоджені, їх кількість має тенденцію до збільшення, оскільки зростає кількість напрямів і видів професійної діяльності. Тому побудувати комплексну концептуальну модель ПТ неможливо.

8.2. Лікарська таємниця

Лікарська таємниця - це інформація, що містить факти звернення за медичною допомогою, результати обстеження особи, про стан здоров'я, діагноз захворювання й інші відомості в медичних документах громадян.

За законодавством України до лікарської таємниці належать такі відомості:

- про хворобу, медичне обстеження, огляд та їх результати, інтимну та сімейну сторони життя громадянина (ст. 40 ЗУ «Основи законодавства України про охорону здоров'я»);

- відомості про реципієнтів, а також про осіб, які заявили про свою згоду або незгоду стати донорами у разі смерті (ст. 17 ЗУ «Про трансплантацію органів та інших анатомічних матеріалів людини»);

- про результати тестування особи з метою виявлення ВІЛ, про наявність або відсутність у особи ВІЛ-інфекції (ст. 13 ЗУ «Про протидію поширенню хвороби, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ»);

- про зараження особи інфекційним захворюванням, що передається статевим шляхом, проведенні медичного огляду і обстеження з цього приводу, відомості інтимного характеру, отримані у зв'язку з виконанням професійних обов'язків посадовими особами та медичними працівниками установами охорони здоров'я (ст. 26 ЗУ «Про захист населення від інфекційних захворювань»);

- про перенесені та наявні в особи, яка виявила бажання здати кров та (або) її компоненти, захворювання, а також про вживання нею наркотичних речовин та властиві їй інші форми ризикованої поведінки, які можуть сприяти зараженню донора інфекційними хворобами, що передаються через кров, і за наявності яких виконання донорських функцій може бути обмежене (ст. 14 ЗУ «Про донорство крові та її компонентах»);

- відомості про наявність у особи психічного розладу, про факти звернення за психіатричною допомогою та лікування у психіатричному закладі або перебування в психоневрологічних закладах для соціального захисту або спеціального навчання, а також інші відомості про стан психічного здоров'я особи, її приватне життя (ст. 6 ЗУ «Про психіатричну допомогу»).

На підставі аналізу нормативно-правової бази можна стверджувати, що *об'єктом лікарської таємниці* є інформація про:

- факти звернення за медичною допомогою;
- стан здоров'я пацієнта;
- діагнозі та хвороби;
- медичний огляд та його результати;
- методи лікування;
- інтимну та сімейну сторони життя;
- інші відомості, отримані при медичному обстеженні.

Суб'єктами збереження лікарської таємниці є медичні працівники та інші особи, яким у зв'язку з виконанням своїх професійних чи службових обов'язків стало відомо про об'єкти лікарської таємниці (лікарі, провізори, санітари, нянечки, студенти медичних вузів і коледжів, немедичний персонал мед установ

та ін.). Вони не можуть бути допитані як свідки відповідно до п. 2 ч. 4 ст. 65 КПКУ.

Зазначені особи не мають права розголошувати такі відомості, крім передбачених законами випадків.

Також, обов'язок по збереженню лікарської таємниці та невикористання її на шкоду людині передбачено в *Клятві лікаря («Клятва Гіппократа»).*

Лікарську таємницю (інформацію про пацієнта) необхідно відрізняти від *медичної таємниці* (інформації для пацієнта).

За нормами, що регулюють лікарську таємницю, лікар зобов'язаний надавати медичну інформацію пацієнтові (ст. 39 ЗУ «Основи законодавства України про охорону здоров'я»): пояснити пацієнту в доступній формі інформацію про стан його здоров'я, мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, зокрема наявності ризику для життя й здоров'я. Пацієнт має право ознайомитися з історією своєї хвороби та іншими документами, що можуть служити для подальшого лікування.

В особливих випадках, коли повна інформація може завдати шкоди здоров'ю пацієнта, лікар може її обмежити. В цьому випадку він інформує членів сім'ї або законного представника пацієнта, враховуючи особисті інтереси хворого. Так само лікар діє, якщо пацієнт знаходиться в несвідомому стані.

Ця норма практично є єдиним випадком, коли людина може бути обмежена в отриманні персональної інформації про себе.

Згідно зі ст. 145 ККУ за «умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки, - карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років».

Також, «розголошення службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником, відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, небезпечної для життя людини, або захворювання на синдром набутого імунодефіциту (СНІДу) і його результатів, що стали їм відомі у зв'язку з виконанням службових або професійних обов'язків - карається штрафом від

п’ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, 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 або без такого» (ст. 132 ККУ).

8.3. Нотаріальна таємниця

Нотаріальна таємниця - «сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов’язки тощо».

Предметом нотаріальної таємниці є не тільки інформація, яка стала відома нотаріусу у процесі нотаріальної діяльності, а й відомості, які нотаріус отримав з інших джерел при виконанні своїх професійних обов’язків, а також процесуальна діяльність самого нотаріуса, спрямована на досягнення певного правового результату.

Нотаріус та особи, визначені у ст. 1 ЗУ «Про нотаріат», а також стажист нотаріуса зобов’язані зберігати нотаріальну таємницю, навіть якщо їх діяльність обмежується наданням правової допомоги чи ознайомленням з документами, а також, якщо нотаріальну дію, або дію, прирівняну до нотаріальної, не вчинили.

Обов’язок дотримання нотаріальної таємниці поширюється також на осіб, яким про вчинені нотаріальні дії стало відомо у зв’язку з виконанням ними службових обов’язків чи іншої роботи, осіб, залучених для вчинення нотаріальних дій у якості свідків, та на інших осіб, яким стали відомі відомості, що становлять предмет даної таємниці.

Порядок надання відомостей, що становлять нотаріальну таємницю, визначений ст. 8 ЗУ «Про нотаріат»:

- довідки про вчинені нотаріальні дії та копії документів, що зберігаються у нотаріуса, видаються нотаріусом виключно фізичним та юридичним особам, за дорученням яких або щодо яких вчинялись нотаріальні дії. У разі смерті особи чи визнанні її померлою, такі довідки видаються спадкоємцям померлого. У разі визнання особи безвісти зниклою, опікун, призначений для охорони майна полеглого, має право отримувати довідки про вчинені нотаріальні дії, якщо це необхідно для збереження майна, над яким встановлено опіку;
- довідки про вчинені нотаріальні дії та інші документи надаються нотаріусом протягом десяти робочих днів на обґрунтовану письмову вимогу

суду, прокуратури, органів, що здійснюють оперативно-розшукову діяльність, органів досудового слідства у зв'язку з кримінальним провадженням, цивільними, господарськими, адміністративними справами, справами про адміністративні правопорушення, що знаходяться в виробництв цих органів, з обов'язковим зазначенням номера справи та, додатково, гербової печатки відповідного органу;

- довідки про суму нотаріально посвідчених договорів, які необхідні виключно для встановлення дотримання законодавства з питань оподаткування, надаються нотаріусом протягом 10 робочих днів на обґрунтовану письмову вимогу органів доходів і зборів.

Довідки про наявність складеного заповіту та витяги із спадкового реєстру за виключенням заповідача видаються тільки після смерті заповідача.

Нотаріус не вправі давати показання як свідок щодо відомостей, що становлять нотаріальну таємницю, крім випадків, коли цього вимагають особи, за дорученням яких або щодо яких вчинялися нотаріальні дії.

Будь-яке втручання в діяльність нотаріуса, зокрема з метою перешкоджання виконанню ним своїх обов'язків або спонукання до вчинення ним неправомірних дій, у тому числі вимоги від нього, його стажиста, інших працівників, які перебувають у трудових відносинах з нотаріусом, відомостей, що становлять нотаріальну таємницю, до забороняється й тягне за собою відповідальність відповідно до законодавства (ст. 8-1 ЗУ «Про нотаріат»).

Однак сьогодні відсутній закон, який би чітко регулював питання відповідальності за розголошення нотаріальної таємниці. Питання відповідальності винних осіб за розголошення нотаріальної таємниці можна розглядати, керуючись загальними нормами українського законодавства. У відповідності зі ст. 1166 ЦКУ *«майнову шкоду, заподіяну неправомірними рішеннями, діями чи бездіяльністю особистим немайновим правам фізичної або юридичної особи, відшкодовується в повному обсязі особою, яка заподіяла шкоду».* Нотаріусу під час нотаріального процесу за участю перекладача необхідно роз'яснювати відповідальність перекладача на підставі цієї статті. Що ж до стажиста і помічника, то при укладанні з ними трудового договору необхідно закріплювати цю норму.

8.4. Адвокатська таємниця

Адвокатська таємниця - «будь-яка інформація, що стала відомою адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у

трудових відносинах з адвокатом, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених Законом підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, змісту рад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, отримані адвокатом при здійсненні адвокатської діяльності».

Суб'єктами, на яких поширюється обов'язок збереження інформації, що становить адвокатську таємницю, є адвокат, його помічник, стажер та особи, що знаходяться в трудових відносинах з адвокатом, адвокатським бюро, адвокатським об'єднанням, а також на особу, щодо якої припинено або призупинено право на зайняття адвокатською діяльністю. їм забороняється розголошувати відомості, що становлять предмет адвокатської таємниці, і використовувати їх у своїх інтересах або в інтересах третіх осіб.

У разі пред'явлення клієнтом вимог до адвоката у зв'язку з адвокатською діяльністю адвокат звільняється від обов'язку збереження адвокатської таємниці в межах, необхідних для захисту його прав та інтересів (ч. 4 ст. 22 ЗУ «Про адвокатуру та адвокатську діяльність»).

У такому випадку суд, орган, що здійснює дисциплінарне провадження стосовно адвоката, інші органи чи посадові особи, які розглядають вимоги клієнта до адвоката або яким стало відомо про пред'явлення таких вимог, зобов'язані вжити заходів для запобігання доступу сторонніх осіб до адвокатської таємниці та її розголошення.

Особи, винні в доступі сторонніх осіб до адвокатської таємниці або її розголошенні, несуть відповідальність згідно із законом.

Документи, пов'язані з виконанням адвокатом доручення, не підлягають оглядові, розголошенню чи вилученню без його згоди.

Відповідно до норм ст. 10 Правил адвокатської етики, «інформація та документи можуть втратити статус адвокатської таємниці за письмовою заявою клієнта (особи, якій відмовлено в укладення договору про надання правової допомоги) з передбачених Законом України «Про адвокатуру та адвокатську діяльність» підстав. При цьому інформація та документи, отримані від третіх осіб, що містять відомості про них, можуть поширюватися з урахуванням вимог законодавства з питань захисту персональних даних».

За розголошення адвокатської таємниці дисциплінарна відповідальність адвоката передбачена ст. 33-42 ЗУ «Про адвокатуру та адвокатську діяльність».

Крім того, відповідно до ч. 3 ст. 47 КПКУ *«захисник не має права розголошувати відомості, що стали йому відомі у зв'язку з участь у кримінальному провадженні і становлять адвокатську або іншу охоронювану законом таємницю».*

9.1. Податкова таємниця

В Україні правового інституту *податкової таємниці* на сьогодні не існує, але встановлені окремі норми чинного законодавства, що стосуються правових обмежень на доступ до інформації, отриманої в ході податкової діяльності.

Відповідно до ст. 17.1.9 Податкового кодексу України платник податків має *право «на нерозголошення контролюючим органом*(посадовими особами) відомостей про такого платника без його письмової згоди, та відомостей, що становлять конфіденційну інформацію, державну, комерційну чи банківську таємницю та стали відомими під час виконання посадовими особами службових обов'язків, крім випадків, коли це прямо передбачено законами». *Згідно зі ст. 21.1 посадові особи контролюючих органів зобов'язані: не допускати розголошення ІзОД, що збирається, використовується, зберігається при реалізації функцій, покладених на контролюючі органи.*

Інформація, що збирається, використовується та формується контролюючими органами у зв'язку з обліком платників податків, вноситься до інформаційних баз даних і використовується з урахуванням обмежень, передбачених для податкової інформації з обмеженим доступом (ст. 63.12 Податкового кодексу України).

9.2. Аудиторська таємниця

Так само як і податкова таємниця, аудиторська таємниця не має свого інституту таємниці.

Аудиторська діяльність визначається як підприємницька діяльність з проведення і надання послуг, супутніх аудиту. Аудит - це незалежна перевірка фінансової або бухгалтерської звітності організації.

До аудиторської таємниці *можна віднести «*інформацію, отриману при проведенні аудиту та виконанні інших видів аудиторських послуг*» (п. 4 ст. 19 ЗУ «Про аудиторську діяльність»).*

Неналежне зберігання аудиторської таємниці аудиторами і аудиторськими фірмами тягне відповідальність, передбачену ст. 21 ЗУ «Про аудиторську діяльність». Аудитор (аудиторська фірма) несе майнову та іншу цивільно-

правову відповідальність відповідно до договору та закону. Але розмір майнової відповідальності аудиторів (аудиторських фірм) не може перевищувати фактично завданих замовнику збитків з їх вини.

За неналежне виконання професійних обов'язків до аудитора (аудиторської фірми) можуть бути застосовані Аудиторською палатою України стягнення у вигляді попередження, зупинення дії сертифіката на строк до одного року або анулювання сертифіката, виключення з Реєстру (ст. 22 ЗУ «Про аудиторську діяльність»).

У разі розголошення аудиторської таємниці, організація має право зажадати компенсації для відшкодування понесених збитків.

9.3. Журналістська таємниця

Журналістська таємниця або як її ще називають, *таємниця журналістських джерел,* також прямо в законодавстві не визначена. Але можна вважати, що її становить інформація про особу, що побажала залишитися анонімним джерелом інформації журналіста, яка стала відома журналісту, посадовим особам, журналістському персоналу та службовому персоналу журналістської установи при здійсненні ними своїх професійних обов'язків.

Захист журналістських джерел закріплений в різних міжнародних документах. Наприклад, ст. 10 Європейської конвенції з прав людини гарантує захист журналістських джерел. Для більш точного зазначення з цього питання Радою Європи була прийнята Рекомендація № К(2000)7 «Про право журналістів не розкривати свої джерела інформації». Це право має бути визнане і забезпечене для будь-якої фізичної та юридичної особи, регулярно або професійно задіяної в зборі та публічному поширенні інформації через будь-які засоби масової інформації.

У нашій країні відповідно до ч. 3 ст. 25 ЗУ «Про інформацію» журналіст має права не розкривати джерело інформації або інформацію, яка дозволяє встановити джерела інформації, крім випадків, коли його зобов'язали для цього рішенням суду.

9.4. Інсайдерська таємниця

Останнім часом в області інформаційної безпеки актуальними стали повідомлення про те, що більшу загрозу ринку цінних паперів представляють угоди вчинені з використанням інсайдерської інформації.

Термін «інсайдерський» в перекладі з англійської означає «внутрішній», тобто *інсайдерська інформація* - це внутрішня інформація компанії. Наслідки використання інсайдерської інформації при здійсненні угод можуть бути наступними:

- використання інформації ставить володаря в переважне становище, що дає йому можливість здійснювати маніпулювання цінами на біржових торгах;
- використання інсайдерської інформації приносить економічну вигоду її володареві після виконання зобов'язань, що виникли на підставі угод, укладених з використанням такої інформації.

У нашій країні інсайдерська таємниця регулюється ЗУ «Про ринки капіталу та організовані товарні ринки». Відповідно до ст. 145, *інсайдерська інформація* - це неоприлюднена інформація про емітента, його цінні папери або інші фінансові інструменти, що перебувають в обігу на організованому ринку капіталу, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість відповідних фінансових інструментів.

Інформація щодо оцінки вартості цінних паперів та/або фінансово-господарського стану емітента, якщо вона отримана виключно на основі оприлюдненої інформації або інформації з інших публічних джерел, не заборонених законодавством, не є інсайдерською інформацією.

Інформація не вважається інсайдерською з моменту її оприлюднення відповідно до закону.

За незаконне використання інсайдерської інформації передбачається кримінальна відповідальність, згідно зі ст. 232, 232-1, 232-2,232-3 ККУ.

9.5. Таємниця страхування

Таємниця *страхування* - сукупність інформації про клієнта та його фінансовий стан, яка стала відома страховику (перестраховику) або страховому посереднику у зв'язку з укладанням та/або виконанням договору страхування (перестрахування) та розголошення якої може заподіяти матеріальну чи моральну шкоду такому клієнту. Таємниця страхування належить до таємниці фінансової послуги *(п. 73 ч. 1 ст. 1 ЗУ «Про страхування»).*

Посадові особи уповноваженого органу у випадку розголошення в будь-якій формі відомостей, що є таємницею страхування, несуть відповідальність, передбачену законом.

Інформація про юридичних та фізичних осіб, яка містить таємницю страхування, подається страхувальником у наступних випадках:

- на письмовий запит або з письмового дозволу власника такої інформації;

- на письмову вимогу суду або за рішенням суду;

- органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, податкової міліції на їх письмову вимогу відносно операцій страхування конкретної юридичної або фізичної особи за конкретним договором страхування у разі порушення кримінальної справи відносно даної фізичної або юридичної особи;

- центральному органу виконавчої влади з питань фінансового моніторингу відповідно до ЗУ «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму».

Обмеження щодо отриманої інформації, що містить таємницю страхування, не поширюються на службовців Уповноваженого органу, які в межах повноважень, наданих чинним Законом, здійснюють державний нагляд за страховою діяльністю.

9.6. Таємниця сповіді

Таємниця сповіді *законодавчо чітко не визначена. Але в ст. 3 ЗУ «Про свободу совісті та релігійні організації» передбачається, що* «ніхто не має права вимагати від священнослужителів відомостей, отриманих ними при сповіді віруючих*»*.

Ця таємниця поширюється тільки на інформацію, передану священнослужителю під час сповіді, а також особливою роллю і статусом церкви. Надати захист відомостям, які довіряються особою під час сповіді представнику релігійної організації, держава визнає особливість відносин між віруючими і церквою і риси, характерні обряду сповіді. Тим самим, законом надається захист прав особистості на недоторканність особистого і сімейного життя, свободи думки, свободи віросповідання.

Згідно з ч. 2 п. 5 ст. 65 КПКУ священнослужителі не можуть бути допитані як свідки про відомості, одержані ними на сповіді віруючих.

Аналогічна норма міститься й в ст. 51 ЦПКУ, де наданий вичерпний перелік осіб, які не підлягають допиту як свідки, в тому числі і священнослужителі - про відомості, одержані ними на сповіді віруючих.

9.7. Таємниця усиновлення

Таємниця усиновлення - *це відомості про* «перебування осіб, які бажають усиновити дитину, на обліку, пошук ними дитини для усиновлення, подання заяви про усиновлення, розгляд справи про усиновлення, здійснення нагляду за дотриманням прав усиновленої дитини тощо» *відповідно до ст. ст. 226-228 Сімейного кодексу України.*

Особи, яким у зв'язку з виконанням службових обов'язків доступна інформація, що містить таємницю усиновлення, а також інші особи, яким стало відомо факт усиновлення, зобов'язані не розголошувати її, зокрема і тоді, коли усиновлення для самої дитини не є таємним. Відомості про усиновлення видаються судом лише за згодою усиновлювача, крім випадків, коли такі відомості потрібні правоохоронним органам, суду у зв'язку з цивільною чи кримінальною справою, яка є у їх провадженні.

За розголошення таємниці усиновлення (удочеріння) всупереч волі усиновителя (удочерителя) - передбачається кримінальна відповідальність відповідно до ст. 168 ККУ.

9.8. Таємниця голосування

Таємниця голосування при виборах до органів державної влади та органів місцевого самоврядування гарантована ст. 71 Конституції України: *«Вибори до органів державної влади та органів* місцевого самоврядування є вільними і відбуваються на основі загального, рівного і прямого виборчого права шляхом таємного голосування».

Таємність волевиявлення виборців під час голосування на виборах встановлена спеціальними законами про вибори (референдум). Очевидно, що таємниця голосування, як вид таємної інформації, поширюється на пряме волевиявлення виборців при обранні представницьких органів влади або на державні посади, наділені представницьким мандатом, і ця таємниця не поширюється на таємне голосування, застосовувана при обранні на будь-які інші посади (наприклад, голосування за керівників колегіальних органів влади).

Умисне порушення таємниці голосування під час проведення передбачених законом України виборів, вчинене членом виборчої комісії або іншою службовою особою з використанням влади чи службового становища, - карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від одного до трьох років з позбавленням права

обіймати певні посади чи займатися певного діяльністю на строк до трьох років (ст. 159 ККУ передбачена кримінальна відповідальність).

9.9. Таємниця зв'язку (листування)

У ст. 1, 3, 6 ЗУ «Про поштовий зв'язок» йде мова про *«таємниці інформації у сфері надання послуг поштового зв'язку».* Це дає підстави говорити про існування *таємниці зв'язку* як різновиду професійної таємниці в Україні.

Це підтверджує і ст. 163 ККУ, яка передбачає кримінальну відповідальність за «порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер».

Лекція 10. ПРАВОВІ ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Питання для опрацювання:

10.1. Поняття, ознаки та законодавче визначення персональних даних

10.2. Обробка персональних даних

10.3. Організаційно-правові методи захисту персональних даних

Джерела:

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 / Рада Європи. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text
2. Про звернення громадян: ЗУ від 02.10.1996 року № 393/96-ВР / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/393/96-вр
3. Про захист персональних даних: ЗУ від 01.06.2010 року № 2297-VI / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/2297-17
4. Про інформацію: ЗУ від 02.10.1992 року № 2657-XII / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2657-12
5. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: від 20.11.2012 року № 5492-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text
6. Цивільний кодекс України від 16.01.2003 року № 435-IV 2341 / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/435-15
7. Кодекс України про адміністративні правопорушення від 07.12.1984 року № 8073-X / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text
8. Кримінальний кодекс України від 05.04.2001 року № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

10.1. Поняття, ознаки та законодавче визначення персональних даних

Передумовою нормативної регламентації поняття «персональні дані» (ПД) в законодавстві України стали міжнародні документи, які узагальнюють юридичне визначення поняття «ПД».

Згідно зі ст. 2 Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» під ПД розуміють «будь-яку інформацію, що стосується конкретно визначеної особи або особи, яка може бути

конкретно визначено (суб'єкт даних)».

В Україні вперше норми, що стосуються ПД, були введені Конституцією України. Ст. 32 визнає, що «ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, встановлених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Також, відповідно до ст. 10 ЗУ «Про звернення громадян» «не допускається розголошення одержаних із звернень відомостей про особисте життя громадян без їх згоди чи відомостей, що становлять державну або іншу таємницю, що охороняється законом, та іншої інформації, якщо це ущемляє права і законні інтереси громадян».

Конфіденційна інформація про особу, визначена Конституцією України, є одним з найважливіших елементів конституційно-правового статусу людини і громадянина, і становить особливий вид ІзОД.

Правовий інститут ПД в Україні можна представити у вигляді трьох складових.

Щодо *загальної частини* - першої складової правового інституту ПД, в ст. 11 ЗУ «Про інформацію» закріплено, що інформація про фізичну особу (персональні дані) - це «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Аналогічне визначення ПД закріплено й в ст. 2 ЗУ «Про захист персональних даних».

Отже, ПД - це будь-які відомості, що відносяться до фізичної особи, на підставі яких ця особа може бути ідентифікована.

В ч. 2 ст. 11 ЗУ «Про інформацію» перераховані відомості, що відносяться до конфіденційної інформації про фізичну особу, зокрема, «дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження».

Звідси видно, що законодавець не наводить вичерпного переліку відомостей, які можуть становити ПД фізичної особи.

На визначення вмісту інформації, що становить ПД, спрямовані й інші нормативно-правові акти, зокрема, органів судової влади. Аналіз їх матеріалів судової практики дає підстави віднести до ПД фізичної особи такі дані:

- інтимні сторони життя;
- захворювання;
- непорядні вчинки;

- злочинну діяльність;

- відомості, які ганьблять потерпілого і його близьких;

- майнове становище та ін.

Також при визначенні ПД законодавець не в повному обсязі врахував ряд положень розглянутого вище міжнародного нормативно- правового акту, згідно з якими ПД можна розділити на дві групи:

- *дані загального вмісту* - прізвище, ім'я, по батькові, дата і місце народження, освіта та ін.;

- *дані приватного змісту* - расове походження, політичні, релігійні та інші віросповідання, а також здоров'я або приватне життя.

При класифікації ПД слід приділити особливу увагу також біометричним (антропометричним) даним, даним про фізіологічні особливості людини, на основі яких можна його ідентифікувати (зріст, вага, колір волосся, група крові, голос, почерк, відбитки пальців, результати аналізу ДНК, цифровий образ особи, сітківка ока тощо). Саме біометрична ідентифікація може дати абсолютно точну картину ідентифікації громадянина за допомогою унікальних біологічних параметрів. Не існує двох людей з однаковими біометричними ознаками.

Потреба в надійній ідентифікації, досягнутий рівень біометрики, а також прагнення України до спрощення візового режиму з державами Європейського Союзу привели до прийняття Закону України «Про Єдиний державний демографічний реєстр і документах, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус».

Перелік біометричних даних особистості в ЗУ «Про захист персональних даних» відсутній, але дії по них, як правило, мають спеціальне правове регулювання, зокрема, такі дані мають особливий статус у сфері оперативно-процесуальної діяльності.

Сьогодні в нашій країні діє більше двох десятків законодавчих актів, що регулюють суспільні відносини, пов'язані з відомостями, що містять ПД. Серед них: Конституція України, Закони України «Про інформацію», «Про нотаріат», «Про електронні телекомунікації», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про Національну поліцію», «Про банки і банківську діяльність», «Основи законодавства про охорону здоров'я» та ін.

В ЗУ «Про захист персональних даних» наведено вичерпний список *суб'єктів* інформаційних відносин, пов'язаних з ПД:

- суб'єкт ПД - це фізична особа, ПД якого обробляються;

- володілець ПД - фізична або юридична особа, яка визначає мету обробки

ПД, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

- розпорядник ПД - фізична або юридична особа, якій володільцем ПД або законом надано право обробляти ПД від імені володільця;

- третя особа - будь-яке особа, за винятком суб'єкта ПД, володільця або розпорядника ПД і Уповноваженого Верховної Ради України по правам людини, якій володільцем або розпорядником ПД здійснює передачу ПД;

Уповноважений Верховної Ради з прав людини.

Володільцем чи розпорядником ПД можуть бути підприємства, установи і організації всіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи - підприємці, які обробляють ПД відповідно до закону.

Розпорядником ПД, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить сфері управління цього органу.

Володілець ПД може доручати обробку ПД розпоряднику, відповідно до договору, складеною в письмовій формі. Розпорядник може обробляти ПД тільки з метою і в обсязі, зазначених у договорі.

Уповноважений Верховної Ради з прав людини (омбудсмен) є посадовою особою, статус якого визначається Конституцією України (ст. 101), Законами України «Про Уповноваженого Верховної Радою з прав людини» та «Про державну службу», а також іншими законами України.

Уповноважений здійснює свою діяльність незалежно від інших державних органів та посадових осіб. Діяльність Уповноваженого доповнює існуючі засоби захисту конституційних прав і свобод людини і громадянина, не відміняє їх і не тягне перегляду компетенції державних органів, що забезпечують захист і відновлення порушених прав і свобод.

Повноваження Уповноваженого не можуть бути припинені чи обмежені у разі закінчення строку повноважень Верховної Ради України або її розпуску (саморозпуску), введення воєнного чи надзвичайного стану в Україні або в окремих її місцевостях. Місцезнаходженням Уповноваженого є столиця України - місто Київ. Для звернення до Уповноваженого можна використовувати й офіційний веб-сайт (http://ombudsman.gov.ua).

Ст. 55 Конституції України проголошено право будь-якого громадянина, звертатися до Уповноваженого з прав людини за захистом своїх прав.

Сфера компетенції українського омбудсмена є досить широкою. Оскільки в законі немає ні єдиного винятку щодо поширення юрисдикції Уповноваженого на конкретних посадових осіб, предметом його контролю є діяльність усіх посадових та службових осіб органів державної влади та органів місцевого самоврядування. Підпадає під юрисдикцію Уповноваженого і діяльність суддів. Але оскільки суди у своїй діяльності є незалежними і під час здійснення своїх функцій не можуть піддаватися ніякому впливу. У своїй діяльності вони підкоряються лише закону. Тому контрольні функції Уповноваженого щодо діяльності суддів стосуються не суті судових рішень, а пов'язані, зокрема, з порушенням термінів розгляду справ в судах, недотриманням процесуальних норм. Сфера компетенції Уповноваженого поширюється також на інших осіб, які в тому чи іншому обсязі виконують державно-владні функції.

В області захисту ПД Уповноважений має досить широке коло повноважень, визначене ст. 23 ЗУ «Про захист персональних даних».

Отже, основні функції омбудсмена полягають у здійсненні контролю над діяльністю виконавчих та інших органів державної влади на дії тих чи інших органів або посадових осіб, що призвели до порушення прав і свобод людини та громадянина. Законодавчо Уповноваженому надано достатньо ефективні засоби впливу на порушників законодавства про захист ПД, контролю діяльності суб'єктів, що здійснюють їх обробку, а також захисту прав суб'єктів відповідної інформації.

Особисті немайнові права на ПД, які належать кожній фізичній особі, є невід'ємними і непорушними. *Суб'єкт ПД має право:*

1) знати джерела збору, місцезнаходження своїх ПД, мета їх обробки, місцезнаходження або місце проживання (перебування) володільця або розпорядника ПД або дати відповідальне доручення для отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до ПД, зокрема, інформацію про третіх осіб, яким передаються його ПД;

3) на доступ до своїх ПД;

4) отримувати не пізніше як за тридцять календарних днів з дня отримання запиту, крім випадків, передбачених законодавством, відповідь на те, обробляються чи його ПД, а також отримувати вміст таких ПД;

5) пред'являти вмотивовану вимогу щодо зміни або знищення своїх ПД будь-яким володільцем і розпорядником, якщо ці дані обробляються незаконно чи є недостовірними;

6) пред’являти вмотивовану вимогу володільцю ПД із забороною проти обробки своїх ПД;

7) на захист своїх ПД від незаконної обробки та випадкової втрати, знищення, пошкодження у зв’язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

8) звертатися із скаргами на обробку своїх ПД до Уповноваженого, або до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист ПД;

10) вносити застереження стосовно обмеження права на обробку своїх ПД;

11) відкликати згоду на обробку ПД;

12) знати механізм автоматичної обробки ПД;

13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Також законодавчо встановлені і *об’єкти захисту,* щодо персоніфікованої інформації та випадки її обмеження:

1) об’єктами захисту є ПД.

2) ПД можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією ПД, які стосуються особи, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень.

3) ПД, зазначені в декларації про майно, доходи, витрати та зобов’язання фінансового характеру, оформленої за формою і в порядку, встановленим ЗУ «Про засади запобігання та протидії корупції», не належать до ІзОД, крім відомостей, визначених ЗУ «Про засади запобігання та протидії корупції».

Не відноситься до ІзОД інформація про отримання в будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених ст. 6 ЗУ «Про доступ до публічної інформації» (публічна ІзОД).

Законом може бути заборонено віднесення інших відомостей, що є ПД, до ІзОД.

10.2. Обробка персональних даних

Відповідно до *другої складової правового інституту ПД* (режиму ПД) визначимо наступне.

Головний зміст і призначення будь-якої інформаційної діяльності полягає в задоволенні політичних, економічних, фінансових, технологічних, культурних, інформаційних та інших потреб людини, суспільства і держави, в результаті здійснення певних дій. Дії з ПД припускають обробку даних в процесі їх збирання, реєстрації, накопичення, збереження і поширення.

Обробка даних - це будь-яка дія або сукупність дії, таких як збір, реєстрація, накопичення, збереження, адаптація, зміна, відновлення, використання та поширення (реалізація, передача), знеособлення, знищення ПД, у тому числі з використанням інформаційних (автоматичних) систем (ст. 2 ЗУ «Про захист персональних даних»).

Основні дії з ПД можна представити у вигляді схеми.

Кожна з дій несе змістовне і правове навантаження.

Збір ПД передбачає дії підбору та впорядкування відомостей про фізичну особу (ст. 12).

Реєстрація ПД - це фіксування ідентифікаційних реквізитів про фізичну особу з метою обліку та систематизації ПД.

Накопичення ПД передбачає дії об'єднання та систематизації відомостей про фізичну особу або групі фізичних осіб, або внесення цих даних до бази ПД (п. 1 ст. 13).

Переробка ПД - внесення змін і доповнень (модифікація) до даних.

Поширення ПД передбачає дії передачі відомостей про фізичну особу за згодою суб'єкта ПД (п. 1 ст. 14).

Доступ до ПД передбачає наявність у фізичних осіб права знати, які відомості, і з якою метою, ким збираються, реєструються, накопичуються, зберігаються і поширюються. Людина не може бути обмежена у праві доступу до своїх ПД.

Порядок доступу до ПД третіх осіб визначається умовами згоди суб'єкта ПД, наданих володільцю ПД на обробку цих даних, або відповідно до вимог закону. Порядок доступу третіх осіб до ПД, які знаходяться у володінні розпорядника публічної інформації, визначається ЗУ «Про доступ до публічної інформації».

Доступ до ПД третій не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог закону або не

може їх забезпечити.

Суб'єкт відносин, пов'язаних з ПД, подає запит щодо доступу до ПД володільцю ці даних.

У запиті зазначається:

- прізвище, ім'я та по батькові, місце проживання (місце знаходження) і реквізити документа, що посвідчує фізичну особу, яка подає запит;
- найменування, місцезнаходження юридичної особи, яка подає запит, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи;
- прізвище, ім'я та по батькові, а також інші відомості, що дозволяють ідентифікувати фізичну особу, про якого запитується;
- відомості про базу ПД, щодо якої подається запит, відомості про володільця чи розпорядника ПД;
- перелік запитуваних ПД;
- мета чи правові підстави для запиту.

Термін вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження. Протягом цього терміну володілець ПД доводить до відома особи, яка подає запит, що запит буде задоволено, або що відповідні ПД не підлягають наданню, із зазначенням підстави, визначеного у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом. Суб'єкт ПД має право на отримання будь-яких відомостей про себе у будь-якого суб'єкта відносин, крім випадків, встановлених законом.

Володіння ПД передбачає право використання та право на захист ПД.

Розпорядження ПД передбачає право визначати використання ПД.

Використання ПД містить в собі право на здійснення дій з ПД і право на захист своїх ПД, а також право на надання третій особі часткового або повного використання відомостей, що становлять ПД.

Збереження ПД передбачає створення умов належної цілісності та достовірності відомостей про особу.

Видалення або *знищення* ПД передбачено у випадках (ст. 15):

1) закінчився строк збереження даних, визначених згодою суб'єкта ПД на обробку цих даних або законом;
2) припинені правовідносини між суб'єктом ПД і володільцем або розпорядником, якщо інше не передбачено законом;

3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;

4) набрання законної сили рішенням суду з видалення або знищення ПД.

Законодавчо передбачено загальні та спеціальні вимоги до обробки ПД.

Згідно зі ст. 6 ЗУ «Про захист персональних даних» обробка ПД здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, який відповідає певним цілям такої обробки.

Обробка ПД здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта цих даних, або у випадках, передбачених законами України, та у порядку, встановленому законодавством.

Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Якщо обробка ПД необхідна для захисту життєво важливих інтересів суб'єкта ПД, обробляти дані без його згоди можна до часу, коли отримання згоди стане можливим.

ПД обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, в яких вони збиралися або подальшому оброблялися.

Згідно зі ст. 7 забороняється обробка ПД про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

На основі розглянутого можна виділити *основні права володільця* ПД. Володілець має право знати:

- хто і де обробляє його ПД;
- кому передаються його ПД;
- де зберігаються його ПД;
- як реалізувати право на доступ до своїх ПД;
- механізм обробка його ПД (у разі їх автоматичної обробки).

Крім того, до основних прав володільця відноситься і право вимагати знищення або виправлення ПД, якщо вони обробляються незаконно чи є недостовірними.

З цими правами пов'язані вісім основних принципів обробки ПД,

сформульованих у Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (ст. 5-8):

1) *принцип законності:* ПД повинні оброблятися сумлінно і законно, причому тільки при наявності підстав і з дотриманням вимог;

2) *принцип конкретності цілей:* ПД повинні виходити з конкретними законними цілями і не оброблятися способами, несумісні з цими цілями;

3) *принцип пропорційності:* ПД повинні бути адекватними, чи не надлишковими і відповідати цілям обробки;

4) *принцип якості даних.* ПД повинні бути точними та своєчасно оновлюватися;

5) *принцип обмеження терміну обробки:* ПД не повинні зберігатися довше, ніж це необхідно;

6) *принцип прозорості та опозиції:* ПД повинні оброблятися з дотриманням прав фізичної особи, включаючи право на доступ до даних і зауважень щодо їх обробки;

7) *принцип захисту даних:* ПД повинні оброблятися з дотриманням технічних вимог щодо захисту даних;

8) *принцип обмеження передачі іноземним суб'єктам:* ПД повинні не передаватися за межі країни без відповідного захисту.

Цих норм і принципів цілком вдавалося дотримуватися в «доцифрову» епоху, коли інформаційні обміни відбувалися безпосередньо у фізичному середовищі, з пристроїв і мереж, які можна було відносно легко ідентифікувати і відстежити (наприклад, телефон або радіо). Але технологічний прогрес і глобалізація значною мірою змінили те, як збираються ПД, як до них здійснюється доступ і яким чином вони використовуються (обробляються). Практично у всіх країнах найбільш проблемною сферою захисту ПД є сьогодні ІКТ та Інтернет, в якому традиційні нормативно-правові механізми та підходи до захисту ПД стають неефективними.

10.3. Організаційно-правові методи захисту персональних даних

Володільці, розпорядники ПД та треті особи зобов'язані забезпечити захист цих даних від випадкових втрат або знищення, від незаконної обробки, у тому числі незаконного знищення або доступу до персональних даних.

В органах державної влади, органах місцевого самоврядування, а також у володільця чи розпорядника ПД, які здійснюють обробку цих даних, що підлягають повідомленню відповідно до закону, створюється (визначається)

структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом ПД при їх обробці. Інформація про зазначений структурний підрозділ або про відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

Структурний підрозділ або відповідальна особа, організує роботу, пов'язану із захистом ПД при їх обробці:

- інформує та консультує володільця чи розпорядника ПД з питань дотримання законодавства про захист ПД;

- взаємодіє з Уповноваженим та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист ПД.

Фізичні особи - підприємці, в тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист ПД, якими вони володіють, згідно з вимогами закону.

Щодо *третій складової* правового інституту ПД визначимо, що чинним законодавством встановлена цивільна і кримінальна відповідальність за порушення встановлених вимог щодо захисту ПД.

Ст. 28 ЗУ «Про захист персональних даних» передбачає відповідальність встановлену законом, але в самому законі немає чіткої конкретизації відповідальності.

У 2011 р. був прийнятий ЗУ «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних», який доповнює КУпАП та ККУ.

Згідно зі ст. 188-39 КУпАП:

Неповідомлення або несвоєчасне повідомлення суб'єкта ПД про його права, у зв'язку з включенням його ПД в базу ПД, мету збору цих даних та осіб, яким ці дані передаються, - тягнуть за собою накладення штрафу на громадян від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб'єктів підприємницької діяльності - від трьохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян.

Неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту ПД про зміну відомостей, що подаються для державної реєстрації бази ПД, - тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб'єктів підприємницької діяльності - від двохсот до чотирьохсот неоподатковуваних

мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу на громадян від трьохсот до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб’єктів підприємницької діяльності - від чотирьохсот до семисот неоподатковуваних мінімумів доходів громадян.

Ухилення від державної реєстрації бази ПД - тягне за собою накладення штрафу на громадян від трьохсот до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб’єктів підприємницької діяльності - від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян.

Недодержання встановленого законодавством про захист ПД порядку захисту ПД в базі ПД, що призвело до незаконного доступу до них, - тягне за собою накладення штрафу від трьохсот до тисячі неоподатковуваних мінімумів доходів громадян.

Згідно зі ст. 188-40 невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту ПД щодо усунення порушень законодавства про захист ПД - тягне за собою накладення штрафу на посадових осіб, громадян- суб’єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян.

Згідно зі ст. 182 ККУ незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, - караються штрафом від п’ятисот до однієї тисячі 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.

Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п’яти років, або позбавленням волі на той самий строк.

Істотною шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, вважається шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Також ст. 163 ККУ встановлює кримінальну відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції,

що передаються засобами зв’язку або через комп’ютер.

Згідно з ЦКУ (ст. 22, 23, 277, 1166, 1167) фізична особа може звернутися до суду за захистом своїх прав, порушених у зв’язку з розголошенням ПД, має право на спростування недостовірної інформації та на відшкодування майнової та моральної шкоди

Лекція 11. ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ ТА СОЦІАЛЬНИХ МЕРЕЖАХ

Питання для опрацювання:

11.1. Захист права на недоторканність приватного життя споживача послуг у мережі Інтернет

12.2. Захист персональних даних в мережі Інтернет та соціальних мережах

Джерела:

1. Керівні принципи для захисту інтересів споживачів: Резолюція 39/248 Генеральної Асамблеї ООН від 09.04.1985 року. URL: https://ips.ligazakon.net/document/MU85305
2. Про захист недоторканності приватного життя в Інтернеті: Рекомендація №К(99)5 Комітету Міністрів держав-членів Ради Європи від 23.02.1999 року. URL: https://cedem.org.ua/library/rekomendatsiya-r-99-5-shhodo-zahystu-nedotorkannosti-pryvatnogo-zhyttya-v-interneti/

11.1.Захист права на недоторканність приватного життя споживача послуг у мережі інтернет

Стрімкий розвиток електронної комерції та повсюдна діджиталізація є безумовно прогресивним моментом еволюції людства. Водночас це спричиняє не тільки позитивні зміни в глобальній економіці, а й створює окремі загрози та виклики, які потребують оперативного реагування та вирішення. На сьогодні значний обсяг торгівлі здійснюється через мережу Інтернет, а тому одним із найбільш вразливих суб'єктів такої торгівлі, закономірно, є споживач.

У сучасному цифровому суспільстві споживачі можуть бути більш схильні до ризику під час здійснення покупок в Інтернеті. Використання кредитних та дебетових карток під час покупок, здійснених через Інтернет, призвело до збільшення кількості випадків, коли здійснюються збирання та обмін особистих даних споживачів постачальниками та посередниками. Особисті дані є цінними для онлайнових компаній, оскільки вони сприяють їхній розвідці ринку та полегшують індивідуальне споживче профілювання (Consumer protection in electronic commerce. URL: https://unctad.org/system/files/official-document/cicplpd7_en.pdf)/

Право на недоторканність приватного життя прямо передбачено

Конституцією України. Так, відповідно до ч. 1, 2 ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Водночас, згідно з п. 1 Рішення Конституційного Суду України № 2-рп/2012 від 20.01.2012 *«... положення частин першої, другої статті 32 ... Конституції України слід розуміти так:*

- інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім 'ї ... . Така інформація про особу є конфіденційною;

- збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя. Таке втручання допускається винятково у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Отже, як бачимо, інформація про особисте і сімейне життя особи є конфіденційною, а право на недоторканність приватного життя є одним із основоположних прав людини та може бути порушено виключно у чітко визначених законом випадках і за наявності конкретних умов. У будь-яких інших випадках таке право є непорушним, особливо, якщо воно стосується споживачів у процесі використання мережі Інтернет в правомірних цілях і з особистою метою.

У західній правовій доктрині для позначення правового інституту, яким охоплюється захист недоторканності приватного життя, використовується термін «прайвесі» (англ. privacy). Найбільш вдалим його перекладом українською мовою є слово приватність, яке співвідноситься зі словом приватний, що характеризує належність до приватної сфери життя людини.

Поява Інтернету змусила поглянути на питання захисту приватності під новим кутом. Фактично онлайнове середовище дозволяє з легкістю відстежити інформаційну активність користувачів. Крім того, доступність даних, розміщених в Інтернеті для практично необмеженого кола осіб, робить їх надзвичайно вразливими, ставлячи під сумнів існування мережевої приватності як такої.

Однією із найбільших сфер, де можуть бути порушені права споживачів на

недоторканність приватного життя, є електронна комерція. На підтвердження цього можна навести Резолюцію Генеральної Асамблеї ООН № 70/186 від 22 грудня 2015 року, де зазначено, що електронна комерція як така, до якої в якості її складової частини слід відносити і торгівлю з використанням мобільних пристроїв, стає все більш значущою для споживачів у всьому світі, і вважаючи, що можливостями, які відкриваються завдяки їй, слід скористатися для сприяння забезпеченню економічного розвитку і зростання на основі нових мережевих технологій, які передбачають залучення комп'ютерів, мобільних телефонів і інших мережевих пристроїв і сприяють підвищенню добробуту споживачів. Відтак стрімке зростання застосування електронної комерції, безумовно, є позитивним кроком у розвитку світової економіки, однак воно жодним чином не має призводити до порушення прав споживачів.

Щодо порушення права на недоторканність приватного життя споживачів варто розрізняти два види вторгнення в приватну інформацію. Один із них називається - крадіжка особистих даних, коли злодій отримує доступ до особистої інформації споживача, що дозволяє йому видати себе за інших споживачів і починає придбавати будь-які товари та послуги, що підлягають оплаті споживачем.

Інший тип вторгнення в приватне життя, на відміну від крадіжки особистих даних, - це поведінка законних компаній електронної комерції, які отримують доступ до інформації про купівельні звички споживачів. Наприклад, багато компаній просять своїх клієнтів зареєструватися в компанії через веб- сайти та надавати особисту інформацію. Однак деякі веб-сайти відмовляються надавати свої послуги тим, хто відмовляється від реєстрації, так само, як споживач, що реєструється, може помилково вважати, що інформація буде використовуватися компанією лише для поточної транзакції. Насправді, компанія може продати інформацію третім особам або використовувати її з будь-якою іншою метою. Компанії також можуть збирати інформацію і тоді, коли споживач відвідує веб-сайт за допомогою тегів кукі, електронного пристрою, що відстежує активність споживачів в Інтернеті. Орієнтуючись на таку діяльність, компанія може почати продавати цю інформацію третім особам, які можуть бути зацікавлені у розширенні свого ринку, шляхом визначення вподобань користувачів.

У наш час повсюдного електронного зв'язку та збільшення промислового тиску для стандартної електронної автентифікації збереження приватності («право бути залишеним у спокої» *(англ. right to be let alone))* стає предметом зростаючого занепокоєння. Характерна ознака «прозорої людини» *(англ.*

transparent human) виявляється найбільш очевидною в галузі електронної торгівлі частково через велику кількість наявних даних, частково через високу віддачу, що очікувана від використання цих даних з маркетинговою метою.

Разом із тим, коли користувачі Інтернету знають про масовий збір даних та спостереження, вони можуть самостійно цензурувати свою поведінку через страх перед несподіваними наслідками. Надмірний збір даних пізніше може мати стримуючий вплив на суспільство, звужуючи право людини на свободу слова та свободу вираження поглядів через цю можливу загрозу. Обмеження свободи слова та вираження може поставити під загрозу демократію і значно обмежити участь громадянського суспільства, зробивши нас «передбачуваними» в наших діях і думках.

У світлі самоцензури доречно навести Керівні принципи ООН для захисту інтересів споживачів, які передбачають, що критерії добросовісності ділової практики в сфері онлайнової і офлайновой роздрібної торгівлі визначаються, зокрема, принципом захисту особистої інформації. Так, відповідно до вказаного принципу *комерційним підприємствам слід захищати особисту інформацію споживачів за допомогою комплексного залучення механізмів забезпечення необхідного контролю, захищеності, прозорості та отримання дозволу в контексті збору та використання їх особистих даних*. Відтак, за загальним правилом і цілком закономірно, що не споживач повинен самостійно цензурувати свою поведінку, а саме компанії мають максимально докладати зусиль для збереження його персональних даних задля унеможливлення порушення його права на приватність. Тому порушення цього принципу має суворо каратися. Сьогодні існує низка документів на міжнародному та національному рівнях, що формують систему захисту права людини на приватне життя та містять відповідні принципи захисту персональної інформації. У цілому таке правове забезпечення має захистити права споживачів, зокрема в мережі Інтернет. Водночас онлайн компанії, як ми бачимо із засобів масової інформації, і надалі здійснюють незаконну обробку, зберігання чи поширення персональних даних споживачів, що свідчить про необхідність посилення їх відповідальності за такі правопорушення та недопущення вказаних порушень у майбутньому.

12.2. Захист персональних даних в мережі Інтернет та соціальних мережах

При роботі в мережі Інтернет користувач отримує масу корисної і не дуже інформації. Однак при цьому нерідко відомості про користувача і про його інформаційних потребах надходять до осіб, про існування яких він навіть не

здогадується. Це відбувається через те, що в мережі Інтернет на базі існуючих протоколів і стандартів при інформаційному обміні здійснюється збір інформації про користувача та про використовуване ним програмному забезпеченні, комп'ютерних даних і комп'ютерах.

Отримувані дані про користувача можуть однозначно його ідентифікувати (наприклад, містити вказані ним ім'я та прізвище, дату народження, місце проживання та ін.), а можуть й ідентифікувати апаратно-програмне забезпечення, за допомогою якого здійснюється доступ в мережу Інтернет.

Також при роботі в мережі Інтернет за допомогою клієнтського програмного забезпечення, призначеного для доступу до веб-сайтів, можливий збір відомостей про встановлене програмне забезпечення і режими роботи комп'ютера. Крім того, за IP-адресою можна визначити інформацію про місцезнаходження комп'ютера або обладнання Інтернет-провайдера (постачальника послуги доступу до мереж Інтернет). Все це створює реальні можливості для порушення інформаційних прав осіб, які отримують інформацію в мережі Інтернет.

Існує два підходи до вирішення даної проблеми: технічний та організаційно-правовий.

Технічний підхід полягає у створенні та розповсюдженні численних програмних і апаратних рішень в сфері інформаційної безпеки для комп'ютерних систем користувача і провайдера, а також у створенні спеціалізованих Інтернет-сервісів.

Організаційно-правовий підхід для захисту користувачів у мережі Інтернет, у тому числі і захист ПД, неможливо забезпечити і застосувати в рамках одного окремо взятого національного законодавства. Мережа Інтернет - транскордонна та має ознаки екстериторіального і загального доступу. У зв'язку з цим виникає велика кількість проблем, пов'язаних з юрисдикцією, контролем, обмеженням, захистом прав та інтересів громадян.

Ще в 1999 р. була розроблена Рекомендація №К(99)5 Комітету Міністрів держав-членів Ради Європи «Про захист недоторканності приватного життя в Інтернеті», яка містить основні принципи щодо захисту особистості щодо збору та обробки ПД:

- при роботі в мережі Інтернет користувачі повинні використовувати всі доступні засоби для захисту своїх даних і ліній зв'язку (наприклад, доступні засоби шифрування для конфіденційної електронної пошти або коди доступу до свого комп'ютера);

- при реєстрації на сайтах необхідно використовувати мінімум особистих даних;

- найкращий спосіб забезпечення безпеки особистості - це анонімний доступ і анонімне використання послуг, анонімні засоби здійснення платежів;

- надавати тільки ті дані, які необхідні для виконання певних дій, про які Ви проінформовані;

- адреса електронної пошти є інформацією персонального характеру, тому необхідно уточнювати про його використання;

- з обережністю ставиться до сайтів, на яких просять інформацію особистого характеру більшу, ніж це потрібно для доступу;

- постачальник послуг Інтернет несе відповідальність за правильне використання ПД та ін.

Однак сьогодні при використанні мережі Інтернет відбувається масове порушення чинного законодавства у сфері захисту ПД. Причому часто витіки ПД з Інтернет-ресурсів пов'язані не з діями віртуальних зловмисників, а зі слабким рівнем захисту інформації. Причиною потрапляння ПД користувача мережі Інтернет в «треті руки» можуть бути дії співробітників Інтернет-компаній, що обробляють ці дані. У той же час, користувачі також зобов'язані самі піклується про захист своєї інформації, в тому числі уважно читати умови ліцензійних і користувальницьких угод.

Так звані «дрібні крадіжки» ПД в мережі відбуваються постійно, найпоширеніші - злом паролів для входу в соціальну мережу або електронну пошту, для того щоб розіслати спам по всім доступним контактам. Але крім цього, інформація про людину та її діях в мережі не тільки записується, а й передається «третім особам», причому без втручання користувача. Наприклад, популярна система електронної пошти Gmail «читає» переписку своїх користувачів - веде аналіз текстів листів за допомогою спеціальних автоматизованих систем, що визначають звідти ключові слова і використовують ці дані для тематики рекламних показів.

Без електронної пошти сьогодні неможливо уявити роботу будь- якого офісу підприємства, організації, органу влади або місцевого самоврядування. Але й тут виникає проблема захисту конфіденційної інформації. У підписах електронних листів містяться відомості про їх кореспондентів - прізвища, імена, по батькові, назви посад, номера телефонів, адреси електронної пошти, це як мінімум. Виникає питання: «Як застосовувати в даному випадку ЗУ «Про захист персональних даних»? Відповіді на нього немає ні в нормативно-правових актах,

ні в методичних рекомендаціях.

Ще один аспект використання ПД в мережі Інтернет - електронна комерція. Здійснюючи покупки в Інтернет-магазинах, покупець надає свої ПД (прізвище, ім'я, номер телефону, домашню адресу для доставки та ін.). І тут виникає ряд питань: Як власник магазину може довести згоду на обробку ПД покупця? Пославшись на те, що той сам заповнив необхідні поля при покупці товару й тим самим висловив непряму згоду на їх обробку? А якщо це ПД не покупця, а іншої людини, які покупець вважав за потрібне використовувати при оформленні замовлення, а ця третя особа не тільки не давало згоди, а й знати не знає про використання його ПД? Чому відповідальність за це повинен нести магазин? Цілком може бути, що відомості, зазначені при замовленні, взагалі не є чиїмись ПД, а вигадані.

При покупці авіаквитків, пасажир цілком може вказати не тільки свої ПД, але відомості про інших осіб, для яких купуються квитки. Дотримуючись вимог закону, перевізник повинен підтвердити згоди на обробку ПД всіх пасажирів, які купили квитки через Інтернет. А в разі, якщо дані представлялися не самим пасажиром, а третьою особою, негайно повідомити такого пасажира про початок опрацювання відомостей про нього, вказавши в повідомленні обов'язкові реквізити, передбачені законом. На практиці такого порядку майже не дотримуються. Але в даному випадку до авіакомпанії можна пред'явити претензії, а до її посадових осіб - застосувати санкції.

Інтернет-рекрутинг теж викликає безліч питань про захист ПД, розміщених на сайтах пошуку роботи. Використання Інтернет-сайтів для пошуку роботи чи кандидатів на заміщення вакантних посад стало сьогодні дуже поширеним. Для цього треба зайти на сайт, авторизуватись і заповнити форму з резюме, тобто вказати свої ПД. Тут знову ж виникає проблема, власники сайт повинні представити згоду суб'єкта на обробку його ПД, а інакше робота цих сайтів стає поза законом.

Соціальні мережі зайняли важливе місце в житті практично кожного користувача Інтернет. Мети їх використання різні - спілкування, вчинення правочинів, розповсюдження реклами, розміщення інформації та ін. Не дивлячись на позитивну сторону розширення соціальних мереж, існують і певні недоліки: поки одні отримують користь від спілкування в соціальній мережі, інші використовують їх для різного роду шахрайства, пропаганди насильства та екстремізму, вчинення злочинів. Практично кожна соціальна мережа виступає оператором ПД, який обробляє персональну інформацію користувачів даної

мережі.

Користувачі соціальних мереж, добровільно розміщуючи інформацію, що містить ПД (прізвище, ім'я, стать, дату народження, освіту, номера телефону) розміщуючи фотографії, що дозволяють зробити ідентифікацію суб'єкта, не замислюються про шкоду, яка може бути їм заподіяна. ПД, завантажені в соціальну мережу, поширюються в мережі Інтернет, і їх практично неможливо видалити.

Розглядаючи розміщення персональної інформації в соціальній мережі, можна говорити про двоїстий характер її доступності. З одного боку, інформація користувача соціальної мережі схована від третіх осіб і є недоступною для пошукових систем, а з іншого боку - відкрита. Відкритість персональної інформації дозволяє сформувати досьє на кожного зареєстрованого користувача соціальної мережі, не порушуючи при цьому положень законодавства. Ще одним недоліком розміщення персональної інформації в соціальних мережах є вільний перегляд третіми особами відкритих даних і можливість їх копіювання. На розсуд користувача доступ до даних, що становить персональний характер, може обмежуватися, якщо ця можливість передбачається оператором соціальної мережі.

Сучасному суспільству, яке активно користується послугами соціальних мереж, повинно бути відоме таке поняття, як фішинг - Інтернет-шахрайство з метою крадіжки ПД. Існують різні форми витоку інформації, наслідками яких є загроза зміни, копіювання, блокування, поширення, знищення ПД та інші несанкціоновані дії, які можуть завдати непоправної шкоди, як суб'єкту ПД, так і репутації організації-роботодавця та ін. Хоча адміністратори сайтів й використовують технології для забезпечення захисту від вірусів та іншого шкідливого програмного забезпечення, ці методи захисту не зможуть убезпечити від пасивного збору інформації про користувачів. В цілях власної безпеки користувачі соціальних мереж в першу чергу повинні самостійно контролювати питання безпеки їх ПД у відкритих ресурсах. Для запобігання фішинг-атак використовувати програми-файрволи, міжмережеві екрани і антивірусне програмне забезпечення.

Дослідження проблеми безпеки користувачів соціальних мереж на прикладі популярної мережі Facebook, показало, що дана соціальна мережа не несе відповідальності за збереження, поширення ПД і їх безпечне використання, що зазначено в угоді з користувачем. І відповідно, дія ЗУ «Про захист персональних даних» на неї не поширюється.

Для захисту своїх ПД в соціальних мережах необхідно дотримуватися таких правил. При роботі в соціальних мережах необхідно ознайомиться з політикою конфіденційності, і налаштувати параметри для захисту своїх даних. Також в політиці конфіденційності можна дізнатися рівень безпеки: яку інформацію, і яким чином збирає сайт, хто має доступ до цієї інформації, які заходи щодо забезпечення інформації реалізовані, як довго зберігається інформація, і як можна зв'язатися з адміністрацією сайту у випадку порушення конфіденційності. Якщо при реєстрації в соціальній мережі запитують занадто багато ПД, можливо, краще від неї відмовитися. Також треба пам'ятати про те, що вся інформація, розміщена в соціальних мережах, залишається в мережі, тому публікувати можна тільки такі повідомлення та фотографії, які не можуть скомпрометувати людину.

Лекція 12. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Питання для опрацювання:

12.1. Концептуальна модель інформаційної безпеки

12.2. Поняття та види інформаційної безпеки

Джерела:

1. Про захист інформації в інформаційно-комунікаційних системах: ЗУ від 05.07.1994 року № 80/94-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
2. Про національну безпеку України: ЗУ від 21.06.2018 року № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Про основні засади забезпечення кібербезпеки України: ЗУ від 05.10.2017 року № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
4. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: ЗУ від 09.01.2007 року №537-V / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/537-16#n71
5. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": указ ПУ від 14.09.2020 року № 392/2020 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n12
6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"": указ ПУ від 26.08.2021 року № 447/2021 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": указ ПУ від 28.12.2021 року № 685/2021 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

12.1. Концептуальна модель інформаційної безпеки

Одним із чинників, що значно ускладнює забезпечення ІБ є постійне протистояння фахівців в області інформаційної безпеки з одного боку, і зловмисників - з іншого.

Зважаючи на необхідність вирішення проблем, що виникають в ході згаданого протистояння, доцільно системно дослідити об’єкти та процеси, ІБ яких необхідно забезпечити, сформувавши умовну концептуальну модель інформаційної безпеки.

Розглядаючи ІБ як стан захищеності інформаційного середовища, в моделі на основі системного підходу доцільно визначити загрози безпеки інформації, джерела цих загроз, способи і цілі їх реалізації.

При цьому слід розглядати і засоби захисту інформації від неправомірних дій, що призводять до нанесення збитку, в контексті їх протиставлення можливим загрозам.

Концептуальна модель інформаційної безпеки складається з наступних елементів: об’єкти захисту; моделі загроз і порушників; джерела інформації; система захисту інформації тощо (рис. 12.1).

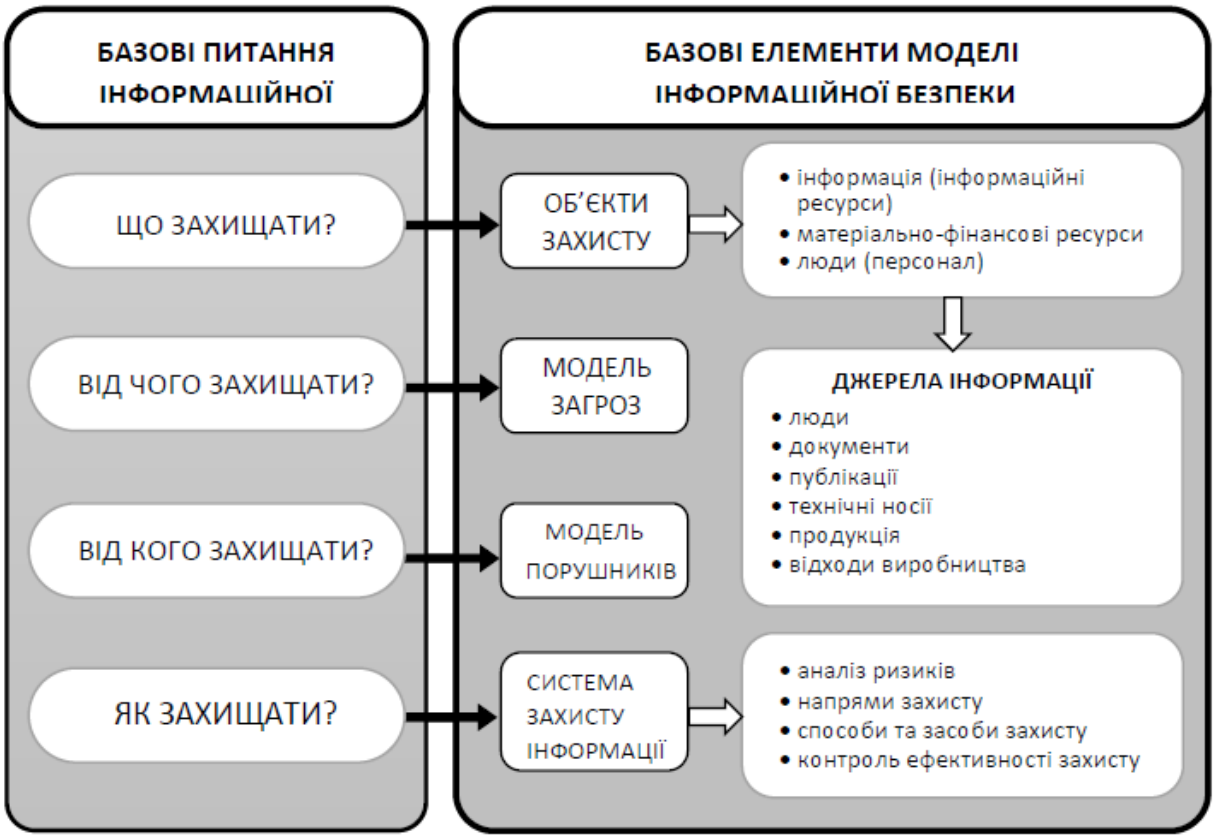

Рис. 12.1. Концептуальна модель інформаційної безпеки

Основним об’єктом захисту є інформаційна система, яка реалізує автоматизований збір і обробку даних, та включає в себе: інформацію (інформаційні ресурси), матеріально-фінансові ресурси і людей (персонал), які мають санкціонований доступ до цих ресурсів.

Слід звернути увагу на нерозривність інформації та певного матеріального

носія. Вираз «отримати доступ до інформації» можна розуміти як отримання доступу саме до певного носія. Відтак, в процесі захисту інформації (даних) необхідно враховувати її місцезнаходження, як наслідок - і стан, в якому вона знаходиться (знаки або сигнали) (рис. 12.2).

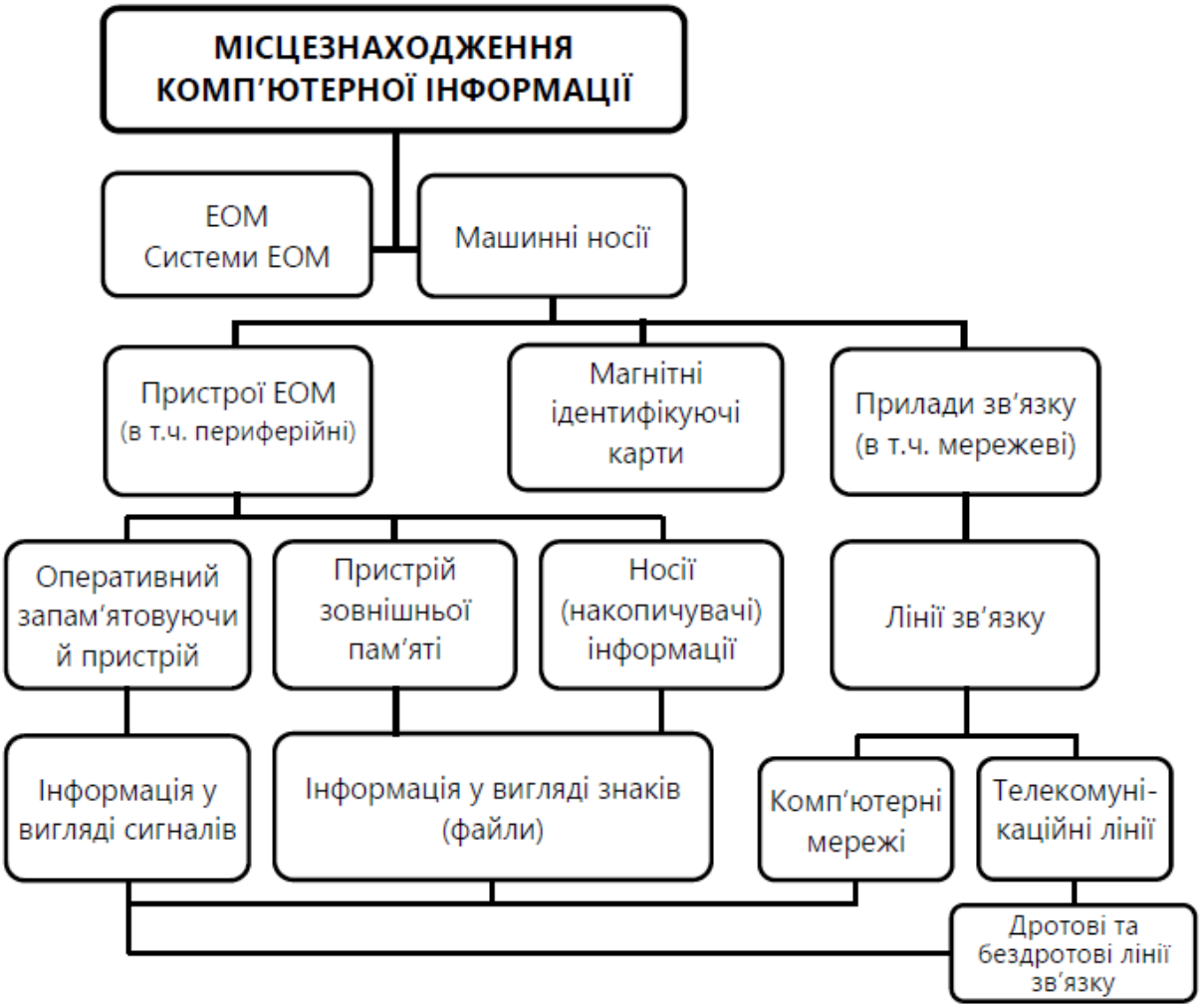

Рис. 12.2. Місцезнаходження «комп'ютерної інформації»

Носій інформації - фізична особа або матеріальний об'єкт, в тому числі фізичне поле, в якому інформація знаходить своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів, кількісних характеристик фізичних величин.

Всі носії інформації умовно можна розділити на дві групи.

Перша група - це безпосередні (первинні) носії інформації. Вони є такими за своєю природою, наприклад: людина (фізична особа), військові об'єкти, або спеціально створені для цілей зберігання інформації або передачі інформації за допомогою носія. Такі носії водночас можна вважати джерелами інформації.

Друга група - опосередковані (вторинні) носії інформації. Такими носіями,

є засоби та системи, що використовуються для обробки інформації (оперативна пам'ять ПК, принтери, сканери тощо), подання (монітори, екрани та ін.), передачі по мережі (комп'ютерні та телекомунікаційні лінії зв'язку) тощо. Опосередкованими носіями також є випромінювання та електромагнітні поля що виникають під час роботи технічних засобів обробки інформації або передачі. В опосередкованих носіях інформація не зберігається (рис. 12.3).

Рис. 12.3. Класифікація носіїв інформації, що захищаються

Загроза безпеки інформації є одним з найважливіших елементів концептуальної моделі ІБ. Загроза безпеки - це сукупність умов, чинників, що створюють небезпеку життєве важливим інтересам особистості, суспільства і держави.

Інформаційні загрози (або загрози інформації) - це події або явища, внаслідок дії яких може відбутися негативний вплив на інформацію: її витік, знищення (руйнування), спотворення (модифікація), блокування доступу до неї санкціонованих користувачів тощо.

Джерелами загроз можуть бути іноземні держави, окремі юридичні або

фізичні особи, криміналітет, природні (стихійні лиха та катастрофи) або технічні (стрибки електроживлення, відмова апаратури та ін.) дестабілізуючі чинники.

При відповіді на запитання «від чого захищати?» створюється модель загроз - формалізований або неформалізований опис (перелік) всіх потенційних загроз інформації та їх можливих джерел; уразливих елементів об'єкта захисту, на які вони спрямовані; шляхів (способів) і ймовірності здійснення загроз; рівнів потенційних збитків (матеріальних та моральних) у разі здійснення загроз та ін.

За природою походження загрози можуть бути природними і штучними.

Природні (об'єктивні) - це загрози, викликані діями або наслідками стихійних природних явищ, незалежних від людини (форс- мажорні обставини).

Штучні (суб'єктивні) - це загрози, викликані діяльністю людини.

За мотивацією дій поділяються на *навмисні (зловмисні)* та *ненавмисні (випадкові)* загрози.

За способами реалізації загрози можуть здійснюватися:

- технічними каналами, включаючи канали побічних електромагнітних випромінювань, акустичні, оптичні, радіо і радіотехнічні, хімічні та ін.;

- каналами спеціального впливу за рахунок формування спеціальних полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкціонованим доступом в результаті підключення до апаратури по лініях зв'язку, маскування під зареєстрованих (законних) користувачів, подолання системи захисту для отримання (використання) інформації або нав'язування хибної, вживання заставних пристроїв і вбудованих програм та використання комп'ютерних вірусів.

Носіями загроз безпеки інформації є джерела загроз**,** які можуть знаходитися як всередині організації (внутрішні загрози), так і ззовні - зовнішні загрози. Всі джерела загроз умовно можна розділити на три групи, які обумовлені:

- діями суб'єктів (антропогенні джерела загроз - кримінальні структури, хакери, недобросовісні партнери, представники силових структур, програмісти, розробники, охорона та ін.);

- технічними засобами (техногенні джерела загроз - засоби зв'язку, мережі інженерних комунікацій, транспорт, сигналізації, телефони, програмні та технічні засоби обробки інформації);

- стихійними джерелами (пожежами, землетруси, повені, урагани, різні непередбачувані обставини та ін.).

В результаті відповіді на питання «від кого захищати?» створюється модель порушників - формалізований або неформалізований опис всіх потенційних зловмисників, які можуть створювати певні загрози для інформації, що захищається. При розробці цього елемента, як правило, враховуються відомості про категорії (статусу) порушників, можливого рівня їх кваліфікації та технічного оснащення, цілей, мотивів і характеру їх впливу на захищається інформацію та ін.

Як і джерела загроз, порушники можуть бути як внутрішніми (так звані «інсайдери»), так і зовнішніми (діяти поза об'єктом захисту). Сучасна статистика загроз ІБ свідчить, що саме інсайдери найбільш часто (близько 80% всіх загроз) реалізують спробу несанкціонованого доступу до інформації.

У науковій літературі виділяють чотири типи порушників за рівнем можливостей, що надаються штатними засобами інформаційних систем.

Перший рівень визначає низькі можливості ведення діалогу в інформаційній системі - запуск задач (програм) з фіксованого набору, що реалізують заздалегідь передбачені функції з обробки інформації.

Другий рівень визначається можливістю створення і запуску власних програм з новими функціями з обробки інформації.

Третій рівень визначається можливістю управління функціонуванням інформаційних систем.

Четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт елементів і системи в цілому, аж до включення до її складу власних технічних засобів з новими функціями.

Переоцінка можливостей порушників призведе до невиправданого збільшення витрат на побудову системи захисту інформації. І навпаки, недооцінка можливостей порушників збільшить ймовірність загроз і збитку від їх реалізації.

Аналіз вищевказаних моделей дозволяє відповісти на питання «як захищати?», тобто побудувати ефективну систему захисту інформації (СЗІ), яка повинна адекватно відповідати можливим ризикам для всіх або для найбільш небезпечних загроз.

У загальному випадку СЗІ можна визначити як організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

Аналіз ризиків - це взаємопов'язаний процес визначення загроз безпеці інформації, уразливих елементів об'єкта захисту, оцінки потенційних збитків від

реалізації конкретних загроз і визначення комплексу контрзаходів, що забезпечують достатній рівень захищеності інформації.

Мета мінімізації ризику при побудові СЗІ полягає в тому, щоб застосувати ефективні заходи (засоби) захисту так, щоб залишковий ризик безпеки інформації став прийнятним. При оцінці ризиків враховуються багато факторів: цінність ресурсів, значимість загроз, уразливість об'єкта захисту, ефективність існуючих і передбачуваних засобів захисту, їх вартість тощо.

Як правило, СЗІ комплексно поєднує всі відомі напрямки захисту**:** правовий, організаційний, інженерно-технічний і використовує відповідні способи та засоби захисту, засновані на різних фізичних принципах і механізмах безпеки.

Заключним етапом у побудові СЗІ є організація контролю ефективності захисту. З точки зору безпосередньої організації контролю на об'єкті захисту необхідно поєднати два його варіанти:

- контроль стану параметрів засобів захисту, основних і допоміжних технічних засобів передачі інформації, які безпосередньо впливають на якість стану захищеності інформації;
- контроль всіх проявів типових порушень політики і правил безпеки інформації на об'єкті захисту.

На підставі зазначених елементів концептуальної моделі інформаційної безпеки (рис. 12.1) будується захист конкретного об'єкта від можливих зовнішніх і внутрішніх загроз.

12.2. Поняття та види інформаційної безпеки

Інформаційну безпеку можна розглядати у двох аспектах: широкому та вузькому. У широкому аспекті інформаційна безпека це сукупність правових актів, уповноважених ними органів, організації та практики діяльності останніх, поєднання яких породжує механізм забезпечення та захисту інформаційних прав та інтересів людини, соціальних груп, інститутів громадянського суспільства, суб'єктів господарських відносин, органів публічної влади та військових формувань. У вузькому аспекті інформаційна безпека – це стан максимальної захищеності людини, суспільства і держави від інформаційних загроз.

У широкому аспекті інформаційна безпека може бути класифікована за:

а) джерелом походження повноважень щодо здійснення заходів із

забезпечення інформаційної безпеки (Конституція України, закони України, підзаконні правові акти);

б) видами суб'єктів, які забезпечують інформаційну безпеку (людина і громадянин, інститути громадянського суспільства, органи державної влади, органи місцевого самоврядування, військові формування, підприємства, установи та організації всіх форм власності);

в) ступенем обов'язковості здійснення заходів із забезпечення інформаційної безпеки:

- основна (для спеціально уповноважених органів публічної влади та військових формувань);

- факультативна (для інших органів публічної влади);

- делегована (для підприємств, установ та організацій, яким повноваження щодо здійснення заходів інформаційної безпеки делеговано відповідними правовими актами;

- необов'язкова (для громадян і суб'єктів громадянського суспільства).

У вузькому аспекті інформаційна безпека включає такі види:

а) за критерієм суб'єктів, охоплених заходами інформаційної безпеки (інформаційна безпека людини, корпорацій, громадянського суспільства і держави);

б) за критерієм інформаційних загроз (політична інформаційна безпека, воєнна інформаційна безпека, економічна інформаційна безпека, екологічна інформаційна безпека тощо);

в) за критерієм досягнутих результатів (досконала і недосконала інформаційна безпека).

Стратегія інформаційної безпеки, затверджена указом Президента України від 28.12.2021 року № 685/2021 дає таке визначення: *інформаційна безпека України* - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації,

деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Це визначення багато в чому ґрунтується на нормі закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», відповідно до якого *інформаційна безпека* визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

При цьому вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Інформаційну безпеку організації можна визначити як цілеспрямовану діяльність її органів та посадових осіб із використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища організації, що забезпечує нормальне функціонування та динамічний розвиток.

Інформаційна безпеки фізичної особи характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати

психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору. Значний вплив на правове регулювання суспільних відносин у сфері інформаційної безпеки має законодавство про національну безпеку.

Система забезпечення інформаційної безпеки України створюється і розвивається відповідно до Конституції України, інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері.

Основу цієї системи становлять органи, сили та засоби забезпечення інформаційної безпеки, які застосовують систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Нормативно-правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України утворюють: Конституція України, закони України: «Про національну безпеку України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про електронні комунікації», «Про критичну інфраструктуру», Стратегія національної безпеки України, Стратегія інформаційної безпеки України та Стратегія кібербезпеки України, інші нормативно-правові акти, що регулюють суспільні відносини в інформаційній сфері.

Відповідно до мети і завдань, доцільно визначити функції системи забезпечення інформаційної безпеки України.

Під функціями системи забезпечення інформаційної безпеки прийнято розуміти здійснення суб’єктами системи забезпечення інформаційної безпеки України діяльності зі створення умов для оптимального управління системою інформаційної безпеки.

Структура системи інформаційної безпеки охоплює два рівні управління:

- стратегічний рівень управління інформаційною безпекою - Рада національної безпеки і оборони України та Кабінет Міністрів України;
- тактичний рівень управління - центральні органи виконавчої влади.

Лекція 13. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БЕЗПЕКИ

13.1. Співвідношення понять інформаційної та кібербезпеки
13.2. Основні положення Стратегії кібербезпеки України
13.3. Повноваження органів сектору безпеки України щодо протидії кіберзлочинності та дезінформації

Джерела:

1. Огляд подій у сучасному кіберпросторі за II квартал 2021 року. URL: https://www.rnbo.gov.ua/files/НКЦК/28072021/Bulltn_NCK_2.pdf
2. Положення про Центр протидії дезінформації, затверджене Указом Президента України від 07.05.2021 року № 187/2021 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text
3. Про кіберзлочинність: конвенція Ради Європи від 23.11.2001 року / Рада Європи. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
4. Про національну безпеку України: ЗУ від 21.06.2018 року № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. Про основні засади забезпечення кібербезпеки України: ЗУ від 05.10.2017 року № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Про розвідку: ЗУ від 17.09.2020 року № 912-IX / Верховна Рада України. URL https://zakon.rada.gov.ua/laws/show/912-20#Text
7. Про Службу безпеки України: ЗУ від 25.03.1992 року № 2229-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text
8. Про Стратегію кібербезпеки України: рішення Ради національної безпеки і оборони України від 14.05.2021 року, введене в дію Указом Президента України від 26.08.2021 року № 447/2021 / Президент України. URL: https://www.president.gov.ua/documents/4472021-40013

13.1. Співвідношення понять інформаційної та кібербезпеки

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення призвело, зрештою, до формування кіберпростору (рис. 13.1) - високорозвиненої моделі об'єктивної реальності, в

якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

- подаються в деякому математичному, символьному (як сигнали, знаки, звуки, рухомі або нерухомі зображення) або в будь-якому іншому вигляді;
- розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації;
- перебувають у постійному русі по сукупності ІТ-систем і мереж.

Уперше термін «кіберпростір» було використано в Конвенції про злочинність у сфері комп'ютерної інформації від 23 листопада 2001 року. Сфера його дії на той час перебувала під впливом загальних механізмів правового регулювання суспільних відносин, обмежуючись специфічними об'єктами й інтересами суб'єктів правовідносин, а також комп'ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах.

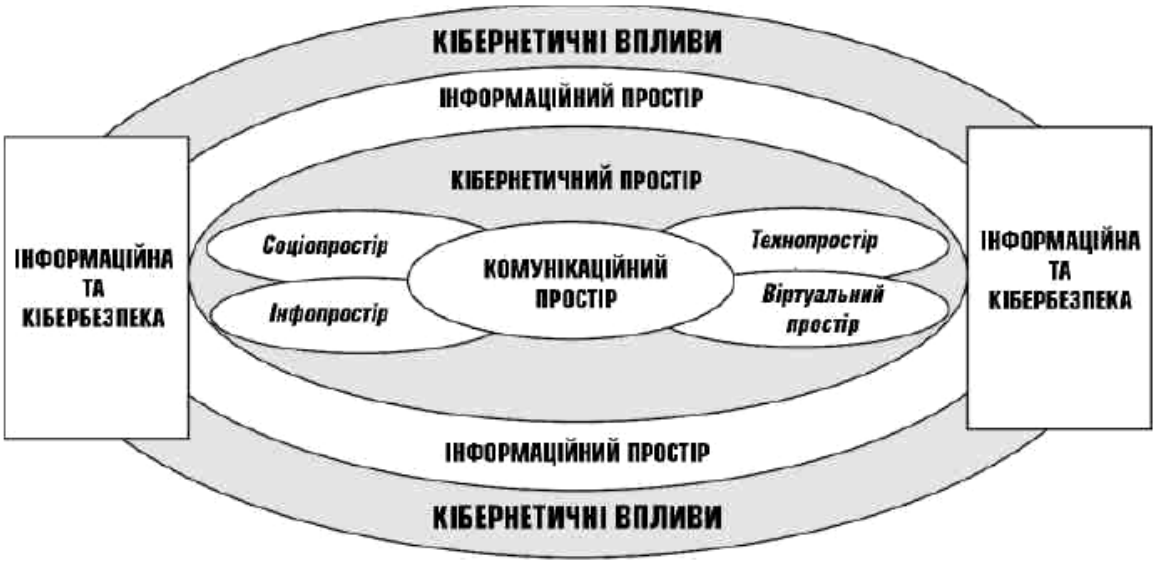

Рис. 13.1. Взаємозв'язок інформаційного та кіберпросторів

Нині кіберпростір має чимало визначень. Серед інших варто також відзначити й такі визначення поняття кіберпростору:

- поліморфний віртуальний простір, що генерує інформаційна система як у формі складних світів, так і у простих реалізаціях (типу електронної пошти, глобальної навігації толю);
- комунікаційне середовище, утворене системою зв'язків між об'єктами кіберінфраструвлури - комп'ютерами, комп'ютерними мережами, програмним забезпеченням та інформаційними ресурсами, використовуване для забезпечення певних інформаційних потреб;
- штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних

комп'ютерних систем управління й обробки інформації, що забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, а також обмін електронними повідомленнями даючи змогу із застосуванням електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо);

- простір, сформований інформаційно-комунікаційними системами, в якому відбуваються процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, поданої у вигляді електронних комп'ютерних даних;

- об'єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює;

- середовище, утворене організованого сукупністю інформаційних процесів на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Найбільш помітними ознаками кіберпростору як субстанції, створенню якої сприяли передусім такі чинники: зміна характеру діяльності людини з ухвалення рішень; упровадження електронно-цифрових форм створення, обробки, зберігання та переміщення інформації, перехід від паперового діловодства до електронного тощо; абсолютна більшість фахівців вважає його неперевершені можливості зі створення незліченних зв'язків між окремими індивідами і соціальними групами та з надання різнопланових інформаційних послуг.

З урахуванням характерних особливостей кіберпростору їх сфери вчиненні заздалегідь спланованих деструктивних дій на кшталт проникнення в ІТС один одного, блокування або виведення з лазу найбільш уразливих елементів цих систем, дезорганізації оборонних автоматизованих систем управління протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із наземною, морською й повітряно-космічною сферами) і своєрідної сполучної ланки між такими поняттями, як Інтернет і кібернетика, усе це. у свою чергу, дає змогу:

- виокремити в цьому просторі систему певних відношень між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури;

- охарактеризувати злочини, втручання і загрози, пов'язані з

особливостями існування та передавання інформації:

- розглядати кіберпростір із позицій власне віртуального і реального (електронного, комунікаційного, кібернетичного, інформаційного, особливого психологічного) тлумачення як додатковий вимір бойового простору, розрізняючи при цьому фізичний (інфраструктура, кабелі та роутери), семантичний (дані) і синтаксичний (протоколи передавання даних) рівні тощо.

Сучасний стан справ зумовлює небачені досі глибинні зміни у ставленні більшості держав світу до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її обробки та кіберсередовища, в якому ця інформація циркулює *(рис. 13.2)*, тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки.

Рис. 13.2. Об'єкти впливу в інформаційному та кіберпросторі

При цьому інформаційну безпеку в найзагальнішому розумінні можна визначити як такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, *і* який гарантує безперешкодне використання й розвиток національної інфосфери в інтересах оборони *(рис. 13.3)*.

Рис 13.3. Структура поняття «інформаційна безпека»

Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об'єктів безпеки можна поділиш на такі основні категорії: *доступність* -

можливість за прийнятний час отримати певну інформаційну послугу; цілісність - актуальність і несуперечливість інформації, а захищеність від руйнування та несанкціонованого змінювання: конфіденційність - захищеність від несанкціонованого ознайомлення.

13.2. Основні положення Стратегії кібербезпеки України

У Законі України «Про основні засади забезпечення кібербезпеки України» сформульовано визначення поняття «кібербезпека».

Кібербезпека - це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Цифровізація життєтворчих галузей діяльності та розвиток бездротових, сенсорних та хмарних технологій, мереж з динамічною топологією призвели до появи кіберфізичних систем, що автономно від людини реалізують фізичні процеси за допомогою обміну даними один із одним. Кіберфізична система є замкненою системою, що реалізує деяку цільову функцію (наприклад, функцію автоматичного очищення води, що реалізується в кілька взаємопов'язаних етапів). Наявність цільової функції системи засвідчує періодичність процесів, що протікають у ній, - у сукупності та окремо.

Успішна реалізація деструктивних впливів, спрямованих на порушення інформаційної безпеки на кіберфізичних систем, які тісно інтегровані з різними галузями діяльності, здатна призвести не лише до фінансових збитків, а й до техногенних та екологічних катастроф.

Більшість атак на промислові об'єкти інфраструктури, як доводить статистика, неухильно зростає, що разом із критичністю порушення коректності функціонування кіберфізичних систем демонструє

необхідність ужиття заходів захисту.

Щодо кіберфізичних систем, то поняття інформаційної безпеки трансформується, поєднуючи з традиційними поняттями цілісності, конфіденційності та доступності необхідність підтримання коректного функціонування системи в умовах деструктивних впливів.

Оскільки пряме перенесення понять інформаційної безпеки у вигляді конфіденційності, доступності та цілісності в кіберфізичних системах неможливе через те, що, на відміну від інформаційних процесів, фізичні процеси незворотні і для них неможливо реалізувати такий самий рівень контролю та управління, пропонується знайти вирішення завдання із забезпечення стійкості кіберфізичних систем до деструктивних дій.

Сучасні наукові підходи та популярні практичні рішення у сфері забезпечення інформаційної безпеки кіберфізичних систем не пропонують способи вирішення деяких науково- технічних завдань. До таких завдань належать:

- розробка методу виявлення порушень інформаційної безпеки кіберфізичних систем, спрямованих на зміну параметрів функціонування;
- створення методів виявлення шкідливого програмного забезпечення, що функціонує на вузлах системи управління кіберфізичних систем;
- розробка підходу забезпечення динамічного захисту кіберфізичних систем шляхом автоматичної підтримки стійкості функціонування за умов комп’ютерних атак;
- реалізація динамічного захисту з використанням можливостей сучасних мережевих технологій.

Сучасні загрози безпеці вимагають вирішення наведених завдань, що регламентовано у Стратегії кібербезпеки України.

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету здійснюватиметься шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави.

Для подальшої розбудови національної системи кібербезпеки на

засадах стримування, кіберстійкості, взаємодії необхідним є:

- посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кібер- злочинності та кібертероризму (стримування);

- набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість);

- забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами-членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія).

Україна, крім основних суб'єктів національної системи кібербезпеки, залучить до вирішення завдань у цій сфері більш широке коло учасників, зокрема суб'єктів господарювання, громадські об'єднання та окремих громадян України.

Ключову об'єднувальну та координаційну роль у цьому процесі виконуватиме Національний координаційний центр кібербезпеки.

Пріоритетами забезпечення кібербезпеки України є:

- убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

- захист прав, свобод і законних інтересів громадян України у кіберпросторі;

- європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї Стратегії.

Для формування потенціалу стримування (С) необхідним є досягнення таких стратегічних цілей:

ціль С.1. Дієва кібероборона - Україна створить і забезпечить розвиток (зокрема кадрово та технологічно) підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформує належну правову,

організаційну, технологічну моделі їх функціонування та застосування, забезпечить ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів із кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності;

ціль С.2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму - Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян;

ціль С.3. Ефективна протидія кіберзлочинності - Україна забезпечить набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів і розслідування кіберзлочинів;

ціль С.4. Розвиток асиметричних інструментів стримування - Україна створить необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, залучення потенціалу приватного сектору.

Для набуття кіберстійкості (К) необхідним є досягнення таких стратегічних цілей:

ціль К.1. Національна кіберготовність та надійний кіберзахист - Україна запровадить і реалізує чіткі та зрозумілі для всіх заінтересованих сторін заходи щодо національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України. Україна посилить кіберготовність, що полягатиме у здатності всіх заінтересованих сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної

інфраструктури. Україна створить національну систему управління інцидентами;

ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки - Україна проведе докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, здійснить заходи щодо збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створення національних інформаційних систем, платформ і продуктів. Вітчизняний науково- технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним стануть невід'ємними елементами освіти кожного громадянина України;

ціль К.3. Безпечні цифрові послуги - Україна забезпечить досягнення балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійність та безпеку цифрових послуг протягом усього їхнього життєвого циклу.

Для удосконалення взаємодії (В) необхідним є досягнення таких стратегічних цілей:

ціль В.1. Зміцнення системи координації - Україна створить умови для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів, скоординує діяльність усіх заінтересованих сторін задля подолання надзвичайних (кризових) ситуацій у кіберпросторі;

ціль В.2. Формування нової моделі відносин у сфері кібербезпеки - Україна запровадить сервісну модель державної участі у заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки;

ціль В.3. Прагматичне міжнародне співробітництво - Україна спрямує відносини з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібера- таки та кіберінциденти, проведення спільних кібероперацій та

розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками. Україна забезпечить активну участь у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Забезпечення координації з міжнародними партнерами здійснюватиметься Міністерством закордонних справ України.

13.3. Повноваження органів сектору безпеки України щодо протидії кіберзлочинності та дезінформації

Стратегія кібербезпеки містить вказівки Кабінету Міністрів України разом із СБУ (Службою безпеки України) та СЗРУ (Службою зовнішньої розвідки України) забезпечити виконання Плану реалізації Стратегії і забезпечити інформування РНБО України кожні півроку про стан реалізації Стратегії. Крім того, політико-правові особливості екосистеми кібербезпеки обумовлює особливу актуальність дослідження прав і обов'язків державного органу спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України, і розвідувального органу, який здійснює розвідувальну діяльність у зовнішньополітичній, економічній, військово-технічній, науково-технічній, інформаційній, екологічній сферах, щодо кібербезпеки. Зокрема, 14.06.2021 р. на саміті НАТО в Брюсселі було ухвалено рішення, відповідно до якого особливо масштабні кібератаки на членів Альянсу можуть розцінюватися як збройний напад із подальшим застосуванням атаки у відповідь з боку всіх країн Альянсу, в тому числі, із застосуванням збройних сил. Таким чином, Україна як член Програми розширених можливостей НАТО, має передбачати відповідні повноваження розвідувальних і контррозвідувальних органів у сфері кібербезпеки щодо атрибуції масштабних кібератак до тієї або іншої країни, а також перспектив політико-правової оцінки імовірних засобів і заходів атак у відповідь (після вступу в НАТО).

Повноваження органів сектору безпеки України щодо протидії кіберзлочинності в Україні значною мірою визначені Законом України «Про основні засади забезпечення кібербезпеки України» (далі – Закон про кібербезпеку). СБУ «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..., протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки». СЗРУ здійснює розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки. Відповідні повноваження СБУ деталізовані у чинному Законі України «Про СБУ». Для СЗР протидія кіберзлочинності не є безпосереднім завданням, цей державний орган зорієнтований на отримання розвідувальної інформації.

У сфері протидії кіберзлочинності залишаються невирішеними питання повної імплементації Конвенції Ради Європи про кіберзлочинність у вітчизняне законодавство України.

Повноваження органів сектору безпеки України щодо протидії дезінформації не мають такої визначеності як у сфері протидії кіберзлочинності. І цьому є причини: по-перше, дезінформаційні повідомлення (фейки) по суті не є протиправними; по-друге, дезінформація – це термін і метод, який був притаманний діяльності спеціальних служб за часів «холодної війни»; по-третє, законодавство України ґрунтується на фундаментальному принципі свободи слова і не криміналізує умисне розповсюдження неправдивої інформації задля досягнення державними і недержавними суб'єктами політичних, економічних, військових та інших цілей; насамкінець, нещодавно створений при Раді національної безпеки і оборони України (РНБО) України Центр протидії дезінформації на виконання відповідного Положення налагодив взаємодію з органами державної влади, правоохоронними та розвідувальними органами, зокрема із СБУ та СЗРУ із можливими пропозиціями щодо коригування їх повноважень.

Задля досягнення цілей протидії дезінформації відповідні заходи з боку контррозвідувального і розвідувального органів незавжди матимуть відкритий, публічний характер. Повноваження розвідувальних органів, наприклад, проводити розвідувальні заходи за межами України та з території України безумовно будуть пов'язані із розвідувальною

таємницею, і не підлягатимуть оприлюдненню та наданню на запити відповідно до Закону України «Про доступ до публічної інформації». Аналогічно, відомості про організацію, плани, зміст, форми, методи, результати контррозвідувальної діяльності тощо, яка здійснюватиметься по відношенню до суб'єктів створення та поширення дезінформаційних повідомлень, буде становити державну таємницю.

Одним із механізмів протидії поточним загрозам національним інтересам України як в інформаційній сфері у контексті протидії дезінформації, так і щодо дій іноземних держав, іноземних юридичної чи фізичних осіб, інших суб'єктів у кіберсфері є застосування санкцій відповідно до Закону України «Про санкції». Серед суб'єктів, які мають право вносити пропозиції щодо застосування, скасування та внесення змін до санкцій на розгляд РНБО України, є СБУ.

Зважаючи на характер сучасної кіберзлочинності та особливості дезінформаційних кампаній, актуальною є деталізація повноважень СБУ з протидії кіберзлочинності і дезінформації, а також СЗРУ – щодо здобування розвідувальної інформації про відповідних іноземних суб'єктів. Крім того, взаємодія Центру СБУ і СЗРУ стосовно протидії дезінформації може ґрунтуватися на засадах, які подібних до тих, що вже апробовані для взаємодії зазначених органів із Національним координаційним центром кібербезпеки при РНБО України.

ЛЕКЦІЯ 14. ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ОБІГУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Питання для опрацювання:

14.1. Дисциплінарна відповідальність за порушення інформаційного законодавства
14.2. Цивільно-правова відповідальність за порушення інформаційного законодавства
14.3. Адміністративна відповідальність за порушення інформаційного законодавства
14.4. Кримінальна відповідальність за порушення інформаційного законодавства

Джерела:

1. Кодекс законів про працю України від 10.12.1971 року № 322-VIII [Електронний ресурс] / Верховна Рада УРСР. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/322-08
2. Кодекс України про адміністративні правопорушення від 07.12.1984 року № 8073-X [Електронний ресурс] / Верховна Рада УРСР. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80731-10
3. Кримінальний кодекс України від 05.04.2001 року № 2341-III [Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14
4. Цивільний кодекс України від 16.01.2003 року № 435-IV 2341 [Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/435-15

14.1. Дисциплінарна відповідальністьза порушення інформаційного законодавства

Юридична відповідальність є специфічним юридичним засобом забезпечення реалізації охорони і захисту права на інформацію, здійснення закріплених обов'язків.

Юридична відповідальність – це передбачені законом вид і міра державно-владного (примусового) зазнання особою втрат благ особистого, організаційного і майнового характеру за вчинене правопорушення. Юридична відповідальність – одна з форм соціальної відповідальності. Крім юридичної відповідальності, у суспільстві діють й інші форми соціальної відповідальності: моральна, політична, організаційна, суспільна, партійна та ін. Організаційна і політична відповідальність застосовується в таких формах, як звіт, відставка; моральна – засудження громадською думкою; партійна –виключення з партії тощо. Юридична відповідальність має свої специфічні ознаки:

спирається на державний примус у формі каральних і правовідновлюючих (компенсаційних) способів; виражається в обов'язку особи зазнавати певних втрат; настає лише за вчинені або вчинювані правопорушення; здійснюється компетентними органами згідно із законом; здійснюється в ході правозастосувальної діяльності за умови дотримання певного процедурно-процесуального порядку і форм, ґрунтується на принципах законності, обґрунтованості, доцільності, невідворотності, своєчасності, справедливості. Залежно від галузевої структури права розрізняють такі види юридичної відповідальності: дисциплінарна, кримінальна, цивільно-правова, адміністративно-правова.

Дисциплінарна відповідальність – вид юридичної відповідальності, яка полягає в обов'язку працівника відповідати перед роботодавцем за дисциплінарний проступок і зазнавати дисциплінарних санкцій, передбачених законодавством про працю. До заходів дисциплінарної відповідальності належать: догана, переведення на іншу роботу, звільнення. Може бути застосована, зокрема, за порушення порядку розгляду звернень громадян тощо.

У зв'язку з прийняттям Закону України від 22.12.2006 року № 534-V «Про внесення змін до деяких нормативних актів України щодо посилення протидії незаконному обігу архівних документів» у ст. 41 Кодексу законів про працю України «Додаткові підстави розірвання трудового договору з ініціативи власника або уповноваженого ним органу з окремими категоріями працівників за певних умов» підставою для звільнення, також, можуть бути винні дії працівника, який безпосередньо обслуговує не лише грошові або товарні, але й культурні цінності, якщо ці дії дають підстави для втрати довір'я до нього з боку власника або уповноваженого ним органу.

Такі ж зміни відбулись і у ст. 133 «Випадки обмеженої матеріальної відповідальності працівників». Матеріальна відповідальність настає за вчинене майнове правопорушення, шкоду, заподіяну підприємству, установі, організації робітниками та службовцями при виконанні ними своїх трудових обов'язків. Вона може бути повною чи обмеженою залежно від ступеня вини, розміру заподіяної шкоди, майнового стану, а також інших конкретних обставин. Притягає до відповідальності адміністрація підприємства.

14.2. Цивільно-правова відповідальність за порушення інформаційного законодавства

Цивільно-правова відповідальність – вид юридичної відповідальності. Полягає в настанні передбачених цивільно-правовою нормою негативних майнових наслідків, які

завжди є для правопорушника додатковим майновим обтяженням (додатковими майновими втратами або майновими обов'язками).

Цивільно-правова відповідальність настає внаслідок порушення зобов'язань, наведених у цивільно-правових або господарських договорах, і позадоговірних зобов'язань, а також у разі завдання шкоди здоров'ю чи майну особи, тобто применшення абсолютного майнового (пошкодження, знищення) або особистого немайнового (здоров'я, прав автора, честі, гідності) блага, охоронюваного законом, а також у разі настання фізичного або морального страждання потерпілого та інших негативних наслідків (моральна шкода).

Види і умови цивільно-правової відповідальності передбачені Цивільним кодексом України.

За цивільним законодавством цивільно-правова відповідальність поділяється на такі види: а) договірна; б) позадоговірна; в) часткова; г) солідарна; д) основна; е) субсидіарна.

Цивільно-правова відповідальність має компенсаційний характер, оскільки пов'язана з відновленням порушених прав потерпілого.

Фізична особа, особисті немайнові права якої порушено внаслідок поширення про неї неправдивої інформації, має право на відповідь, а також на спростування цієї інформації. Спростування здійснюється у такий самий спосіб, у який була поширена неправдива інформація. Питання притягнення винних до цивільної відповідальності вирішується у судовому порядку.

14.3. Адміністративна відповідальність за порушення інформаційного законодавства

Адміністративна відповідальність – вид юридичної відповідальності громадян і службових осіб за вчинені ними адміністративні правопорушення.

В Україні порядок застосування адміністративної відповідальності регулюється Кодексом України про адміністративні правопорушення та іншими законодавчими актами, які передбачають адміністративну відповідальність. Метою адміністративної відповідальності є виховання особи, яка вчинила адміністративне правопорушення, у дусі дотримання законів, поваги до правил співжиття, а також запобігання вчиненню нових правопорушень як самим порушником, так і іншими особами. Адміністративній відповідальності підлягають особи, які досягли на момент вчинення адміністративного правопорушення 16-річного віку. Службові особи несуть адміністративну відповідальні

за адміністративні правопорушення, вчинені внаслідок недотримання установлених правил, забезпечення виконання яких є їхнім службовим обов'язком.

Передбачені такі види покарань: попередження; штраф; оплатне вилучення предмета; конфіскація предмета; позбавлення спеціального права; виправні роботи; адміністративний арешт. Перелік адміністративних покарань не є вичерпним. Зокрема, Національна рада України з питань телебачення і радіомовлення може призупинити дію ліцензії телерадіоорганізації у разі порушення нею чинного законодавства та умов ліцензії.

Перелік правопорушень, за які настає адміністративна відповідальність, передбачений Кодексом України про адміністративні правопорушення. Ним передбачається адміністративна відповідальність і за порушення інформаційного законодавства.

Так, адміністративній відповідальності підлягають особи, які відмовили у наданні за запитами повної та достовірної екологічної інформації, передбаченої законодавством, або несвоєчасно надали її. У такому випадку на службових та посадових осіб накладається штраф від трьох до десяти неоподатковуваних мінімумів доходів громадян.

Адміністративним правопорушенням визнається недбале зберігання, псування, знищення, приховування, незаконна передача іншій особі документів Національного архівного фонду або документів, що підлягають внесенню до нього, незаконний доступ до зазначених документів. Такі дії тягнуть за собою попередження або накладення штрафу на громадян від трьох до семи неоподатковуваних мінімумів доходів громадян і попередження або накладення штрафу На посадових осіб – від п'яти до десяти неоподатковуваних мінімумів доходів громадян.

Адміністративним правопорушенням є публічні заклики або агітація за бойкотування референдуму, перешкоджання членам ініціативної групи у збиранні підписів громадян під вимогою про проведення референдуму, а так само будь-яка агітація в день проведення референдуму. Такі дії тягнуть за собою накладення штрафу від трьох до шести неоподатковуваних мінімумів доходів громадян.

Порушеннями законодавства про друковані засоби масової інформації є виготовлення, видання або розповсюдження продукції друкованого засобу масової інформації після припинення діяльності цього друкованого засобу масової інформації, а так само ухилення від перереєстрації друкованого засобу масової інформації у передбаченому законом порядку чи від повідомлення реєструючому органу про зміну виду видання, юридичної адреси засновника, (співзасновників), місця розташування редакції. Такі дії тягнуть за собою накладення штрафу від десяти до тридцяти

неоподатковуваних мінімумів доходів громадян. Порушеннями законодавства про державну таємницю є:

1) недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

2) засекречування інформації: про стан довкілля, про якість харчових продуктів і предметів побуту; про аварії, катастрофи, небезпечні природні явища та надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян; про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, обслуговування та соціальне забезпечення, а також про соціально-демографічні вибухи, стан правопорядку, освіти та культури населення; про факти порушення прав і свобод людини і громадянина; про незаконні дії органів державної влади, органів місцевого самоврядування та їхніх посадових осіб; іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;

3) безпідставне засекречування інформації;

4) надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становлять державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;

5) порушення передбаченого законодавством порядку надання допуску та доступу до державної таємниці;

6) невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;

7) провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

8) недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними;

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї

інформації або просочування її технічними каналами. Такі порушення тягнуть за собою накладення штрафу на громадян від одного до трьох неоподатковуваних мінімумів доходів громадян і на посадових осіб – під трьох до десяти неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення особою, яка притягалася до адміністративної відповідальності, тягне за собою накладення штрафу на громадян від трьох до восьми неоподатковуваних мінімумів доходів громадян і на посадових осіб – від п'яти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян.

Порушеннями законодавства про інформацію є неправомірна відмова у наданні інформації, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, у разі, коли така інформація підлягає наданню на запит громадянина чи юридичної особи відповідно до законів України. Посадові особи, які скоїли таке адміністративне правопорушення, притягуються до відповідальності у вигляді штрафу від п'ятнадцяти до двадцяти п'яти неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення особою, яка притягалася до адміністративної відповідальності, тягне за собою накладення штрафу на посадових осіб від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Адміністративним правопорушенням визнається порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які місять конфіденційну інформацію, що є власністю держави, яке призвело до розголошення такої інформації. Такі дії тягнуть за собою накладення штрафу на громадян від одного до двох неоподатковуваних мінімумів доходів громадян і на посадових осіб – від трьох до восьми неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення особою, яка притягалася до адміністративної відповідальності, тягне за собою накладення штрафу на громадян від двох до семи неоподатковуваних мінімумів доходів громадян і на посадових осіб – від восьми до тринадцяти неоподатковуваних мінімумів доходів громадян.

Адміністративним правопорушенням визнається здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах. Такі неправомірні дії тягнуть за собою накладення штрафу від п'яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої. Та сама дія, вчинена особою, яку протягом року було піддано адміністративному стягненню за порушення, тягне за собою накладення штрафу від десяти до двадцяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу.

14.4. Кримінальна відповідальність за порушення інформаційного законодавства

Кримінальна відповідальність - вид юридичної відповідальності, суть якого полягає в застосуванні судом від імені держави примусу у формі покарання.

Кримінальна відповідальність настає за вчинення злочинів, вичерпний перелік яких міститься в Кримінальному кодексі України і реалізується виключно в судовому порядку.

Міри кримінальної відповідальності: довічне позбавлення волі, позбавлення волі на певний строк, тримання в дисциплінарному батальйоні, обмеження волі, арешт, конфіскація майна, службові обмеження для військовослужбовців, виправні роботи, громадські роботи, позбавлення прав обіймати певні посади або займатися певною діяльністю, позбавлення військового спеціального звання, рангу, чину або кваліфікаційного класу, штраф.

Порушенням інформаційного законодавства, за яке може наступити кримінальна відповідальність, є розголошення службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, що є небезпечною для життя людини, або захворювання на синдром набутого імунодефіциту (СНІД) та його результатів, що стали їм відомі у зв'язку з виконанням службових або професійних обов'язків. Такі дії караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років з позбавленням права обіймати посади чи займатися певною діяльністю на строк до трьох років або без такого.

Кримінальна відповідальність настає і за умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки. Такі дії караються штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або позбавленням права обіймати посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років.

Кримінальний кодекс України містить розділ V «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина», у якому

передбачається кримінальна відповідальність за порушення інформаційного законодавства.

Таким порушенням є умисне порушення таємниці голосування під час проведення передбачених законом України виборів, вчинене членом виборчої комісії або іншою службовою особою з використанням влади чи службового становища. Такі дії караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від одного до трьох років з позбавленням права обіймати посади чи займатися певною діяльністю на строк до трьох років.

Порушенням інформаційного законодавства, за яке передбачається кримінальна відповідальність, є незаконне знищення матеріальних носіїв інформації, зокрема, виборчої документації або документів референдуму поза визначеним законом строком зберігання у державних архівних установах та в Центральній виборчій комісії України після проведення виборів або референдуму, а так само пошкодження виборчої документації або документів референдуму. Такі дії караються обмеженням волі на строк від трьох до п'яти років або позбавленням волі на строк від двох до чотирьох років. Ті ж самі діяння, вчинені за попередньою змовою групою осіб або членом виборчої комісії чи іншою службовою особою з використанням влади або службового становища, караються позбавленням волі на строк від трьох до п'яти років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років або без такого.

Порушенням інформаційного законодавства, за яке передбачається кримінальна відповідальність, є порушення гарантованої Конституцією України таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. Такі дії караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років. Ті самі дії, вчинені щодо державних чи громадських діячів або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації, караються позбавленням волі на строк від трьох до семи років.

До кримінальної відповідальності притягаються особи за розголошення таємниці усиновлення (удочеріння) всупереч волі усиновителя (удочерителя). Такі дії караються штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. Те саме діяння, вчинене службовою особою або працівником медичного закладу, яким відомості про усиновлення (удочеріння) стали відомі по службі чи по роботі, або якщо воно спричинило тяжкі наслідки, карається штрафом до двохсот неоподатковуваних мінімумів доходів

громадян або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк з позбавленням права обіймати посади чи займатися певною діяльністю на строк до трьох років або без такого.

До порушень інформаційного законодавства належить умисне перешкоджання законній професійній діяльності журналіста, за яке передбачається відповідальність у вигляді штрафу до п'ятдесяти неоподатковуваних мінімумів доходів громадян або арешту на строк до шести місяців, або обмеження волі на строк до трьох років. Переслідування журналіста за виконання професійних обов'язків, за критику, здійснюване службовою особою або групою осіб за попередньою змовою, карається штрафом до двохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням права обіймати певні посади на строк до трьох років.

Окремі порушення інформаційного законодавства тягнуть за собою кримінальну відповідальність, передбачену відповідними нормами глави Кримінального кодексу України «Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації».

Зокрема, до таких порушень інформаційного законодавства належать: розголошення державної таємниці; втрата документів, що становлять державну таємницю; передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави.

Розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, 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 або без такого. Те саме діяння, якщо воно спричинило тяжкі наслідки, карається позбавленням волі на строк від п'яти до восьми років.

Втрата документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації або предметами, карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. Те саме діяння, якщо воно спричинило тяжкі наслідки, карається позбавленням волі на строк від двох до п'яти років.

Передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їхнім представникам економічних, науково-технічних або інших відомостей, що становлять конфіденційну інформацію, яка є власністю держави, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, караються обмеженням волі на строк до трьох років або 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 або без такого. Ті самі дії, вчинені з корисливих мотивів, або якщо вони спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб, караються обмеженням волі на строк від чотирьох до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Треба зауважити, що термін «конфіденційна інформація, що перебуває у власності держави» з прийняттям Закону України «Про доступ до публічної інформації» у більшості нормативних актів був замінений на «службова інформація», але ці зміни поки що не торкнулись Кримінального кодексу України, який продовжує використовувати термін «конфіденційна інформація, що перебуває у володінні держави».

Окрема глава в Кримінальному кодексі України присвячена злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

До таких злочинів законодавець відносить: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; створення з метою використання, розповсюдження або збуту шкідливих програмних технічних засобів, а також їх розповсюдження або збут; несанкціоновані дії з інформацією, яка обробляється 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; 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 обробляється; перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (спаму).

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку,

що призвело до витоку, втрати, підроблення, блокування інформації, спотворення процесу оброблення інформації або до порушення встановленого порядку її маршрутизації, карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох років до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Створення з метою використання, розповсюдження або збуту шкідливих програмних технічних засобів, а також їх розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, карається штрафом під п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк з конфіскацією програмних та технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк до п'яти років з конфіскацією програмних та технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

Несанкціоновані дії з інформацією, яка обробляється 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, караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи. 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, карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних та технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи. Зазначені дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

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 п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи.

Попри те, що новий Кримінальний кодекс України відповідає основним вимогам Ради Європи в галузі прав і свобод людини і громадянина, на нашу думку, він не вирішує всі назрілі проблеми в нашому суспільстві, оскільки до нього не включено ряд порушень, відповідальність за які нині є актуальною. Йдеться, зокрема, про відповідальність посадових осіб за: необґрунтовану відмову від надання відповідної інформації; надання інформації, що не відповідає дійсності; навмисне приховування інформації; використання і поширення інформації щодо особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків, тощо.

Таким чином, правові обмеження як елемент (наслідок) юридичної відповідальності можна розглядати як самостійний та ефективний засіб правового забезпечення права на інформацію. Шляхом застосування спеціальних нормативно-

правових обмежень створюються умови, які спонукають конкретних осіб до неухильного виконання конституційних обов’язків.

Лекція 15. МІЖНАРОДНО-ПРАВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Питання для опрацювання:

15.1. Використання міжнародно-правового досвіду протидії комп'ютерній злочинності

15.2. Загальна характеристика комп'ютерних злочинців

Джерела:

1. Computer-related Crime: Recommendation No. R(89)9 on Computer-related Crime and Final Report of the European Committee on Crime Problems / Council of Europe. URL: Pagis Document (oas.org)
2. Класифікація комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу / Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій (kre.dp.ua)
3. Про кіберзлочинність: конвенція Ради Європи від 23.11.2001 року / Рада Європи. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

15.1. Використання міжнародно-правового досвіду протидії комп'ютерній злочинності

Міжнародне співробітництво правоохоронних та судових органів розвинених країн є одним з основних аспектів боротьби з комп'ютерною злочинністю.

З метою уніфікації кримінального законодавства Європейський Комітет з проблем злочинності Ради Європи в 1989 р. підготував спеціальні Рекомендації №R(89)9, в яких були визначені загальні характеристики комп'ютерних злочинів. Ці рекомендації складаються з двох списків *(рис. 15.1.):*

- *мінімальний:* обов'язковий список правопорушень, який необхідно включити в національні кримінальні законодавства;
- *необов'язковий* (вибірковий або факультативний) список правопорушень.

Рис. 15.1. Рекомендація № R(89)9 Ради Європи

У перелік правопорушень, рекомендованих для обов'язкового включення у внутрішні національні законодавства всіх країн Ради Європи **(***мінімальний список***)** було внесені 8 складів злочинів, пов'язаних з *використанням комп'ютерних технологій:*

1) *Комп'ютерне шахрайство.* Введення, зміна, вилучення, видалення або пошкодження комп'ютерних даних або програм, або інше втручання в процес обробки даних, яке впливає на результат обробки даних таким чином, що це веде до економічних збитків або втрати власності іншої людини, з метою отримання незаконним шляхом економічного прибутку для себе чи іншої особи.

2) *Комп'ютерна підробка.* Введення, зміна, вилучення, видалення або пошкодження комп'ютерних даних або програм, або інше втручання в процес обробки даних, що здійснюється таким способом або за таких умов, при яких вони класифікувалися б національним законодавством як фальсифікація, досконалий проти традиційного об'єкта такого правопорушення.

3) *Викривлення комп'ютерної інформації або комп'ютерних програм.*

Протиправне видалення, заподіяння шкоди, погіршення якості або придушення комп'ютерних даних чи програм.

4) *Комп'ютерний саботаж.* Введення, зміна, видалення комп'ютерних даних або програм, або створення перешкод комп'ютерним системам з наміром перешкоджати роботі комп'ютера або телекомунікаційної системі.

5) *Несанкціонований доступ.* Неправомірний доступ до комп'ютерної системи або мережі шляхом обходу захисних механізмів.

6) *Несанкціонований перехоплення.* Неправомірний перехоплення повідомлень, що чиниться з допомогою технічних засобів, які входять в комп'ютерну систему або мережу, виходять з комп'ютерної системи або мережі, або передаються в рамках комп'ютерної системи або мережі.

7) *Несанкціоноване копіювання захищеної авторським правом комп'ютерної програми.* Неправомірне відтворення, розповсюдження або передача в спільне використання комп'ютерної програми, охороняється законом.

8) *Несанкціоноване копіювання мікросхем.* Незаконне відтворення мікросхеми або вироби на напівпровідниках, охоронюваних законом, або неправомірне комерційне використання або імпорт з цією метою мікросхем або виробів на напівпровідниках, виготовлених з використанням цієї мікросхеми.

Інші 4 склади злочинів склали необов'язковий список, так як щодо них не було досягнуто загальної згоди:

1) *Зміна комп'ютерної інформації або комп'ютерних програм.* Неправомірне зміна комп'ютерної інформації або комп'ютерних програм.

2) Комп'ютерне шпигунство. Протиправне придбання недозволеними методами або використання торговельної або комерційної таємниці, з метою нанесення економічної шкоди особі, яка має доступ до цієї таємниці, або отримання незаконної економічного прибутку для себе або третьої особи.

3) *Протизаконне використання комп'ютера.* Використання комп'ютера без відповідного дозволу:

- вчинене з ризиком нанесення збитку особі, якій дано право використовувати систему, або заподіяння шкоди самій системі або її роботі;
- вчинене з метою заподіяння шкоди особі, якій надано право використовувати систему або заподіяння шкоди самій системі або її роботі;
- нанесення збитку особі, якій надано право використовувати системою або заподіяння шкоди самій системі або її роботі.

4) *Несанкціоноване використання захищеної авторським правом комп'ютерної програми.* Використання без відповідного дозволу комп'ютерних

програм, які захищені законом, і були скопійовані без дозволу з метою отримання протизаконного економічного прибутку для себе та інших осіб, або заподіяння шкоди власнику програми.

Поява таких списків завершила багаторічну роботу різних правових систем та інститутів по боротьбі з комп'ютерною злочинністю і створила об'єктивні передумови для міжнародного співробітництва в цій галузі. Однак, в силу рекомендаційного характеру цього документа, не по всіх напрямах була досягнута домовленість, що на практиці призводило до появи нових проблем у боротьбі з цими злочинами.

Наступним кроком у розвитку міжнародного співробітництва в боротьбі з комп'ютерними злочинами з'явилася розробка на початку 90-х років минулого століття робочою групою Інтерполу *кодифікатора комп'ютерних злочинів* (Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій (kre.dp.ua), с.22):

QA - втручання в роботу або перехоплення інформації в комп'ютерній системі:

QAH - незаконний (несанкціонований) доступ до комп'ютерної системи;

QAI - перехоплення інформації, циркулюючої в комп'ютерній мережі;

QAT - крадіжка часу за надані платні послуги (наприклад, ухилення від сплати за інформаційні послуги телефонного або комп'ютерного зв'язку в Інтернет або переведення їх на іншого користувача подібних послуг);

QAZ - інші випадки несанкціонованого доступу або перехоплення інформації.

Дані діяння, що класифікуються як комп'ютерні злочини, є попередніми і, як правило, необхідними для здійснення інших протиправних діянь, що розглядаються далі.

QD - заміна (модифікація) або спотворення інформації в автоматизованій (комп'ютерній) системі:

QDL - «логічна бомба»;

QDT - «троянський кінь»;

QDV - «комп'ютерні програми-віруси»;

QDW- «комп'ютерні програми-черв'яки»;

QDZ - інші випадки спотворення інформації в автоматизованих системах.

Розглянемо більш докладно дані програми.

«Логічна бомба» - програма, що запускається при певних тимчасових або інформаційних умовах для здійснення несанкціонованого доступу до інформації.

«Троянський кінь» - спеціальна підпрограма, яка маскується в тексті вільно розповсюджуваних програм і виконує дії, відмінні від

зазначених у специфікації для загальної програми.

«Комп'ютерна програма-вірус» - невелика програма, здатна мимовільно створювати свої копії і модифікувати (заражати) інші програми, файли. Часто містить «логічні бомби» і «трояни». Може супроводжуватися різними аудіо-та відео ефектами та ін.

«Комп'ютерні програми-черв'яки» - програма, впроваджувана в систему, часто зловмисно, і що перериває хід обробки інформації в системі. На відміну від вірусів черв'як не спотворює файли даних і програми. Зазвичай черв'як виконується, залишаючись невиявленим, і потім самознищується.

QF - комп'ютерне шахрайство:

QFC - шахрайство з банкоматами;

QFF - комп'ютерна підробка (підробка інформації в автоматизованих системах);

QFG - шахрайство з комп'ютерними ігровими автоматами;

QFM - шахрайство за рахунок неправильного вводу / виводу або маніпуляції програмами;

QFP - шахрайство з платіжними електронними засобами;

QFT - телефонне шахрайство;

QFZ - інші випадки комп'ютерного шахрайства.

QR - несанкціоноване копіювання програмних продуктів:

QRG - несанкціоноване тиражування комп'ютерної гри;

QRS - несанкціоноване тиражування комп'ютерного програмного забезпечення (комп'ютерних програм);

QRT - несанкціоноване тиражування напівпровідникової продукції (топологій, топографій, інтегральних мікросхем);

QRZ - інші випадки несанкціонованого копіювання комп'ютерної інформації.

OS - комп'ютерний саботаж:

QSH - саботаж з допомогою технічного забезпечення комп'ютерної системи;

QSS - саботаж з допомогою програмного забезпечення комп'ютерної системи;

QSZ - інші види комп'ютерного саботажу.

OZ - злочини, пов'язані з комп'ютерами і комп'ютерними технологіями:

QZB - незаконне використання дошки електронних оголошень (BBS);

QZE - крадіжка комерційної таємниці;

QZS - збір, збереження або поширення матеріалів, які є об'єктом судового розгляду або переслідування;

QZZ - інші випадки вчинення КП.

З цього переліку можна судити про те, що до злочинів у сфері комп'ютерної інформації ставиться дуже широкий спектр діяльності. Але, не всі ці діяння були прийняті в національному законодавстві України.

У 2001 р. було розроблено Конвенцію Ради Європи «Про кіберзлочинність», що є на сьогодні базовим міжнародним нормативно-правовим актом у сфері боротьби з комп'ютерною злочинністю, який підписала і ратифікувала (із застереженнями та заявами), і Україна.

Аналіз норм цієї Конвенції показує, що вони спрямовані на регулювання трьох основних блоків питань:

- наближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації;
- наближення національних кримінально-процесуальних заходів, направлених на забезпечення збору доказів при розслідуванні таких злочинів;
- можливі форми міжнародного співробітництва у кримінально-процесуальної діяльності.

Конвенція є комплексним документом, що містить норми різних галузей права: кримінального, кримінально-процесуального, авторського, цивільного, інформаційного.

Основною ідеєю цього документа є включення в національне законодавство країн-учасників норми про кримінальну відповідальність за злочини у сфері комп'ютерної інформації. В ній також не дається визначення поняттю «злочини у сфері комп'ютерної інформації». Воно замінено терміном «кіберзлочини», який розкривається за допомогою наступного переліку:

- дії, спрямовані проти комп'ютерної інформації (як предмета злочинного посягання) і використання її як унікальне знаряддя вчинення злочину;
- дії, предметом посягання яких є інші блага, охоронювані законом, а інформація, комп'ютери та інше, є тільки одним з елементів об'єктивної сторони злочину, виступаючи як предмет, знаряддя його вчинення, складової частини способу його вчинення або приховування.

Об’єктом кіберзлочинів, відповідно до Конвенції, є широкий спектр суспільних відносин, що виникають при вчиненні інформаційних процесів з приводу виробництва, збору, обробки, накопичення, збереження, пошуку, розповсюдження та споживання комп’ютерної інформації, а також в інших областях, де використовуються комп’ютери, комп’ютерні системи та мережі. Серед них, враховуючи підвищене громадянське значення, виділяються правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності та доступності комп’ютерних даних і систем, законного використання комп’ютерів і комп’ютерної інформації (даних), авторського та суміжних прав.

15.2. Загальна характеристика комп’ютерних злочинців

Особистість злочинця досліджується різними науками, в тому числі кримінологією і криміналістикою. Кримінологічні дослідження обмежуються, головним чином, тими особливостями людини, які необхідні для кримінальної профілактики, запобігання та попередження злочинів. Криміналістика вивчає в першу чергу «професійні» якості злочинців, які проявляються, переважно в певних способах, методах, прийомах здійснення злочинів.

Загальновідомо, що на місці злочину залишаються сліди, що визначають характерний «почерк» злочинця. Результати злочинної діяльності містять образні сліди людини. Виявлення на місці злочину речових доказів дає можливість отримати відомості про деякі соціально-психологічних ознаках злочинця. Також сліди злочину свідчать про кримінальний досвід злочинця, професію, його соціальне становище, стать, вік, особливості відносин з потерпілим та ін.

Криміналістичні дані про особу злочинця базуються на двох специфічних групах інформації.

Перша група включає дані про особу невідомого злочинця по залишених ним слідах, як на місці злочину, так і в пам’яті свідків, в інших джерелах з метою встановлення напрямів його пошуку і затримання. Ця інформація дає уявлення про загальні ознаки певної групи людей, до яких може відноситися і злочинець.

Друга група об’єднує інформацію, отриману при вивченні особистості вже затриманого підозрюваного або обвинуваченого з метою вичерпної криміналістичної оцінки особи - суб’єкта злочину. З цією метою збираються відомості не тільки про ціннісні орієнтири, особливості соціальних поглядів, але і про його зв’язки, поведінку до, під час і після вчинення злочину. Це може допомогти знайти зі злочинцем психологічний контакт, отримати правдиві показання або вибрати ефективні способи впливу на нього.

Вважається, що ця інформація з урахуванням різних відомостей, що відображаються в інших елементах криміналістичної характеристики**,** може бути покладена в основу типізації злочинців**.** Формування банку типових моделей злочинців, вивчення спільних рис таких людей, дозволяє оптимізувати процес виявлення кола осіб, серед яких доцільний пошук злочинців, що й обумовлює актуальність розгляду цього питання, щодо комп'ютерних злочинців.

Характеризуючи комп'ютерного злочинця, необхідно відзначити, що до сфери комп'ютерних злочинів, входить дуже широке коло осіб. В коло цих осіб входять як висококласні фахівці, що мають спеціальну освіту (математики, програмісти, інженери-електронники та ін.), так і дилетанти. Як відомо правопорушники мають різний соціальний статус і рівень освіти.

Вітчизняні та зарубіжні дослідження дають можливість сформувати абстрактні портрети правопорушників, тобто відповідний профіль соціального типу злочинця.

В якості однієї з базових ознак, при дослідженні комп'ютерної злочинності розглядають мету і сферу (вид) протизаконної діяльності.

Серед фахівців відсутнє єдине тлумачення терміну «хакер»**.** Спочатку під хакером (hacker) розумівся високопрофесійний програміст, здатний розробляти і модернізувати комп'ютерні програми, не маючи детальних специфікацій та документації до них. Таке трактування було панівною на рубежі 70-80-х років минулого сторіччя, коли саме зародився і розвинувся світовий хакерський рух. Пізніше, зі зростанням масштабів комп'ютерної злочинності і перетворення їх на самостійний вид злочинності, цей термін набув кримінальний відтінок і став означати комп'ютерного зломщика, здатного незаконним способом отримати доступ в комп'ютерні інформаційні системи або мережі.

Однак більшість вчених небезпідставно вважають, що для останньої зазначеної категорії суб'єктів протиправної діяльності більш доцільне використання терміну «кракер» (cracker).

Головна відмінність між зазначеними категоріями полягає, не у віці або в рівні майстерності (новачок, професіонал, суперпрофесіонал), а в характері впливу на інформацію і в цільової установці. Суб'єкти обох зазначених категорій шукають і аналізують уразливості («дірки», «люки» та ін.) в апаратно-програмному забезпеченні та здійснюють злом комп'ютерних систем і мереж. Хакери, наприклад, часто мають дослідницькі мети, не роблять шкідливого впливу на інформацію і повідомляють про результати своїх атак. Навпаки, кракери здійснюють злом комп'ютерних систем з метою отримання

несанкціонованого доступу до чужої інформації, характер впливу на яку набагато більш небезпечний залежно від їх мотивів (рис. 15.3).

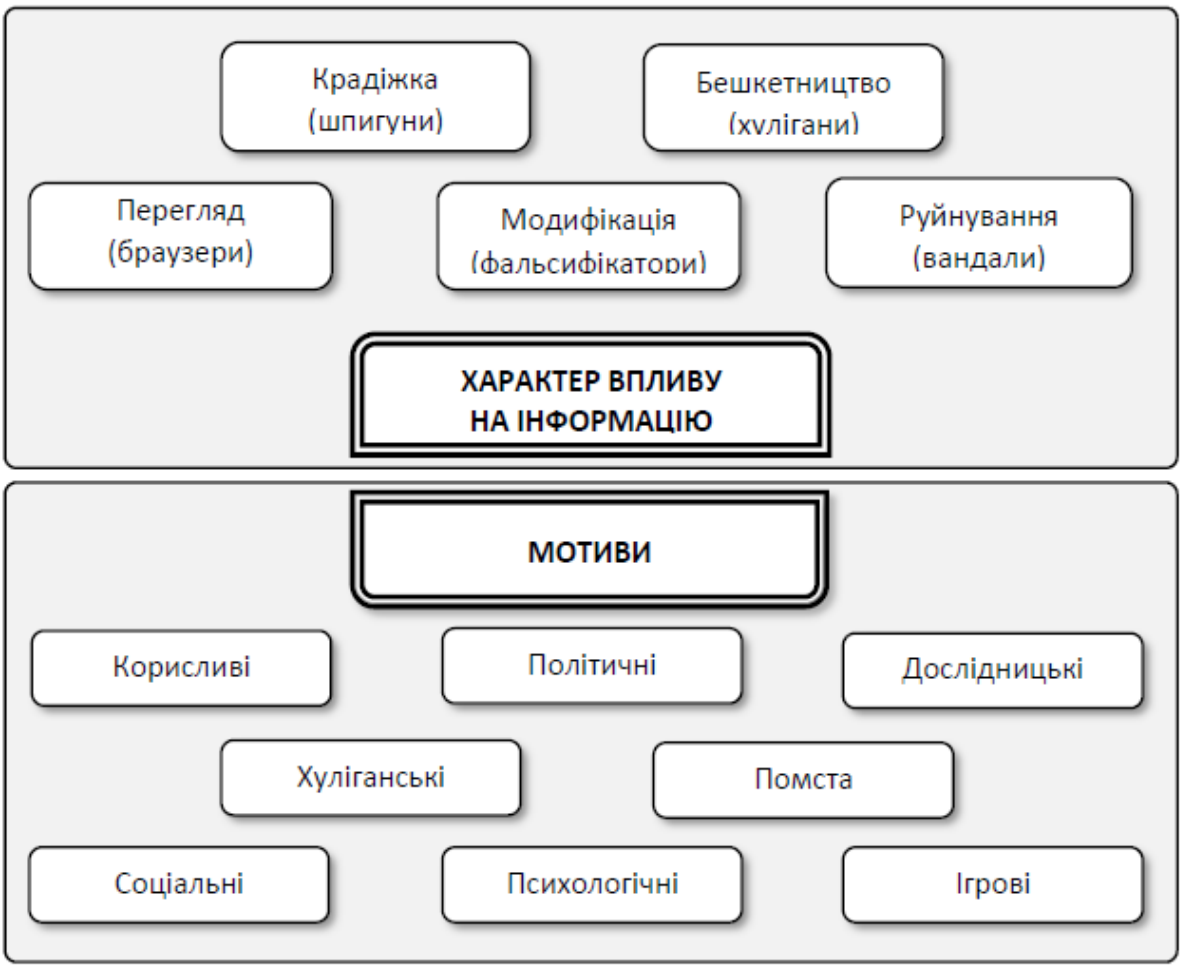

Рис. 15.3. Характер впливу на інформацію та мотивація комп'ютерних злочинців

Статистичні співвідношення різного роду мотивів при вчиненні комп'ютерних злочинів за експертними оцінками складають:

- корисливі мотиви - 60 ... 70%;
- політичні мотиви (тероризм, шпигунство, дисидентство та ін.) - 15 ... 20%;
- дослідницький інтерес (допитливість) - 5 ... 7%;
- хуліганські спонукання і бешкетництво - 8 ... 10%;
- помста - 4%.

Інші мотиви скоєння комп'ютерних злочинів є відносно новими і менш вивченими.

Розглянемо докладно класифікації комп'ютерних злочинців.

Кодувальники (coders) здійснюють злом програмних продуктів, усуваючи або обходячи в них програмні механізми захисту. «Трасує» (розкладають) тексти програм, використовуючи для цього комп'ютерні мови високого рівня, в тому числі, на машинних кодах. «Роздягнені» програми передають (продають) потім, наприклад, комп'ютерним піратам або колекціонерам. Типовий «крек» - обхід необхідності введення реєстраційного або серійного номера ліцензійної програми при її інсталяції на ПК.

Комп'ютерні пірати (wares dudes) спеціалізуються на незаконному (без згоди правовласника) копіюванні ліцензійних програмних продуктів та їх розповсюдженні з метою отримання матеріальної вигоди. Наносять багатомільйонної шкоди розробникам програмних продуктів і проявляються в різних формах: «чорного» і «білого» копіювання, завантаження жорстких дисків ПК при їх продажу, перекачуванні через Інтернет тощо.

Слід зазначити, що в 2007 р., завдяки успіхам, перш за все, в нормотворчій, правозастосовній та профілактичній діяльності державних структур з України знято статус пріоритетної країни- порушника авторських прав (рівень піратства менше 90%).

Колекціонери (codes kids) колекціонують, використовують і обмінюються захищеними комп'ютерними програмними продуктами, що мають коди доступу, паролі та інші вбудовані програмні засоби захисту, а також кодами телефонного виклику і номерами телефонних компаній, що мають вихід до комп'ютерних мереж загального користування, наприклад Інтернет.

Кардери (card) - спеціалізуються на махінаціях з пластиковими картками, оплачуючи свої витрати з чужих кредитних карт. Типова процедура кардинг полягає в копіюванні інформації, що міститься на магнітній смузі кредитної картки (дамп) і виробництві фальшивої картки - «фантома» з нанесенням на неї скопійованого дампа або отриманням індивідуального PIN-коду від власника реальної карти, наприклад, методами соціальної інженерії.

Кіберкруки (cybercrooks) - спеціалізуються на несанкціоноване проникнення в комп'ютерні системи та мережі (КСС) фінансово- банківських установ і закриті КСС державних силових структур та органів. Використовують КСС для викрадення коштів, отримання цінної фінансової інформації. Популярним товаром є кредитна інформація, інформаційні бази даних правоохоронних органів та інших державних і комерційних структур.

Фішинг (phishing - з англ.: рибна ловля) - відносно новий вид мережевого шахрайства. Його метою є заволодіння шляхом обману персональними даними

клієнтів онлайнових аукціонів, Інтернет - магазинів, сервісів грошових переказів та іншої конфіденційної інформації. Постійно вдосконалюються шахраями різні «виверти» спрямовані, в основному, на занадто довірливих або неуважних користувачів, самі (добровільно) розлучаються з конфіденційною інформацією, коли їх просять повторити введення пароля, повідомити номер рахунку та пароль для реєстрації покупки або грошового переказу, зареєструватися на хибному сайті-двійнику Інтернет- магазину та ін., причому бурхливий розвиток Інтернет, мережевий комерції і банкінгу обумовлюють перетворення фішингу в один з найпоширеніших видів комп'ютерного шахрайства. Сьогодні вже можна виділити три популярних види фішингу: поштову, онлайновий і комбінований (фарминг). В останньому випадку змінюється адреса DNS Domain Name System) таким чином, щоб користувач взаємодіяв з фальшивим сервером-постачальником послуг (товарів).

Спамери (spam, spiced ham - з англ. - «шинка зі спеціями») займаються масовим (більше 5-ти адресатам) розсилкою непрошених (часто анонімних) повідомлень засобами електронних комунікацій, в першу чергу - по електронній пошті або мобільного зв'язку.

Вірусописаки (Virus Writers, вірмейкерів) здійснюють протиправне пошкодження КСС з метою порушення її функціонування за допомогою програмних (комп'ютерних або мережевих) вірусів.

Порнографи використовують можливості Інтернет для платного розповсюдження матеріалів порнографічного характеру, які вченими називаються «кокаїном для нового покоління». Більше 75% всієї дитячої порнографії поширюється в Інтернет, де, за деякими оцінками, налічується майже 40 тисяч порно сайтів. Моніторинг українських Інтернет-сайтів показав, що на них міститься приблизно 20% забороненої порно продукції, в тому числі і дитяча порнографія.

Кіберсквотинг (cybersquatting) - захоплення доменних імен з метою наживи. Доменні імена найчастіше називають «нерухомістю» онлайнового століття. Добре підібране ім'я може саме по собі забезпечувати досить сильний потік відвідувачів, а значить, і потенційних клієнтів: вдала назва інтуїтивно знаходиться і легко запам'ятовується. Усвідомлення цінності доменів постійно зростає, а слідом росте й їхня ціна.

Фрікери (phreak = phone+break) спеціалізуються на використанні телефонних систем, зломі цифрових АТС телефонних компаній, несанкціонованому отриманні кодів доступу до платних послуг ISDN, крадіжці і

підробці телефонних карток тощо, з метою уникнути сплати за надані послуги в сфері ІКТ. У своїй діяльності використовують не тільки програмне забезпечення, але і спеціальну апаратуру, що генерує імпульсні або тональні сигнали виклику телефонних систем. Фрікінг є одним з найстаріших видів протиправної діяльності в сфері високих технологій.

З правової точки зору, відносити хакерів, кракерів, фрікерів, кардерів та інших суб'єктів вище розглянутих категорій до комп'ютерних злочинцям може тільки суд.

ЛІТЕРАТУРА:

1. Барасюк Я.М., Стець О.В. Інформаційні системи і технології в економіці. Навчально-методичний посібник. Чернівці: ЧТЕІ КНТЕУ, 2016. 409 с.
2. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. Київ: Видавництво НА СБ України, 2015. 251 с.
3. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ ім. О.С. Попова, 2019. 320 с.
4. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека». Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
5. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. Львів: «Магнолія 2006», 2018. 320 с.
6. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2022. 416 с.
7. Кормич Б.А. Інформаційне право. Підручник. Харків: БУРУН і К, 2011. 334. с.
8. Логінов Н.І., Дробожур Р.Р. Правовий захист інформації: Навчальний посібник. Одеса: Фенікс, 2015. 264 с.
9. Максимус Д.О., Юхно О.О. Використання сучасних інформаційних технологій працівниками ОВС України при проведенні негласних слідчих (розшукових) дій: навч. посіб. Харків: НікаНова, 2013. 102 с.

10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
11. Правове регулювання інформаційних відносин: Навч. посіб. / В.Ю. Жарких та ін. Київ: Каравела, 2013. 232 с.
12. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері: навч. посіб. Київ: Нац. акад. СБУ, 2015. 172 с.