О. В. МАНЖАЙ,
І. А. МАНЖАЙ

ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ

Підручник

Видання друге, перероблене та доповнене

Харків
2020

УДК 343.1 : 65.012.8
67.9(4Укр)6я73
М 23

Рекомендовано до друку Вченою радою ТОВ «Харківський університет»
Протокол № 14 від 25 листопада 2019 р.

Рецензенти:
Павликівський В. І., завідувач кафедри кримінально-правових дисциплін та адміністративного права Харківського університету, д.ю.н., доцент;
Тулупов В. В, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент.

Манжай О. В., Манжай І.А.

М 23 Правові засади захисту інформації: підручник. – Харків : Панов, 2020. – 162 с. : іл.

ISBN 978-617-7634-85-9

У підручнику розкрито основні поняття та інститути правового захисту інформації. Досліджено властивості інформації, важливі з точки зору її включення до правового обігу, поняття та загальні засади забезпечення інформаційної безпеки держави, нормативний порядок захисту окремих видів інформації в Україні та за її межами, убезпечення електронного документообігу та його організаційну структуру. Також схематично наведено побудову інституту інтелектуальної власності згідно з українським законодавством та окремі механізми її захисту. Підручник розрахований на курсантів, студентів, слухачів і фахівців з безпеки. Він може бути корисним викладачам та аспірантам вищих навчальних закладів, які займаються дослідженнями у сфері правового забезпечення безпеки інформації.

67.9(4Укр)6я73
УДК 343.1:65.012.8

ISBN 978-617-7634-85-9

Зміст

Вступні зауваження

Останніми роками можна спостерігати інтенсифікацію процесів, пов'язаних з упровадженням безпекових механізмів у всі сфери суспільного життя. Інформація при цьому є одним з основних об'єктів, який підлягає захисту за допомогою технічних, організаційних і правових заходів. Захист інформації за допомогою правових механізмів відіграє одну з провідних ролей у забезпеченні інформаційної безпеки та кібербезпеки держави.

Донедавна проблематика інформаційної безпеки була предметом дослідження здебільшого технічної науки, однак сьогодні вона набуває вже міжгалузевого характеру. Це підтверджується дослідженнями науковців, матеріалами Національного інституту стратегічних досліджень, результатами діяльності силових підрозділів тощо.

Велика кількість завдань із забезпечення інформаційної безпеки держави вирішуються правовими методами шляхом вдосконалення нормативно-правової бази у сфері забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії кіберзлочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері.

Мета цього підручника – допомогти зрозуміти шляхи захисту інформації за допомогою різних інститутів права, відповідальність за порушення умов обробки, засоби накопичення та зберігання певних видів інформації, загальний порядок захисту електронного документообігу. Крім того, наведені в підручнику матеріали сприяють засвоєнню курсантами, студентами, слухачами правових методів захисту інформації та його процедур на різних стадіях циркуляції інформації, здійснення контрольно-перевірочного процесу з метою підтвердження відповідності наявної комплексної системи захисту інформації вимогам чинного законодавства тощо.

Вивчення такої дисципліни допоможе курсантам, студентам, слухачам більш повно аналізувати інформаційну діяльність підприємств, установ, організацій та уміло керувати правовим забезпеченням їх інформаційної безпеки.

Тема 1. Інформація як об'єкт правового захисту

План

1. Поняття інформації.
2. Класифікація інформації.
3. Право на інформацію.

1. Поняття інформації

Слово інформація походить від латинського *informatio*, що перекладається як роз'яснення, викладення. На сьогодні існує досить багато визначень цього поняття. Здебільшого вони окреслюють найбільш важливу його складову, притаманну конкретній науці. Вивчення сутності та властивостей інформації найбільш повно реалізується в рамках теорії інформації, кібернетики, інформаційного права.

У тлумачному словнику української мови наведено загальне поняття інформації – це відомості про які-небудь події, чиюсь діяльність і т. ін.; повідомлення про щось[1].

У незалежній Україні закріплення поняття «інформація» на законодавчому рівні відбулося в 1992 р. з ухваленням Закону України «Про інформацію». Відповідне визначення було радикально змінене у 2011 році. На сьогодні згідно зі ст. 1 цього закону під ***інформацією*** розуміються будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді[2].

Узагалі залежно від галузі науки існують різні визначення поняття «інформація», їх безліч. До завдань цього розділу не входить формулювання загальнотеоретичного визначення інформації, нам необхідно дослідити її у правовому контексті. Для цього визначимо її юридично значущі ознаки, які обумовлюють

[1] Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. С. 512.

[2] Про інформацію : Закон України від 02.10.1992 [із змінами і доповненнями на 01.01.2017]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

специфіку інформації як об'єкта правового регулювання. До таких ознак найчастіше відносять:

– нематеріальний характер («самостійність відносно носія», тобто цінність інформації полягає в її суті, а не в матеріальному носії, на якому вона закріплена);

– суб'єктивний характер («інформація виникає в результаті діяльності суб'єкта, який усвідомлює свої дії», тобто є результатом інтелектуальної діяльності);

– необхідність об'єктивування для включення у правовий обіг;

– кількісна визначеність;

– невживаємість, можливість багатократного використання;

– збереження інформації, яка передається, у передавального суб'єкта;

– здатність до відтворення, копіювання, збереження і накопичення[3].

Для включення інформації у правовий обіг важливо, щоб вона мала певну об'єктивну форму, а саме була задокументована. Відповідно до ст. 1 Закону України «Про інформацію» ***документом*** є матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

Інформація не може існувати без носія. Вона взаємодіє з носієм за допомогою її запису, зберігання та зчитування. Принцип зберігання інформації на будь-якому носієві можна умовно представити як зміну однорідності деяких параметрів носія. Тому основною ознакою їх класифікації виступатиме принцип зчитування/запису інформації на носій (рис. 1.1–1.3), а додатковими – обсяг збережуваної інформації, швидкість доступу до даних, ступінь захищеності, поширеність, робоче призначення (рис. 1.4)[4].

Систематизовані зібрання документів складають *інформаційні ресурси*, процес роботи з якими називається *інформаційними процесами*. Саме ці два об'єкти потребують першочергового

[3] Мордвинова В. А., Фомина А. Б. Защита информации и информационная безопасность. МГДД(Ю)Т, МИРЭА, ГНИИ ИТТ «Информика». М., 2004. С. 56.

[4] Манжай А. В. Проблемы борьбы с компьютерным пиратством и легализации программного обеспечения в Украине. Разработка комплексной системы защиты информации на носителях от несанкционированного копирования // Компьютерная преступность и кибертерроризм: сборник научных работ. Запорожье: Центр исследования компьютерной преступности, 2004. Вып. 2. С. 278-280.

захисту, для них держава встановлює правові, організаційні й апаратно-програмні механізми забезпечення безпеки.

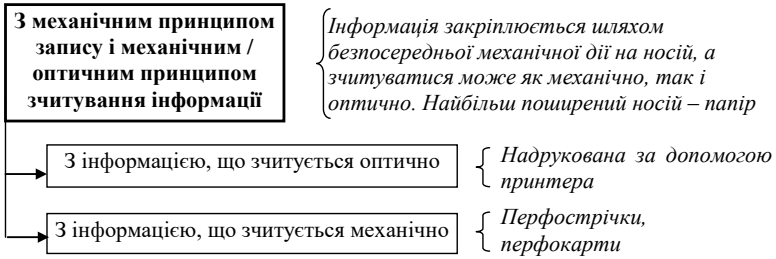


Рис. 1.1. Класифікація носіїв з механічним принципом запису

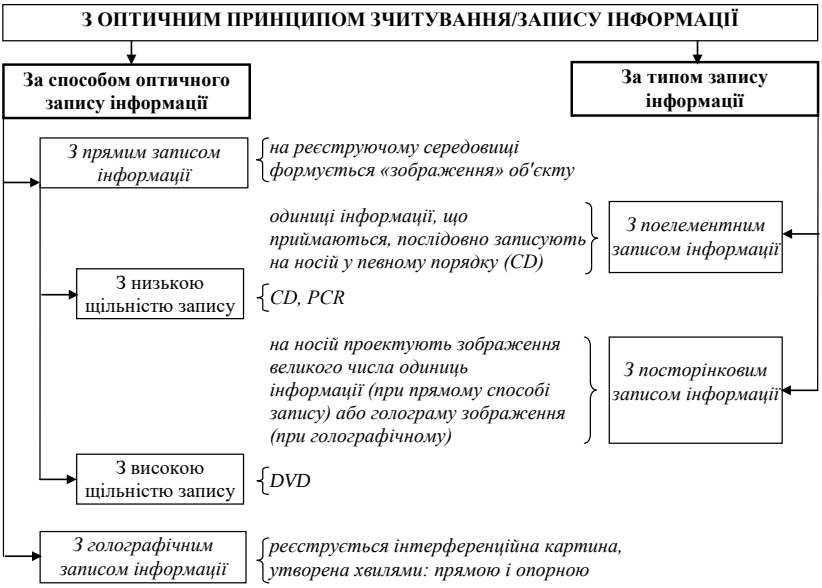


Рис. 1.2. Класифікація носіїв з оптичним принципом зчитування/запису

Рис. 1.3. Класифікація носіїв з магнітним, магнітооптичним, електронним та іншими принципами зчитування/запису

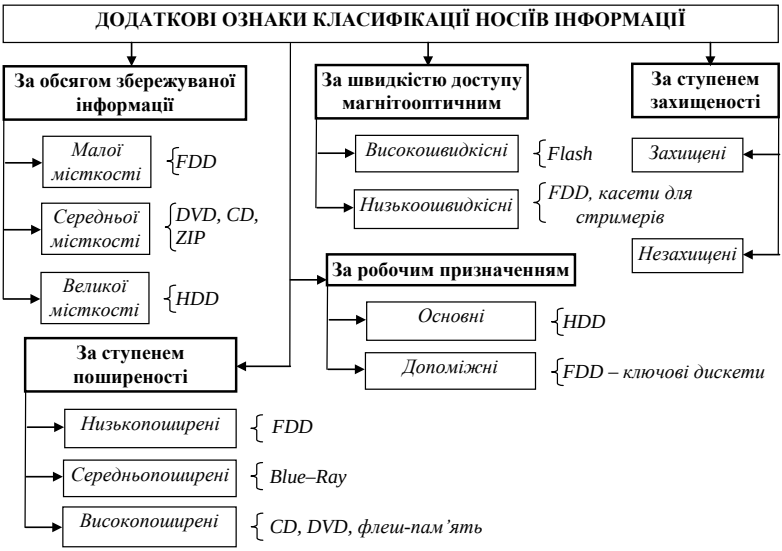


Рис. 1.4. Додаткові ознаки класифікації носіїв

Нормативно-правове забезпечення захисту інформації складається з низки законів і підзаконних актів, пов'язаних з різними галузями права: кримінальним, цивільним, адміністративним тощо.

Правові механізми захисту різних видів інформації в Україні закріплені, перш за все, в таких нормативних актах, як:

1) Конституція України від 28.06.1996;
2) Цивільний кодекс України від 16.01.2003;
3) Кримінальний кодекс України від 05.04.2001;
4) Кримінальний процесуальний кодекс України від 13.04.2012;
5) Кодекс України про адміністративні правопорушення від 07.12.1984;
6) Кодекс адміністративного судочинства від 06.07.2005;
7) Закон України «Про захист персональних даних» від 01.06.2010;
8) Закон України «Про оперативно-розшукову діяльність» від 18.02.1992;
9) Закон України «Про Національну поліцію» від 02.07.2015;
10) Закон України «Про інформацію» від 02.10.1992;
11) Закон України «Про державну таємницю» від 21.01.1994;
12) Закон України «Про національну безпеку України» від 21.06.2018;
13) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994;
14) Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017;
15) Доктрина інформаційної безпеки, затверджена Указом Президента України від 25.02.2017 № 47/2017;
16) Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373;
17) Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету Міністрів України від 19.10.2016 № 736;
18) інші нормативно-правові акти, що містять окремі питання захисту інформації.

Окрім законів і підзаконних актів правове забезпечення системи захисту інформації складають внутрішні нормативно-організаційні документи: накази та розпорядження; інструкції, в тому числі посадові; положення; договори; пам'ятки, протоколи тощо.

2. Класифікація інформації

Залежно від конкретного виду інформації встановлюються різні рівні її захисту. Для визначення конкретних захисних механізмів використовується принцип поділу інформації за порядком доступу на відкриту та з обмеженим доступом. Загальна структура такого поділу наведена на рис. 1.5.

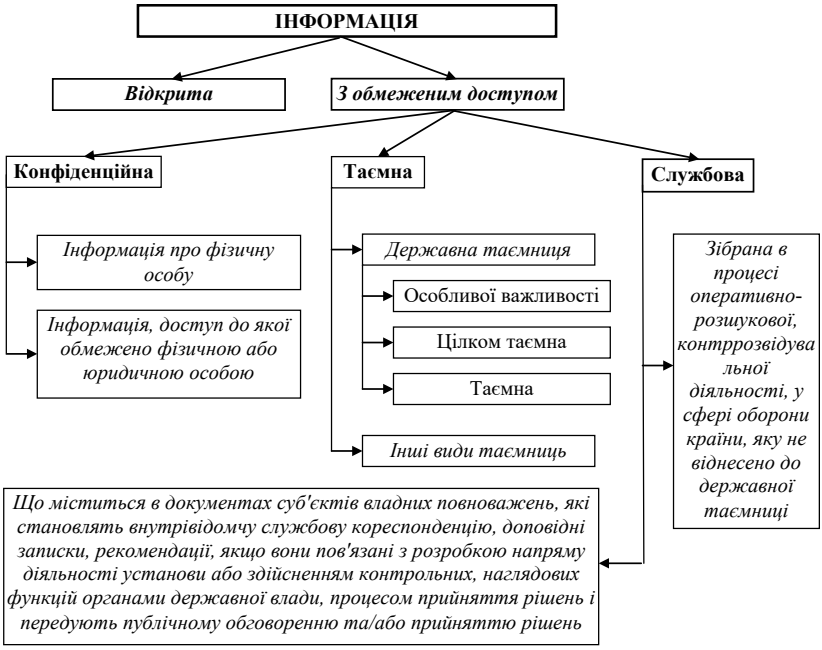


Рис. 1.5. Класифікація інформації за порядком доступу

1. **Відкрита інформація:**
   1.1. Про стан довкілля, якість харчових продуктів і предметів побуту (Закон України «Про інформацію» від 02.10.1992).
   1.2. Про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей (Закон України «Про інформацію» від 02.10.1992).
   1.3. Про стан здоров'я населення, його життєвий рівень, враховуючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення (Закон України «Про інформацію» від 02.10.1992).
   1.4. Про факти порушення прав і свобод людини, враховуючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932–1933 років в Україні й іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів (Закон України «Про інформацію» від 02.10.1992).
   1.5. Про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб (Закон України «Про інформацію» від 02.10.1992).
   1.6. Щодо діяльності державних і комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону (Закон України «Про інформацію» від 02.10.1992).
   1.7. Інші відомості, доступ до яких не може бути обмежено відповідно до законів і міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України (Закон України «Про інформацію» від 02.10.1992).
2. **Інформація з обмеженим доступом:**
   2.1. Державна таємниця (Закон України «Про державну таємницю» від 21.01.1994):

2.1.1. ***Особливої важливості***.
2.1.2. ***Цілком таємна***.
2.1.3. ***Таємна***.

2.2. Інші види таємниць:

2.2.1. ***Комерційна таємниця*** (Цивільний кодекс України від 16.01.2003).

2.2.2. ***Ноу-хау*** (Закон України «Про інвестиційну діяльність» від 18.09.1991; Податковий кодекс України від 02.12.2010).

2.2.3. ***Нерозголошувана інформація*** (Угода «Про торговельні аспекти прав інтелектуальної власності» від 15.06.1994 (TRIPS)).

2.2.4. ***Професійна таємниця*** (Кримінальний процесуальний кодекс України від 13.04.2012).

2.2.4.1. Таємниця нарадчої кімнати (Цивільний процесуальний кодекс України від 18.03.2004).

2.2.4.2. Таємниця спілкування (Кримінальний процесуальний кодекс України від 13.04.2012).

2.2.4.3. Банківська таємниця (Закон України «Про банки і банківську діяльність» від 07.12.2000).

2.2.4.4. Службова таємниця (Податковий кодекс України від 02.12.2010).

2.2.4.5. Таємниця сповіді (Кримінальний процесуальний кодекс України від 13.04.2012).

2.2.4.6. Таємниця усиновлення (Кримінальний кодекс України від 05.04.2001).

2.2.4.7. Лікарська (медична) таємниця (Закон України «Основи законодавства України про охорону здоров'я» від 19.11.1992).

2.2.4.8. Нотаріальна таємниця (Закон України «Про нотаріат» від 02.03.1993).

2.2.4.9. Адвокатська таємниця (Закон України «Про адвокатуру та адвокатську діяльність» від 05.07.2012) *тощо*.

2.3. Службова (Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету Міністрів України від 19.10.2016 № 736).

2.4. Конфіденційна інформація (Закон України «Про інформацію» від 02.10.1992):

2.4.1. ***Інформація про особу або персональні дані*** (Закон України «Про інформацію» від 02.10.1992; Закон України «Про захист персональних даних» від 01.06.2010; Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997).

2.4.2. ***Інші види конфіденційної інформації***[5].

Слід наголосити, що під час побудови системи захисту інформації часто виникають труднощі з визначенням виду інформації, яка циркулює на об'єкті інформаційної діяльності. Це обумовлено двома основними факторами:

1) *деякою неузгодженістю чинного законодавства щодо чіткого розмежування видів інформації за порядком доступу.* Прогалини у праві з цього питання створюють суперечності, які по-різному трактуються тими чи іншими правниками. Ця проблема є особливо актуальною для державних органів;

2) *великою кількістю нормативних актів, які регламентують той чи інший вид інформації.* Сьогодні виникла ситуація, наслідком якої є гальмування процесу побудови системи захисту інформації, перш за все, через складність пошуку необхідного виду інформації у величезній сукупності нормативних актів. Особливо незручним такий пошук є для спеціаліста з неюридичною освітою.

Саме через ці обставини важливо чітко орієнтуватися в нормативно-правовій базі та вміти правильно визначити вид інформації, яка потребує захисту, і в подальшому застосувати необхідні безпекові механізми.

---

[5] Манжай О. В., Нікітіна О. В. Деякі аспекти автоматизації визначення виду інформації за режимом доступу відповідно до чинного законодавства України // Інформатизація вищих навчальних закладів МВС України: матеріали науково-практичної конференції (27 квітня 2007 р.). Харків: Вид-во Харківського національного ун-ту внутр. справ, 2008. Вып. 2. С. 184–186.

3. Право на інформацію

Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій. Така вимога встановлюється ст. 5 Закону України «Про інформацію». На сьогодні в Україні право на інформацію найчастіше реалізується через інститути речового права та права інтелектуальної власності.

В окремих випадках доступ громадян до певних категорій інформації може бути обмеженим. Йдеться, передусім, про державну таємницю, адже її розголошення може завдати непоправної шкоди національним інтересам.

Існують випадки, коли інформація не може бути засекреченою, наприклад, екологічна інформація. Так, згідно зі ст. 50 Конституції України кожен має право на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди. Кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким *не може бути засекречена*. Однак у випадках воєнного або надзвичайного станів доступ до такого виду інформації може бути обмежений (ст. 64 Конституції України).

Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні й інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Важливим аспектом реалізації права на інформацію є можливість вільного доступу до правової інформації, адже саме вона містить перелік прав і обов'язків, які дозволяють особі зрозуміти сутність інформаційних прав та мати відповідне підґрунтя для їх реалізації.

Стаття 57 Конституції України чітко визначає, що в Україні кожному гарантується право знати свої права й обов'язки. Це право є абсолютним, тобто не може бути обмеженим ні за яких умов. Гарантія, прописана в наведеній нормі, забезпечується через інститут оприлюднення нормативно-правових актів, закріплений в Конституції України.

Оприлюднення відповідних нормативно-правових актів зазвичай здійснюється в офіційних друкованих виданнях. Лише в окремих випадках допускається офіційне оприлюднення актів Верховної Ради України, Президента України, Кабінету Міністрів України через телебачення і радіо.

На сьогодні існують п'ять офіційних друкованих видань:

- «Офіційний вісник України»;
- газета «Урядовий кур'єр»;
- газета «Голос України»;
- «Відомості Верховної Ради України»;
- інформаційний бюлетень «Офіційний вісник Президента України».

Такий перелік наведено у ст. 139 Закону України «Про Регламент Верховної Ради України»[6] та Указі Президента України «Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності» [7].

Акти, які не мають загального значення чи нормативного характеру, можуть не публікуватися за рішенням відповідного органу. Вони оприлюднюються шляхом надіслання відповідним підприємствам, установам, організаціям та особам, на яких поширюється їх чинність.

Закони й інші нормативно-правові акти, що визначають права і обов'язки громадян, не доведені до відома населення в порядку, встановленому законом, є нечинними.

Питання для самоконтролю

1. Універсальне поняття інформації, інформація як об'єкт правовідносин, інформаційні ресурси та процеси.
2. Юридично значущі ознаки інформації. Поняття «документ».
3. Класифікація носіїв інформації.
4. Нормативно-правова база захисту інформації.
5. Розгорнута класифікація інформації за порядком доступу.

---

[6] Про Регламент Верховної Ради України : закон України від 10.02.2010 р.; [із змінами і доповненнями на 11.01.2019]. *Офіційний вісник України*. 2010. № 12 (01.03.2010). ст. 565.

[7] Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності: указ Президента України від 10.06.1997 р.; [із змінами і доповненнями на 23.11.2007]. *Урядовий кур'єр*. 1997. № 107–108 (14.06.1997).

6. Загальні питання права на інформацію.
7. Доступ до правової інформації.

План практичної підготовки за темою:
«Загальні питання захисту інформації»

Вид: семінарське заняття.

Мета: провести гру «Дебати» за темою для виявлення та закріплення знань.

Порядок проведення заняття

1. Курсанти (слухачі) заздалегідь отримують перелік питань для підготовки та ознайомлюються з правилами гри.

2. Групу поділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).

3. Команда доповідачів називає будь-яке число в межах кількості питань для підготовки. Після цього викладач ставить питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає, то вона має право на ще одну спробу вибору питання.

4. Далі команда доповідачів протягом трьох хвилин готує розгорнуту відповідь на поставлене викладачем питання. У цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.

5. Доповідачі відповідають на питання викладача протягом п’яти хвилин. Опоненти та рецензенти в цей час корегують свої питання відповідно до відповіді доповідачів.

6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом сорока секунд і відповідають. Час відповіді необмежений.

7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом сорока секунд і відповідають. Час відповіді необмежений.

8. Рецензенти протягом трьох хвилин дають оцінку обом командам.

9. Полеміка між командами протягом п’яти хвилин.

10. Викладач ставить контрольне питання за розглянутим питанням кожній із команд.
11. Викладач оцінює якість роботи кожної з команд.

Критерії оцінювання (за п'ятибальною шкалою кожний):

– повнота й аргументованість відповідей;

– робота в команді;

– дотримання правил етикету.

12. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
13. По закінченню гри підбиваються підсумки.

План практичної підготовки за темою:
«Класифікація інформації»

Вид: семінарське заняття.

Мета: провести гру «Дебати» за темою для виявлення та закріплення знань.

Порядок проведення заняття

1. Курсанти (слухачі) заздалегідь отримують перелік питань для підготовки та ознайомлюються з правилами гри.
2. Групу розділяють на три команди.
3. Кожна команда протягом 20 хвилин готує 10 прикладів інформації та передає створений перелік іншим командам.
4. Далі команди протягом 30 хвилин вказують вид інформації, до якого належить кожен приклад, коротко обґрунтовуючи відповідь.
5. Доповідь протягом 5 хвилин кожної команди (загалом 15 хвилин).
6. Полеміка між командами протягом 10 хвилин.
7. По закінченню гри підбиваються підсумки (5 хвилин).

Тема 2. Структура та засади правового забезпечення інформаційної безпеки та кібербезпеки України

План

1. Поняття інформаційної безпеки.
2. Інформаційна війна.
3. Захист України від негативного інформаційного впливу.

1. Поняття інформаційної безпеки

25 лютого 2016 р. Президент України Указом № 47/2017 затвердив «Доктрину інформаційної безпеки України», в якій зазначено, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту і розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Інформаційна безпека держави є складовою частиною її національної безпеки. В Україні питанню забезпечення національної безпеки традиційно приділяють велику увагу. Здійснивши екскурс в історію, можна побачити, що від самого початку становлення України як незалежної держави методично ухвалювалися нормативно-правові акти, які містили безпосередні вказівки для того чи іншого напряму забезпечення національної безпеки. Серед таких актів можна назвати:

1) *Декларацію про державний суверенітет України* від 16.07.1990, що містить в собі окремі розділи «Екологічна» та «Зовнішня і внутрішня безпека»;

2) *Акт проголошення незалежності України* від 24.08.1991, в якому по суті наголошується, що одним з факторів, які спонукали до проголошення незалежності України, були інтереси національної безпеки («виходячи зі смертельної небезпеки, яка нависла над Україною в зв'язку з державним переворотом в СРСР 19 серпня 1991

року» … Верховна Рада Української Радянської Соціалістичної Республіки урочисто проголошує незалежність України»);

3) *Концепцію (основи державної політики) національної безпеки України*, затверджену Постановою Верховної Ради України від 16.01.1997 № 3/97-ВР, в якій вперше було нормативно визначено поняття національної безпеки як стану захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз, окреслено національні інтереси України, загрози національній безпеці, основні напрями та систему забезпечення національної безпеки України;

4) *Закон України «Про основи національної безпеки України»* від 19.06.2003, в якому на законодавчому рівні було закріплено засадничі принципи забезпечення національної безпеки взагалі та інформаційної безпеки зокрема.

У зв'язку з появою нових системних загроз національній безпеці 21 червня 2018 р. було ухвалено новий Закон України «Про національну безпеку України», який відобразив сучасні безпекові реалії та стратегічні напрямки розвитку сектора безпеки України.

Відповідно до п. 9 ч. 1 ст. 1 цього Закону ***національна безпека*** – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз.

Складові частини національної безпеки можна представити як на рис. 2.1.

За вказаними напрямами безпеки здійснюється планування. Документи, що містять довгострокові плани, отримали назву стратегії. Відповідно в законі описуються в загальному вигляді стратегії національної безпеки, воєнної безпеки, громадської безпеки та цивільного захисту України тощо.

Наприклад, ***Стратегія кібербезпеки України*** – це документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Більш докладно структуру вказаного документа зображено на рис. 2.2.

Рис. 2.1. Структура національної безпеки України

Рис. 2.2. Основні елементи стратегії кібербезпеки України

Слід наголосити, що в Законі України «Про національну безпеку України» не надається визначення термінів «інформаційна безпека» та «кібербезпека». На законодавчому рівні їх закріпили законами України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 та «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007.

Зокрема ***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.

Об'єктами кібербезпеки є

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

Національна поліція України як суб'єкт національної системи кібербезпеки забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі

Згідно з п. 13 розділу ІІІ Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки під ***інформаційною безпекою*** розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження,

використання і порушення цілісності, конфіденційності та доступності інформації.

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 та прогнозування загроз інформаційній безпеці, запобігання таким загрозам і 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.

Виходячи зі змісту Доктрини інформаційної безпеки України, на рис. 2.3 представлено основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.

Суб'єктами забезпечення інформаційної безпеки як складової національної безпеки України є:

– громадяни України та їх об'єднання;

– Верховна Рада України, яка серед іншого ухвалює закони у сфері інформаційної безпеки, визначаючи тим самим державну політику в цій сфері;

– Президент України, який забезпечує послідовне проведення державної інформаційної політики, інформаційний суверенітет та інформаційну безпеку України;

– Кабінет Міністрів України, який організовує діяльність виконавчої влади щодо забезпечення інформаційної безпеки;

– Рада національної безпеки і оборони України, яку очолює Президент України, координує та контролює діяльність органів виконавчої влади у сфері інформаційної безпеки України;

– інші центральні органи виконавчої влади та органи сектору безпеки і оборони України

– засоби масової інформації та інші суб'єкти, які здійснюють інформаційну діяльність;

– наукові установи та навчальні заклади, які серед іншого проводять наукові дослідження та здійснюють підготовку фахівців з інформаційної безпеки.

Рис. 2.3. Основні пріоритети забезпечення інформаційної безпеки

Ширше бачення проблеми захисту інформації дозволяє більш активно й ефективно вирішувати її, перш за все на концептуальному рівні. Держава повинна йти в ногу з розвитком сучасної науки. Саме внесення перспективних змін до законодавства України допоможе більш чітко визначитися із загальною концепцією побудови системи захисту інформації в державі, що у свою чергу

сприятиме не тільки декларуванню необхідності вирішення проблеми захисту інформації, а й вирішенню її по суті. Це стає найбільш актуальним в умовах прогресуючого з кожним роком кібертероризму.

2. Інформаційна війна

Однією з концепцій постіндустріального суспільства є концепція так званого інформаційного суспільства, яка передбачає перенесення значної частини виробництва до інформаційного сектора економіки. Відбувається перехід більшої частини робочої сили в цей сектор, побудова розгалуженої інформаційної інфраструктури, однією зі складових якої є мережа Інтернет, поступова інтеграція економіки розвинених країн. Очевидно, що з упровадженням цієї концепції активізується також інформаційне протиборство країн.

Інформаційне протиборство – це форма боротьби сторін з використанням спеціальних (політичних, економічних, дипломатичних, воєнних тощо) методів, способів і засобів для впливу на інформаційне середовище протилежної сторони та захисту власного середовища в інтересах досягнення поставлених цілей[8].

Інформаційну війну можна розглядати як найбільш агресивну форму вказаного протиборства. На сьогодні єдиного визначення поняття «інформаційна війна» не існує.

До перших офіційних документів з цієї проблеми належить директива Міністерства оборони США Т 3600.1 «Інформаційна війна» від 21.12.1992[9]. У 1997 р. було надано офіційне визначення ***інформаційної війни***, під якою розумілися дії, вжиті для досягнення інформаційної переваги в інтересах національної стратегії та реалізуються шляхом впливу на інформацію й інформаційні системи противника з одночасним захистом власної інформації та власних інформаційних систем.

---

[8] Панарин И. Н. Информационная война и геополитика. М.: Издательство «Поколение», 2006. С. 172.

[9] TS-3600.1 Information Warfare. URL: https://ia600604.us.archive.org/5/items/14F0492Doc01DirectiveTS3600.1/14F0492_doc_01_Directive_TS-3600.1.pdf (дата звернення: 11.11.2019).

Існують також інші визначення інформаційної війни. Наприклад, це цілеспрямовані інформаційні впливи, що здійснюються суб'єктами впливу на мішені (об'єкти впливу) з використанням інформаційної зброї для досягнення запланованої мети.

Тісно пов'язаним з інформаційною війною є поняття ***інформаційна зброя*** – засіб проведення запланованих дій з інформацією або алгоритм цілеспрямованого впливу на інформаційну систему шляхом передавання такій системі інформації (або здійснення з інформацією інших запланованих дій).

Форми інформаційної війни можуть бути такі:

1) командно-управлінська;
2) розвідувальна;
3) психологічна;
4) хакерська;
5) економічна;
6) електронна;
7) кібервійна[10].

Основною метою інформаційної війни є оволодіння свідомістю населення та особового складу збройних сил країни (об'єкта впливу), тобто підготовка підґрунтя для досягнення конкретних політичних, економічних і військових цілей.

Потрібно *відрізняти війну інформаційної ери від інформаційної війни*. Війна інформаційної ери використовує інформаційні технології для успішного проведення бойових операцій. Інформаційна війна розглядає інформацію як окремий об'єкт або потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активну протидію в інформаційному просторі[11].

Характерними рисами інформаційної війни є:

1) відсутність видимих фізичних руйнувань, через що оборонна реакція країни може бути запізнілою;

2) засоби ведення інформаційної війни є майже непередбачуваними, вони постійно змінюються в оперативному плані, тому варіанти протидії таким засобам мають спиратися на

[10] Панарин И. Н. Информационная война и геополитика. М.: Издательство «Поколение», 2006. С. 222-223.

[11] Леонтєва, Л. Інформаційна війна в епоху глобалізації URL: http://www.ji-magazine.lviv.ua/seminary/2000/sem13-04.htm (дата звернення: 13.03.2019).

високий інтелектуальний потенціал, зокрема аналітичні здібності, всіх ланок управління країни, що є досить складним в умовах сьогодення;

3) під час ведення інформаційної війни не обов'язково відбувається фізичне захоплення людських ресурсів, але встановлюється контроль над їх свідомістю;

4) вибірковість за принципом досягнення найбільшого ефекту, тобто інформаційна війна буде результативною, коли досягатиме реального ефекту у впливі на суб'єктів прийняття рішень у країні, щодо якої відбувається атака;

5) короткострокова інформаційна війна є малоефективною у випадку слабкої інформаційної інфраструктури країни впливу[12];

6) розуміння правди нівелюється, дискусії зводяться до абсурду, здійснюється саботаж здорового глузду;

7) вплив на хід думок супротивника з метою прийняття останнім вигідного для атакуючого рішення;

8) переведення переваг супротивника в його недоліки;

9) гра на емоціях, відволікання розуму на негідний об'єкт.

Схожою за змістом до поняття «інформаційна війна» є дефініція «*інформаційний тероризм*», які відрізняються, перш за все, суб'єктом відповідних дій. Якщо у першому випадку це держава, то у другому – це, як правило, різного виду терористичні угруповання.

Сьогодні можна спостерігати ефективне ведення інформаційної війни в мережі Інтернет. Її елементами можуть є так звані фейки – неправдиві сторінки, що містять, зокрема, інформацію з минулого, яку видають за новину дня. Фейк може бути візуальним, для чого використовуються графічні та відеоредакторами. У межах інформаційного впливу під час доведення до відома інформації використовується певний набір характеристик: видовищність, порушення звичної моделі світу, примушуюча пропаганда, «наклеювання ярликів», «тролінг» (активна участь у багатьох дискусіях під вигаданими іменами), копіпастинг. У розрізі інформаційного протиборства застосовується спеціальна термінологія, наприклад, «хом'ячки» – це довірлива та легко маніпульована частина населення, яка, на думку британських учених, є домінуючою. При цьому кожен «хом'ячок» упевнений, що

[12] Манжай О. В. Правові засади захисту інформації: навчальний-посібник. Харків : Ніка Нова, 2014. С. 25.

він розумніший за інших. Вони беруть участь в усіх флешмобах і піарах, підписують онлайн-петиції тощо[13]. Типові ознаки троля: емоційні меседжі, чіткі тези із закликами, одноманітний профіль у мережі, незначна кількість віртуальних друзів, відсутність власних постів, створена нещодавно сторінка[14].

Інформаційне протиборство залежно від виду операції здійснюється на стратегічному, оперативному або тактичному рівнях за допомогою інформаційних засобів впливу, які застосовуються з метою нанесення відповідного інформаційного або психологічного впливу на середовище.

Інформаційний вплив застосовується з метою порушення роботи та виведення з ладу різних державних систем управління і баз даних за рахунок створення електромагнітних перешкод або дезорганізації їх роботи при несанкціонованому доступі. Психологічний вплив застосовується на людську психологію відповідних груп населення, військ або людини з метою здійснення відповідної зміни за визначеною, заздалегідь спланованою схемою поведінки у відповідній частині суспільства за допомогою засобів масової інформації та інших джерел інформації, а також різних методів психологічного впливу. Засоби здійснення інформаційного впливу постійно змінюються та вдосконалюються відповідно до розвитку теорії ведення збройної боротьби[15].

Інформаційна війна складається із сукупності *інформаційних атак*, об'єднаних єдиним замислом. С. Шарма та Дж. Гупта виділяють декілька типів таких атак: соціальна інженерія, одержання віддаленого доступу за допомогою вірусів, вплив на інфраструктуру стільникового зв'язку, маніпуляція через ЗМІ, застосування електромагнітної зброї, атаки відмови в обслуговуванні, атаки на енергетичні системи та комунікації, політичний спамінг, атаки на системи управління та провайдерів[16].

---

[13] Зеленина Е. В Королевстве кривых зеркал… *Время*. Вторник. Декабрь 17 2013. № 181 (17337). С. 2.

[14] Іванцова А. Інтернет-тролі на службі в олігархів та політиків. URL: https://www.radiosvoboda.org/a/27042051.html (дата звернення: 15.03.2019).

[15] Медведєв В. К., Кучеренко Ю. Ф., Гузько Р. М. Сучасна інформаційна війна та її обрис. *Системи озброєння і військова техніка*. 2008. № 1. С. 53.

[16] Sharma S. Gupta J. N. D. Securing Information Infrastructure from Information Warfare. *Logistics Information Management*. 2002. № 15(5/6). P. 416.

Як зазначає Т. А. Пода, однією з основних ознак інформаційної атаки є різкий дисбаланс позитивних і негативних повідомлень у доборі матеріалів, відсутність коректного обговорення різних точок зору, коли у ЗМІ витісняється раціональна складова й обговорення відбувається на рівні емоцій та особистих звинувачень. Така ситуація сприяє формуванню в масовій свідомості міфів, похідних від інтересів впливових соціальних груп. У сучасному інформаційному просторі у значній кількості виникають соціальні, політичні, художні, релігійні міфи, які, незважаючи на свій ілюзорний характер, здійснюють досить реальний вплив на соціальне життя. У підсумку сучасний міф перетворився на засіб соціальної мобілізації та маніпуляції суспільною свідомістю. Істина, яку для себе визначає людина, відкривається у формі міфу, тому що у ньому концентрується певне світорозуміння, аутентичне певній культурі, і при цьому не вимагає будь-яких аргументів. Міф, який виступає як колосальне джерело масової енергії, здатний мобілізувати навіть групи людей до певних дій. Інформація, оформлена в оболонку міфу, набуває чуттєво-виразної конкретності, легко запам'ятовується, естетизуючи життєвий світ сучасної людини, кидає її в кращому випадку в обійми ілюзій, а в гіршому – робить її об'єктом різних маніпуляцій, в тому числі політичних. Масовокомунікаційний міф є найвагомішим ефектом масового спілкування, який відображає його сутність, сенс, цілі та мотивацію професійних комунікантів, пов'язану з необхідністю чинити вплив на людину та маси[17].

Емоційна складова є характерною рисою інформаційно-психологічного впливу під час інформаційної війни. Як зазначає О. Г. Ющенко, коли людина лякається, в неї перестають працювати аналітичні центри. Психовіруси розраховані на те, щоб викликати в людини паніку та страх шляхом спекуляції на базових потребах. Наприклад, панічні новини про те, що все «жахливо подорожчає» уводять особу у стан паніки, вона стає не в змозі нормально аналізувати дійсність. Коли людину «зомбують», регулярно підкидаючи їй певні ідеї, то вони приживаються як негласні аксіоми.

[17] Пода Т. А. Інформаційна війна як стратегія формування політичної свідомості(соціально-філософський аналіз). *Вісник Національного авіаційного університету*. Сер. : Філософія. Культурологія. 2014. № 1. С. 69.

Така людина буде вкрай важко сприймати будь-які нові ідеї, якщо вони входять у конфлікт з укоріненими старими[18].

Інколи, вивчаючи елементи інформаційної війни, говорять про інформаційну експансію. Однак *інформаційна експансія*, як зазначає О. Саприкін, є технологією набагато місткішою, ніж інформаційна війна або інформаційна атака. Власне ці терміни можна вважати складовими інформаційної експансії. У свою чергу, терміном «інформаційна експансія» позначають систему, що склалася в засобах інформації розвинених держав, і методи, використані для пропагандистського забезпечення певних геополітичних цілей. Інформаційну експансію можуть створювати та поширювати як державні органи (за допомогою державних і приватних інформаційних установ і заходів), так і транснаціональні корпорації для досягнення власної вигоди: забезпечення ринку збуту, участі у великих міжнародних тендерах, доступу до дешевої сировини і робочої сили, з метою досягнення політичних та військових цілей тощо[19].

Одним з інструментів ведення інформаційної війни є пропаганда. В. Яковлев[20] розрізняє такі її методи:

– *«гнилий оселедець»*. Використовується проти конкретної особи або групи осіб, стосовно яких висуваються неправдиві звинувачення, які мають бути якомога скандальнішими (розбещення дітей, убивство з корисливих мотивів тощо). Метою обвинувачення є виклик широкого обговорення несправедливості, неправдивості обвинувачення. Поступово згадування об'єкта у зв'язку зі скандалом наростає та немовби в'їдається в його одяг, залишаючи за ним шлейф «гнилого оселедця». Таким чином, під час згадування імені об'єкта він постійно асоціюється з брудним скандалом;

– *«перегорнута піраміда»* є прийомом створення текстів, коли пріоритетність інформації зменшується від початку тексту до його

[18] Ющенко А. Г. Украина обязана выиграть информационную войну. *Україна третє тисячоліття*. 2014. № 3. С. 22.

[19] Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати*. 2013. № 1. С. 40.

[20] Яковлев В. «Гнилая селедка», «большая ложь», «40 на 60» — Владимир Яковлев о приемах пропаганды. URL: https://www.stopfake.org/gnilaya-seledka-bolshaya-lozh-40-na-60-vladimir-yakovlev-o-priemah-propagandy/ (дата звернення: 15.03.2019).

закінчення. Цим досягається приковування уваги до гучного початку матеріалу. Об'єкт впливу може не дочитувати матеріал до кінця, проте основний посил залишиться в його пам'яті;

– *«велика брехня»* полягає в тому, що аудиторії впевнено пропонується скомпонована та добре продумана велика брехня, здатна викликати емоційну травму. Це така глобальна та страшна брехня, коли практично неможливо повірити, що можна брехати про таке (наприклад, інформація про розп'ятого хлопчика);

– *«40 на 60»* полягає в донесенні інформації, в якій 60 % інформації дається на користь супротивника, а інші 40 % – на користь суб'єкта інформаційного впливу. Перша частина інформації спрямована на заслуговування довіри супротивника, друга – на донесення дезінформації;

– *«абсолютна очевидність»* спрямована на створення у групи людей ефекту приєднання. Інформація, яку планується впровадити в маси, не доказується, а позиціонується як очевидний факт, що підтримується більшістю людей. Незважаючи на свою простоту, цей метод є дуже ефективним, оскільки людська психіка автоматично реагує на думку більшості, намагаючись долучитися до неї. Більшість має бути переважаючою, а її підтримка абсолютною та безумовною, в іншому випадку ефект приєднання буде відсутнім. Найбільш вразливими до ефекту приєднання є представники низьких соціальних прошарків.

Нерідко інформаційна війна відбувається разом зі звичайною або *гібридною*, що можна було спостерігати під час військових дій на Балканах у 1990-ті роки, в Іраці на початку XXI ст., в Естонії у 2007 р., в Грузії у 2008 р., в Україні з початку 2014 р.

Щодо останнього доречно навести думку авторів монографії «Світова гібридна війна: український фронт», які небезпідставно вважають, що «інформаційний складник гібридної війни став наскрізним для всієї російської агресії в її активній фазі. Спираючись на потужну багаторічну підготовку та інформаційно-психологічну обробку громадян України, часткове скуповування українських ЗМІ (в тому числі загальнонаціональних), використання стратегічного контенту (книги, телесеріали, фільми, псевдонаукові та наукові дослідження тощо), активну кампанію в соціальних мережах, Росії на перших етапах агресії вдавалося істотно дезорганізувати населення України, грати на багаторічних деструктивних тематиках, зменшити підтримку громадянами дій

керівництва держави в умовах неоголошеної війни. Крім того, безпосередньо в зоні конфлікту супротивник застосовував (і застосовує) методи радіоелектронної боротьби, захоплення телекомунікаційних об'єктів, а також здійснює частково успішні кібератаки проти державних органів чи об'єктів критичної інфраструктури»[21].

Що стало передумовою для ефективного ведення інформаційної війни проти України у 2014 році? Декілька причин цього явища були викладені С. П. Смольцем, який у 2011 році відзначав, що соціальна апатія, песимізм переважають в українському (і не тільки) суспільстві. Падіння якості та престижності освіти, небажання навчатися, розвиватися, викривлення життєво-світоглядних орієнтирів стали причинами різкого зростання безграмотності населення, незважаючи на збільшення кількості осіб, які отримали дипломи про вищу освіту. Зростання загальної пасивності в суспільно-політичному житті, повна деградованість політичних еліт. Відповідно ми отримуємо інертне суспільство з пасивними громадянами. Все це є наслідком тоталітарного минулого нашого суспільства та тих інформаційних впливів на його суспільну свідомість, яких воно зазнавало і продовжує зазнавати. Таким чином, деструктивні установки, закладені у свідомості, спричинили зміни в суспільному бутті, моделях поведінки[22].

Наведені причини не є вичерпними, проте їх усунення сприятиме оздоровленню вітчизняного інформаційного простору та створить передумови для провадження ефективної національної інформполітики всередині країни.

Для ефективної протидії інформаційній війні потрібно регулярно вживати заходів протидії. Велика роль у вирішенні цього завдання відводиться засобам масової інформації. Саме факти, які висвітлюють медіа, акценти на певні явища чи аспекти протистояння, як стверджує М. О. Кондратюк, формують думку аудиторії про конфлікт, стимулюючи до потрібної реакції. Засоби масової інформації дають можливості перетворити маленький

[21] Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. К. : НІСД, 2017. С. 262.

[22] Смольц С. П. Інформаційна війна як чинник формування суспільного буття. *Вісник Національного технічного університету України «Київський політехнічний інститут»*. Філософія. Психологія. Педагогіка. 2011. № 3. С. 73.

конфлікт на велике протистояння або швидко нівелювати серйозну проблему. Саме від ставлення медіа до події, їхньої упередженості та заангажованості значною мірою залежить перебіг самого конфлікту [23].

Значу роль у протидії інформаційній війні відіграють громадськість, особи з активною життєвою позицією, які через мережу Інтернет доносять інформацію, відмінну від тієї, яка нав'язується суспільству ззовні. Тут можна згадати як досвід Грузії[24], так і сучасний досвід України щодо створення проукраїнських і викриваючих інтернет-ресурсів (http://www.stopfake.org/) тощо.

Інформаційні ресурси подекуди самі можуть ставати інструментом маніпуляції та ведення інформаційної війни. Особливо це актуально для тих ресурсів, які не проводять ретельний аналіз наданих їм даних на достовірність. Б. Буткевич[25] наводить таку схему: через спеціально-створений ресурс запускається недостовірна інформація → цю інформацію без перевірки публікують інші засоби масової інформації та інформаційні ресурси країни → ЗМІ іншої країни, зацікавленої у проведенні інформаційної операції, викривають представлену інформацію як недостовірну, тим самим формуючи суспільну думку як у своїй країні, так і в державі – цілі проведення інформаційної операції.

У 2018 р. О. Юркова на підставі сучасного практичного досвіду представила декілька способів створення недостовірних новин[26]. Серед них:

1. Маніпуляції з медіа-даними:

– редагування;

---

[23] Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах. *Вісник Харківської державної академії культури*. 2013. Вип. 41. С. 112-113.

[24] Osepashvili D. New Media and Russian-Georgian August 2008 War. *Journalism and Mass Communication*. 2014. Vol. 4, No. 6. P. 365.

[25] Буткевич Б. Фабрика фейков. Какую угрозу несут сайты-паразиты. URL: https://vlada.io/articles/fabrika-feykov-kakuyu-ugrozu-nesut-saytyi-parazityi/ (дата звернення: 15.03.2019).

[26] Yurkova O. Six Fake News Techniques and Simple Tools to Vet Them. URL: https://gijn.org/six-fake-news-techniques-and-simple-tools-to-vet-them/ (дата звернення: 08.04.2019).

– подання справжніх медіа-даних в іншому контексті, зміна часу і місця їх створення;

– створення повністю недостовірного медіа-контенту.

2. Маніпулювання новинами:

– викривлення сенсу заголовків новин;

– подання окремої думки як факту;

– викривлення фактів;

– подання повністю недостовірної інформації як факту;

– ігнорування важливих деталей, які змінюють контекст.

3. Маніпулювання експертними оцінками:

– використання думок псевдоекспертів (несправжніх експертів, експертів в інших сферах тощо) та аналітичних центрів;

– перекручування заяв експертів або приписування видуманих заяв справжнім експертам;

– викривлення перекладу.

4. Маніпулювання повідомленнями:

– використання повідомлень маргінальних суб'єктів;

– перекручування реальних повідомлень з авторитетних джерел;

– посилання на неіснуючі повідомлення з авторитетних джерел.

5. Маніпуляції з результатами досліджень:

– використання слабкої або несправжньої методології;

– невірна інтерпретація результатів;

– неправильні порівняння.

У цій же праці було розкрито методи та інструменти викриття подібного виду підробок.

Корисними також вважаємо розроблені для бізнесу рекомендації з протидії негативу в інформаційному просторі, які можуть бути адаптовані до більш широкого вжитку[27].

Найбільш складним і часовитратним, проте достатньо ефективним методом протидії інформаційній війні, на нашу думку, є підвищення аналітичних здібностей суспільства, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій.

[27] Противодействие негативу в информационном пространстве: методические рекомендации / З. Чистяков, М. Шпаченко. Агентство конфликтного PR - /PR і Z/, 2012. 32 с.

Наведене також дає підстави говорити про необхідність активізації в нашій країні зусиль з розбудови ефективної структури інформаційного протиборства.

Шляхами вирішення цього питання можуть бути:

1) діяльність волонтерів з моніторингу медіа-ресурсів на наявність матеріалів, які містять згубний інформаційний вплив. Це може бути, наприклад, відслідковування матеріалів, в яких містяться заклики до порушення територіальної цілісності, насильницького повалення конституційного ладу тощо. За результатами моніторингу відповідна інформація має доводитися до правоохоронних органів за належністю;

2) заохочення громадськості до створення ресурсів з викриття неправдивих інформаційних повідомлень, а також доведення результатів у доступній формі до населення;

3) формування пропозицій до чинного законодавства органам законодавчої та виконавчої влади щодо вдосконалення системи інформаційної безпеки країни;

4) доведення до мешканців країни, яка чинить деструктивний інформаційний вплив, правдивої інформації та створення умов для критичного аналізу громадянами цієї країни відомостей з відповідних медіа;

5) адаптація сучасних методик інформаційного протиборства до вітчизняних реалій і надання рекомендацій щодо їх застосування відповідним державним органам.

Враховуючи наведене, можна зробити висновок, що протидія інформаційній війні й інформаційному тероризму є одним з напрямів забезпечення інформаційної безпеки як складової частини національної безпеки держави. Механізми протидії зазначеним загрозам мають бути високотехнологічними та мати системний характер[28].

3. Захист України від негативного інформаційного впливу

Проблема захисту від інформаційно-психологічного впливу складається з таких основних аспектів:

[28] Носов В .В., Манжай О. В. Окремі аспекти протидії інформаційній війні в Україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. № 1(29). С. 26-29.

– інформаційна безпека індивідуальної, групової та суспільної свідомості у сфері комерційної реклами;

– інформаційна безпека індивідуальної, групової та суспільної свідомості від впливу відео-, аудіо- і друкованих творів, комп'ютерних програм та ігор тощо;

– інформаційна безпека громадян як суб'єктів політичного процесу.

У перших двох випадках проблема інформаційної безпеки охоплює саме можливість провокування в людини певних несвідомих дій або дій, які не ґрунтуються на власному розсуді, досягнення яких було метою інформаційного впливу, а також побічних ефектів: певних протиправних дій або дій, які створюють небезпеку самій особі або третім особам, суспільству, досягнення яких не було метою інформаційного впливу, але було ним спровоковане.

Розглянемо окремо кожну з наведених складових захисту від негативного інформаційного впливу.

Для першого випадку основним нормативно-правовим актом, в якому детально прописано механізм розповсюдження комерційної реклами, є Закон України «Про рекламу» від 03.07.1996.

Стаття 7 цього закону закріплює основні принципи реклами, серед яких:

– законність;

– точність;

– достовірність;

– використання форм і засобів, які не завдають споживачеві реклами шкоди.

Крім того, в цій же статті наголошується, що реклама не повинна підривати довіру суспільства до реклами, містити інформацію або зображення, які порушують етичні, гуманістичні, моральні норми, нехтують правилами пристойності, та повинна відповідати принципам добросовісної конкуренції, враховувати особливу чутливість дітей і не завдавати їм шкоди.

Вимоги до реклами, що безпосередньо захищають особу від негативного інформаційного впливу, викладені в ст. 8 Закону України «Про рекламу». Зокрема, забороняється:

– поширювати інформацію щодо товарів, виробництво, обіг чи ввезення на митну територію України яких заборонено законом;

– вміщувати твердження, які є дискримінаційними за ознаками походження людини, її соціального і майнового стану, расової та національної належності, статі, освіти, політичних поглядів, ставлення до релігії, за мовними ознаками, родом і характером занять, місцем проживання, а також такі, що дискредитують товари інших осіб;

– подавати відомості або закликати до дій, які можуть спричинити порушення законодавства, завдають чи можуть завдати шкоди здоров'ю або життю людей та/чи довкіллю, а також спонукають до нехтування засобами безпеки;

– використовувати засоби і технології, які діють на підсвідомість споживачів реклами;

– наводити твердження, дискримінаційні щодо осіб, які не користуються рекламованим товаром;

– вміщувати зображення фізичної особи або використовувати її ім'я без письмової згоди цієї особи;

– розповсюджувати рекламу (враховуючи анонси кіно- і телефільмів), яка містить елементи жорстокості, насильства, порнографії, цинізму, приниження людської честі та гідності. Анонси фільмів, які мають обмеження щодо глядацької аудиторії, розміщуються лише у час, відведений для показу таких фільмів.

У Законі України «Про рекламу» також встановлюються певні заборони, що мають на меті захист дитячої аудиторії, серед яких *заборона* реклами з: використанням зображень дітей, які споживають або використовують продукцію, призначену тільки для дорослих чи заборонену законом для придбання або споживання неповнолітніми; інформацією, яка може підірвати авторитет батьків, опікунів, піклувальників, педагогів і довіру до них дітей; уміщенням закликів до дітей придбати продукцію або звернутися до третіх осіб з проханням зробити покупку; використанням зображень справжньої або іграшкової зброї, вибухових пристроїв.

Також реклама не повинна завдавати дітям моральної чи фізичної шкоди, викликати в них відчуття неповноцінності та містити зображення дітей у небезпечних ситуаціях чи за обставин, що в разі їх імітації можуть завдати шкоди дітям або іншим особам, а також інформації, здатної викликати зневажливе ставлення дітей до небезпечних для здоров'я і життя ситуацій.

Таким чином, законодавець встановив низку вимог, які утворюють систему інформаційної безпеки громадян під час

розповсюдження рекламної продукції. Ця система не є самодостатньою, паралельно з нею мають функціонувати інші захисні механізми, які дозволятимуть повною мірою вирішувати завдання державної політики з питань національної безпеки, передбачені Законом України «Про національну безпеку України».

Механізм притягнення до відповідальності за порушення законодавства про рекламу передбачено Порядком накладення штрафів за порушення законодавства про рекламу, затвердженим Постановою Кабінету Міністрів України від 04.10.2012 № 693. Для доведення порушення законодавства про рекламу потрібно одержати відповідні експертні висновки. Їх, зокрема, надають Всеукраїнська рекламна коаліція, Індустріальний гендерний комітет з реклами та Експертна рада (з питань розгляду звернень за фактами дискримінації за ознакою статі) при Мінсоцполітики. У разі доведення порушення накладання штрафу здійснює Держспоживінспекція. Підставою для розгляду справи про порушення законодавства про рекламу є відповідний протокол, складений уповноваженою посадовою особою Антимонопольного комітету, Національної ради з питань телебачення і радіомовлення, Мінфіну, НКЦПФР або Держспоживінспекції та її територіальних органів.

Як приклад реалізації описаного механізму можна навести випадок, який стався в Харківській області. Так, у Харківському обласному територіальному відділенні Антимонопольного комітету України[29] повідомили, що Харківський молочний завод на обгортках з назвами «Масло солодковершкове “Селянське” 73 % (Новобаварське)» та «Масло солодковершкове селянське 73 % ТМ “Гаврюша”» поширив неправдиві відомості про вид продукту. Під обгорткою виявили немолочні жири. Згідно з чинним законодавством масло має містити тільки молочні жири. Рослинні жири можуть бути у складі спреду або маргарину. Таким чином, молочний завод поширив неправдиві відомості та інформацію, що вводить в оману. Дії заводу кваліфікували за ст. 15-1 Закону України «Про захист від недобросовісної конкуренції» (поширення інформації, що вводить в оману).

[29] Маргарин під виглядом масла виробляли у Харкові. URL: https://kharkov.comments.ua/news/margarin-pid-vigljadom-masla-virobljali-u-harkovi-/ (дата звернення: 09.12.2019).

Друга складова захисту від негативного інформаційного впливу передбачає *інформаційну безпеку індивідуальної, групової та суспільної свідомості від впливу відео-, аудіо- і друкованих творів, комп'ютерних програм та ігор* тощо.

Така безпека забезпечується вимогами законів України:

– «Про видавничу справу» від 05.06.1997;

– «Про культуру» від 14.12.2010;

– «Про телебачення і радіомовлення» від 21.12.1993;

– «Про кінематографію» від 13.01.1998;

– «Про захист суспільної моралі» від 20.11.2003;

– «Про оперативно-розшукову діяльність» від 18.02.1992 тощо.

Так, у ст. 9 Закону України «Про оперативно-розшукову діяльність» вказується, що для одержання інформації забороняється застосовувати технічні засоби, психотропні, хімічні та інші речовини, які пригнічують волю або завдають шкоди здоров'ю людей і навколишньому середовищу.

Закон України «Про захист суспільної моралі» є одним із системозабезпечуючих нормативно-правових актів у сфері захисту від негативного інформаційного впливу. Зокрема, у 2010 р. до вказаного закону було внесено низку суттєвих змін, що посилюють боротьбу з дитячою порнографією в Україні.

У ст. 2 згаданого закону міститься заборона на виробництво та розповсюдження продукції, яка:

– пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України;

– пропагує фашизм і неофашизм;

– принижує або ображає націю чи особистість за національною ознакою;

– пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святинь;

– принижує особистість, є проявом знущання з приводу фізичних вад (каліцтва), з душевнохворих, літніх людей;

– пропагує невігластво, неповагу до батьків;

– пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички.

Більшість цих вимог у тій чи іншій формі викладені також в інших наведених законах.

З метою реалізації та додержання вимог чинного законодавства у сфері захисту суспільної моралі, обігу продукції та видовищних заходів сексуального чи еротичного характеру, продукції, що містить пропаганду культу насильства, жорстокості і порнографії, було створено Національну експертну комісію України з питань захисту суспільної моралі. Рішення Національної комісії, ухвалені в межах її повноважень, є обов'язковими для розгляду центральними і місцевими органами влади, засобами масової інформації всіх форм власності, а також фізичними та юридичними особами.

Інформаційна безпека громадян як суб'єктів політичного процесу досягається, перш за все, вимогами, встановленими в Конституції України, що стосуються волевиявлення громадян. Крім того, вона забезпечується Виборчим кодексом України від 19.12.2019, законами України «Про Центральну виборчу комісію» від 30.06.2004, «Про державний реєстр виборців» від 22.02.2007 тощо.

Так, наприклад, ст. 21 Виборчого кодексу України визначає основні засади виборчого процесу, однією з яких є дотримання рівного доступу всіх кандидатів і суб'єктів їх висування на відповідних виборах до засобів масової інформації незалежно від їх форми власності, крім засобів масової інформації, засновниками яких є партії (організації партій).

Підсумовуючи викладене, зауважимо, що захист від негативного інформаційного впливу не повинен порушувати право людини на інформацію, тому у визначенні того чи іншого інформаційного продукту шкідливим потрібно бути дуже обережним та не допускати порушення свободи слова під егідою боротьби за чистоту моралі.

Питання для самоконтролю

1. Історія становлення системи національної безпеки України.
2. Складові частини національної безпеки України.
3. Визначення понять «інформаційна безпека» та «кібербезпека».
4. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
5. Основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.

6. Поняття інформаційної війни.
7. Форми та мета ведення інформаційної війни.
8. Відмінні риси інформаційної війни.
9. Інформаційна безпека індивідуальної, групової та суспільної свідомості у сфері комерційної реклами.
10. Інформаційна безпека індивідуальної, групової та суспільної свідомості від впливу відео-, аудіо- і друкованих творів, комп'ютерних програм та ігор тощо.
11. Інформаційна безпека громадян як суб'єктів політичного процесу.

План практичної підготовки за темою:
«Протидія інформаційній війні»

Вид: семінарське заняття.
Мета: відпрацювати навички аналізу інформації.

Вхідні дані
Пропагандистські ресурси

Порядок проведення заняття

1. Групу поділяють на три команди.
2. Кожна команда виконує такі завдання:

– додатково до теоретичного матеріалу ознайомитися з методикою перевірки фактів, викладеною за посиланням https://gijn.org/2018/08/20/шесть-способов-создания-фейковых-нов-2/;

– проаналізувати одну зі статей на пропагандистському ресурсі. Виявити ознаки маніпуляції, викривлення фактів тощо. Сформулювати аналітичний висновок;

– доповісти результати.

3. Підбиваються підсумки.

План практичної підготовки за темою:
«Захист від негативного інформаційного впливу»

Вид: практичне заняття.
Мета: розв'язання задач.
Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Розв'язання задач (60 хв).
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Задача № 1

У телепередачі «Здорова їжа» ведучий, демонструючи приготування страв, цілеспрямовано звертав увагу телеглядачів на декілька продуктів, потрібних для приготування. При цьому він постійно згадував спеціальний засіб «Т» – одну з дуже корисних для здоров'я сучасних добавок.

Перегляд цієї передачі викликав у фірми «Фітнес» інтерес до продукту «Т», який вона купила для постачання іншим компаніям. Пізніше було встановлено, що добавка «Т» належить до лікарських рецептурних засобів. Деякі клієнти фірми, вживаючи продукт «Т», одержали алергічні розлади, що було зафіксовано лікарями.

У результаті керівництво фірми «Фітнес» звернулося до суду з позовом до телевізійної компанії, зажадавши від неї компенсацію моральних збитків і відшкодування шкоди, заподіяної здоров'ю своїх клієнтів. Крім того, керівництво фірми «Фітнес» звернулося до Держспоживінспекції зі скаргою.

Як необхідно кваліфікувати дії ведучого та чи правомірні вимоги фірми «Фітнес»?

Відповідь: дивіться Закон України «Про рекламу», Цивільний кодекс України, Порядок накладення штрафів за порушення законодавства про рекламу, затверджений Постановою Кабінету Міністрів України від 04.10.2012 № 693.

Задача № 2

Адміністрація Енської області з метою недопущення публікації неперевіреної інформації про стан справ в області та підсилення контролю за функціонуванням підвідомчих служб ухвалила рішення про додаткове уточнення і перевірку всіх матеріалів з цієї тематики, що підлягають публікації в місцевих засобах масової інформації.

Оцініть законність рішення, ухваленого адміністрацією Енської області.

Відповідь: дивіться Конституцію України, закони України «Про друковані засоби масової інформації (пресу) в Україні», «Про інформацію», «Про доступ до публічної інформації».

Задача № 3

Журналісти молодіжного відділу газети підготували добірку листів читачів, велика частина яких підтримувала погляди легально діючих у країні політичних партій. Цю добірку планували опублікувати окремим додатком до газети і вже направили до друкарні. Проте директор друкарні відмовився друкувати вказаний додаток. Він мотивував свою відмову тим, що до нього звернувся голова адміністрації області і попросив не публікувати матеріали, які можуть призвести до поляризації місцевих політичних сил напередодні виборів.

Чи відповідають закону офіційне звернення голови адміністрації і рішення самого голови друкарні?

Відповідь: дивіться Конституцію України, закони України «Про друковані засоби масової інформації (пресу) в Україні», «Про інформацію», «Про доступ до публічної інформації».

Задача № 4

На закритому хімічному підприємстві, розташованому у межах міста та поблизу державного кордону, в результаті аварії відбувся викид шкідливих речовин в атмосферу. Обласна адміністрація вжила необхідних заходів з евакуації населення із заражених місць і запобігання витоку небажаної інформації про аварію. При цьому вона заборонила керівництву підприємства передавати ЗМІ і фахівцям інформацію про масштаби аварії та відомості, які стосуються життя населених пунктів, що входять до зони досяжності розповсюдження шкідливих речовин. Одночасно

адміністрація, ухвалюючи рішення про нерозповсюдження вказаної інформації, посилалася на закритість виробництва хімічного підприємства.

Чи правомірні дії адміністрації?

Відповідь: дивіться Конституцію України, Конвенцію «Про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля» від 25.06.1998 (ратифікована Верховною Радою України 06.07.1999), закони України «Про друковані засоби масової інформації (пресу) в Україні», «Про інформацію», «Про доступ до публічної інформації».

Задача № 5

Наприкінці року по телебаченню повідомили, що всі борги по зарплаті працівникам бюджетної сфери погашені. У цей час у деяких районах Енської області вчителі оголосили страйк у зв'язку з невиплатою заробітної платні за останні чотири місяці. Журналіст Воронцов звернувся до адміністрації Енської області з проханням надати йому документи, що містять докладні відомості про використання бюджетних коштів області за минулий рік. Йому в цьому проханні відмовили, посилаючись на те, що запрошувана інформація має обмежений доступ. Журналіст написав скаргу.

Чи має рацію Воронцов? Необхідно дати інформаційно-правову оцінку позиції адміністрації області.

Відповідь: дивіться Конституцію України, закони України «Про друковані засоби масової інформації (пресу) в Україні», «Про інформацію», «Про доступ до публічної інформації».

Задача № 6

Хімічний комбінат м. Енська здійснив викид отруйних речовин у місцеву річку. Міська влада, одержавши від представника Державної екологічної інспекції відповідну інформацію, не оповістили громадян про небезпеку. У результаті купання в річці шестеро дітей одержали серйозні шкірні захворювання.

Хто повинен нести відповідальність за приховування інформації? Яка це має бути відповідальність?

Відповідь: дивіться Конституцію України, Конвенцію «Про доступ до інформації, для громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля» від

25.06.1998 (ратифікована Верховною Радою України 06.07.1999), закони України «Про друковані засоби масової інформації (пресу) в Україні», «Про інформацію», «Про доступ до публічної інформації», Кримінальний кодекс України.

Задача № 7

Головний редактор філіалу іноземного журналу дав завдання журналісту зібрати дані для статті про стан води в місцевій річці. Журналіст звернувся до місцевого державного науково-дослідного інституту зі зразками води для експертизи. Дані експертизи показали значний вміст шкідливих речовин. Працівники інституту також повідомили журналіста, що єдине підприємство, яке проводить роботу з відповідними хімічними речовинами в регіоні, є фірма «Алмаз».

Після отримання результатів аналізу журналіст звернувся до органу місцевого самоврядування із запитом щодо надання інформації про це підприємство. Відповідь на свій запит журналіст отримав через 1,5 місяці, причому ця інформація не відповідала дійсності.

Через 2 місяці журналіст звернувся до фахівців архіву й аудиторської фірми, де за окрему плату йому допомогли знайти інформацію стосовно шкідливих речовин, виявлених у річці, дані про грошові перекази на проведення дослідів із цими речовинами та розподілення прибутку від утилізації шкідливих речовин. Знайдені документи журналіст сфотографував, після чого підготував статтю з оціночними судженнями про діяльність підприємства, що проводить досліди зі шкідливими речовинами. У кінці статті журналіст навів фотографії документів, зроблені ним в архіві.

Наступного дня до редакції прибув посадовець органу місцевого самоврядування та заборонив публікацію інформації, що була отримана, на його думку, з порушенням чинного законодавства про інформацію.

Дайте правову оцінку ситуації. Чи є правомірними дії журналіста та посадовця органу місцевого самоврядування?

Відповідь: дивіться Конституцію України, Конвенцію «Про доступ до інформації, для громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля» від 25.06.1998 (ратифікована Верховною Радою України 06.07.1999), закони України «Про порядок висвітлення діяльності органів державної влади

та органів місцевого самоврядування в Україні засобами масової інформації», «Про друковані засоби масової інформації (пресу) в Україні», «Про інформацію», «Про доступ до публічної інформації».

Задача № 8

26 липня громадянин, який проживає в місті К., звернувся до органів виконавчої влади м. С. із запитом про надання йому можливості ознайомлення з усіма документами, що стосуються діяльності міської влади та особисто мера міста С. з ремонту міського стадіону. Актуальність цього питання виникла після офіційної заяви мера про те, що він бере під свій особистий контроль будівельні роботи на стадіоні. Цю заяву мер зробив 20 липня по місцевому телебаченню.

30 липня запитувачу інформації зателефонувала секретар мера та повідомила про відмову в наданні даних через те, що запитувач не є мешканцем міста С.

Дайте правову оцінку ситуації. Чи правомірною була відмова в наданні даних? Чи зміниться відповідь у випадку, якщо запитувача зробити запит попросив його приятель, що мешкає в місті С.? Яку інформацію повинен містити запит про надання можливості ознайомлення з офіційними документами?

Відповідь: дивіться Конституцію України, закони України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про інформацію», «Про доступ до публічної інформації», «Про звернення громадян».

Тема 3. Правові засади захисту інтелектуальної власності

План

1. Об'єкти інтелектуальної власності.
2. Характеристика окремих об'єктів промислової власності.
3. Авторське та суміжне право.

1. Об'єкти інтелектуальної власності

Історія становлення інтелектуальної власності сягає у глибину століть. Багато вчених-цивілістів вважають, що вона бере початок у середньовічній Англії. Вперше термін «інтелектуальна власність» у правовому контексті вжив у 1845 р. суддя Окружного суду штату Массачусетс Чарльз Вудбарі.

Знаковою подією, яка сприяла розвитку інтелектуальної власності, стало заснування у 1967 р. Всесвітньої організації інтелектуальної власності, про що було підписано відповідну Конвенцію у м. Стокгольм. У ст. 2 цієї Конвенції визначено об'єкти, стосовно яких використовується право інтелектуальної власності (рис. 3.1).

В Україні питанню захисту інтелектуальної власності на законодавчому рівні приділено значну увагу, зокрема в законах України «Про авторське право і суміжні права» від 23.12.1993[30], «Про охорону прав на винаходи і корисні моделі» від 15.12.1993[31], Податковому кодексі України від 02.12.2010[32], Кримінальному

[30] Про авторське право і суміжні права: закон України від 23.12.1993; [із змінами і доповненнями на 04.11.2018]. *Офіційний вісник України*. 1993. № 12 (01.03.1993). ст. 234.

[31] Про охорону прав на винаходи і корисні моделі: закон України від 15.12.1993; [із змінами і доповненнями на 05.12.2012]. *Офіційний вісник України*. 1993. № 12 (01.03.1993). ст. 204.

[32] Податковий кодекс України від 02.12.2010; [із змінами і доповненнями на 01.03.2019]. *Офіційний вісник України*. 2010. № 23 (23.12.2010). ст. 543.

кодексі України від 05.04.2001[33] тощо. Ключові положення права інтелектуальної власності викладено у Четвертій книзі Цивільного кодексу України.

Рис. 3.1. Об'єкти права інтелектуальної власності

Загальну структуру інтелектуальної власності України можна представити як на рис. 3.2.

[33] Кримінальний кодекс України від 05.04.2001; [із змінами і доповненнями на 26.02.2019]. *Офіційний вісник України*. 2001. № 17 (18.04.2001). ст. 432.

Рис. 3.2. Структура інтелектуальної власності за законодавством України

2. Характеристика окремих об'єктів промислової власності

Розглянемо деякі, найбільш поширені об'єкти права інтелектуальної власності більш докладно.

Двома найбільшими групами об'єктів інтелектуальної власності є промислова власність та об'єкти авторських і суміжних прав. Якщо перший напрям правового захисту забезпечує охорону ідей, викладених у певній формі, то другий навпаки охороняє форму викладення певних ідей.

Одними з найпоширеніших об'єктів промислової власності є винахід і корисна модель. Для здійснення правової охорони на ці об'єкти може бути одержано патент. Отриманню патенту передує ретельна оцінка комерційної цінності нового винаходу або корисної моделі та здійснення відповідного патентного пошуку.

Для того, щоб винахід був патентоздатним, він повинен відповідати трьом критеріям:

– бути *новим* (не є частиною рівня техніки);

– бути *промислово придатним* (способи отримання результату мають дозволяти практичне використання);

– мати достатній *винахідницький рівень* (суб'єктивна ознака, яка випливає з існуючого рівня техніки).

Для патентоздатності корисної моделі достатньо виконання перших двох умов.

Об'єктами винаходу та корисної моделі можуть бути *продукт* (пристрій/машини, прилади, …/, речовина/продукти ядерного перетворення, індивідуальні хімічні сполуки, …/ тощо) або *спосіб*. При цьому не можуть бути визнані такими об'єктами відкриття, комп'ютерні програми, різного виду плани, розклади, умовні позначення, топографії інтегральних мікросхем тощо.

Промисловий зразок здебільшого знаходиться поряд із дизайнерським мистецтвом, оскільки є творчим естетичним зразком у сфері художнього конструювання. Критеріями патентоздатності промислового зразка є новизна та промислова придатність. На промисловий зразок видається патент. При цьому внутрішня конструкція промислового зразка не підпадає під охорону, охороняється лише зовнішня форма. Прикладом промислового зразка може бути корпус мобільного телефону, форма пляшки тощо. Об'єктами промислового зразка є малюнки, форми, розфарбування та їх поєднання.

Не можуть бути визнані промисловими зразками друкована продукція як така, об'єкти архітектури за окремими виключеннями тощо.

Ще одним об'єктом промислової власності є знак для товарів і послуг, правова охорона якого засвідчується свідоцтвом. Знаки для товарів і послуг можуть бути словесними, візуальними, об'ємними або комбінованими.

Не можуть бути визнанні знаками для товарів і послуг різного виду нагородні відзнаки, державні герби, прапори і емблеми, емблеми, скорочені або повні найменування міжнародних міжурядових організацій, офіційні назви держав, офіційні печатки, клейма тощо.

3. Авторське та суміжне право

Процедура отримання авторського права та/або суміжних прав на творчі об'єкти є набагато простішою за аналогічну процедуру щодо промислової власності. Так, наприклад, для виникнення авторського права не вимагається відповідна реєстрація, але при цьому необхідно, щоб твір існував в об'єктивній формі, тобто не був лише в думках автора. За допомогою авторського права охороняються літературні та наукові твори, твори мистецтва. На творах, які охороняються авторським правом, можуть проставлятися відповідні знаки охорони, наприклад, ©, (найменування) володільця виключних авторських прав, рік першого опублікування твору. Проте для виникнення авторського права знаки охорони не є обов'язковими.

Авторське право має дві великі групи прав: майнові й особисті немайнові. Майнові права автора можуть передаватись іншим особам на підставі договору, а особисті немайнові права є невід'ємними від автора. Якщо особисті немайнові права автора, наприклад, право на ім'я, охороняються безстроково, то майнові права автора мають певний строк охорони, який в Україні в загальному випадку діє протягом усього життя автора і 70 років після його смерті.

Схематично структуру особистих немайнових прав автора можна представити як на рис. 3.3.

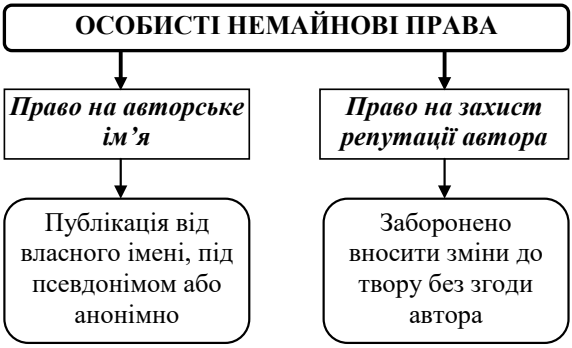


Рис. 3.3. Класифікація особистих немайнових прав автора

Перелік майнових прав автора є більш широким і умовно може бути зображений як на рис. 3.4.

Право на *відтворення* твору полягає в тому, що автор на власний розсуд може виготовляти потрібну йому кількість примірників твору, водночас дозволяти або не дозволяти робити це іншим особам. Після цього автор може *розповсюджувати* свій твір у будь-який законний спосіб. Як правило розповсюдження творів здійснюється за договором із торговельною мережею або мережами, який може укласти сам автор або уповноважений ним посередник. Тісно пов'язаним із правом на розповсюдження є право автора на контроль за *імпортом* примірників свого твору, виготовлених за кордоном до країни дії його авторських прав.

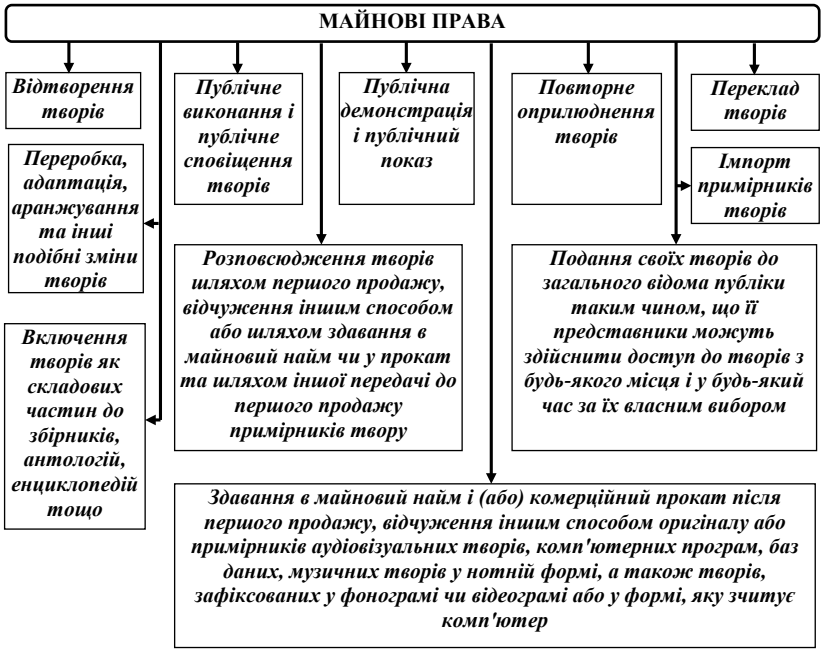


Рис. 3.4. Класифікація майнових прав автора

Публічне виконання та публічне сповіщення творів забезпечується здійсненням автором певних дій, спрямованих на

доведення до широкого загалу свого творчого доробку у вигляді виступу, презентації, лекційного курсу тощо.

Стосовно *публічної демонстрації чи показу* потрібно зазначити, що дане право реалізується здебільшого щодо творів образотворчого мистецтва шляхом безпосереднього зорового відчуття аудиторією.

Повторне оприлюднення творів може відбуватися, наприклад, після їх корекції автором. Так, якщо йдеться про підручник, то це може бути перероблений і доповнений матеріал, в якому враховано зміни наукового та методичного характеру, що відбулися з часу першого його оприлюднення.

Право на *переклад* твору іншими мовами полягає в тому, що автор може сам або уклавши угоду з перекладачем перетворити об'єкт своєї творчої діяльності в іншомовний продукт, більш доступний для іноземної аудиторії. У випадку здійснення неякісного перекладу перекладачем автор має право заборонити його використання.

Якщо автор вважає за потрібне, то він може *переробити* твір, *адаптувати* його до сучасних реалій або для іншої аудиторії, здійснити інші зміни. Така переробка або адаптація може супроводжуватися наступним *додаванням творів як складових частин до інших об'єктів інтелектуальної власності*: збірників, антологій, енциклопедій тощо. При цьому автор не втрачає права на свою частину твору, а стає учасником іншого творчого проєкту.

Автор має право *подати свої твори до загального відома публіки* з використанням сучасних технологій, наприклад, відкривши власний сайт, що висвітлюватиме його творчу діяльність.

Для окремих об'єктів авторського права передбачена можливість їх *здачі у майновий найм і (або) комерційний прокат*. Часто реалізацію цього права можна зустріти під час розповсюдження примірників аудіовізуальних творів через електронні бібліотеки у всесвітній мережі Інтернет.

В окремих випадках дозволяється вільне використання творів автора, тобто без згоди автора чи іншої особи, яка має авторське право (рис. 3.5), проте обов'язковим залишається зазначення імені автора і джерела запозичення.

Рис. 3.5. Випадки вільного використання творів

Існують також інші випадки вільного відтворення твору із зазначенням імені автора (рис. 3.6).

Для передачі майнових авторських прав іншій особі автор може укласти відповідний договір. Найбільш поширеними видами авторських договорів є:

– видавничий;
– замовлення;
– на створення та використання комп'ютерних програм.
– постановчий;

– сценарний.

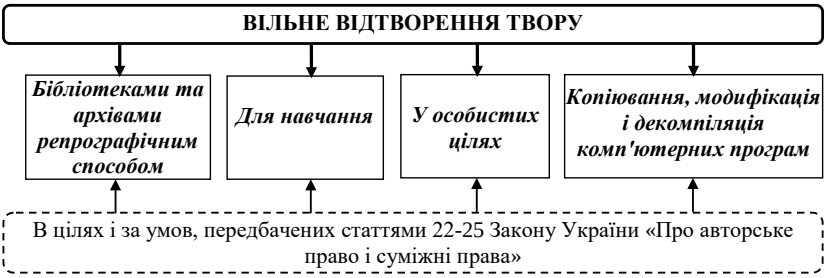


Рис. 3.6. Окремі випадки вільного відтворення твору

Отже, інститут права інтелектуальної власності має досить вагомі важелі захисту інтелектуального продукту фізичних та юридичних осіб. Проте зі зміною технології виробництва інтелектуального продукту потрібно динамічно вносити потрібні суспільству зміни до законодавства. Особливо це стосується спірних питань форми правового захисту комп'ютерних програм.

Питання для самоконтролю

1. Об'єкти права інтелектуальної власності, визначені міжнародними конвенціями.
2. Об'єкти права інтелектуальної власності, визначені законодавством України.
3. Винахід і корисна модель.
4. Знаки для товарів і послуг, промисловий зразок.
5. Структура особистих немайнових прав автора.
6. Класифікація майнових прав автора.
7. Випадки вільного використання творів.
8. Окремі випадки вільного відтворення твору. Авторські договори.

План практичної підготовки за темою:
«Захист авторського права»

Вид: практичне заняття.
Мета: розв'язання задач.
Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Розв'язання задач (140 хв).
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Задача № 1

Ільєнко, Кашпор, Сухно та Гнатенко заснували ТОВ «Соло». При цьому Ільєнко як статутний внесок надав права інтелектуальної власності на низку книг із підприємницької діяльності. Решта учасників внесли грошові внески. Розмір внеску кожного учасника було оцінено у 25 %. Описане було закріплено у статуті й установчому договорі. Через 2 роки було вирішено припинити діяльність ТОВ «Соло». Кашпор, Сухно та Гнатенко зажадали розподілу активів підприємства відповідно до розміру та форми статутного внеску. Ільєнко ж наполягав, що йому також мають бути повернені активи у грошовій та майновій формах. Загальні збори відхилили цю вимогу, тому Ільєнко звернувся до суду.

Яке рішення повинен винести суд? Які особливості інтелектуальних прав? На цьому прикладі поясніть природу права інтелектуальної власності та їх види. Чи можна як статутний внесок вносити права інтелектуальної власності?

Задача № 2

Після смерті письменника Куженка його донька стала єдиною спадкоємицею та правонаступницею відповідних авторських прав свого батька. Через деякий час вона подала позов проти видавництва К., оскільки останнє видало книгу її батька накладом 5000 примірників без її дозволу.

При цьому представник видавництва пояснив, що перед смертю з письменником Куженком було досягнуто попередню домовленість про видання книги та йому було виплачено частину авторського гонорару, про що є відповідний документ. Лише смерть письменника завадила підписанню виключної ліцензійної угоди.

Дочка письменника Куженка наполягала, що про вказані домовленості їй нічого не відомо, як і про надану авторську винагороду.

Яке рішення повинен винести суд? Чи є порушення прав інтелектуальної власності позивачки? Якщо є, то які заходи їх захисту передбачає чинне законодавство?

Задача № 3

Вікторов звернувся з позовом до суду, в якому просив припинити розповсюдження роману свого батька видавництвом «Вікно», яке не повідомило його про видання роману. Свої вимоги він обґрунтував тим, що його батько написав роман у 1970 р. та опублікував його в журналі, а помер у 1980 році. Відтоді Вікторов як син та єдиний спадкоємець батька має відповідні виключні права на вказаний роман.

Представник видавництва заперечив вимоги і вказав, що строк дії авторського права закінчився.

Проаналізуйте ситуацію. Яке рішення повинен винести суд?

Задача № 4

Працівники інвестиційної компанії «Нова» розробили та надіслали до Верховної Ради України проєкт закону. Відповідний проєкт також було надіслано низці інших інвестиційних компаній для обговорення. Згодом у компанії «Нова» дізналися, що деякі з інвестиційних компаній, яким було надіслано законопроєкт, використали ідеї, викладені в ньому, для покращення свого бізнесу, що було зафіксовано у відповідних інструкціях для працівників.

Компанія «Нова» звернулася до суду з позовом про відшкодування заподіяної матеріальної та моральної шкоди.

Проаналізуйте вказану ситуацію та підготуйте письмові відповіді на питання: що є об'єктом авторського права та які об'єкти цим правом не охороняються. Чи підлягають задоволенню вимоги позивача?

Задача № 5

Письменнику Баглаєнку стало відомо про декілька фактів самовільного використання його творів:

1) фрагмент його роману було процитовано під час радіопередачі;

2) відбулося додаткове видання повісті тиражом 100 примірників рельєфно-крапковим шрифтом;

3) уривок оповідання було опубліковано у збірнику диктантів для школярів.

Поясніть на цьому прикладі межі дії авторського права.

Задача № 6

Видавництво «ІО» випустило збірку жартів одного з відомих коміків, до якої серед іншого увійшли декілька творів інших авторів, які артист виконував на концертах. При цьому згоди авторів на видання їх творів отримано не було. Після цього деякі автори заявили виданню претензію. Оскільки конфлікт не вдалося владнати, автори звернулися до суду.

Проведіть юридичний аналіз наведеної ситуації. Яке рішення повинен винести суд?

Задача № 7

Під час видання повісті автора, який помер у 1950 р., було з декількома помилками надруковано його прізвище. Нащадки автора звернулися з претензією до видавництва, представник якого вказав, що строк дії авторського права вже минув, а помилок у прізвищі припустилася типографія, якій видавництво передало правильні дані автора.

Позивачі вимагали:

– вилучення з реалізації всіх примірників видання;

– вилучення отриманої винагороди (комерційного доходу);

– компенсації завданої моральної шкоди.

Чи правомірні вимоги позивачів? Яке рішення повинен ухвалити суд?

Тема 4. Захист відкритої інформації в Україні

План

1. Концептуальні питання захисту відкритої інформації.
2. Публічна інформація.
3. Порядок створення комплексної системи захисту відкритої інформації.

1. Концептуальні питання захисту відкритої інформації

Захист відкритої інформації в державних органах регламентують:

1. Концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету Міністрів України від 08.10.1997 № 1126[34].

2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373[35].

Згідно з Концепцією технічного захисту інформації в Україні одним із принципів формування і проведення державної політики у сфері технічного захисту інформації (ТЗІ) є обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну й іншу передбачену законом таємницю, службової інформації,

[34] Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України № 1126 від 8.10.1997 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/1126-97-%D0%BF (дата звернення: 12.07.2017).

[35] Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями на 13.10.2011]. *Офіційний вісник України*. 2006. № 13 (12.04.2006), стор. 164, стаття 878.

відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також *відкритої інформації, важливої для особи та суспільства*, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, у державних установах і організаціях.

Захисту потребують такі властивості відкритої інформації, як *цілісність і доступність*.

Наведемо приклад. У м. Ф сталася техногенна аварія, про що надійшло повідомлення до засобу масової інформації К., який повинен оприлюднити його за допомогою радіо чи телевізійного мовлення з використанням відповідної радіопередавальної станції. Зловмисник пошкодив антенну систему станції, тим самим реалізувавши загрозу доступності інформації про аварію. Багато людей не змогли вчасно евакуюватися, внаслідок чого сталося лихо державного масштабу. Або зловмисник перехопив повідомлення, що повинно було надійти до ЗМІ К., та замінив у ньому місце, де сталася аварія. Таким чином успішно була реалізована загроза цілісності інформації. Наслідки очевидні.

Віднесення тієї чи іншої інформації до категорії відкритої проводиться згідно із Законом України «Про інформацію» та Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Будь-яка інформація є **відкритою**, крім тієї, що віднесена законом до інформації з обмеженим доступом. До відкритої інформації, що підлягає захисту, відносять інформацію, яка належить до державних інформаційних ресурсів, а також про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами.

В окремих випадках відкриту інформацію доцільно захищати від несанкціонованого копіювання. З правової точки зору йдеться, насамперед, про використання інституту інтелектуальної власності.

В інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах для захисту відкритої інформації створюється комплексна система захисту інформації (КСЗІ) та *підтверджується її відповідність*. Відповідно до ч. 2 ст. 8 Закону

України «Про захист інформації в інформаційно-телекомунікаційних системах»[36] підтвердження відповідності здійснюється за результатами *державної експертизи* в порядку, встановленому законодавством. Також відповідно до ч. 3. ст. 8 цього закону для створення КСЗІ використовуються *засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок* за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством[37].

Завдання, які вирішує КСЗІ для відкритої інформації, наведено на рис. 4.1.

Рис. 4.1. Призначення КСЗІ

Між Концепцією технічного захисту інформації та Правилами забезпечення захисту інформації в інформаційних,

[36] Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994; [із змінами і доповненнями на 19.04.2014]. Відомості Верховної Ради України. 1994. № 31 (02.08.1994). ст. 286.

[37] Носов В. В., Манжай І. А. Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2017. № 2 (34). С. 56.

телекомунікаційних та інформаційно-телекомунікаційних системах існує певна неузгодженість, оскільки перша наголошує на необхідності захисту відкритої інформації, **важливої для держави, особи та суспільства**, а Правила зобов'язують захищати **всю відкриту інформацію**, що є важко виконуваним на практиці і відповідно економічно недоцільним[38]. Враховуючи те, що Правила мають розпорядчий характер, можна зробити висновок, що *захисту мають підлягати всі відкриті державні інформаційні ресурси*[39].

2. Публічна інформація

Особливою формою відкритої інформації є публічна інформація. Згідно зі ст. 1 Закону України «Про доступ до публічної інформації» від 13.01.2011[40] ***публічна інформація*** – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом «Про доступ до публічної інформації».

Публічна інформація є *відкритою*, крім випадків, установлених законом.

Доступ до інформації забезпечується шляхом:

1) систематичного та оперативного оприлюднення інформації:

– в офіційних друкованих виданнях;

– на офіційних веб-сайтах у мережі Інтернет;

– на єдиному державному веб-порталі відкритих даних;

– на інформаційних стендах;

---

[38] Носов В. В., Манжай О. В. Актуальні питання правового захисту відкритої інформації та інформації про особу. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2006. Вип. 2 (13). С. 34, 36, 37.

[39] Носов В. В., Манжай І. А. Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2017. № 2(34). С. 56.

[40] Про доступ до публічної інформації: закон України від 13.01.2011; [із змінами і доповненнями на 01.05.2015]. *Офіційний вісник України*. 2011. № 10 (18.02.2011), стор. 29, стаття 446.

– будь-яким іншим способом;

2) надання інформації за запитами на інформацію.

Публічна інформація у формі відкритих даних – це публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний і безоплатний доступ до неї, а також її подальше використання.

Публічна інформація у формі відкритих даних оприлюднюється на єдиному державному веб-порталі відкритих даних і на своїх веб-сайтах (електронне урядування – новела 2015 року).

Суб'єктами відносин у сфері доступу до публічної інформації є:

1) *запитувачі інформації* – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;

2) *розпорядники інформації* – суб'єкти, визначені ст. 13 цього Закону України «Про доступ до публічної інформації»;

3) *структурний підрозділ або відповідальна особа* з питань доступу до публічної інформації розпорядників інформації.

Для забезпечення збереження та доступу до публічної інформації документи, що знаходяться у суб'єктів владних повноважень, підлягають обов'язковій реєстрації *в системі обліку*.

Система обліку публічної інформації не може бути віднесена до категорії інформації з обмеженим доступом.

Запитувач має право **звернутися** до розпорядника інформації **із запитом** на інформацію, **незалежно від того, стосується ця інформація його особисто чи ні**, **без пояснення причини подання запиту**.

Запит на інформацію може бути індивідуальним або колективним. **Запити можуть подаватися в усній, письмовій чи іншій формах** (поштою, факсом, телефоном, електронною поштою) на вибір запитувача.

Згідно з ч. 5 ст. 19 Закону України «Про доступ до публічної інформації» запит на інформацію *має містити:*

1) ім'я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є;

2) загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо;

3) підпис і дату за умови подання запиту в письмовій формі.

Форму запиту можна одержати на веб-сайті розпорядника.

Розпорядник інформації повинен дати відповідь на запит на інформацію не пізніше **п'яти робочих днів** з дня отримання запиту. В окремих випадках строк може бути зменшено – не пізніше *48 годин* (наприклад, про аварії, що загрожують безпеці громадян) або збільшено – до *20 робочих днів* (наприклад, великий обсяг інформації).

Розпорядник інформації має право *відмовити* в задоволенні запиту в таких випадках:

1) розпорядник інформації не володіє і не зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит;

2) інформація, що запитується, належить до категорії інформації з обмеженим доступом відповідно до ч. 2 ст. 6 Закону України «Про доступ до публічної інформації»;

3) особа, яка подала запит на інформацію, не оплатила передбачені ст. 21 Закону України «Про доступ до публічної інформації» фактичні витрати, пов'язані з копіюванням або друком (більше 10 сторінок);

4) не дотримано вимог щодо запиту на інформацію, передбачених ч. 5 ст. 19 Закону України «Про доступ до публічної інформації».

Рішення, дії чи бездіяльність розпорядників інформації можуть бути оскаржені у керівника розпорядника, вищого органу або суді.

Відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень:

1) ненадання відповіді на запит;

2) ненадання інформації на запит;

3) безпідставна відмова в задоволенні запиту на інформацію;

4) неоприлюднення інформації відповідно до ст. 15 Закону України «Про доступ до публічної інформації»;

5) надання або оприлюднення недостовірної, неточної або неповної інформації;

6) несвоєчасне надання інформації;

7) необґрунтоване віднесення інформації до інформації з обмеженим доступом;

8) нездійснення реєстрації документів;

9) навмисне приховування або знищення інформації чи документів.

3. Порядок створення комплексної системи захисту відкритої інформації

Основні процедурні моменти створення КСЗІ викладено в нормативних документах системи технічного захисту інформації, а саме у НД ТЗІ 3.7-003-05[41]. КСЗІ створюється на підставі Технічного завдання, розробленого згідно з вимогами НД ТЗІ 3.7-001-99[42].

Для інформаційно-телекомунікаційних систем (ІТС) з відкритою інформацією, що підлягає обов'язковому захисту, відповідно до НД ТЗІ 3.7-003-2005[43] має бути також передбачено створення *комплексу засобів захисту від несанкціонованого доступу*. Комплекс засобів захисту інформації охоплює програмні, апаратні, програмно-апаратні засоби та засоби криптографічного захисту інформації.

Розробці КСЗІ передує створення служби захисту інформації, вимоги до якої визначені в НД 1.4-001-2000[44].

Виконавцем робіт зі створення (експертизи) КСЗІ може бути суб'єкт господарської діяльності або орган виконавчої влади, який має *ліцензію або дозвіл* на право провадження хоча б одного виду

---

[41] НД ТЗІ 3.7-003-05. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106350 (дата звернення: 17.03.2019).

[42] НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106349 (дата звернення: 17.03.2019).

[43] НД ТЗІ 3.7-003-05. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106350 (дата звернення: 17.03.2019).

[44] НД 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106341 (дата звернення: 17.03.2019).

робіт у сфері ТЗІ, необхідність проведення якого визначено технічним завданням на створення системи захисту[45].

Відповідно до нормативних вимог[46] ліцензуванню підлягають надання послуг з:

1) оцінювання захищеності інформації, що не становить державної таємниці;

2) оцінювання захищеності інформації всіх видів, у тому числі інформації, що становить державну таємницю;

3) виявлення закладних пристроїв.

Під час створення (експертизи) КСЗІ для відкритої інформації має бути ліцензія або дозвіл за першим або другим напрямом.

Послідовність дій власника (розпорядника) ІТС із організації розробки КСЗІ

Організація – власник (розпорядник) ІТС:

а) визначає правові підстави необхідності створення КСЗІ для ІТС;

б) визначає для ІТС відповідальну за захист інформації особу (службу захисту інформації), яка буде забезпечувати функціонування КСЗІ і повноваження якої визначено у НД 1.4-001-2000[47];

в) здійснює вибір ліцензіата – виконавця робіт зі створення КСЗІ для ІТС та заключає з ним договір на виконання робіт:

---

[45] Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями на 13.10.2011]. *Офіційний вісник України*. 2006. № 13 (12.04.2006), стаття 23.

[46] Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: постанова Кабінету Міністрів України № 821 від 16.11.2016. *Офіційний вісник України*. 2016. № 93, стор. 39, стаття 3033.

[47] НД 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106341 (дата звернення: 17.03.2019).

– вимоги, що висуваються до ліцензіатів, наведено в Постанові Кабінету Міністрів України від 16.11.2016 № 821[48];

– перелік ліцензіатів наведений на веб-сторінці Держспецзв'язку[49].

Обсяг послуг виконавця з розробки КСЗІ

Ліцензіат-виконавець згідно з НД ТЗІ 3.7-003-05[50] поетапно створює КСЗІ для ІТС:

1) формує загальні вимоги до КСЗІ;
2) розробляє політику безпеки інформації в ІТС;
3) розробляє технічне завдання на створення КСЗІ;
4) розробляє проєкт КСЗІ;
5) уводить КСЗІ в дію;
6) за узгодженням з Адміністрацією Держспецзв'язку оцінює захищеність інформації (проводить державну експертизу) в ІТС;
7) виконує роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.

Більш розгорнутий перелік послуг зі створення та супроводження КСЗІ може виглядати таким чином[51].

[48] Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: постанова Кабінету Міністрів України № 821 від 16.11.2016. *Офіційний вісник України*. 2016. № 93, стор. 39, стаття 3033.

[49] Перелік суб'єктів господарювання, що мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=284081&cat_id=266373 (дата звернення: 19.03.2019).

[50] НД ТЗІ 3.7-003-05. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106350 (дата звернення: 17.03.2019).

1. *Підготовка організаційно-розпорядчої документації*. У межах цього етапу спочатку проводиться аналіз існуючої організаційно-розпорядчої документації (організаційної структури, штатного розкладу, положення про відділи та посадових інструкцій працівників, пов'язаних з експлуатацією системи, документів, що регламентують доступ до системи, тощо). За результатами проведеного аналізу готуються проєкти документів, які визначають організаційну складову КСЗІ (проєкт наказу про створення КСЗІ, проєкт положення про службу захисту інформації, проєкти посадових інструкцій і процедур тощо), які затверджуються Замовником.

2. *Обстеження інформаційної інфраструктури Замовника*. На цьому етапі аналізуються архітектура системи, її топологія та складові елементи. Визначаються типи користувачів системи, типізується інформація, що обробляється в системі. У результаті розробляються акт обстеження системи (містить її опис, принципи побудови й архітектуру) та перелік об'єктів системи, що підлягають захисту, які затверджуються Замовником.

3. *Розробка «Плану захисту інформації»*. За підсумками цього етапу мають бути підготовлені такі документи: модель загроз інформації, модель порушника; Положення про Службу захисту інформації; політика безпеки інформації. Вказані документи мають бути затверджені Замовником.

4. *Розробка технічного завдання на створення КСЗІ*. У технічному завданні викладаються вимоги до функціонального складу і порядку розробки й упровадження технічних засобів, які забезпечують безпеку інформації в процесі її обробки в обчислювальній системі, а також вимоги до організаційних, фізичних та інших заходів захисту, які реалізуються поза обчислювальною системою в доповнення до комплексу програмно-технічних засобів захисту інформації. Технічне завдання може розроблятися для вперше створюваних систем, а також під час модернізації вже існуючих у вигляді окремого розділу технічного завдання на створення системи, окремого (часткового) технічного

---

[51] Побудова Комплексних Систем Захисту Інформації (КСЗІ). URL: http://www.iqusion.com/ua/produkti-i-servisi/zakhist-informatsiji/120-kszi.html (дата звернення: 12.07.2017);
Етапи побудови КСЗІ. URL: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi (дата звернення: 17.03.2019).

завдання або доповнення до технічного завдання на створення системи.

5. *Розробка технічного проєкту на створення КСЗІ*. Цей документ розробляється після узгодження технічного завдання з Держспецзв'язком. До цього комплекту документів входить частина документів, розроблених на попередніх етапах, і низка нових, в яких описано, як саме створюватиметься, експлуатуватиметься та за потреби модернізуватиметься КСЗІ. Технічний проект на створення КСЗІ розробляється на підставі та відповідно до технічного завдання. Під час розробки проєкту КСЗІ обґрунтовуються та приймаються проєктні рішення, які дають можливість реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. У результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

6. *Приведення інформаційної інфраструктури Замовника у відповідність до технічного проєкту на створення КСЗІ*. Особливістю цього етапу є те, що на момент ухвалення рішення про створення КСЗІ вартість цього етапу є невідомою як для Замовника, так і для Виконавця. Також, зважаючи на великий можливий спектр виконання робіт, на цьому етапі існує велика вірогідність підключення до його виконання Підрядників. На цьому етапі можуть виконуватися монтажні, будівельні, пусконалагоджувальні роботи, роботи, пов'язані зі встановленням необхідних технічних або криптографічних засобів захисту інформації, засобів фізичного захисту елементів системи (встановлюється необхідне устаткування і програмне забезпечення, засоби контролю доступу, охоронна і пожежна сигналізації) тощо.

7. *Розробка експлуатаційної документації на КСЗІ*. У кінці цього етапу мають бути підготовлені такі документи: інструкції з експлуатації КСЗІ та її елементів; процедури регламентного обслуговування КСЗІ; правила і положення проведення тестування та аналізу роботи КСЗІ; керівництво адміністраторів і користувачів; формуляр КСЗІ системи.

8. *Упровадження КСЗІ*. На цьому етапі здійснюється організація захисту інформації від несанкціонованого доступу та

антивірусного захисту інформації, розробка програми і методики попередніх випробувань, проведення попередніх випробувань.

9. *Випробування КСЗІ.* Під час випробувань виконуються тестові завдання та контролюються отримані результати, які є індикатором працездатності спроєктованої КСЗІ. За результатами випробування КСЗІ робиться висновок про можливість представлення КСЗІ на державну експертизу. Під час дослідної експлуатації: відпрацьовують технології обробки інформації, облік машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів системи і автоматизованого контролю за діями користувачів; працівники служби захисту інформації та користувачі системи набувають практичних навичок використання технічних і програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних і розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів; здійснюється (за потреби) доопрацювання програмного забезпечення, додаткове налагодження і конфігурація комплексу засобів захисту інформації від несанкціонованого доступу; здійснюється (за потреби) коректування робочої та експлуатаційної документації.

10. *Проведення державної експертизи КСЗІ і отримання Атестата відповідності.*

11. *Підтримка й обслуговування КСЗІ.*

Підтвердження якості створеної КСЗІ

Після введення КСЗІ у дію і проведення випробувань необхідно провести державну експертизу КСЗІ, порядок організації і проведення якої викладено в роботі «Організація та забезпечення інформаційної безпеки»[52].

Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам нормативних документів ТЗІ і проводиться шляхом *експертних випробувань* або шляхом *аналізу декларації про відповідність КСЗІ вимогам нормативних документів з ТЗІ.*

Метою проведення первинної державної експертизи у сфері технічного захисту інформації КСЗІ є отримання Експертного

[52] Носов В. В., Манжай О. В. Організація та забезпечення інформаційної безпеки: навчальний посібник. Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. 216 с.

висновку про відповідність КСЗІ вимогам нормативних документів у сфері технічного захисту інформації та Атестату відповідності КСЗІ вимогам нормативних документів у сфері технічного захисту інформації.

Державна експертиза проводиться для визначення відповідності КСЗІ технічному завданню, вимогам нормативних документів із захисту інформації та визначення можливості введення КСЗІ у складі інформаційно-телекомунікаційної системи в промислову експлуатацію.

Державна експертиза КСЗІ для ІТС з відкритою інформацією і доступом до неї через інтернет проводиться шляхом експертних випробувань. Порядок її організації та проведення можна представити як на рис. 4.2[53] [15, с. 156–157].

Експертиза охоплюватиме такі послуги:

– *аналіз технічної документації на КСЗІ, середовища її функціонування*;

– *розробка Програми і методик проведення експертизи* (документи: Програма та методика проведення державної експертизи);

– *проведення експертного оцінювання КСЗІ* (документи: Протокол експертних випробувань);

– *оформлення результатів експертизи та* підготовка *експертного висновку відповідно до вимог НД ТЗІ*;

– *супроводження розгляду в Державній службі спеціального зв'язку та захисту інформації результатів проведення експертизи* (документи: Атестат відповідності, Акт введення в дію КСЗІ).

Виявлені під час державної експертизи недоліки повинні усуватися до її завершення. Якщо через якісь причини усунути недоліки під час експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок і рекомендації щодо їх виконання. Після завершення передбачених актом заходів проводиться повторна експертиза.

Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювалися за єдиним технічним завданням, то їх експертиза виконується в два етапи: на першому проводиться в повному обсязі експертиза одного обраного типового модуля, на другому

[53] Там само. С. 156-157.

здійснюється перевірка відповідності умов експлуатації типовим на кожному конкретному об’єкті для всіх модулів КСЗІ цього типу.

Рис. 4.2. Порядок організації та проведення державної експертизи шляхом експертних випробувань

Після завершення державної експертизи власнику системи видається Атестат відповідності КСЗІ, зареєстрований у Державній службі спеціального зв’язку та захисту інформації України, та позитивний експертний висновок, якщо під час проведення експертизи не було виявлено недоліків, які не було усунуто до її завершення.

Отже, в результаті проведення державної експертизи КСЗІ шляхом експертних випробувань необхідно мати:

– *протоколи* виконання робіт відповідно до окремої методики експертизи КСЗІ;

– *експертний висновок*, зареєстрований і затверджений Експертною радою Держспецзв'язку;

– *Атестат відповідності*, зареєстрований і виданий Держспецзв'язком.

Для того, щоб ввести в дію КСЗІ, проводяться відповідні заходи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в системі, якщо цього не було зроблено на попередніх етапах. Також на етапі введення в дію КСЗІ виконуються заходи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.

Контроль за функціонуванням КСЗІ

Після проведення державної експертизи згідно з нормативними документами[54] передбачається контроль за функціонуванням КСЗІ ІТС з боку Держспецзв'язку. Ця діяльність здійснюється шляхом організації та проведенням контрольно-інспекторської роботи з питань ТЗІ.

Порушення встановлених норм і вимог ТЗІ, що можуть бути виявлені під час проведення перевірок, розділяються на *три категорії порушень*. Для КСЗІ ІТС з відкритою інформацією і доступом до неї через інтернет може бути порушення тільки третьої категорії, яка не пов'язана із загрозою порушення конфіденційності.

Ліцензіат-виконавець, який створював КСЗІ для ІТС, у подальшому може бути залучений або для вдосконалення стану ТЗІ,

[54] Положення про державний контроль за станом технічного захисту інформації: наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України №87 від 16.05.07 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon5.rada.gov.ua/laws/show/z0785-07 (дата звернення: 17.03.2019);

Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних, та інформаційно-телекомунікаційних системах: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 660 від 02.12.2014 // База даних «Законодавство України» / Верховна Рада України. URL:
http://zakon3.rada.gov.ua/laws/show/z0090-15 (дата звернення: 17.03.2019).

або для усунення недоліків, виявлених під час проведення Держспецзв'язком перевірок.

Варто зазначити, що процедура створення КСЗІ загалом і для систем з відкритою інформацією зокрема є доволі заплутаною. Відсутній єдиний нормативно-методичний документ, в якому було повно та послідовно викладено описаний процес. Це створює певні обмеження та незручності для осіб, які не мають профільної освіти або відповідного досвіду роботи, адже вони не можуть швидко зрозуміти без сторонньої допомоги, що і як їм робити для розбудови КСЗІ. Пропозиції відповідних програмних комплексів для створення КСЗІ в системах з відкритою інформацією також є доволі обмеженими, а вартість відповідних послуг доволі високою, що свідчить про неконкурентність середовища та надмірну заорганізованість процесу розбудови КСЗІ[55].

Питання для самоконтролю

1. Нормативно-правова база захисту відкритої інформації.
2. Доступ до публічної інформації.
3. Комплексна система захисту відкритої інформації.
4. Види робіт, які здійснюються в межах технічного захисту інформації.
5. Захист відкритої інформації, важливої для особи та суспільства.
6. Послідовність дій власника (розпорядника) інформаційно-телекомунікаційної системи із організації розробки комплексної системи захисту інформації.
7. Обсяг послуг виконавця з розробки комплексної системи захисту інформації.
8. Підтвердження якості створеної комплексної системи захисту інформації.
9. Контроль за функціонуванням комплексної системи захисту інформації.

[55] Носов В. В., Манжай І. А. Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2017. № 2(34). С. 60-68.

План практичної підготовки за темою:
«Побудова комплексної системи захисту відкритої інформації»

Вид: семінарське заняття.

Мета: отримати практичні навички пошуку та аналізу даних, необхідних для оцінки витрат і часу на побудову комплексної системи захисту інформації.

Порядок проведення заняття.

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Курсанти оцінюють орієнтовний час і витрати на розробку комплексної системи захисту відкритої інформації (140 хв). Для вивчення ринку послуг здійснюється аналіз пропозицій компаній у мережі Інтернет, тендерної документації державних закупівель послуг у сфері створення та експертизи комплексної системи захисту інформації.
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Приклад висновку. Виходячи з проведеного аналізу, встановлено, що:

1) розробка документації на створення КСЗІ здійснюється в середньому протягом 1–4 місяців залежно від складності системи, в якій планується її створити. Вартість відповідних робіт становить 27000–36000 грн (в окремих випадках розробити КСЗІ пропонують за ціною 64000, 158000 грн без наведення розшифровки виконуваних робіт). Відповідні послуги враховують:

– обстеження середовища функціонування системи;

– розробку документації на комплекс технічного захисту інформації *об'єкта інформаційної діяльності*. Для ІТС з відкритою інформацією і доступом до неї через інтернет – це приміщення, де розташовуватиметься серверне обладнання та саме обладнання (1500–2000 грн);

– налаштування комплексу засобів захисту інформації від несанкціонованого доступу (6000–10000 грн);

– розробку технічного завдання на створення КСЗІ (3000–4000 грн);

– розробку документації на КСЗІ для декларування в галузі технічного захисту інформації, що потрібно для проведення експертизи (15800–19000 грн);

– розробку декларації на КСЗІ для реєстрації в Держспецзв'язку (700–1000 грн).

2) експертиза КСЗІ (як правило виконується незалежною третьою стороною) відбуватиметься протягом 2–6 місяців залежно від складності системи. Строк перебування заяви на розгляді в Держспецзв'язку становить до 30 днів. Вартість експертизи орієнтовно становитиме 48000–73000 грн:

– попереднє ознайомлення з об'єктом експертизи (10000–19000 грн);

– поглиблене обстеження об'єкта експертизи (3000–4000 грн);

– формування програми та методики проведення експертизи (6000–10000 грн);

– проведення експертних випробувань і досліджень за розробленими програмою та методикою (20000–29000 грн);

– документування та затвердження результатів експертизи (91000–11000 грн).

Окремо можна зазначити, що простий аналіз декларації допускається лише для автоматизованої системи класу 1 (локальна робоча станція без підключення до комп'ютерної мережі). Вартість цієї послуги становитиме орієнтовно 6000–15000 грн.

План практичної підготовки за темою:
«Доступ до публічної інформації»

Вид: практичне заняття.

Мета: складання запиту.

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. На сайті одного з органів виконавчої влади потрібно знайти інтерактивну форму для подання запиту про публічну інформацію. Підготувати запит (60 хв).
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Тема 5. Правові засади захисту інформації з обмеженим доступом, що не належить до державної таємниці

План

1. Захист конфіденційної та службової інформації.
2. Захист інформації про особу.

1. Захист конфіденційної та службової інформації

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію»[56] ***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*. Встановлення системи захисту є правом, а не обов'язком власника. Конфіденційна та службова інформація належать до інформації з обмеженим доступом, але не всяка інформація може бути визнана такою. Законодавець встановлює з цього приводу певні обмеження (рис. 5.1).

Важливою гарантією свободи слова в Україні є норма, згідно з якою інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

[56] Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями на 01.01.2017]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

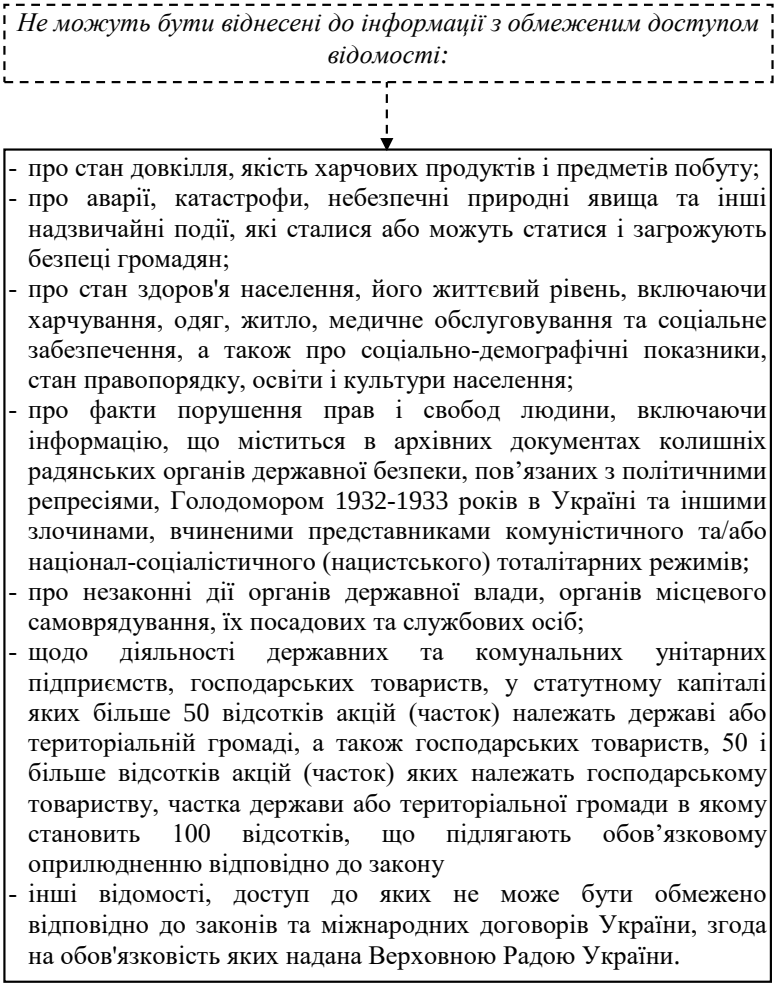


Рис. 5.1. Відомості, які не можуть бути визнані інформацією з обмеженим доступом

За розголошення конфіденційної інформації, що не є власністю держави, може наступати адміністративна відповідальність у порядку, визначеному ст. 164-3 Кодексу України про адміністративні правопорушення (КУпАП) від 07.12.1984. Відповідно до вказаної статті отримання, використання,

розголошення комерційної таємниці, а також іншої конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця належить до недобросовісної конкуренції та карається накладенням штрафу від дев'яти до вісімнадцяти неоподатковуваних мінімумів доходів громадян.

Крім того, адміністративна відповідальність може наставати також за порушення порядку використання конфіденційної інформації (ст. 186-3 КУпАП).

Більш урегульованими з правової точки зору є питання захисту службової інформації. Порядок ведення обліку, зберігання, використання та знищення документів і інших матеріальних носіїв інформації, що містять службову інформацію, детально прописаний у Типовій інструкції, затвердженій Постановою Кабінету Міністрів України від 19.10.2016 № 736[57].

Документам, які містять службову інформацію, надається гриф **«для службового користування»** (ДСК). На документах ДСК з:

– мобілізаційних питань додатково проставляється відмітка «Літер «М»;

– питань криптографічного захисту службової інформації – відмітка «Літер «К»;

– питань спеціальної інформації – відмітка «СІ».

Категорії документів, на яких проставляється відмітка «Літер «К», визначаються нормативно-правовими актами Адміністрації Держспецзв'язку.

В установі утворюється комісія або декілька комісій з питань роботи зі службовою інформацією, які на підставі пропозицій структурних підрозділів установи та з урахуванням вимог законодавства складають перелік відомостей, що становлять службову інформацію, який у подальшому затверджує керівник установи.

Прикладами вказаних переліків можуть слугувати:

[57] Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету міністрів України від 19.10.2016 № 736. *Офіційний вісник України*. 2016. № 85 (04.11.2016), стор. 102, стаття 2783.

– Перелік відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України, затверджений Наказом МВС України від 26.12.2016 № 1351;

– Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений Наказом Національної поліції України від 12.10.2018 № 945.

Організаційно роботу з документами ДСК у конкретному підрозділі можна представити як на рис. 5.2.

Рис. 5.2. Організація роботи з інформацією ДСК

Друкування та розмноження документів ДСК проводиться з урахуванням вимог законодавства у сфері захисту інформації. Схематично це можна окреслити як на рис. 5.3.

Рис. 5.3. Друкування (розмноження) документів ДСК

Окремі реквізити, які повинні мати документи ДСК, наведено на рис. 5.4.

Рис. 5.4. Титульний та зворотний аркуш документу ДСК

Документи і справи із грифом «ДСК» зберігаються в *шафах, сейфах*, що розташовані у службових приміщеннях або сховищах архіву. Шафи, сейфи, службові приміщення, сховища архіву повинні надійно *замикатися та опечатуватися* металевими печатками.

Зберігання документів і справ із грифом «ДСК» здійснюється працівниками, які безпосередньо отримали їх під розписку, у спосіб, що унеможливлює доступ до них сторонніх осіб.

Модель руху документів ДСК зображено на рис. 4.6.

За порушення роботи зі службовою інформацією передбачена адміністративна, а в окремих випадках кримінальна відповідальність.

Рис. 4.6. Приблизна модель руху документів ДСК

Так, згідно зі ст. 212-5 КУпАП порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб – від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян. Повторне вчинення правопорушення збільшує розмір штрафу.

Кримінальна відповідальність встановлюється за розголошення службової інформації (зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни) *нерезидентам* України (іноземним підприємствам, установам, організаціям або їх представникам) (ст. 330 Кримінального кодексу України).

2. Захист персональних даних (інформації про особу)

Захист персональних даних, які містять інформацію про особу, є одним із найважливіших аспектів побудови громадянського суспільства.

Як і в Україні (2010 р.), спеціальні закони про захист персональної інформації були ухвалені в більшості європейських країн: Австрії (1978 р.), ФРН (1977 р.), Великобританії (1984 р.),

Франції (1987 р.), Норвегії (1988 р.), Португалії (1991 р.), Бельгії (1992 р.), Іспанії (1993 р.) та ін.

Радою Європи ухвалено Конвенцію про захист особи у зв'язку з автоматизованою обробкою персональних даних (1981 р.), 15 директив і рекомендацій у галузі захисту даних, у тому числі про захист: персональних даних у приватному (1973 р.) та державному (1974 р.) секторах; даних, що використовуються у медичних цілях (1981 р.), наукових дослідженнях та статистиці (1983 р.), прямому маркетингу (1985 р.), соціальному забезпеченні (1986 р.), правоохоронній сфері (1987 р.); даних у галузях зайнятості (1981 р.), платежів (1990 р.) тощо. Нормативні акти та рекомендації у вказаній сфері ухвалені також Європейським Союзом (95/46/CE), Організацією економічного співробітництва та розвитку[58].

Наразі в Україні є чинним Закон України «Про захист персональних даних» від 01.06.2010[59]. Відповідно до п. 2 ст. 5 цього закону персональні дані, крім знеособлених персональних даних, за порядком доступу є інформацією з обмеженим доступом. При цьому, ***персональні дані*** – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Таке саме визначення наведено у ст. 11 Закону України «Про інформацію» від 02.10.1992. Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

Інформацію про особу можна поділити на:

– загальну, яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого відповідно до п. 3 ст. 296 Цивільного кодексу України допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що

[58] Капица, Ю. Проблемы правовой охраны конфиденциальной информации в Украине (часть 2). *Інтелектуальна власність*. 2004. № 3. С. 27-33.

[59] Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями на 30.01.2018]. *Офіційний вісник України*. 2010. № 49 (09.07.2010), стор. 199, стаття 1604.

ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо).

– вразливі персональні дані (конфіденційна інформація про особу), що є інформацією з обмеженим доступом. Саме про такі дані йдеться у ст. 32 Конституції України та у ст. 302 Цивільного кодексу України: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до кримінального покарання. Також згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 *до конфіденційної інформації про особу*, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані).

Оскільки персональні дані є інформацією, вимога щодо захисту якої встановлена законом «Про захист персональних даних», то відповідно до п. 4 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 № 373, вона підлягає захисту в системі.

Враховуючи викладене, відповідно до Закону України «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 № 373 та інших нормативних актів у сфері захисту інформації **загальна інформація про особу**, що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані** - як службова інформація відповідно до вимог чинного законодавства у державних органах, або як окремий вид інформації згідно з вимогами Закону України «Про захист персональних даних» від 01.06.2010.

Дія цього закону *не поширюється* на діяльність з обробки персональних даних, яка здійснюється повністю або частково *із застосуванням автоматизованих засобів*, а також на обробку персональних даних, що містяться в *картотеці* (будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами) чи призначені до внесення до картотеки, із застосуванням *неавтоматизованих засобів*.

Відповідно до ст. 3 Закону України «Про захист персональних даних» ***база персональних даних*** – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

Суб'єктами відносин, пов'язаних із персональними даними, є:

– суб'єкт персональних даних;
– володілець бази персональних даних;
– розпорядник бази персональних даних;
– третя особа;
– Уповноважений Верховної Ради України з прав людини.

Володільцем чи розпорядником бази персональних даних можуть бути *підприємства, установи й організації* ***всіх форм власності****, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці*, які обробляють персональні дані відповідно до законодавства.

Розпорядником бази персональних даних, володільцем якої є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише *підприємство державної або комунальної форми власності*, що належить до сфери управління цього органу.

Персональні дані, крім знеособлених персональних даних, за порядком доступу **є інформацією з обмеженим доступом**.

Законом може бути заборонено віднесення окремих персональних даних до інформації з обмеженим доступом. Наприклад, згідно з ч. 6 ст. 6 Закону України «Про доступ до публічної інформації» не належать до інформації з обмеженим доступом відомості, зазначені в декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до Закону України «Про запобігання корупції», крім відомостей, зазначених в абз. 4 ч. 1 ст. 47 вказаного закону.

Склад і зміст персональних даних мають бути **відповідними та ненадмірними** стосовно визначеної мети їх обробки.

Первинними джерелами відомостей про фізичну особу є: *видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.*

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.

Для обробки персональних даних суб'єктом персональних даних має бути надана **згода на обробку його даних**.

Сьогодні збирати, обробляти, зберігати та використовувати персональні дані дозволено лише після отримання попередньої згоди особи. Згідно із законом така згода повинна бути задокументованою, зокрема, письмовою або в окремих випадках в електронному вигляді.

У загальному випадку **забороняється** обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

Суб'єкта персональних даних наділено низкою прав, зокрема на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних. Причому відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості.

Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю бази персональних даних на обробку цих даних, або відповідно до вимог закону. Для отримання доступу складається запит.

Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, в тому числі незаконного знищення чи доступу до персональних даних.

В органах державної влади та органах місцевого самоврядування, організаціях, установах і на підприємствах усіх форм власності створюється *структурний підрозділ або*

відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних під час їх обробки відповідно до закону.

За незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації передбачено кримінальну відповідальність згідно зі ст. 182 Кримінального кодексу України.

Питання для самоконтролю

1. Поняття конфіденційної інформації та порядок встановлення доступу до неї.
2. Обмеження щодо визнання інформації конфіденційною.
3. Відповідальність за розголошення конфіденційної інформації.
4. Організація роботи з інформацією ДСК.
5. Друкування (розмноження) документів ДСК.
6. Приблизна модель руху документів ДСК.
7. Окремі реквізити, які повинні мати документи ДСК.
8. Відповідальність за розголошення службової інформації.
9. Поняття та нормативно-правове регулювання інформації про особу.
10. Види інформації про особу.

План практичної підготовки за темою:
«Захист службової інформації в органах
Національної поліції України»

Вид: практичне заняття.

Мета: розв'язання задач.

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Розв'язання задач (140 хв).
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Задача № 1

Інженер відділення технічного захисту інформації ГУНП, не встигаючи оформити документацію з атестації робочих приміщень, набрав їх перелік у себе вдома на комп'ютері, роздрукував і долучив до відповідного комплекту документації.

У чому помилка інженера? Дайте правову оцінку ситуації.

Відповідь: дивіться Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджену Постановою Кабінету Міністрів України від 19.10.2016 № 736, Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений наказом Національної поліції України від 12.10.2018 № 945.

Задача № 2

Працівники відділення зв'язку ГУНП надрукували довідник телефонів керівництва. За цим фактом було розпочато службове розслідування, оскільки в довіднику вказувалися прізвища осіб, яким надано допуск до державної таємниці.

Чи правильно було почато службове розслідування? Дайте правову оцінку ситуації.

Відповідь: дивіться Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджену Постановою Кабінету Міністрів України від 19.10.2016 № 736, Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений наказом Національної поліції України від 12.10.2018 № 945.

Задача № 3

Науковий співробітник науково-дослідної установи Національної поліції України опублікував у відкритому збірнику статтю, в якій наводилася інформація, що розкриває технологію подвійного призначення, розроблену за державним замовленням. За цим фактом було розпочато службове розслідування. У своєму поясненні з цього приводу науковий співробітник пояснив, що інформація, наведена у статті, не дає можливості відтворення цієї технології, тому звинувачення безпідставні.

Чи має рацію науковий співробітник? Дайте правову оцінку ситуації.

Відповідь: дивіться Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджену Постановою Кабінету Міністрів України від 19.10.2016 № 736, Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений наказом Національної поліції України від 12.10.2018 № 945.

Задача № 4

Директор професійно-технічного училища, шефство над яким мав один із райвідділів поліції, опублікував у місцевій газеті інформацію про обсяги фінансування заходів цивільного захисту училища. Керівництво райвідділу, довідавшись про це, вирішило притягти директора училища до відповідальності, оскільки згідно з п. 12 Переліку відомостей, що становлять службову інформацію в системі Національної поліції України, інформація про обсяги фінансування заходів цивільного захисту в закладах та установах, що належать до сфери управління Національної поліції України, є службовою.

Чи правильно тлумачить положення цього переліку керівництво райвідділу? Дайте правову оцінку ситуації.

Відповідь: дивіться Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджену Постановою Кабінету Міністрів України від 19.10.2016 № 736, Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений наказом Національної поліції України від 12.10.2018 № 945.

Задача № 5

Начальник районного відділу поліції наказав своєму підлеглому Опанасику В. В. скласти вдома Порядок доступу працівників райвідділу до приміщення режимно-секретного сектору та наступного дня принести його на підпис. Опанасик В. В. відмовився це робити, пославшись на те, що такий документ повинен мати гриф обмеженого доступу, тому він не зможе створити його на своєму домашньому ПК.

Чи обґрунтована відмова Опанасика В. В.? Дайте правову оцінку ситуації.

Відповідь: дивіться Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджену Постановою Кабінету Міністрів України від 19.10.2016 № 736, Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений наказом Національної поліції України від 12.10.2018 № 945.

Задача № 6

Інженер відділення технічного захисту інформації отримав графік прийому іноземних делегацій у ГУНП на рік, в якому зазначалися дата приїзду делегації та країна, з якої вона прибуває. Інженер передрукував цей графік на атестованому комп'ютері, надавши цьому документу гриф обмеженого доступу «для службового користування».

Чи правильно він вчинив? Дайте правову оцінку ситуації.

Відповідь: дивіться Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджену Постановою Кабінету Міністрів України від 19.10.2016 № 736, Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений наказом Національної поліції України від 12.10.2018 № 945.

Задача № 7

Інспектор районного відділу поліції за дорученням керівника повинен був підготувати функціональні обов'язки старшого оперуповноваженого сектору кримінальної поліції того ж відділу. Не встигаючи це зробити, інспектор надіслав скановану копію типових обов'язків своєму синові та попросив надрукувати їх удома на комп'ютері із вказівкою імені та посади старшого оперуповноваженого. Отримавши від сина документи в месенджері «Telegram», інспектор переписав їх на зовнішній носій, який підключив до атестованого комп'ютера, з якого і роздрукував їх, вказавши потрібні реквізити.

Чи правильно вчинив інспектор? Дайте правову оцінку ситуації.

Відповідь: дивіться Кодекс України про адміністративні правопорушення, Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджену Постановою Кабінету Міністрів України від 19.10.2016 № 736, Перелік відомостей, що становлять службову інформацію в системі Національної поліції України, затверджений наказом Національної поліції України від 12.10.2018 № 945.

Тема 6. Особливості правового регулювання захисту державної таємниці в Україні та за її межами

План

1. Захист державної таємниці в Україні.
2. Зарубіжний досвід захисту державної таємниці та службової інформації.

1. Захист державної таємниці в Україні

Захист інформації, яка становить державну таємницю, регламентується, перш за все, Конституцією України, кількома міжнародними договорами, ратифікованими Верховною Радою України, Законом України «Про державну таємницю» від 21.01.1994[60], Кримінальним кодексом України та низкою підзаконних актів.

Прикладами двосторонніх договорів можуть слугувати Угода між Кабінетом Міністрів України та Урядом Республіки Польща про взаємну охорону секретної інформації від 04.09.2001 (ратифікована 26.09.2002); Угода між Урядом України та Урядом Сполучених Штатів Америки про охорону секретної інформації у сфері оборони від 04.08.2003 (ратифікована 04.06.2004) тощо.

Згідно зі ст. 1 Закону України «Про державну таємницю» ***державна таємниця*** – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законом, державною таємницею і підлягають охороні державою.

[60] Про державну таємницю: закон України від 21.01.1994 ; [із змінами і доповненнями на 05.08.2018]. *Відомості Верховної Ради України*. 1994. № 16 (19.04.1994). стор. 422. ст. 93.

Організаційну структуру охорони державної таємниці умовно можна представити як на рис. 6.1.

Рис. 6.1. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Сфери, в яких може циркулювати державна таємниця, є вичерпними і випливають з її визначення. Це:

– сфера оборони;

– сфера економіки, науки і техніки;

– сфера зовнішніх відносин;

– сфера державної безпеки та охорони правопорядку.

Не належить до державної таємниці інформація:

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

– про аварії, катастрофи, небезпечні природні явища й інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

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

– про факти порушень прав і свобод людини та громадянина;

– про незаконні дії державних органів, 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 надана Верховною Радою України, не може бути обмежено.

Віднесення інформації до державної таємниці здійснює спеціальний суб'єкт – *державний експерт з питань таємниць*. Вказану категорію осіб призначає своїм Указом Президент України.

Наприклад, у системі *Міністерства внутрішніх справ України* державними експертами з питань таємниць є:

– Міністр внутрішніх справ України;

– Перший заступник Міністра внутрішніх справ України;

– Державний секретар Міністерства внутрішніх справ України;

– Заступник Міністра внутрішніх справ України;

– Командувач Національної гвардії України;

– Перший заступник командувача Національної гвардії України.

У системі *Національної поліції України*:

– Голова Національної поліції України;

– Перший заступник Голови Національної поліції України – начальник кримінальної поліції;

– Заступник Голови Національної поліції України – начальник Головного слідчого управління[61].

На підставі рішень державних експертів з питань таємниць Служба безпеки України формує та публікує в офіційних виданнях *Звід відомостей, що становлять державну таємницю*. На сьогодні в

[61] Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць, затверджений Указом Президента України від 01.12.2009 № 987/2009; [із змінами і доповненнями на 13.02.2019]. *Офіційний вісник України*. 2009. № 94 (14.12.2009). ст. 3204.

Україні діє Звід відомостей, що становлять державну таємницю (далі ЗВДТ), затверджений наказом Служби безпеки України від 12.08.2005 № 440[62]. Надання грифу секретності документам, що містять інформацію, яка є державною таємницею, здійснюється на підставі ЗВДТ. Схематично ЗВДТ зображено на рис. 6.2.

Рис. 6.2. Схематичне зображення ЗВДТ

На підставі та в межах ЗВДТ з метою конкретизації та систематизації даних про секретну інформацію органи державної влади створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану з державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються зі Службою безпеки України, затверджуються державними експертами з питань таємниць і реєструються у Службі безпеки України.

[62] Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України № 440 від 12.08.2005 ; [із змінами і доповненнями на 17.09.2019]. *Офіційний вісник України*. 2005. № 34 (09.09.2005). ст. 2089.

Для державної таємниці існують такі *ступені секретності* (в дужках вказаний строк дії рішення про віднесення інформації до державної таємниці):

– **особливої важливості** (30 років);

– **цілком таємно** (10 років);

– **таємно** (5 років).

Після закінчення відповідного строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць робить висновок про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії зазначеного рішення в межах строків, вказаних вище.

Реквізити матеріальних носіїв інформації, що містять державну таємницю, подібні до реквізитів на документах ДСК. У випадку державної таємниці вказуються:

– *гриф секретності* – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності інформації;

– *дата та строк засекречування* матеріального носія секретної інформації тощо.

З метою охорони державної таємниці впроваджуються:

– єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації (*встановлюються Кабінетом Міністрів України*);

– дозвільний порядок провадження органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею (*за результатами спеціальної експертизи*);

– 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 державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать (окремо дивись Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства[63]);

[63] Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства, затверджене указом

– особливості здійснення органами державної влади їх функцій щодо органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

– режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

– спеціальний порядок допуску та доступу громадян до державної таємниці;

– технічний і криптографічний захист секретної інформації.

Основним підрозділом, який здійснює заходи щодо забезпечення режиму секретності та контроль за їх додержанням, є режимно-секретний орган (РСО).

Завдання РСО:

– недопущення необґрунтованого допуску та доступу осіб до секретної інформації;

– своєчасне розроблення та реалізація разом з іншими структурними підрозділами органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій заходів, що забезпечують охорону державної таємниці;

– запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;

– виявлення та закриття каналів витоку секретної інформації в процесі діяльності органів державної влади, органів місцевого самоврядування, підприємства, установи, організації;

– забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин;

– організація та ведення секретного діловодства;

– здійснення контролю за станом режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

Президента України від 17.07.2006 № 621/2006. *Офіційний вісник України*. 2006. № 29 (02.08.2006). ст. 2083.

Для початку роботи з державною таємницею особі необхідно отримати відповідний ***допуск*** – оформлення права громадянина на доступ до секретної інформації (рис. 6.3).

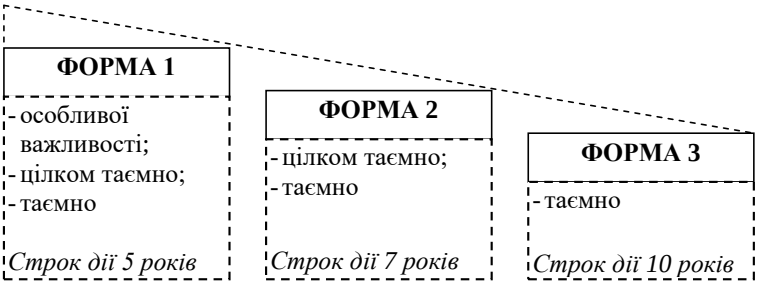


Рис. 6.3. Форми допуску до державної таємниці

Допуск до державної таємниці не надається в разі:

1) відсутності у громадянина обґрунтованої необхідності в роботі із секретною інформацією;

2) сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом;

3) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

4) наявності у громадянина судимості за тяжкі або особливо тяжкі злочини, не погашеної чи не знятої у встановленому порядку;

5) наявності у громадянина психічних розладів, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого Міністерством охорони здоров'я України і Службою безпеки України.

У наданні допуску до державної таємниці може бути відмовлено також у разі:

1) повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;

2) постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;

3) невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше.

При оформленні допуску до державної таємниці оформлюються документи, форми яких наведено в наказі Служби безпеки України від 18.07.2001 № 190[64].

Після оформлення допуску особа має отримати ***доступ до державної таємниці*** – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Громадянин, якому надано допуск до державної таємниці, *зобов'язаний*:

– не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

– не брати участі в діяльності політичних партій і громадських організацій, діяльність яких заборонена в порядку, встановленому законом;

– не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України;

– виконувати вимоги режиму секретності;

– повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні режимно-секретні органи про виникнення обставин, що виключають надання допуску до державної таємниці або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти у письмовій формі про свій виїзд з України;

---

[64] Про затвердження зобов'язання громадянина України у зв'язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці: наказ Служби безпеки України від 18.07.2001 № 190. *Офіційний вісник України*. 2001. № 35 (14.09.2001). ст. 1655.

– додержуватися інших вимог законодавства про державну таємницю.

У разі, коли за умовами своєї професійної діяльності громадянин *постійно* працює з відомостями, що становлять державну таємницю, йому повинна надаватися відповідна компенсація за роботу в умовах режимних обмежень, передбачена Положенням про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці[65] (рис. 6.4).

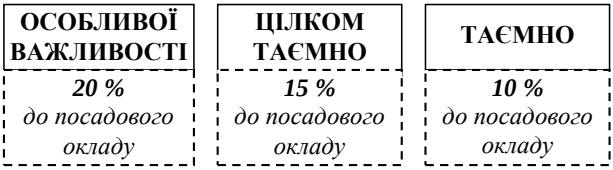


Рис. 6.4. Розміри компенсації

Для працівників РСО відповідні надбавки є більшими та складають:

– при роботі з інформацією особливої важливості – 60 %;

– при роботі з інформацією з грифом «цілком таємно» – 50 %;

– при роботі з інформацією з грифом «таємно» – 30 %.

Конкретні заходи з охорони державної таємниці на об'єктах інформаційної діяльності здійснюються відповідно до Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 № 939.

Державні органи, органи місцевого самоврядування, підприємства, установи і організації мають право провадити діяльність, пов'язану з державною таємницею, за умови надання їм відповідного спеціального дозволу на провадження такої діяльності.

[65] Положення про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці, затверджене постановою Кабінету Міністрів України від 15.06.1994 № 414 ; [із змінами і доповненнями на 15.01.2019]. *Офіційний вісник України*. 2008. № 58 (15.08.2008). ст. 1957.

Спеціальний дозвіл надається органами Служби безпеки України вказаним суб'єктам за умови, що вони:

– провадять або планують провадити діяльність, пов'язану з державною таємницею, відповідно до повноважень, державних завдань, програм, замовлень, договорів (контрактів);

– мають режимні приміщення та сховища матеріальних носіїв секретної інформації, які відповідають вимогам до забезпечення режиму секретності, виключають можливість доступу до них сторонніх осіб (тобто таких осіб, які не мають наданого в установленому порядку доступу до матеріальних носіїв секретної інформації) та гарантують збереження таких матеріальних носіїв;

– дотримуються передбачених законодавством вимог щодо забезпечення режиму секретності під час проведення секретних робіт і здійснення заходів, пов'язаних з використанням секретної інформації, а також порядку допуску та доступу осіб до державної таємниці, прийому іноземних громадян та іноземних делегацій, здійснення технічного та криптографічного захисту секретної інформації;

– мають режимно-секретний орган або режим секретності забезпечується його керівником чи працівником, призначеним для цього наказом керівника підприємства, установи, організації[66].

За порушення законодавства про державну таємницю передбачена дисциплінарна, адміністративна (ст. 212-2 КУпАП) та кримінальна відповідальність (ст. 111, 114, 328, 329, 422 Кримінального кодексу України).

2. Зарубіжний досвід захисту державної таємниці та службової інформації

Приблизно так само, як і в Україні, врегульовано питання захисту державної таємниці та службової інформації обмеженого поширення в Російській Федерації.

Нормативно-правовою базою обмеження доступу до окремих відомостей є Федеральний Закон «Про державну таємницю» від

[66] Порядок отримання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею URL: https://ssu.gov.ua/ua/pages/171 (дата звернення: 17.03.2019).

21.07.1993[67], Указ Президента Російської Федерації «Про затвердження переліку відомостей, віднесених до державної таємниці» від 30.11.1995 № 1203[68], Положення про порядок поводження зі службовою інформацією обмеженого поширення у федеральних органах виконавчої влади, затверджене Постановою Уряду РФ від 03.11.1994 № 1233; Указ Президента Російської Федерації «Про затвердження переліку відомостей конфіденційного характеру» від 06.03.1997 № 188[69].

Відмінність законодавства Росії в цій сфері від українського полягає в тому, що в указаному вище Указі Президента РФ № 1203 вказується лише перелік відомостей, які становлять державну таємницю, а відповідні ступені секретності цим відомостям надають уповноважені Президентом органи державної влади в розгорнутих переліках відомостей, що підлягають засекречуванню. Так, наприклад, щодо відомостей, в яких розкриваються сили, засоби, джерела, методи, плани, результати оперативно-розшукової діяльності, такими повноваженнями наділено Міністерства внутрішніх справ, оборони, юстиції, Службу зовнішньої розвідки, Федеральну службу безпеки Росії тощо[70].

У ст. 5 Федерального Закону «Про державну таємницю» викладено відомості, що підлягають віднесенню до державної таємниці, які поділяються на чотири основні групи. Схематично це зображено на рис. 6.5.

Основним критерієм віднесення відомостей до державної таємниці є необхідність забезпечення оборони безпеки держави та правоохоронної діяльності в Російській Федерації.

---

[67] О государственной тайне: федеральный закон от 21.07.1993; [с изм. и доп. на 29.07.2018]. *Российская газета*. №182. 21.09.1993.

[68] Перечень сведений, отнесенных к государственной тайне, утвержденный указом Президента РФ № 1203 от 30.11.1995; [с изм. и доп. на 14.01.2019]. *Российская газета*. № 246. 27.12.1995.

[69] Об утверждении перечня сведений конфиденциального характера: указ Президента РФ №188 от 06.03.1997; [с изм. и доп. на 13.07.2015] // Собрание законодательства РФ. – 10.03.1997. – № 10. – ст. 1127.

[70] Перечень сведений, отнесенных к государственной тайне, утвержденный указом Президента РФ № 1203 от 30.11.1995; [с изм. и доп. на 14.01.2019]. *Российская газета*. № 246. 27.12.1995.

Рис. 6.5. Сфера охорони державної таємниці РФ

Також у ст. 7 Федерального Закону «Про державну таємницю» визначено відомості, що не підлягають віднесенню до державної таємниці та засекречуванню. Перелік цих відомостей зображено на рис. 6.6.

Надання відомостям, що становлять державну таємницю, того чи іншого ступеня секретності залежить від того, яку шкоду буде завдано безпеці держави.

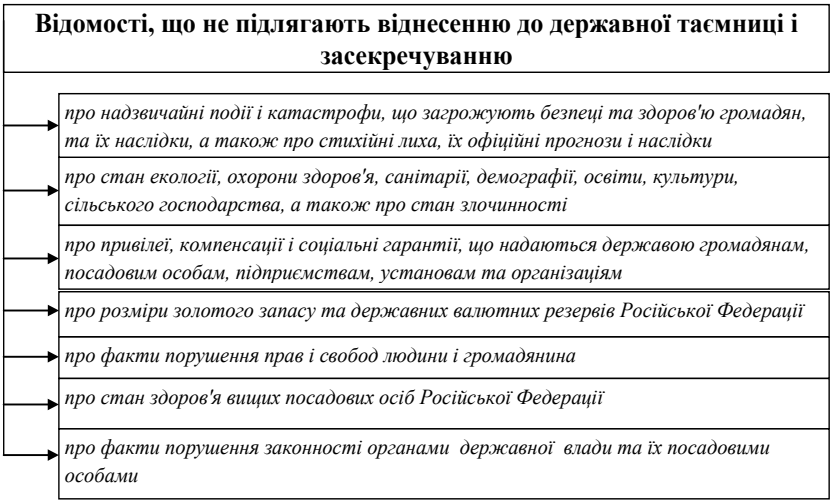


Рис. 6.6. Відомості, що не підлягають віднесенню до державної таємниці і засекречуванню

Особливу роль серед органів захисту державної таємниці відіграє Міжвідомча комісія із захисту державної таємниці. Цей орган має надвідомчий характер і займається виключно питаннями захисту державної таємниці, на відміну від інших органів захисту такої таємниці, до функцій яких входить виконання також інших обов'язків згідно з їх основним профілем.

Як випливає зі ст. 8 Федерального Закону «Про державну таємницю» Уряд РФ має встановлювати порядок визначення розміру шкоди, яка виникла в результаті несанкціонованого поширення відомостей, що становлять державну таємницю, а також шкоди, що завдається власникові інформації в результаті її засекречування.

На рис. 6.7 відображено повноваження органів державної влади та посадових осіб у сфері віднесення відомостей до державної таємниці та їх захисту відповідно до ст. 4. Федерального Закону «Про державну таємницю».

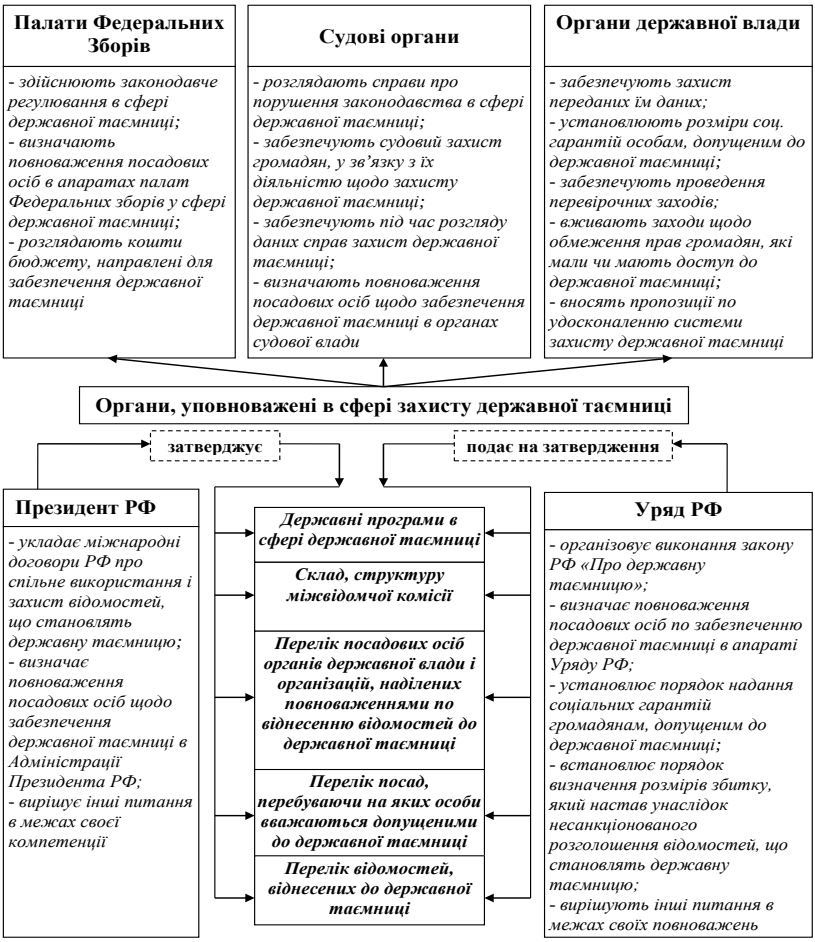


Рис. 6.7. Повноваження органів державної влади і посадових осіб у сфері віднесення відомостей до державної таємниці та її захисту

На відміну від України, в Росії немає державних експертів з питань таємниць. Частково їхню функції виконують інші особи відповідно до розпорядження Президента РФ «Про затвердження

переліку посад, при заміщенні яких особи вважаються допущеними до державної таємниці»[71].

Кримінальну відповідальність за порушення законодавства РФ у сфері державної таємниці встановлено у Кримінальному кодексі РФ (рис. 6.8)[72].

Рис. 6.8. Кримінальна відповідальність за порушення законодавства РФ про державну таємницю

Законодавством України та РФ встановлена кримінальна відповідальність за подібні діяння у сфері порушення законодавства про державну таємницю, різниця полягає в тому, що Кримінальний кодекс РФ передбачає більш суворе покарання, ніж Кримінальний кодекс України.

У США система обмеження доступу до певних відомостей регулюється Указом Президента «Секретна інформація у сфері національної безпеки»[73], відповідно до якого існують три ступені секретності: цілком таємно (Top Secret), таємно (Secret) та конфіденційно (Confidential).

---

[71] Об утверждении перечня должностей, при замещении которых лица считаются допущенными к государственной тайне: распоряжение Президента Российской Федерации от 15 января 2010 года N 24-рп. URL: http://www.rg.ru/2010/04/28/tayna-site-dok.html (дата звернення: 17.03.2019).

[72] Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ: [по состоянию на 27.12.2018]. *Собрание законодательства Российской Федерации*. 1996. № 25. Ст. 2954.

[73] Executive Order 13526 Classified National Security Information, December 29, 2009. URL: http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf (дата звернення: 17.03.2019). Section 1.2.

Причому до інформації зі ступенем секретності «цілком таємно» належать відомості, несанкціоноване розкриття яких може завдати тяжкої шкоди національній безпеці, до інформації зі ступенем секретності «таємно» – відомості, несанкціоноване розкриття яких може завдати значної шкоди національній безпеці, до інформації зі ступенем секретності «конфіденційно» – відомості, несанкціоноване розкриття яких може завдати шкоди національній безпеці.

До інформації, яка може бути засекречена, належать: відомості про військові плани, озброєння або операції; інформація іноземних урядів; відомості про розвідувальні заходи (в тому числі спеціальні заходи), розвідувальні джерела чи методи або криптологію; інформація про іноземні відносини або закордонні заходи США, враховуючи конфіденційні джерела; інформація про наукову, технологічну або економічну діяльність щодо забезпечення національної безпеки, яка забезпечує захист від міжнародного тероризму; інформація про програми США щодо безпеки ядерних матеріалів та обладнання; інформація щодо вразливості та можливості систем, установок, інфраструктур, проєктів, планів або захисних служб національної безпеки, які забезпечують захист від міжнародного тероризму або зброї масового знищення.

Всі інші категорії інформації засекречувати забороняється.

На базі вищезгаданого Указу Президента США відповідні державні органи розробляють власні інструкції щодо роботи з державною таємницею.

Крім зазначеного вище указу слід також відзначити, ухвалений 07.10.2011 Президентом США Указ № 13587 «Про структурну реформу щодо підтримання безпеки секретних мереж та обґрунтованого поширення й убезпечення секретної інформації» («Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information»), який присвячено захисту секретної інформації, що циркулює в комп'ютерних мережах.

У Великій Британії закон з охорони державної таємниці також має назву «Про державну таємницю» («Official Secrets Act»). Він був ухвалений у 1989 році. Однак історія законодавства з охорони державної таємниці у Великобританії значно довша. Вона бере початок ще у 1889 році, коли було вперше ухвалено закон з аналогічною назвою.

Систему охорони державної таємниці викладено в Настанові з охорони державної таємниці (Manual of Protective Security), на базі якої міністерства розробляють власні настанови.

Згідно з чинним законодавством Великобританії інформація з обмеженим доступом може мати чотири ступені секретності: цілком таємно (Top Secret); таємно (Secret); конфіденційно (Confidential); для службового користування (Restricted).

До інформації зі ступенем «цілком таємно» належать відомості, несанкціоноване розголошення яких може призвести до: безпосередньої загрози внутрішній стабільності Об'єднаного Королівства або дружніх йому країн; значних людських втрат; може завдати тяжкої шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; заподіяти тяжку шкоду взаєминам із дружніми урядами або нанести довгострокові збитки економіці Королівства.

Прикладом правоохоронної інформації, яка належить до цієї категорії відомостей у Великій Британії, є перелік потенційних мішеней терористів, база даних інформаторів і кримінальної розвідки тощо.

До інформації зі ступенем «таємно» належать відомості, несанкціоноване розголошення яких може: обернутися підвищенням рівня міжнародної напруженості; серйозно зашкодити відносинам з дружніми урядами; безпосередньо загрожувати життю або завдати значної шкоди громадському порядку або безпеці та свободам особистості; завдати значної шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; спричинити істотну матеріальну шкоду національним фінансам чи економіці та комерційним інтересам.

Прикладом правоохоронної інформації, яка належить до цієї категорії відомостей у Великій Британії, є об'єкти спеціальних операцій, інформація, яка розшифровує особу інформатора, оскільки її розголошення може загрожувати його життю.

До інформації зі ступенем «конфіденційно» належать відомості, несанкціоноване розголошення яких може: завдати матеріальної шкоди дипломатичним стосункам, що матиме наслідком офіційний протест або інші санкції; заподіяти шкоду безпеці та свободам особистості; завдати шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; спричинити шкоду національним фінансам чи економіці

та комерційним інтересам; істотно підірвати фінансову спроможність основних (крупних) організацій; перешкодити розслідуванню або полегшити вчинення тяжкого злочину тощо.

Прикладом правоохоронної інформації, яка належить до цієї категорії відомостей у Великій Британії, є: відомості про інформаторів, які не розкривають їх справжньої особи, проте розголошення яких може загрожувати безпеці інформаторів; відомості про спеціальні операції, розкриття яких може зашкодити розслідуванню тяжких злочинів; відомості про характер злочинної діяльності та можливі методи її припинення.

До інформації зі ступенем «для службового користування» належать відомості, несанкціоноване розголошення яких може: зашкодити міжнародним стосункам, ускладнити забезпечення ефективності або безпеки британських чи союзницьких сил; завдати шкоди розслідуванню або полегшити скоєння злочину; завдати фінансової шкоди фізичним або юридичним особам, підірвати належний рівень управління державним сектором тощо.

Прикладом правоохоронної інформації, яка належить до цієї категорії відомостей у Великій Британії, може бути інформація, отримана від поліції іншої країни, якщо така передача інформації не була загальновідомою, покази осіб у справі, розголошення яких може зашкодити розслідуванню тощо[74].

У Німеччині система захисту державних секретів перетинається із загальною системою захисту значущих секретів у сфері промисловості й торгівлі (промислове шпигунство) та регулюється нормами низки законів, до яких належать: Кримінальний кодекс, Закон про боротьбу з недобросовісною конкуренцією, Постанова про боротьбу з підкупом непосадових осіб, Федеральний закон про охорону даних тощо. Кримінальний кодекс Німеччини, наприклад, містить положення про те, що державною таємницею є факти, об'єкти й інформація, доступні лише обмеженому колу осіб, які повинні зберігатися в секреті від іноземних держав з метою недопущення нанесення шкоди зовнішній безпеці Федеративної республіки.

[74] Перепелиця М. М., Манжай О. В. Провадження оперативно-розшукових заходів у Великій Британії, Росії, США та Україні: монографія. Харків : Вид-во КП Друкарня № 13, 2008. 248 с.: іл.

Удосконалення захисту державних секретів здійснюється за трьома напрямами: вдосконалення законодавства у сфері захисту державних секретів і секретів фірм; посилення органів контррозвідки та надання їм великих повноважень, у тому числі у сфері захисту державних секретів; створення організацій «самодопомоги» у промисловості та розгортання їх діяльності.

Важливим у вдосконаленні захисту секретів під час проведення науково-дослідних робіт військового призначення в Німеччині є посилення органів контррозвідки, зокрема тих її підрозділів, які покликані вести боротьбу зі шпигунством і займатися питаннями захисту державних секретів, у тому числі у промисловості.

У системі забезпечення захисту державних секретів у питаннях боротьби з «промисловим шпигунством» іноземних держав важлива роль відводиться об'єднанням промисловців – так званим організаціям самодопомоги. До таких організацій належить, наприклад, Координаційний центр із забезпечення безпеки в промисловості, створений у Кельні в 1969 р., який вирішує проблеми забезпечення режиму секретності у промисловості держави[75].

У ФРН інформація з обмеженим доступом може мати три ступені секретності: цілком таємно (Streng Geheim); таємно (Geheim); конфіденційно (VS-Vertraulich).

Слід зазначити, що у ФРН до державної таємниці належать лише відомості, які необхідно зберігати в секреті від іноземних держав з метою недопущення нанесення шкоди зовнішній безпеці країни. Водночас, наприклад, відомості, які містять інформацію про проведення оперативно-розшукових заходів, належать до службової таємниці й охороняються відповідним законодавством. Зокрема, відповідальність за порушення службової таємниці встановлена у 28 Розділі Кримінального кодексу ФРН. Відповідні документи, що містять службову таємницю, позначають грифом «для службового користування» (VS nur fur den dienstgebrauch).

Якщо документи для службового користування обробляються в автоматизованих системах, то мають бути дотримані певні вимоги безпеки. Зокрема, автоматизована система має бути обладнана

[75] Шавкеро А. Зарубежный опыт защиты государственной тайны и возможности его использования в России. *Право и жизнь*. 2008. №124 (7). URL: https://studylib.ru/doc/3749864/shavkero-a.---zarubezhnyj-opyt-zashhity-gosudarstvennoj-tajny (дата звернення: 17.03.2019).

брандмауером, у випадку підключення до мережі Інтернет має бути затверджений перелік осіб, які мають доступ до автоматизованої системи, використовуватися механізми автентифікації та ідентифікації (ім'я користувача та пароль), обов'язковою є наявність інструкції з ІТ-безпеки тощо[76].

Кримінальна відповідальність за порушення законодавства у сфері державної таємниці в Німеччині передбачена Кримінальним кодексом ФРН[77]. Наочно це зображено на рис. 6.9.

Рис. 6.9. Кримінальна відповідальність за порушення законодавства Німеччини у сфері охорони державної таємниці

Кримінальний кодекс Німеччини в § 93 дає визначення, що *державною таємницею* є факти, об'єкти й інформація, доступні лише обмеженому колу осіб, які повинні зберігатися в секреті від

[76] Instruction sheet on the Handling of Protectively Marked Information Classified VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VS-MerkblattEnglisch_pdf.pdf?__blob=publicationFile (дата звернення: 17.03.2019). Section II (1).

[77] German criminal code Уголовный кодекс ФРГ. URL: https://www.gesetze-im-internet.de/englisch_stgb/ (дата звернення: 17.03.2019).

іноземних держав з метою недопущення нанесення шкоди зовнішній безпеці Федеративної республіки.

Систему захисту державної таємниці у Китайській Народній Республіці представлено Законом КНР «Про захист державної таємниці» (中华人民共和国保守国家秘密法) від 29.04.2010[78]. Згідно зі ст. 9 цього закону до державної таємниці відносяться, зокрема, окремі відомості, що стосуються діяльності з охорони державної безпеки та розслідування кримінальних злочинів.

Сфера охорони державної таємниці у КНР зображена на рис. 6.10[79].

За ступенем секретності державна таємниця в Китаї поділяється на три рівні: цілком таємна (绝密); таємна (机密); конфіденційна (秘密).

Цілком таємна інформація – це найважливіша державна таємниця, розголошення якої може завдати дуже значної шкоди національній безпеці та національним інтересам.

Таємна інформація – це важлива державна таємниця, розголошення якої може завдати значної шкоди національній безпеці та національним інтересам.

Конфіденційна інформація – це державна таємниця, розголошення якої може завдати шкоди національній безпеці та національним інтересам.

Конкретні сфери та категорії державної таємниці визначаються спеціально уповноваженим органом з охорони державної таємниці спільно з міністерствами закордонних справ, громадської безпеки, державної безпеки та іншими відповідними центральними органами[80].

---

[78] Law of the People's Republic of China on Guarding State Secrets (2010 Revision) URL: http://en.pkulaw.cn/display.aspx?id=8039&lib=law&SearchKeyword=&SearchCKeyword= (дата звернення: 17.03.2019). Article 10.

[79] State Secrets China's Legal Labyrinth. URL: http://www.lapres.net/statesecrets.pdf (дата звернення: 17.03.2019).

[80] Law of the People's Republic of China on Guarding State Secrets (2010 Revision) URL: http://en.pkulaw.cn/display.aspx?id=8039&lib=law&SearchKeyword=&SearchCKeyword= (дата звернення: 17.03.2019). Article 11.

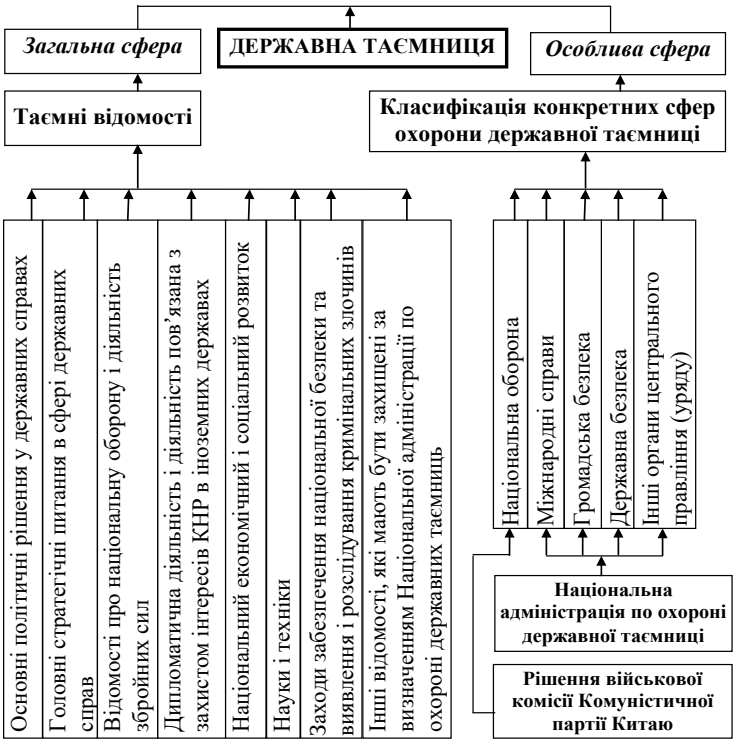


Рис. 6.10. Сфера охорони державної таємниці у КНР

Особливе місце в законі відведено врегулюванню питання безпеки державної таємниці в інформаційних системах (рис. 6.11).

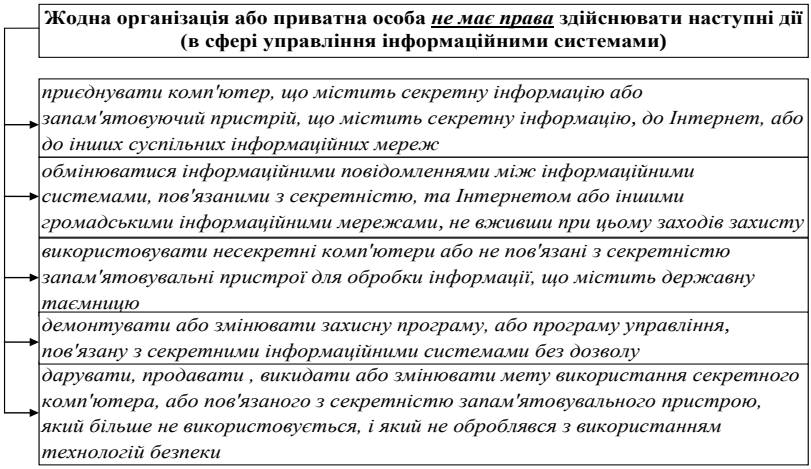


Рис. 6.11. Заборонені законом дії у сфері управління інформаційними системами

Спеціально уповноваженим органом захисту державної таємниці є Національна адміністрація з охорони державної таємниці КНР (中共中央保密委员会办公室) – орган державної влади КНР, який відповідає за захист державної таємниці. Також існує аналогічний партійний орган – Центральний комітет із захисту державної таємниці, що підпорядковується Центральному комітету Комуністичної партії Китаю. В особливих адміністративних районах Китаю – Гонконгу і Макао – діє своя система класифікації та захисту секретної інформації[81]. Систему адміністративних органів, що відповідають за охорону державної таємниці в КНР, схематично зображено на рис. 6.12.

[81] Национальная администрация по охране государственных тайн. URL: http://ru.wikipedia.org/wiki/Национальная_администрация_по_охране_государственных_тайн (дата звернення: 17.03.2019).

Рис. 6.12. Система адміністративних органів, що відповідають за охорону державних таємниць у КНР

Кримінальна відповідальність за порушення законодавства у сфері державної таємниці в КНР передбачена Кримінальним кодексом КНР[82]. Наглядно це зображено на рис. 6.13.

Покарання за злочини у сфері охорони державної таємниці, на відміну від попередньо розглянутих країн, у КНР є дуже суворими, аж до смертної кари[83].

[82] Criminal Law of the People's Republic of China. URL: https://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm (дата звернення: 17.03.2019).

[83] Манжай О. В. Космиця А. П. Аналіз системи охорони державної таємниці в Китайській Народній Республіці. *Право і безпека*. 2014. № 4 (51). С. 40-41.

Рис. 6.13. Кримінальна відповідальність за порушення законодавства КНР у сфері охорони державної таємниці

На відміну від КНР, ФРН, а також країн пострадянського простору, для США та Великобританії характерними є більш докладні приписи щодо віднесення тієї чи іншої правоохоронної інформації до державної таємниці. Це зумовлено прецедентною системою права, яка тяжіє до якомога більшої конкретизації рішень, що можуть бути прийняті в рамках тих чи інших суспільних відносин. Серед розглянутих систем захисту інформації за допомогою інституту таємниць найбільш схожими до української є системи Російської Федерації, КНР та Великобританії, хоча існує і певна структурна різниця в загальному підході до захисту державних секретів.

Питання для самоконтролю

1. Нормативно-правова база захисту державної таємниці.
2. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці.
3. Спеціальний суб’єкт, який здійснює віднесення інформації до державної таємниці.

4. Звід відомостей, що становлять державну таємницю, та документи, які складаються на його основі.

5. Реквізити матеріальних носіїв інформації, що містять державну таємницю та ступені секретності.

6. Завдання РСО.

7. Допуск до державної таємниці.

8. Доступ до державної таємниці.

9. Обов'язки громадянина, якому надано допуск до державної таємниці.

10. Компенсація за роботу в умовах режимних обмежень.

11. Відповідальність за порушення законодавства про державну таємницю.

12. Досвід Російської Федерації щодо правого регулювання захисту державної таємниці.

13. Досвід США щодо правого регулювання захисту державної таємниці.

14. Досвід Великої Британії та ФРН щодо правого регулювання захисту державної таємниці.

15. Досвід КНР щодо правого регулювання захисту державної таємниці.

План практичної підготовки за темою:
«Захист державної таємниці в Україні»

Вид: практичне заняття.

Мета: розв'язання задач.

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.

2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).

3. Розв'язання задач (140 хв).

4. Викладач оцінює якість роботи за чотирьохбальною шкалою.

5. По закінченні заняття підбиваються підсумки (10 хв.).

Задача № 1

Публіцист Юрков надрукував у газеті цікаву статтю «Неоцінимий капітал України», в якій навів одержані від експерта Ради національної безпеки та оборони Короткіх загальні відомості про державні запаси дорогоцінних металів і каменів, а також назвав розміри золотого запасу та валютних резервів України.

Начальник відділу Ради національної безпеки та оборони Романів, прочитавши в газеті статтю Юркова і з'ясувавши, звідки він одержав інформацію, поставив перед своїм керівництвом питання про притягнення до відповідальності Короткіх за розголошування відомостей, які належать до державної таємниці.

Проаналізуйте цю ситуацію.

Відповідь: дивіться Закон України «Про державну таємницю», Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12.08.2005 № 440.

Задача № 2

Програміста Науково-дослідного інституту засобів зв'язку Суходольського запросив до себе начальник Департаменту МВС України Виськуб і запропонував йому очолити відділ закритих програм. Суходольській подумав і погодився. Згодом він в установленому порядку звільнився з НДІ, його призначили на нову посаду, він приступив до роботи. Проте буквально через декілька днів після призначення Виськуб зайшов до Суходольського і сказав: «Пробачте, вас не допустили до роботи із секретною інформацією, оскільки ви свого часу працювали в інформаційній комерційній фірмі. Нам доведеться вас звільнити».

Проаналізуйте цю ситуацію.

Відповідь: дивіться Закон України «Про державну таємницю».

Задача № 3

Державним експертом з питань таємниць під час виконання своїх функціональних обов'язків 1 жовтня минулого року було віднесено до державної таємниці дані, що стосуються життєвого рівня населення та визначено цим даним ступінь секретності «таємно».

Після винесення рішення про віднесення цих відомостей до державної таємниці державний експерт надав його 25 жовтня минулого року до Служби безпеки України.

Дайте правову оцінку ситуації. Чи правильно вчинив державний експерт?

Відповідь: дивіться Закон України «Про державну таємницю», Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12.08.2005 № 440.

Задача № 4

Юрист Воробйов спільно з головним бухгалтером Синіциним, які працювали на заводі «Танк», що займався випуском танків для Міністерства оборони України, підготували на вимогу генерального директора Абрамова докладний звіт про діяльність підприємства за рік. У звіті містились як копії договорів, які підприємство уклало протягом року, так і документи, що характеризують фінансову діяльність заводу. Підготувавши документ, Синіцин вирішив, що ця інформація не повинна стати відомою широкому колу осіб, у зв'язку з чим звернувся до генерального директора Абрамова з письмовим проханням про віднесення інформації, що міститься у звіті, до комерційної таємниці. Воробйов зробив на документі позначку «таємно» та сховав його в сейф.

Через місяць правоохоронними органами на заводі проводилася перевірка у зв'язку з підозрою підприємства в ухиленні від сплати податків. Коли правоохоронці почали вимагати документи, які характеризують діяльність підприємства за минулий рік, їм було відмовлено. Генеральний директор разом із головним бухгалтером мотивували свою відмову тим, що ці документи віднесено до комерційної таємниці, вони не можуть бути видані.

Дайте правову оцінку ситуації. Охарактеризуйте дії учасників.

Відповідь: дивіться Закон України «Про державну таємницю», Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12.08.2005 № 440.

Задача № 5

Підприємство «Енкодінг», яке здійснює свою діяльність, пов'язану з державною таємницею, за ініціативою та погодженням із замовником робіт винайшло нову технологію виготовлення державних шифрів. З урахуванням ступеня секретності інформації директор підприємства «Енкодінг» встановив, що ця інформація належить до категорії «таємно», тому строк дії рішення про віднесення її до державної таємниці складатиме 10 років.

Дайте правову оцінку ситуації.

Відповідь: дивіться Закон України «Про державну таємницю», Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12.08.2005 № 440.

План практичної підготовки за темою: «Судова практика щодо правопорушень, пов'язаних із державною таємницею»

Вид: семінарське заняття.

Мета: розглянути типові порушення режиму секретності, спираючись на судову практику.

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (10 хв.).
3. Групу потрібно поділити на три команди. Кожна команда отримує завдання. Через визначений час команди по черзі відповідають на поставлені завдання. Дискусія (60 хв).
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (10 хв.).

Справа № 1

Фабула

Працівниками управління режимно-секретного та документального забезпечення ГУ МВС України в м. Києві 1 вересня 2014 року була проведена перевірка дотримання порядку обробки та зберігання інформації з обмеженим доступом на електронно-обчислювальній техніці, дотримання законодавства у сфері охорони державної таємниці та технічного захисту інформації в управлінні боротьби зі злочинами, пов'язаними з торгівлею людьми ГУ МВС України в м. Києві.

Під час перевірки підрозділу у службовому кабінеті на робочому столі було виявлено сумку з ноутбуком, в якій також знаходився робочий зошит, що має гриф секретності «таємно», оперуповноваженого СБЗПТЛ Оболонського районного управління ГУ МВС України в м. Києві.

?

Під час огляду вказаного ноутбука було встановлено, що він не перебуває на балансі органів і підрозділів ГУ МВС України в м. Києві, має вихід до глобальної комп'ютерної мережі Інтернет та використовується для обробки інформації, яка утворилась у процесі оперативно-службової діяльності. При цьому оперативний працівник не отримував дозволу на використання в роботі приватного ноутбуку.

Оперативного працівника було притягнуто до дисциплінарної відповідальності у вигляді догани. Не погоджуючись із вищевикладеними обставинами, він звернувся до суду з відповідним позовом.

Проаналізуйте цю ситуацію.

Витяг з ухвали суду[84]

У жовтні 2014 року оперуповноважений сектора боротьби зі злочинами, пов'язаними з торгівлею людьми Оболонського РУ ГУ МВС України у м. Києві звернувся до суду з адміністративним позовом про: визнання протиправними дій начальника Управління режимно-секретного та документального забезпечення Головного управління Міністерства внутрішніх справ України в м. Києві, які полягали у незаконному проведенні перевірки дотримання режиму секретності позивача, незаконному вилученні робочого зошиту та персонального комп'ютеру; визнання протиправним рішення ГУ МВС України в м. Києві про притягнення до дисциплінарної відповідальності; скасування наказу про притягнення позивача до дисциплінарної відповідальності.

Серед іншого судом було встановлено, що працівниками управління режимно-секретного та документального забезпечення ГУ МВС України в м. Києві 1 вересня 2014 року була проведена перевірка дотримання порядку обробки та зберігання інформації з обмеженим доступом на електронно-обчислювальній техніці, дотримання законодавства у сфері охорони державної таємниці та технічного захисту інформації в управлінні боротьби зі злочинами, пов'язаними з торгівлею людьми ГУ МВС України в м. Києві.

Під час перевірки підрозділу у службовому кабінеті на робочому столі було виявлено сумку з ноутбуком, в якій також знаходився робочий зошит, що має гриф секретності «таємно», оперуповноваженого СБЗПТЛ Оболонського районного управління ГУ МВС України в м. Києві.

Під час огляду вказаного ноутбука було встановлено, що він не перебуває на балансі органів і підрозділів ГУ МВС України в м. Києві, має вихід до глобальної комп'ютерної мережі Інтернет і використовується для обробки інформації, яка утворилась у процесі

---

[84] Ухвала Вищого адміністративного суду України від 08.07.2015 : К/800/9670/15 URL: http://www.reyestr.court.gov.ua/Review/46642786 (дата звернення: 17.03.2019); Ухвала Київського апеляційного адміністративного суду від 03.02.2015 : Справа: № 826/15971/14 URL: http://www.reyestr.court.gov.ua/Review/42559191 (дата звернення: 17.03.2019); Постанова Київського окружного адміністративного суду від 06.11.2014 : № 826/15971/14 URL: http://www.reyestr.court.gov.ua/Review/41338639 (дата звернення: 17.03.2019).

оперативно-службової діяльності. При цьому позивач не отримував дозволу на використання в роботі приватного ноутбуку.

Згідно з викладеними у довідці від 8 вересня 2014 року відомостями начальника режимно-секретного сектору Оболонського районного управління ГУ МВС України в м. Києві позивач не отримував дозволу на використання в роботі приватного ноутбука. 9 вересня 2014 року членом комісії було взято у позивача пояснення за фактами порушення вимог режиму секретності та технічного захисту інформації.

14 серпня 2012 року позивач взяв на себе зобов'язання виконувати вимоги режиму секретності у зв'язку з допуском до державної таємниці та був ознайомлений з нормами законодавства щодо обмеження прав у зв'язку з допуском до державної таємниці та попереджений про відповідальність за порушення законодавства у сфері охорони державної таємниці.

Відповідно до вимог п. 116 Порядку № 939 громадянин, якому надано допуск і доступ до державної таємниці, зобов'язаний: виконувати вимоги режиму секретності; зберігати секретні документи тільки у спецпортфелі, спецвалізі, робочій папці, металевій шафі чи сейфі; закривати у сейфі чи металевій шафі носії секретної інформації, в тому числі такі, що містяться в робочій папці, в разі залишення службового приміщення; здавати своєчасно до режимно-секретного органу (уповноваженому режимно-секретного органу) виконані секретні документи за підписом у внутрішньому описі за формою згідно з додатком 18 або у відповідних облікових картках чи журналах обліку; повертати своєчасно секретні документи та вироби після закінчення роботи з ними до режимно-секретного органу (уповноваженому режимно-секретного органу); здавати своєчасно до режимно-секретного органу (уповноваженому режимно-секретного органу) всі секретні документи і вироби, відповідальність за зберігання яких на них покладено, а також до бібліотеки секретні видання, науково-технічну документацію й інші матеріальні носії секретної інформації; користуватися секретними документами та виробами так, щоб виключити можливість ознайомлення з ними інших осіб, у тому числі тих, які допущені до подібних робіт, документів і виробів, якщо на цей час вони не мають прямого відношення до роботи з ними; додержуватися встановленого порядку пересилання,

перевезення та передачі матеріальних носіїв секретної інформації; додержуватись інших вимог законодавства про державну таємницю.

Згідно з п. 262 Порядку № 939 для зберігання секретних документів та інших матеріальних носіїв секретної інформації виконавцям видаються робочі папки, спецпортфелі, спецвалізи. У кінці робочого часу виконавці зобов'язані повернути робочу папку (спецпапку, спецвалізу) на зберігання до режимно-секретного органу.

Згідно з викладеними у довідці від 9 вересня 2014 року відомостями начальника режимно-секретного сектору Оболонського районного управління ГУ МВС України в м. Києві позивач у період з 28 серпня 2014 року по 1 вересня 2014 року спецвалізу не отримував. З вимогами Порядку № 939 був ознайомлений.

На підставі викладеного суд дійшов висновку, що відповідачем було правомірно притягнуто позивача до дисциплінарної відповідальності у вигляді оголошення догани. Суди апеляційної та касаційної інстанцій залишили скарги позивача без задоволення.

Справа № 2

Фабула

У 2014 р. начальник ГУ МВС України в Запорізькій області здійснив виїзди за кордон (Австрія, Чехія, Італія, Сполучене Королівство Великобританії) без погодження в установленому порядку з керівництвом МВС України. У результаті проведення службового розслідування було встановлено, що цими діями він порушив вимоги ст. 28 Закону України «Про державну таємницю», п. 696 Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 № 939, та п. 7.8. Інструкції про порядок забезпечення режиму секретності, охорони конфіденційної інформації, що є власністю держави, під час міжнародного співробітництва та виїзду за кордон працівників органів та підрозділів внутрішніх справ, яким надано допуск до державної таємниці, затвердженої наказом МВС України від 31.03.2009 № 142.

?

На начальника ГУ МВС України в Запорізькій області було накладено стягнення у вигляді попередження про неповну посадову відповідність.

Не погоджуючись із викладеними обставинами, він звернувся до суду з відповідним позовом.

Проаналізуйте цю ситуацію.

Витяг з ухвали суду[85]

Надаючи правову оцінку спірним відносинам, що виникли між сторонами у справі, суд виходив із такого.

За результатами проведеного службового розслідування 26 грудня 2014 р. складено висновок службового розслідування за фактами виїзду за кордон у 2014 році без погодження з керівництвом Міністерства начальника ГУМВС України в Запорізькій області.

Згідно з матеріалами розслідування позивач усно пояснив, що коли йому було надано короткострокову відпустку з 20 по 23 жовтня 2014 року, він з дозволу керівництва Міністерства виїжджав до м. Прага (Чеська Республіка).

Стосовно обставин виїзду позивача за кордон у 2014 році матеріали справи містять інформацію, надану Адміністрацією державної прикордонної служби, згідно з якою позивач: 8 вересня 2014 р. вилетів до Австрії (м. Відень) і 10 вересня 2014 р. повернувся з Австрії (м. Відень); 19 жовтня 2014 р. вилетів до Великобританії (м. Лондон) та 23 жовтня 2014 р. повернувся з Італії (м. Мілан). Також у висновку службового розслідування вказано, що при перевірці журналу РСУ ДРСДЗ щодо обліку виїздів за кордон працівників, яким надано допуск до державної таємниці, встановлено, що записи про виїзд за кордон начальника ГУ МВС України в Запорізькій області протягом 2014 року відсутні.

Однак матеріали справи не містять доказів одержання від будь-яких осіб, крім позивача, пояснень щодо виїзду останнього за кордон у 2014 році без відповідного дозволу.

При цьому за змістом довідки Управління режимно-секретного та документального забезпечення Головного управління МВС України в Запорізькій області згідно з Журналом обліку виїзду за кордон працівників, яким надано допуск до державної таємниці РСВ ГУМВС України в Запорізькій області (далі – Журнал), протягом 2014 року відповідно до вимог п. 696 Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 № 939, начальник ГУ МВС України в Запорізькій

[85] Постанова Запорізького окружного адміністративного суду від 26.05.2015 : Справа № 808/1268/15 URL: http://www.reyestr.court.gov.ua/Review/44702406 (дата звернення: 17.03.2019).

області двічі повідомляв УРСДЗ ГУМВС області про виїзди за кордон:

– про виїзд до Австрії у приватних справах у період з 8 вересня 2014 р. по 10 вересня 2014 р. Інструктаж з питань охорони державної таємниці проведено 5 вересня 2014 р. начальником УРСДЗ ГУ МВС. Про проведений інструктаж здійснено запис у Журналі, за який начальник ГУ МВС України в Запорізькій області поставив свій особистий підпис. Копія рапорту про виїзд у зазначений період до Австрії до УРСДЗ ГУМВС не надавалась;

– про виїзд до Чехії на відпочинок у період з 19 жовтня 2014 р. по 23 жовтня 2014 р. Інструктаж з питань охорони державної таємниці проведено 14 жовтня 2014 р. начальником УРСДЗ ГУ МВС. Про проведений інструктаж здійснено запис у Журналі, за який начальник ГУ МВС України в Запорізькій області поставив свій особистий підпис. Копія рапорту про виїзд у зазначений період до Чехії до УРСДЗ ГУМВС не надавалась.

Суд прийняв до уваги посилання відповідача на приписи ст. 28 Закону України «Про державну таємницю», згідно з якими громадянин, якому надано допуск до державної таємниці, зобов'язаний виконувати вимоги режиму секретності, та п. 7.8 Інструкції про порядок забезпечення режиму секретності, охорони конфіденційної інформації, що є власністю держави в системі МВС під час міжнародного співробітництва та виїзду за кордон працівників органів і підрозділів внутрішніх справ, яким надано допуск та доступ до державної таємниці, яка затверджена наказом МВС України від 31.03.2009 № 142, згідно з якими керівники ГУМВС перед виїздом до зарубіжної країни у приватних справах зобов'язані поінформувати про це рапортом із зазначенням країни, до якої буде здійснено виїзд, та терміну перебування в ній Міністра або особу, яка його заміщує.

Разом із тим, суд звернув увагу на те, що відповідно до вимог ст. 14 Дисциплінарного статуту при визначенні виду дисциплінарного стягнення має враховуватися, зокрема, заподіяна шкода. У судовому засіданні 25 травня 2015 р. на запитання суду представник відповідача не надав доказів наявності встановлених під час проведення службового розслідування фактів витоку інформації з обмеженим доступом та причетність до цього позивача.

Водночас суд звернув увагу на те, що інформація з обмеженим доступом, якою володіє позивач, може бути передана

різноманітними способами, які не потребують та не залежать від перебування особи за кордоном. При цьому посилання на те, що пересування позивача за кордоном може призвести до витоку інформації, є припущеннями, які не підтверджені будь-якими фактичними оцінками ризиків безпеки. Вказаний висновок суду узгоджується з практикою Європейського суду з прав людини, викладеною в Постанові ЄСПЛ у справі «Солтисяк проти Росії» (Soltysyak v. Russia, скарга № 4663/05), яка згідно з вимогами ч. 2 ст. 8 Кодексу адміністративного судочинства України у взаємозв'язку з приписами ст. 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» застосовується судами при розгляді справ як джерело права.

Виходячи з меж заявлених позовних вимог, системного аналізу положень чинного законодавства України та матеріалів справи, суд дійшов висновку, що викладені в позовній заяві докази позивача є обґрунтованими та такими, що підлягають задоволенню.

Справа № 3

Фабула

Комісією Служби безпеки України було проведено тематичну перевірку стану охорони державної таємниці у Дарницькому районному у м. Києві військовому комісаріаті, за результатами якої було складено акт.

Під час тематичної перевірки Службою безпеки України було виявлено низку порушень стану охорони державної таємниці в Дарницькому РВК, зокрема в режимному приміщенні на жорсткому магнітному диску персональної обчислювальної машини, яка не призначена для обробки секретної інформації, зберігалися електронні варіанти документів, що мають реквізити секретних документів. Вказана ПЕОМ у травні 2014 р. була підключена до мережі Інтернет і використовується для адміністрування внутрішньої безпровідної мережі Wi-Fi, до якої підключено 3 власні ноутбуки працівників Дарницького РВК, чим створено передумови до витоку секретної інформації.

?

Крім того, у цьому режимному приміщенні 18 червня 2014 р. працювали на ноутбуках посадові особи Комісаріату, які не мають допуску до державної таємниці.

На підставі висновків акта тематичної перевірки від 07.07.2014 Службою безпеки України 30 липня 2014 р. було затверджено висновок про скасування Дарницькому районному у м. Києві військовому комісаріату допуску до державної таємниці.

Не погоджуючись із викладеними обставинами, військовий комісар звернувся до суду з відповідним позовом.

Проаналізуйте цю ситуацію.

Витяг з ухвали суду[86]

Актом тематичної перевірки було встановлено, що означені порушення свідчать про зберігання протягом 5 років на зазначеній ПЕОМ секретної інформації без застосування комплексної системи захисту інформації з підтвердженою відповідністю (порушення вимог ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», п. 442 Порядку та створення передумов до витоку секретної інформації).

Військовим комісаром як керівником військової установи не вжито вичерпних заходів з контролю за станом охорони державної таємниці в Дарницькому РВК, чим порушено вимоги статей 5, 37 Закону та пунктів 3, 749 Порядку, внаслідок чого створено умови для ознайомлення зі змістом секретних документів сторонніх осіб і загрозу витоку секретної інформації. Цим він порушив взяті на себе зобов'язання громадянина, якому надано допуск до державної таємниці, щодо виконання вимог режиму секретності та додержання інших вимог законодавства про державну таємницю.

Водночас військовий комісар Дарницького районного у м. Києві військового комісаріату пояснив, що йому допуск до держаної таємниці було скасовано незаконно, оскільки ним не було допущено невиконання обов'язків щодо збереження державної таємниці, яка йому була довірена чи довірялась раніше. Також військовий комісар жодним чином не сприяв іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України, не вчиняв інших дій, які відповідно до вимог ст. 23 Закону України «Про державну таємницю» є підставою для скасування допуску.

Крім того він зазначив, що інформація, яка містилась у виявлених на ПЕОМ електронних варіантах документів, не була довірена йому та не довірялась, тому в нього не могло виникнути обов'язку зберігати державну таємницю. Документи, які зберігалися на жорсткому магнітному диску персональної обчислювальної машини, непризначеної для обробки секретної інформації, розміщеної в режимному приміщенні, не містили відомостей, що відповідно до Зводу відомостей, що становлять державну таємницю,

[86] Постанова Окружного адміністративного суду м. Києва від 10.03.2015 : Справа № 826/12140/14 URL: http://www.reyestr.court.gov.ua/Review/43227496 (дата звернення: 17.03.2019).

затвердженому наказом Служби безпеки України від 12.08.2005 № 440, є державною таємницею.

Аналізуючи положення Закону України «Про державну таємницю», суд дійшов висновку, що обов'язками, невиконання яких тягне за собою відповідальність у вигляді скасування допуску до державної таємниці, фактично є:

– недопущення розголошення будь-яким способом державної таємниці, яка була довірена або стала відомою у зв'язку з виконанням службових обов'язків;

– сприяння іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України.

Цей перелік є вичерпним, до компетенції Служби безпеки України не віднесено його розширення або тлумачення окремих положень.

Також Службою безпеки України не доведено належними та допустимими доказами факту виникнення або виявлення обставин, передбачених ст. 23 Закону України «Про державну таємницю», відносно позивачів.

Виявлені під час тематичної перевірки порушення, покладені в основу висновків про скасування позивачу допуску до державної таємниці та прийняття оскаржуваного розпорядження стосовно позивача, також не підтверджені належними та допустимими доказами, виходячи з наступного.

З акту службового розслідування по факту знаходження інформації з обмеженим доступом на ПЕОМ заступника військового комісара – начальника мобілізаційного відділення вбачається, що в результаті службового розслідування комісією проведена експертна оцінка знайдених матеріальних носіїв інформації.

За результатами експертної оцінки документів, указаних в акті перевірки, вони не містять державної таємниці, а лише службову таємницю та відкриту інформацію.

Водночас листом Генеральний штаб Головного управління оборонного та мобілізаційного планування Генерального штабу Збройних Сил України повідомив позивача, що експертний висновок державного експерта з питань таємниць – начальника Головного управління оборонного та мобілізаційного планування Генерального штабу Збройних Сил України про відсутність відомостей, що

становлять державну таємницю, надісланий на реєстрацію до Служби безпеки України.

Під час судового розгляду відповідачем не надано суду доказів, які підтверджували б надання грифу «таємно» виявленим під час перевірки документам.

Крім того, суд звертає увагу на те, що вказані документи позивачу не довірялися, не видавалися та не передавалися, відповідно в нього не виникало обов'язку щодо збереження відомостей, які містили наведені вище документи.

При цьому працівниками Служби безпеки України не встановлювалися час, дата внесення вказаних файлів на ПЕОМ, особу – користувача ПЕОМ, яка їх вносила, та не було перевірено, чи відповідають електронні версії документів, що зберігалися на ПЕОМ, змісту самих секретних документів на паперових носіях, яким надавався гриф «таємно».

Більше того, суд не залишає поза увагою той факт, що з Порядком організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України, затвердженого Постановою Кабінету Міністрів України від 18.12.2013 № 939 (далі – Порядок), позивач був ознайомлений лише 16 липня 2014 р., тобто після проведення відповідачем тематичної перевірки. Отже, посилання відповідача на порушення позивачем вимог Порядку є безпідставними, оскільки посилання на порушення норм, з якими особа не була належним чином ознайомлена, є неприпустимим. Слід зазначити, що нормативний документ, про порушення якого зазначено в акті, у вільному доступу відсутній, має гриф «для службового користування» та міг бути відомий позивачам до дня ознайомлення. Суд критично сприймає пояснення відповідачів про те, що з урахуванням подібного змісту Постанови Кабінету Міністрів України від 18.12.2013 № 939 та попереднього Порядку позивачі мали здогадуватися про його зміст.

Також суд звертає увагу на те, що відповідно до п. 444 Порядку контроль за забезпеченням режиму секретності під час обробки секретної інформації в автоматизованих системах підприємства, установи, організації здійснюється підрозділами технічного захисту інформації, а відповідно до функціональних обов'язків військового комісара, затверджених військовим

комісаром Київського міського військового комісаріату, військовий комісар відповідає лише за забезпечення охорони державної таємниці.

Щодо інших порушень встановлено, що на момент перевірки ПЕОМ у кабінеті знаходилися декілька осіб, які відпрацьовували файли з повістки для подальшого друку та проведення мобілізаційних заходів на власних ПЕОМ з відповідною відміткою про заборону обробки таємної інформації, при цьому маючи допуск та доступ до державної таємниці, документи з обмеженим доступом вони не відпрацьовували та не відпрацьовують. Належних і допустимих доказів, які б спростовували пояснення зазначених осіб, відповідачем суду не подано.

Таким чином, об'єктивно оцінивши наведені вище обставини та вимоги чинного законодавства у сфері захисту державної таємниці, суд вважає, що фактично на момент складання відповідачем висновку про скасування позивачу допуску до державної таємниці та прийняття оскаржуваного розпорядження щодо скасування позивачу допуску до державної таємниці в його основу покладені недостовірні (не підтверджені належним чином) висновки.

Отже, суд вважає розпорядження відповідача щодо скасування позивачу допуску до державної таємниці протиправним і таким, що підлягає скасуванню.

Тема 7. Захист електронного документообігу в Україні

План

1. Правове регулювання електронного документообігу в Україні.
2. Організаційна структура забезпечення використання електронного підпису.
3. Загальний порядок накладання та перевірки електронного підпису.

1. Правове регулювання електронного документообігу в Україні

Сьогодні в розвинених країнах можна спостерігати перехід від паперового до електронного документообігу. Такий перехід дозволяє швидше здійснювати управлінські рішення, оперативно передавати важливі документи на великі відстані і, звичайно, економить значні матеріальні та фінансові ресурси, які залучаються для виготовлення паперової документації. Першою країною Європи, яка законодавчо закріпила правомочність електронного підпису, була Ірландія.

В Україні електронний документообіг почали впроваджувати ще з середини 90-х років XX ст. Провідну роль у такому впровадженні та відповідальність за правила накладання електронного підпису взяв на себе Національний банк України.

22 травня 2003 р. Верховна Рада України ухвалила два рамкових закони «Про електронні документи та електронний документообіг» і «Про електронний цифровий підпис», які набули чинності у 2004 р.

Законодавчо було закріплено низку важливих термінів, які до цього регулювалися підзаконними актами, було визначено організаційну структуру накладання та перевірки електронного підпису і низку інших не менш важливих аспектів.

Так, згідно зі ст. 5 Закону України «Про електронні документи та електронний документообіг»[87] ***електронний документ*** – це документ, інформація в якому зафіксована у вигляді електронних даних, враховуючи **обов'язкові реквізити документа**.

Реквізитом електронного документа є ***електронний підпис*** – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються та використовуються ним як підпис.

Відповідно, ***електронний документообіг*** *(обіг електронних документів)* – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та в разі необхідності з підтвердженням факту одержання таких документів.

Державне регулювання у сфері електронного документообігу спрямоване на:

– реалізацію єдиної державної політики електронного документообігу;

– забезпечення прав і законних інтересів суб'єктів електронного документообігу;

– нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення електронних документів.

Важливим положенням, яке було закріплене законодавцем, стало те, що *юридична сила електронного документа та його допустимість як доказу не може бути заперечена виключно через те, що він має електронну форму.*

Згодом на заміну Закону України «Про електронний цифровий підпис» було ухвалено Закон України «Про електронні довірчі послуги» від 05.10.2017[88]. Відповідно до ст. 16 цього закону до електронних довірчих послуг належать:

– створення, перевірка та підтвердження вдосконаленого електронного підпису чи печатки;

---

[87] Про електронні документи та електронний документообіг: закон України від 22.05.2003 ; [із змінами і доповненнями на 05.08.2018]. *Офіційний вісник України*. 2003. № 25 (04.07.2003). ст. 1174.

[88] Про електронні довірчі послуги: закон України від 05.10.2017. *Офіційний вісник України*. 2017. № 91 (21.11.2017). ст. 2764.

– формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки;

– формування, перевірка та підтвердження чинності сертифіката автентифікації веб-сайту;

– формування, перевірка та підтвердження електронної позначки часу;

– реєстрована електронна доставка;

– зберігання вдосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами.

У законі усунуто плутанину в термінах «електронний підпис» та «електронний цифровий підпис», залишилася тільки дефініція «електронний підпис». Також забезпечується взаємне визнання українських та іноземних засобів ідентифікації, впроваджується принцип інтероперабельності (забезпечення функціональної сумісності технічних рішень, що використовуються під час надання електронних послуг, та їх здатності взаємодіяти між собою). Закон передбачає ідентифікацію громадян за електронним підписом Bank ID і Mobile ID.

Електронний підпис накладається за допомогою *особистого ключа* та перевіряється за допомогою *відкритого ключа*.

При цьому ***особистий ключ*** – це параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів, а ***відкритий ключ*** – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

Згідно зі ст. 15 Закону України «Про електронні довірчі послуги» залежно від ступеня довіри до засобів електронної ідентифікації вводиться три рівні електронного підпису:

– простий електронний підпис та печатка – низький рівень довіри;

– удосконалений електронний підпис та печатка – середній рівень довіри;

– кваліфікований електронний підпис та печатка – високий рівень довіри[89].

Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов'язана.

Перехід до використання на практиці електронного підпису є черговим важливим кроком на шляху втілення електронного урядування, адже електронний підпис є важливим компонентом електронного документообігу.

Упровадження електронного підпису, зокрема, робить можливим:

– подання різноманітної бухгалтерської, податкової, статистичної та іншої звітності до державних органів в електронному вигляді телекомунікаційними каналами, зокрема через інтернет;

– організацію онлайн закупівель державних суб'єктів господарювання через систему електронних торгів, що сприятиме забезпеченню прозорості їх діяльності та зменшенню зловживань;

– юридично значущий електронний документообіг між органами державної влади, підприємствами й організаціями;

– отримання громадянами різноманітних офіційно засвідчених документів та участь у виборах через мережу Інтернет[90].

2. Організаційна структура забезпечення використання електронного підпису

Для накладання та перевірки електронного підпису законодавець визначив розгалужену організаційну структуру, яка наведена на рис. 7.1.

---

[89] Степаненко В. АУБ: Тепер кожен має можливість засвідчувати електронні документи своїм власним цифровим підписом. URL: http://www.uabanker.net/daily/2006/01/011806_1430.shtml (дата звернення: 17.03.2019).

[90] Закон «Про електронні довірчі послуги»: що це означає для замовника та постачальника. URL: https://education.zakupki.prom.ua/zakon-pro-elektronni-dovirchi-poslugi-shho-tse-oznachaye-dlya-zamovnika-ta-postachalnika/ (дата звернення: 19.03.2019).

Рис. 7.1. Організаційна структура накладання та перевірки електронного підпису

На сьогодні функції центрального засвідчувального органу виконує Міністерство юстиції України.

Повноваження центрального засвідчувального органу визначено у ст. 7 Закону України «Про електронні довірчі послуги». До повноважень центрального засвідчувального органу відносно кваліфікованих надавачів електронних довірчих послуг належить надання таких послуг:

– адміністративна послуга внесення юридичних осіб і фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку;

– надання кваліфікованих електронних довірчих послуг надавачам електронних довірчих послуг з використанням самопідписаного сертифіката електронної печатки центрального засвідчувального органу, що призначений для надання таких послуг;

– надання послуги постачання передачі сигналів точного часу, синхронізованого з Державним еталоном одиниць часу і частоти.

Технічне і технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу – державним підприємством, яке належить до сфери управління головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг (державним підприємством «Національні інформаційні системи»)[91].

Перше в Україні свідоцтво про акредитацію Центру сертифікації ключів отримала виробнича фірма «Українські національні інформаційні системи» з м. Дніпропетровськ у 2006 р.

Для органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності законодавець установив додаткові вимоги щодо використання електронного підпису. Державні установи для засвідчення чинності відкритого ключа використовують лише *кваліфікований сертифікат відкритого ключа*, а для здійснення повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи відповідно до закону, здійснення інформаційного обміну з іншими юридичними особами, – виключно *захищені носії особистих ключів*.

Крім того, в Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженому Постановою Кабінету Міністрів України від 19.09.2018 № 749, детально розписано механізм використання електронних довірчих послуг у державних установах.

Організацію використання кваліфікованих електронних довірчих послуг у державній установі забезпечує відповідальний підрозділ, що виконує відповідні функції, або працівник, визначений рішенням такої установи (її керівника). Відповідальний підрозділ (працівник) забезпечує:

– підготовку та подання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг;

[91] Про центральний засвідчувальний орган . URL: https://czo.gov.ua/ (дата звернення: 19.03.2019).

– надання допомоги підписувачам під час генерації їх особистих і відкритих ключів;

– ознайомлення підписувачів з правилами застосування кваліфікованих електронних довірчих послуг і здійснення контролю за їх дотриманням;

– взаємодію з кваліфікованим надавачем з питань використання кваліфікованих електронних довірчих послуг;

– подання кваліфікованому надавачу заяв про скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів;

– ведення обліку захищених носіїв особистих ключів і засобів кваліфікованого електронного підпису чи печатки;

– зберігання оригіналів документів та/або їх копій (крім копій особистих документів підписувачів, що містять їх персональні дані), на підставі яких отримано кваліфіковані електронні довірчі послуги;

– здійснення контролю за використанням підписувачами засобів кваліфікованого електронного підпису чи печатки та зберіганням ними особистих ключів.

3. Загальний порядок накладання та перевірки електронного підпису

Загальна схема накладання електронного підпису наведена на рис. 7.2., а його перевірки – на рис. 7.3.

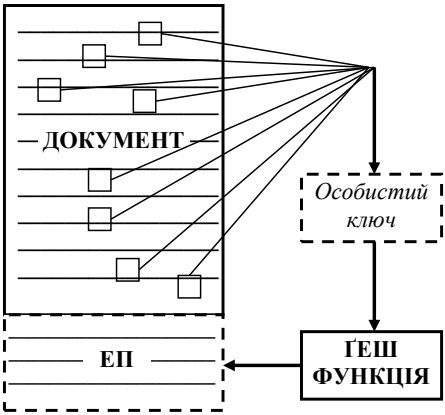
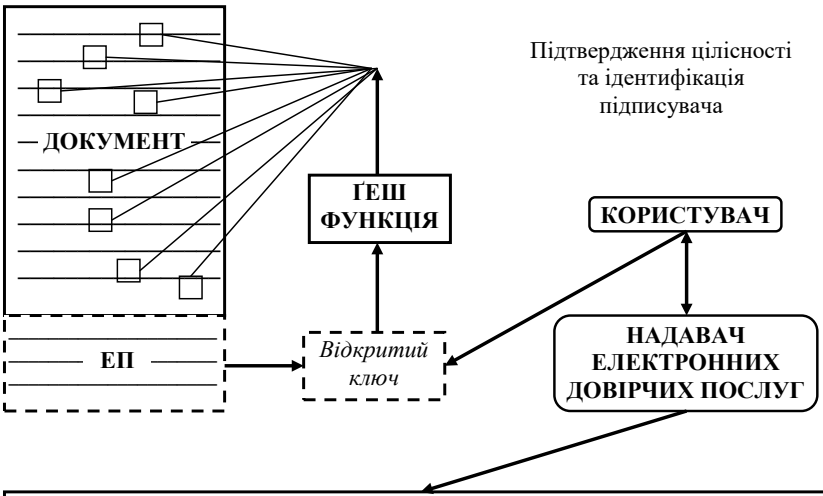


Рис. 7.2. Приблизна модель накладання електронного підпису



КВАЛІФІКОВАНИЙ СЕРТИФІКАТ КЛЮЧА

- позначка, що сертифікат відкритого ключа виданий як кваліфікований сертифікат відкритого ключа;
- позначка, що сертифікат відкритого ключа виданий в Україні;
- ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа;
- ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг;
- місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;
- значення відкритого ключа, який відповідає особистому ключу;
- відомості про початок та закінчення строку дії кваліфікованого сертифіката відкритого ключа;
- серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;
- кваліфікований електронний підпис або кваліфікована електронна печатка, створені суб'єктом, який видав сертифікат;
- відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;
- відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;
- відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
- відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
- ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації веб-сайту).

Рис. 7.3. Приблизна модель перевірки електронного підпису

Підсумовуючи викладене, необхідно зазначити, що накладання електронного підпису не забезпечує конфіденційності документа, тобто його зміст **не шифрується**, але при цьому можна впевнитись у *цілісності* документа й *ідентифікувати його підписувача*.

Питання для самоконтролю

1. Електронний документ та електронний документообіг.
2. Цілі державного регулювання у сфері електронного документообігу.
3. Електронний підпис.
4. Види та визначення ключів у сфері застосування електронних підписів.
5. Організаційна структура накладання та перевірки електронного підпису.
6. Взаємодія суб'єктів правових відносин у сфері електронних довірчих послуг.
7. Особливості електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності.
8. Приблизна модель накладання електронного підпису.
9. Приблизна модель перевірки електронного підпису.

План практичної підготовки за темою: «Електронні довірчі послуги»

Вид: практичне заняття.

Мета: розв'язання задач.

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (15 хв.).
3. Розв'язання задач (60 хв).
4. Викладач оцінює якість роботи за чотирьохбальною шкалою.
5. По закінченні заняття підбиваються підсумки (5 хв.).

Задача № 1

Громадянин Федотенко придбав у фірми «Комп'ютерна техніка» 4 стаціонарних комп'ютери, 2 ноутбуки та 3 лазерні принтери. Відповідно було укладено договір купівлі-продажу в електронному вигляді. Фірма «Комп'ютерна техніка» надала гарантійний талон на придбану техніку строком на 1 рік. Через 4 місяці Федотенко звернувся до фірми з проханням обміняти ноутбук, який зламався не з його вини. Фірма відмовила. Федотенко подав позов проти фірми «Комп'ютерна техніка» до місцевого суду з вимогою повернути гроші за ноутбук або обміняти його на новий такої самої моделі. Фірма «Комп'ютерна техніка» подала зустрічний позов з вимогою визнати договір купівлі-продажу техніки недійсним, оскільки Федотенко, укладаючи договір, використав електронний підпис, який не має сертифіката ключа.

Дайте правову оцінку ситуації.

Відповідь: дивіться Цивільний кодекс України, закони України «Про електронні документи та електронний документообіг в Україні» та «Про електронні довірчі послуги».

Задача № 2

Єгоренко займався підприємницькою діяльністю за допомогою мережі Інтернет, для чого зареєструвався відповідно до вимог законодавства як приватний підприємець. Договори він укладав з використанням електронного підпису. Його відкритий та особистий ключі були сертифіковані центром сертифікації ключів, який діяв на законних підставах.

О 21:00 12 липня минулого року на комп'ютер Єгоренка було здійснено атаку, в результаті якої зловмиснику став відомий особистий ключ Єгоренка. Підприємець виявив вторгнення і визначив, що саме стало відомо зловмиснику. О 22:00 він звернувся до центру сертифікації ключів із заявою про блокування сертифікату свого ключа. Але йому було відмовлено в цьому через те, що центр зможе прийняти заяву тільки вранці.

Дайте правову оцінку ситуації.

Відповідь: дивіться Цивільний кодекс України, закони України «Про електронні документи та електронний документообіг в Україні» та «Про електронні довірчі послуги».

Задача № 3

У Назарова І. І. та Назарової Ю. І. помер дядько Соломін Г. Н. Вони згідно з нормами цивільного законодавства в шестимісячний строк подали заяву про включення їх у склад спадкоємців до нотаріальної контори. Оскільки ближчих родичів у Соломіна Г. Н. не було, через 6 місяців нотаріус визнав їх єдиними спадкоємцями. Через те, що Назаров І. І. проживав в іншому місті та не зміг приїхати до нотаріуса за свідоцтвом про право на спадщину, нотаріус вирішив відправити цей документ в електронному вигляді за допомогою електронної пошти, підписавши документ за допомогою електронного підпису, тому що вважав електронний підпис аналогом власного підпису.

Дайте правову оцінку ситуації.

Відповідь: дивіться Цивільний кодекс України, закони України «Про електронні документи та електронний документообіг в Україні» та «Про електронні довірчі послуги».

Задача № 4

10 жовтня минулого року між директором ТОВ «Омега» та директором ТОВ «Дельта» було укладено письмовий договір. За цим договором ТОВ «Омега» має отримати комп'ютерну техніку (20 персональних комп'ютерів) у користування на строк 60 днів, починаючи з дня укладання договору.

У договорі було вказано, що техніка буде використовуватися за її цільовим призначенням, а саме для обладнання комп'ютерного салону та надання послуг населенню (з цією метою директор ТОВ «Омега» уклав договір оренди приміщення з фізичною особою). Крім цього, в договорі було вказано про сплату 20 % прибутку, який отримано з кожної одиниці комп'ютерної техніки, починаючи з дня набрання чинності договором.

Договір було укладено в офісі ТОВ «Дельта». Причому один примірник договору був на папері (залишився в ТОВ «Дельта»), а інший (за бажанням ТОВ «Омега») – в електронному вигляді з накладанням електронного підпису – було відправлено через електронну мережу за адресою електронної пошти ТОВ «Дельта». Одержання примірника договору було підтверджено електронним повідомленням цього ж дня.

11 жовтня минулого року комп'ютерна техніка не була передана в користування. Наступного дня директор ТОВ «Омега»

звернувся до ТОВ «Дельта» з вимогою про розірвання договору у зв'язку з цими обставинами. Однак отримав відповідь про те, що ніякого договору між ними укладено не було, а копія договору в електронній формі не є оригіналом і не може бути представлена як доказ.

Директор ТОВ «Омега» звернувся до суду з позовом про визнання чинності договору та відшкодування йому завданих збитків.

Дайте правову оцінку ситуації. Яке рішення повинен ухвалити суд?

Відповідь: дивіться Цивільний кодекс України, закони України «Про електронні документи та електронний документообіг в Україні» та «Про електронні довірчі послуги».

План практичної підготовки за темою: «Накладання електронного підпису»

Вид: практичне заняття.

Мета: розв’язання задач.

Порядок проведення заняття

1. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування за результатами теоретичної підготовки (5 хв.).
3. Завдання: одержати ключі електроннного підпису через електронний кабінет у банку.
4. З використанням ресурсу ca.informjust.ua/sign накласти електронний підпис на довільний файл трьома способами. За допомого сервісу informjust.ua/verify перевірити цілісність документа. Змінити підписаний файл. Провести повторну перевірку (15 хв).
5. З використанням електронного підпису авторизуватись в онлайн будинку юстиції (online.minjust.gov.ua/login). Одержати інформацію з державного реєстру речових прав (15 хв.).
6. З використанням електронного підпису авторизуватися на порталі електронних послуг пенсійного фонду (portal.pfu.gov.ua). Перевірити відомості про свої відрахування (15 хв.).
7. З використанням електронного підпису авторизуватися в електронному кабінеті на порталі Державної фіскальної служби України (cabinet.sfs.gov.ua). Перевірити відомості про свої доходи (15 хв.).
8. Відпрацювати роботу програми «ІІТ Користувач ЦСК-1» за адресою acskidd.gov.ua/korustyvach_csk (10 хв.).
9. Викладач оцінює якість роботи за чотирьохбальною шкалою.
10. По закінченні заняття підбиваються підсумки (5 хв.).

Інформаційно-методичне забезпечення

1. Criminal Law of the People's Republic of China. URL: https://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm (дата звернення: 17.03.2019).

2. Executive Order 13526 Classified National Security Information, December 29, 2009 URL: http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf (дата звернення: 17.03.2019).

3. German criminal code Уголовный кодекс ФРГ. URL: https://www.gesetze-im-internet.de/englisch_stgb/ (дата звернення: 17.03.2019).

4. Instruction sheet on the Handling of Protectively Marked Information Classified VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VS-MerkblattEnglisch_pdf.pdf?__blob=publicationFile (дата звернення: 17.03.2019).

5. Law of the People's Republic of China on Guarding State Secrets (2010 Revision) URL: http://en.pkulaw.cn/display.aspx?id=8039&lib=law&SearchKeyword=&SearchCKeyword= (дата звернення: 17.03.2019).

6. Osepashvili D. New Media and Russian-Georgian August 2008 War. *Journalism and Mass Communication*. 2014. Vol. 4, No. 6. P. 360-366.

7. Sharma S. Gupta J. N. D. Securing Information Infrastructure from Information Warfare. *Logistics Information Management*. 2002. № 15(5/6). P. 414-422.

8. State Secrets China's Legal Labyrinth. URL: http://www.lapres.net/statesecrets.pdf (дата звернення: 17.03.2019).

9. TS-3600.1 Information Warfare. URL: https://ia600604.us.archive.org/5/items/14F0492Doc01DirectiveTS3600.1/14F0492_doc_01_Directive_TS-3600.1.pdf (дата звернення: 11.11.2019).

10. Yurkova O. Six Fake News Techniques and Simple Tools to Vet Them. URL: https://gijn.org/six-fake-news-techniques-and-simple-tools-to-vet-them/ (дата звернення: 08.04.2019).

11. Буткевич Б. Фабрика фейков. Какую угрозу несут сайты-паразиты. URL: https://vlada.io/articles/fabrika-feykov-kakuyu-ugrozu-nesut-saytyi-parazityi/ (дата звернення: 15.03.2019).

12. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. К.; Ірпінь: ВТФ «Перун», 2005. 1728 с.

13. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: постанова Кабінету Міністрів України № 821 від 16.11.2016. *Офіційний вісник України*. 2016. № 93, стор. 39, стаття 3033.

14. Етапи побудови КСЗІ. URL: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi (дата звернення: 17.03.2019).

15. Закон «Про електронні довірчі послуги»: що це означає для замовника та постачальника. URL: https://education.zakupki.prom.ua/zakon-pro-elektronni-dovirchi-poslugi-shho-tse-oznachaye-dlya-zamovnika-ta-postachalnika/ (дата звернення: 19.03.2019).

16. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України № 440 від 12.08.2005 ; [із змінами і доповненнями на 17.09.2019]. *Офіційний вісник України*. 2005. № 34 (09.09.2005). ст. 2089.

17. Зеленина Е. В Королевстве кривых зеркал… *Время*. Вторник. Декабрь 17 2013. № 181 (17337). С. 1-2.

18. Іванцова А. Інтернет-тролі на службі в олігархів та політиків. URL: https://www.radiosvoboda.org/a/27042051.html (дата звернення: 15.03.2019).

19. Капица Ю. Проблемы правовой охраны конфиденциальной информации в Украине (часть 2). *Інтелектуальна власність*. 2004. № 3. С. 27-33.

20. Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах. *Вісник Харківської державної академії культури*. 2013. Вип. 41. С. 108-113.

21. Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України № 1126 від 8.10.1997 // База даних «Законодавство України» / Верховна Рада України. URL:

http://zakon3.rada.gov.ua/laws/show/1126-97-%D0%BF (дата звернення: 12.07.2017).

22. Кримінальний кодекс України від 05.04.2001; [із змінами і доповненнями на 26.02.2019]. *Офіційний вісник України*. 2001. № 17 (18.04.2001). ст. 432.

23. Леонтєва, Л. Інформаційна війна в епоху глобалізації URL: http://www.ji-magazine.lviv.ua/seminary/2000/sem13-04.htm (дата звернення: 13.03.2019).

24. Манжай А. В. Проблемы борьбы с компьютерным пиратством и легализации программного обеспечения в Украине. Разработка комплексной системы защиты информации на носителях от несанкционированного копирования // Компьютерная преступность и кибертерроризм: сборник научных работ. Запорожье: Центр исследования компьютерной преступности, 2004. Вып. 2. С. 278–294.

25. Манжай О. В. Космиця А. П. Аналіз системи охорони державної таємниці в Китайській Народній Республіці. *Право і безпека*. 2014. № 4 (51). С. 38-42.

26. Манжай О. В. Правові засади захисту інформації: навчальний-посібник. Харків : Ніка Нова, 2014. 104 с. з іл.

27. Манжай О. В., Нікітіна О. В. Деякі аспекти автоматизації визначення виду інформації за режимом доступу відповідно до чинного законодавства України // Інформатизація вищих навчальних закладів МВС України: матеріали науково-практичної конференції (27 квітня 2007 р.). Харків: Вид-во Харківського національного ун-ту внутр. справ, 2008. Вып. 2. С. 184–187.

28. Маргарин під виглядом масла виробляли у Харкові. URL: https://kharkov.comments.ua/news/margarin-pid-vigljadom-masla-virobljali-u-harkovi-/ (дата звернення: 09.12.2019).

29. Медведєв В. К., Кучеренко Ю. Ф., Гузько Р. М. Сучасна інформаційна війна та її обрис. *Системи озброєння і військова техніка*. 2008. № 1. С. 52-54.

30. Мордвинова В. А., Фомина А. Б. Защита информации и информационная безопасность. МГДД(Ю)Т, МИРЭА, ГНИИ ИТТ «Информика». М., 2004. 69 с.

31. Национальная администрация по охране государственных тайн. URL: http://ru.wikipedia.org/wiki/Национальная_администрация_по_охране_государственных_тайн (дата звернення: 17.03.2019).

32. НД 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106341 (дата звернення: 17.03.2019).

33. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106349 (дата звернення: 17.03.2019).

34. НД ТЗІ 3.7-003-05. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106350 (дата звернення: 17.03.2019).

35. Носов В .В., Манжай О. В. Окремі аспекти протидії інформаційній війні в Україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. № 1(29). С. 26-29.

36. Носов В. В., Манжай І. А. Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2017. № 2(34). С. 56-68.

37. Носов В. В., Манжай О. В. Актуальні питання правового захисту відкритої інформації та інформації про особу. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2006. Вип. 2 (13). С. 33-38.

38. Носов В. В., Манжай О. В. Організація та забезпечення інформаційної безпеки: навчальний посібник. Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. 216 с.

39. О государственной тайне: федеральный закон от 21.07.1993; [с изм. и доп. на 29.07.2018]. *Российская газета*. №182. 21.09.1993.

40. Об утверждении перечня должностей, при замещении которых лица считаются допущенными к государственной тайне: распоряжение Президента Российской Федерации от 15 января 2010 года N 24-рп. URL: http://www.rg.ru/2010/04/28/tayna-site-dok.html (дата звернення: 17.03.2019).

41. Об утверждении перечня сведений конфиденциального характера: указ Президента РФ №188 от 06.03.1997; [с изм. и доп. на 13.07.2015] // Собрание законодательства РФ. – 10.03.1997. – № 10. – ст. 1127.

42. Панарин И. Н. Информационная война и геополитика. М.: Издательство «Поколение», 2006. 560 с.

43. Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць, затверджений Указом Президента України від 01.12.2009 № 987/2009; [із змінами і доповненнями на 13.02.2019]. *Офіційний вісник України*. 2009. № 94 (14.12.2009). ст. 3204.

44. Перелік суб'єктів господарювання, що мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=284081&cat_id=266373 (дата звернення: 19.03.2019).

45. Перепелиця М. М., Манжай О. В. Провадження оперативно-розшукових заходів у Великій Британії, Росії, США та Україні: монографія. Харків : Вид-во КП Друкарня № 13, 2008. 248 с.: іл.

46. Перечень сведений, отнесенных к государственной тайне, утвержденный указом Президента РФ № 1203 от 30.11.1995; [с изм. и доп. на 14.01.2019]. *Российская газета*. № 246. 27.12.1995.

47. Побудова Комплексних Систем Захисту Інформації (КСЗІ). URL: http://www.iqusion.com/ua/produkti-i-servisi/zakhist-informatsiji/120-kszi.html (дата звернення: 12.07.2017).

48. Пода Т. А. Інформаційна війна як стратегія формування політичної свідомості(соціально-філософський аналіз). *Вісник Національного авіаційного університету*. Сер. : Філософія. Культурологія. 2014. № 1. С. 67-70.

49. Податковий кодекс України від 02.12.2010; [із змінами і доповненнями на 01.03.2019]. *Офіційний вісник України*. 2010. № 23 (23.12.2010). ст. 543.

50. Положення про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці, затверджене постановою Кабінету Міністрів України від 15.06.1994 № 414 ; [із змінами і доповненнями на

15.01.2019]. *Офіційний вісник України*. 2008. № 58 (15.08.2008). ст. 1957.

51. Положення про державний контроль за станом технічного захисту інформації: наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України №87 від 16.05.07 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon5.rada.gov.ua/laws/show/z0785-07 (дата звернення: 17.03.2019).

52. Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства, затверджене указом Президента України від 17.07.2006 № 621/2006. *Офіційний вісник України*. 2006. № 29 (02.08.2006). ст. 2083.

53. Порядок отримання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею URL: https://ssu.gov.ua/ua/pages/171 (дата звернення: 17.03.2019).

54. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних, та інформаційно-телекомунікаційних системах: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 660 від 02.12.2014 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/z0090-15 (дата звернення: 17.03.2019).

55. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями на 13.10.2011]. *Офіційний вісник України*. 2006. № 13 (12.04.2006), стор. 164, стаття 878.

56. Про авторське право і суміжні права: закон України від 23.12.1993; [із змінами і доповненнями на 04.11.2018]. *Офіційний вісник України*. 1993. № 12 (01.03.1993). ст. 234.

57. Про державну таємницю: закон України від 21.01.1994 ; [із змінами і доповненнями на 05.08.2018]. *Відомості Верховної Ради України*. 1994. № 16 (19.04.1994). стор. 422. ст. 93.

58. Про доступ до публічної інформації: закон України від 13.01.2011; [із змінами і доповненнями на 01.05.2015]. *Офіційний вісник України*. 2011. № 10 (18.02.2011), стор. 29, стаття 446.

59. Про електронні довірчі послуги: закон України від 05.10.2017. *Офіційний вісник України*. 2017. № 91 (21.11.2017). ст. 2764.

60. Про електронні документи та електронний документообіг: закон України від 22.05.2003 ; [із змінами і доповненнями на 05.08.2018]. *Офіційний вісник України*. 2003. № 25 (04.07.2003). ст. 1174.

61. Про затвердження зобов'язання громадянина України у зв'язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці: наказ Служби безпеки України від 18.07.2001 № 190. *Офіційний вісник України*. 2001. № 35 (14.09.2001). ст. 1655.

62. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994; [із змінами і доповненнями на 19.04.2014]. Відомості Верховної Ради України. 1994. № 31 (02.08.1994). ст. 286.

63. Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями на 30.01.2018]. *Офіційний вісник України*. 2010. № 49 (09.07.2010), стор. 199, стаття 1604.

64. Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями на 01.01.2017]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

65. Про охорону прав на винаходи і корисні моделі: закон України від 15.12.1993; [із змінами і доповненнями на 05.12.2012]. *Офіційний вісник України*. 1993. № 12 (01.03.1993). ст. 204.

66. Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності: указ Президента України від 10.06.1997 р.; [із змінами і доповненнями на 23.11.2007] // Урядовий кур'єр. 1997. № 107–108 (14.06.1997).

67. Про Регламент Верховної Ради України : закон України від 10.02.2010 р.; [із змінами і доповненнями на 11.01.2019]. *Офіційний вісник України*. 2010. № 12 (01.03.2010). ст. 565.

68. Про центральний засвідчувальний орган . URL: https://czo.gov.ua/ (дата звернення: 19.03.2019).

69. Противодействие негативу в информационном пространстве: методические рекомендации / З. Чистяков, М. Шпаченко. Агентство конфликтного PR - /PR і Z/, 2012. 32 с.

70. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати*. 2013. № 1. С. 40-43.

71. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. К. : НІСД, 2017. 496 с.

72. Смольц С. П. Інформаційна війна як чинник формування суспільного буття. *Вісник Національного технічного університету України «Київський політехнічний інститут»*. Філософія. Психологія. Педагогіка. 2011. № 3. С. 70-74.

73. Степаненко В. АУБ: Тепер кожен має можливість засвідчувати електронні документи своїм власним цифровим підписом. URL: http://www.uabanker.net/daily/2006/01/011806_1430.shtml (дата звернення: 17.03.2019).

74. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету міністрів України від 19.10.2016 № 736. *Офіційний вісник України*. 2016. № 85 (04.11.2016), стор. 102, стаття 2783.

75. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ: [по состоянию на 27.12.2018]. *Собрание законодательства Российской Федерации*. 1996. № 25. Ст. 2954.

76. Шавкеро А. Зарубежный опыт защиты государственной тайны и возможности его использования в России. *Право и жизнь*. 2008. №124 (7). URL: https://studylib.ru/doc/3749864/shavkero-a.---zarubezhnyj-opyt-zashhity-gosudarstvennoj-tajny (дата звернення: 17.03.2019).

77. Ющенко А. Г. Украина обязана выиграть информационную войну. *Україна третє тисячоліття*. 2014. № 3. С. 21-23.

78. Яковлев В. «Гнилая селедка», «большая ложь», «40 на 60» — Владимир Яковлев о приемах пропаганды. URL: https://www.stopfake.org/gnilaya-seledka-bolshaya-lozh-40-na-60-vladimir-yakovlev-o-priemah-propagandy/ (дата звернення: 15.03.2019).

Абетковий покажчик

Деякі визначення

База персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних

Відкрита інформація – будь-яка інформація крім тієї, що віднесена законом до інформації з обмеженим доступом

Відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законом, державною таємницею і підлягають охороні державою

Документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі

Допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації

Доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та

	провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень
Електронний документ	– документ, інформація в якому зафіксована у вигляді електронних даних, враховуючи обов'язкові реквізити документа
Електронний документообіг (обіг електронних документів)	– сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та в разі необхідності з підтвердженням факту одержання таких документів
Засвідчувальний центр	– суб'єкт, який надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки кваліфікованим надавачам електронних довірчих послуг з використанням самопідписаного сертифіката відкритого ключа засвідчувального центру
Інтероперабельність електронних послуг	– забезпечення функціональної сумісності технічних рішень, що використовуються під час надання електронних послуг, та їх здатності взаємодіяти між собою
Інформаційна безпека	– стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації

Інформаційна війна – дії, вжиті для досягнення інформаційної переваги в інтересах національної стратегії, які реалізуються шляхом впливу на інформацію й інформаційні системи противника з одночасним захистом власної інформації та власних інформаційних систем

Інформаційна зброя – засіб проведення запланованих дій з інформацією або алгоритм цілеспрямованого впливу на інформаційну систему шляхом передавання такій системі інформації (або здійснення з інформацією інших запланованих дій)

Інформаційне протиборство – форма боротьби сторін з використанням спеціальних (політичних, економічних, дипломатичних, воєнних тощо) методів, способів і засобів для впливу на інформаційне середовище протилежної сторони та захисту власного середовища в інтересах досягнення поставлених цілей

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді

Кваліфікований надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам Закону України «Про електронні довірчі послуги» та відомості про яку внесені до Довірчого списку

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз

	національній безпеці України у кіберпросторі
Конфіденційна інформація	– інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень
Користувачі електронних довірчих послуг	– підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог закону
Надавач електронних довірчих послуг	– юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну або більше електронних довірчих послуг
Національна безпека України	– захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз
Органи з оцінки відповідності	– підприємство, установа, організація чи їх структурний підрозділ, що пройшли акредитацію в національному органі з акредитації та провадять діяльність з оцінки відповідності у сфері електронних довірчих послуг
Особистий ключ	– параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів

Персональні дані	– відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована
Публічна інформація	– відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом України «Про доступ до публічної інформації»
Службова інформація	– інформація, зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці, а також інформація, 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
Стратегія кібербезпеки України	– документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави

Навчальне видання

Олександр Володимирович МАНЖАЙ

Ірина Андріївна МАНЖАЙ

ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ

Підручник

Верстка, редакторське опрацювання
О. В. Манжай, І. А. Манжай

Дизайн обкладинки
В. В. Плеханов

Підп. до друку 05.02.2020. Формат 60х841/16. Папір офсетний.
Ум. друк. арк. 6,1. Обл.-вид. арк. 4,6. Тираж 300 прим. Зам. № 47

ТОВ «ПромАрт»
61023, м. Харків, вул. Весніна, 12
Свідоцтво суб'єкта видавничої справи серія ДК № 5748 від 06.11.2017. тел. (057)
717–28–80
www.promart.in.ua
e-mail: promart.izdat@gmail.com