**ЗАВДАННЯ ДО САМОСТІЙНОЇ РОБОТИ**

**з навчального курсу «Інформаційне право в медіа сфері»**

В межах самостійної роботи студенту пропонується опрацювати додатковий лекційний матеріал та вирішити практичні завдання.

**Тема № 1. Законодавство в сфері забезпечення інформаційної безпеки**

Питання для самостійної роботи:

1.Інформаційна безпека: поняття, структура, зміст.

2.Інформаційна безпека: міжнародний досвід.

3.Інформаційна безпека у США та ЄС.

4.Інформаційна безпека та Інтернет.

5.Державна політика України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави, сучасних автоматизованих і телекомунікаційних систем.

6.Класифікація та структура нормативних правових актів в сфері інформаційної безпеки України.

Тема № 2. «Основні положення інформаційної безпеки» ( до самостійного опрацювання)

1. Предмет, об’єкт і суб’єкти інформаційної безпеки.
2. Види інформаційної безпеки.
3. Концепція інформаційної безпеки держави.
4. Державна таємниця як особливий вид інформації, що захищається.
5. ***Предмет, об’єкт і суб’єкти інформаційної безпеки***

**Основні положення інформаційного права як системи соціальних норм і відношень, які виникають в інформаційній сфері та охороняються державою, стверджують, що забезпечення інформаційної безпеки спрямовано *на основний об’єкт правового регулювання – інформаційні відносини*, які виникають при здійснюванні інформаційних процесів** (створення, збирання, накопичення, зберігання, пошук, розповсюдження і використання інформації).

*Предметом інформаційних відносин,* які при цьому утворюються, є інформація та інформаційні ресурси в різних видах і формах, що захищається.

*Об’єктами інформаційної безпеки* можуть бути: свідомість, психіка людини, інформаційні системи різного масштабу і різного призначення.

*Соціальними об’єктами інформаційної безпеки* є особистість, колектив, суспільство, держава, світове товариство.

До *суб’єктів інформаційної безпеки* відносяться:

* держава, яка здійснює свої функції через відповідні органи;
* громадяни, суспільні та організації і об’єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

Інформаційні відносини, у яких названі суб’єкти «беруть участь як носії прав і обов’язків, встановлених нормами інформаційного права, називаються *інформаційно-правовими відносинами* (інформацій­ними правовідносинами)»[[1]](#footnote-1). Ці правові норми регламенту­ють параметри інформаційних процесів, за якими відбу­вається обіг інформації в суспільстві. Залежно від виду інформації законодавство передбачає відсутність тих чи інших обмежень або заборон.

Першим законодавчим актом, що стверджує інформаційний суверенітет України, закріплює право громадян на інформацію, закладає правові основи інформаційної діяльності і визначає правові форми міжнародного співробітництва у сфері інформації, став Закон України «Про інформацію». Згідно зі ст. 1 цього Закону, під інформацією розуміють «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі».

*Особливістю правового регулювання обігу інформації* є те, що залежно від типу інформації існують і відповідні специфічні правила поведінки при здійсненні інформаційної діяльності, що встановлені правовими нормами. Стаття 28 Закону України «Про інформацію» визначає режим доступу до інформації як передбачений правовими нормами порядок отримання, використання, поширення і зберігання інформації і поділяє інформацію на відкриту та інформацію з обмеженим доступом.

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну й таємну.

*Конфіденційною інформацією* є відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умовах.

До *таємної інформації* належить інформація, що містить відомості, які становлять державну таємницю, а також іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі (службова, військова, комерційна, банківська, лікарська, адвокатська, досудового слідства та дізнання тощо).

1. ***Види інформаційної безпеки***

*Інформаційна безпека особистості* – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо.

*Інформаційна безпека держави* (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т.ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси тощо) інформаційних впливів, причому як з упровадження, так і добування інформації.

Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

1. ***Концепція інформаційної безпеки держави***

*Концепція інформаційної безпеки держави –* це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення.

В концепції інформаційної безпеки держави:

* проводиться системна класифікація дестабілізуючих факторів і інформаційних загроз безпеці особливості ,суспільства і держави;
* обґрунтовуються основні положення організації забезпечення інформаційної безпеки держави;
* розробляються пропозиції по способах і формах забезпечення інформаційної безпеки.

У зв’язку з рішенням Ради національної безпеки і оброни України від 21.03.2008 р. «Про невідкладні заходи щодо забезпечення інформаційної безпеки України», введеним у дію [Указом Президента України від 23.04.2008 р. № 377](http://search.ligazakon.ua/l_doc2.nsf/link1/ed_2008_04_23/U377_08.html), було затверджено *Доктрину інформаційної безпеки України* (Указ Президента України від 08.07.2009 р. № 514/2009).

У Доктрині наголошується, що інформаційна безпека є невід’ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

В *інформаційній сфері* України вирізняються такі *життєво важливі інтереси*:

1) особи:

– забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

– недопущення несанкціонованого втручання у зміст, процеси оброблення, передання та використання персональних даних;

– захищеність від негативного інформаційно-психологічного впливу;

2) суспільства:

– збереження і примноження духовних, культурних і моральних цінностей українського народу;

– забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди;

– формування і розвиток демократичних інститутів громадянського суспільства;

3) держави:

– недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;

– побудова та розвиток інформаційного суспільства;

– забезпечення економічного та науково-технологічного розвитку України;

– формування позитивного іміджу України;

– інтеграція України у світовий інформаційний простір.

*Діяльність органів виконавчої владиу сфері забезпечення інформаційної безпеки України* має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за такими трьома головними напрямами:

1) інформаційно-психологічний (зокрема, забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей);

2) технологічний розвиток (зокрема, розбудова та інноваційне оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, оброблення та поширення інформації);

3) захист інформації (зокрема, забезпечення конфіденційності, цілісності та доступності інформації, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак).

1. ***Державна таємниця як особливий вид інформації, що захищається***

Найважливішим кроком на шляху нормативно-правового закріплення системи та органів захисту інформації з обмеженим доступом стало прийняття Закону України «Про державну таємницю» від 21 січня 1994 р., № 3855-ХІІ який регулює суспільні відносини, пов’язані з віднесенням певних відомостей до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці в інтересах національної безпеки України. Цей Закон визначив орган, що забезпечуватиме охорону одного з найважливіших видів інформації з обмеженим доступом – державної таємниці. Спеціально уповноваженим органом влади стала Служба безпеки України.

Відносини у сфері охорони державної таємниці регулюються Конституцією України, Законом України «Про інформацію», Законом України «Про державну таємницю», міжнародними договорами, згода на обов’язковість яких надана Верховною Радою України, та іншими нормативно-правовими актами.

Закон «Про державну таємницю» уперше визначив основні поняття у сфері захисту інформації.

*Державна таємниця* (секретна інформація) – вид таємної інформації, що охоплює відповідні відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені в порядку, встановленому цим законом, державною таємницею і підлягають охороні державою.

*Віднесення інформації до державної таємниці* – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з визначенням можливої шкоди національній безпеці України в разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього.

*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.

*Засекречування матеріальних носіїв інформації* – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

*Звід відомостей, що становлять державну таємницю*, – акт, у якому зведено переліки відомостей, що згідно з рішенням державних експертів із питань таємниць становлять державну таємницю у визначених цим Законом сферах.

*Категорія режиму секретності* – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю і зосереджені в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях.

*Криптографічний захист секретної інформації* – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

*Матеріальні носії секретної інформації* – матеріальні об’єкти, у тому числі фізичні поля, у яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

*Охорона державної таємниці* – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

*Режим секретності* – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці.

*Ступінь секретності* («Особливої важливості», «Цілком таємно», «Таємно») – категорія, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

*Технічний захист секретної інформації* – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Крім основних понять, Закон України «Про державну таємницю» також визначає:

– компетенцію органів державної влади, органів місцевого самоврядування та їхніх посадових осіб у сфері охорони державної таємниці;

– здійснення права власності на секретну інформацію та її матеріальні носії;

– фінансування витрат на здійснення діяльності, пов’язаної з державною таємницею;

– порядок віднесення інформації до державної таємниці;

– порядок засекречування і розсекречування матеріальних носіїв інформації;

– порядок охорони державної таємниці;

– контроль за забезпеченням охорони державної таємниці;

– відповідальність за порушення законодавства про державну таємницю.

*Питання віднесення інформації* у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та розсекречування покладено на державних експертів з питань державної таємниці. Експерти з питань державної таємниці у Верховній Раді України призначаються Головою Верховної Ради, в інших органах державної влади – Президентом України за поданням керівника відповідного державного органу.

*Рішення про засекречування інформації* приймається державним експертом з питань державної таємниці за власною ініціативою або за зверненням керівника відповідного органу державної влади, виключно на підставах, передбачених у ст. 8 Закону «Про державну таємницю». Державні експерти з питань таємниць (ст. 9 Закону) відповідають за віднесення інформації у відповідних сферах до державної таємниці, зміну ступеня секретності цієї інформації та її розсекречування. Виконання функцій державного експерта з питань таємниць покладається на конкретних посадових осіб:

– у Верховній Раді України – Головою Верховної Ради України;

– в інших державних органах, Національній академії наук України, на підприємствах, в установах і організаціях – Президентом України за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій.

Строк дії режиму таємності залежить від ступеня таємності інформації. Згідно зі ст. 13 Закону «Про державну таємницю», строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України. Цей строк не може перевищувати для інформації із ступенем секретності «Особливої важливості» 30 років, для інформації «Цілком таємно» – 10 років, для інформації «Таємно» – 5 років.

Інформація, що може бути віднесена до державної таємниці, визначається відповідно до норм ст. 8 Закону «Про державну таємницю» і викладена у Зводі відомостей, що становлять державну таємницю України[[2]](#footnote-2) (ЗВДТ), який «є єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування ЗВДТ держава забезпечує захист і в правову охорону відомостей, які зареєстровані в ньому».

*Звід відомостей* є систематизованим переліком відомостей, що становлять державну таємницю, котрі упорядковані за чотирма великими групами (статті) відповідно до сфери державної діяльності:

– сфера оборони;

– сфера економіки, науки і техніки;

– сфера зовнішніх відносин;

– сфера державної безпеки і охорони правопорядку.

Відомості, що належать до цих груп, класифікуються на окремі пункти та підпункти за основними характеристиками:

– зміст відомостей, які становлять державну таємницю;

– ступінь секретності («Особливої важливості», «Цілком таємно», «Таємно»);

– строк дії рішення про віднесення інформації (30 років, 10 років, 5 років).

*Реєстрація відомостей у Зводі* є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифа секретності, який відповідає ступеню секретності, встановленому для них у Зводі. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи змін до нього у порядку, встановленому Законом «Про державну таємницю».

Перелік відомостей, котрі становлять державну таємницю, у рамках визначених Законом «Про державну таємницю» і Зводу чотирьох основних сфер умовно класифікуються за напрямками та видами інформації.[[3]](#footnote-3)

Згідно *зі ст. 9 Конституції України*, чинні міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, є частиною національного законодавства, норми міжнародного гуманітарного права являють собою внутрішні юридичні норми. Норми міжнародного гуманітарного права значною мірою є нормами *jus cogens*[[4]](#footnote-4). Стаття 19 Закону України «Про міжнародні договори України» від 29 червня 2004 р. № 1906-ІV передбачає: «якщо міжнародним договором України, який набрав чинності в установленому порядку, встановлено інші правила, ніж ті, що передбачені у відповідному акті законодавства України, то застосовуються правила міжнародного договору».

Указ Президента України «Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації» від 14 грудня 2004 р. № 1483/2004 містить Положення про порядок підготовки документів щодо передачі державної таємниці іноземній державі чи міжнародній організації, що визначає порядок підготовки документів щодо здійснення державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями передачі секретної інформації до скасування рішення про віднесення її до державної таємниці та матеріальних носіїв такої інформації до їх розсекречування іноземним державам чи міжнародним організаціям з урахуванням необхідності забезпечення національної безпеки України.[[5]](#footnote-5)

*Режим секретної інформації в таких випадках визначається міжнародним договором* і, відповідно, ці режими відрізняються, залежно від країни чи міжнародної організації, від якої надійшла інформація, що охороняється, тобто можливе застосування правових режимів захисту інформації інших, ніж ті, що передбачені національним законодавством. Визначення таємної інформації при цьому також різняться.

Щодо визначення режиму захисту таємної інформації визначаються два основних підходи:

1) міжнародною угодою запроваджується класифікація таємної інформації, згідно з якою інформація з певним грифом таємності однієї сторони відповідає певному грифу таємності іншої сторони, і сторони угоди забезпечують стосовно такої таємної інформації щонайменше такий самий захист, який передбачається при поводженні з власною таємною інформацією з відповідним ступенем секретності;

2) у запровадженні на території однієї держави специфічного режиму захисту інформації, який застосовується щодо отриманої інформації іншою державою, з якої цю інформацію було отримано.

**Література:**

1. Продержавнутаємницю: закон України від 21 січ. 1994 р. № 3855-ХІІ//ВідомостіВерховноїРадиУкраїни. – 1994. – № 16. – Ст. 93. – Редакціявід 24 лют. 2011 р.
2. Продеякіпитанняпередачідержавноїтаємниціінозем­нійдержавічиміжнароднійорганізації [Електроннийресурс]:указПрезидентаУкраїнивід 14 груд. 2004 р. № 1483/2004. – Режим доступу:http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1483%2F2004.
3. Про Національну програму інформатизації України: закон України від 4 лют. 1998 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 181. – Редакція від 30 лип. 2010 р.
4. Про Основні засади розвитку інформаційного суспіль­ства в Україні на 2007–2015 роки: закон України від 9 січ. 2007 р. № 537-V// Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.
5. ПроСтратегію національної безпеки України [Електрон­ний ресурс]: указ Президента України від 12 лют. 2007 р. № 105/2007. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=105%2F2007.
6. Про телекомунікації: закон України від 18 листоп. 2003 р. № 1280-IV// Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155. – Редакція від 27 січ. 2011 р.

Тема № 3 «Правові питання захисту інформації з використанням технічних засобів» ( до самостійного опрацювання)

1. Особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації та при розробці шифрувальних засобів.
2. Правове регулювання захисту інформації в засобах зв’язку.
3. Правове регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу.

***1. Особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації та при розробці шифрувальних засобів***

Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері.[[6]](#footnote-6)

Правову основу технічного захисту інформації в Україні становлять Конституція України, закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України, інших державних органів, міжнародні договори України з питань технічного захисту інформації, згода на обов’язковість яких надана Верховною Радою України, а також Положення про технічний захист інформації в Україні.

Концепція технічного захисту інформації в Україні[[7]](#footnote-7) визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами, забезпечуючи єдність принципів формування і проведення такої політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо). Технічний захист інформації є складовою частиною забезпечення національної безпеки України.

*Технічний захист інформації* (ТЗІ) – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

*Система ТЗІ* – це сукупність суб’єктів, об’єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база.

*Комплекс технічного захисту інформації* – це сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об’єкті.

Державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень цієї Концепції, а також програм розвитку ТЗІ та окремих проектів.

*Основними напрямами державної політики у сфері ТЗІ* є:

1) нормативно-правове забезпечення;

2) організаційне забезпечення;

3) науково-технічна та виробнича діяльність.

*Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ* є:

– створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

– визначення перспективних напрямів розроблення нормативних документів з питань ТЗІ на основі аналізу стану відповідної вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;

– визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв`язку, призначених для оброблення інформації з обмеженим доступом, інших засобів забезпечення ТЗІ в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних силах, інших військових формуваннях, органах внутрішніх справ;

– налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв’язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;

– завершення створення та розвиток системи сертифікації вітчизняних та закордонних засобів забезпечення ТЗІ;

– визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

Указом Президента України «Про Положення про технічний захист інформації в Україні» від 27 вересня 1999 р. № 1299/99 визначається, що технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій.

Рівень безпеки інформації, що обробляється в системах та на об’єктах інформаційної інфраструктури, визначається такими властивостями:

– *конфіденційність* – властивість інформації бути захищеною від несанкціонованого ознайомлення;

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

– *доступність* – властивість інформації бути захищеною від несанкціонованого блокування.

Суб’єктами системи технічного захисту інформації є:

1) Державна служба спеціального зв’язку та захисту інформації України;

2) органи, щодо яких здійснюється ТЗІ;

3) науково-дослідні та науково-виробничі установи Держспецзв’язку України, державні підприємства, що перебувають в управлінні Держспецзв’язку України та виконують завдання з питань технічного захисту інформації;

4) військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

5) навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

– забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

– видання в межах своїх повноважень нормативно-правових актів із зазначених питань;

– здійснення контролю за станом технічного захисту інформації.

Згідно з наказом адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про затвердження Положення про державний контроль за станом технічного захисту інформації» від 16 травня 2007 р. № 87, визначаються порядок організації та здійснення державного контролю за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.[[8]](#footnote-8)

Основними нормативними актами, що регулюють використання *криптографії в Україні*, є закони «Про інформацію», «Про науково-технічну інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про Національну систему конфіденційного зв’язку» від 10 січня 2002 р. № 2919-ІІІ, «Про електронний цифровий підпис».

*Криптографічний захист інформації* – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

*Засіб криптографічного захисту інформації* – апаратний, програмний, апаратно-програмний або інший засіб, призначений для криптографічного захисту інформації.

*Криптографічний алгоритм*– алгоритм, який визначає правила перетворення інформації з метою її криптографічного захисту.

*Криптографічна система* – сукупність засобів КЗІ, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та/або передається.

Залежно від призначення встановлюються такі категорії засобів КЗІ:

– засоби шифрування інформації;

– засоби, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ;

– засоби захисту від нав’язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізовують алгоритми криптографічного перетворення інформації, у тому числі засоби імітозахисту та електронного цифрового підпису;

– засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми.[[9]](#footnote-9)

Залежно від способу реалізації розрізняють такі типи засобів КЗІ:

– апаратні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізовується в оптичних, механічних мікроелектронних або інших спеціалізованих пристроях та не може бути змінений під час експлуатації;

– апаратно-програмні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізується програмним забезпеченням, яке встановлюється під час виробництва засобу КЗІ у спеціальному запам’ятовуючому пристрої, виконується в ньому та може бути змінено лише під час виробництва;

– програмні засоби, алгоритм функціонування яких реалізується програмним забезпеченням, що функціонує під управлінням операційних систем електронно-обчислювальної техніки; окремі функції програмного засобу КЗІ (у тому числі криптографічні перетворення) можуть виконуватися апаратними або апаратно-програмними пристроями, що функціонують під управлінням програмного забезпечення засобу КЗІ.[[10]](#footnote-10)

Засоби криптографічного захисту інформації без уведених ключових даних мають *гриф обмеження доступу*, який відповідає грифу обмеження доступу опису криптосхеми. Гриф обмеження доступу засобів криптографічного захисту інформації з уведеними ключовими даними визначається грифом обмеження доступу ключових документів, але не нижче грифа обмеження доступу опису криптосхеми.

Гриф обмеження доступу ключових документів, що використовуються для криптографічного захисту інформації, повинен відповідати грифу обмеження доступу інформації, що захищається.

***2. Правове регулювання захисту інформації в засобах зв’язку***

Закон України «Про телекомунікації» вiд 18 листоп. 2003 р. № 1280-IV визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов’язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами.[[11]](#footnote-11)

Сфера телекомунікацій є складовою частиною галузі зв’язку України.[[12]](#footnote-12)

*Метою регулювання у сфері телекомунікацій* є максимальне задоволення попиту споживачів на телекомунікаційні послуги, створення сприятливих організаційних та економічних умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних мереж з урахуванням інтересів національної безпеки.

Надання телекомунікаційних послуг на території України є виключним правом юридичних осіб з місцезнаходженням на території України, які зареєстровані відповідно до законодавства України, та/або фізичних осіб – суб’єктів підприємницької діяльності з постійним місцем проживання на території України.[[13]](#footnote-13)

Оператори, провайдери телекомунікацій зобов’язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.[[14]](#footnote-14)

Персонал оператора, провайдера телекомунікацій несе відповідальність за порушення вимог законодавства України щодо збереження таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер, а також інформації з обмеженим доступом щодо організації та функціонування телекомунікаційних мереж в інтересах національної безпеки, оборони та охорони правопорядку.

Закон України «Про Національну систему конфіденційного зв’язку» від 10 січня 2002 р. № 2919-ІІІ зазначає, що *Національна система конфіденційного зв’язку*  сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану.

*Суб’єкти Національної системи конфіденційного зв’язку* – органи державної влади та органи місцевого самоврядування, юридичні та фізичні особи, що беруть участь у створенні, функціонуванні, розвитку та використанні цієї системи.

*Складовими Національної системи конфіденційного зв’язку* є спеціальні телекомунікаційні системи (мережі), їх фіксовані і мобільні компоненти, централізовані системи захисту інформації та оперативно-технічного управління. (Частина друга статті 5 із змінами, внесеними згідно із Законом N 2599-IV від 31.05.2005)

*Структура побудови Національної системи конфіденційного зв’язку* повинна забезпечувати відокремлення конфіденційної інформації органів державної влади та органів місцевого самоврядування, інших юридичних та фізичних осіб з використанням криптографічних та/або технічних засобів.

***3. Правове регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу***

Основна *мета застосування електронного цифрового підпису* разом з інститутом сертифікації «відкритих ключів» – це надання електронному повідомленню статусу електронного документа за принципом функціональної еквівалентності.[[15]](#footnote-15)

Електронний зв’язок та комерція обумовлюють використання електронних підписів та суміжних послуг, що роблять можливим засвідчення достовірності інформації.[[16]](#footnote-16)

Закон України «Про електронний цифровий підпис» від 22 травня 2003 р. № 852-IV визначає правовий статус електронного цифрового підпису, регулює відносини, що виникають при його використанні та визначає основні терміни в цій сфері:

Відповідно до ст. 4 Закону України «Про електронний цифровий підпис», *електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів*.

*Електронний підпис* – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації підписувача цих даних.

*Електронний цифровий підпис* – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.[[17]](#footnote-17)

Електронний цифровий підпис використовується фізичними та юридичними особами – суб’єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.[[18]](#footnote-18)

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у тому разі, якщо:

– електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

– під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

– особистий ключ підписувача відповідає відкритому ключу, зазначеному в сертифікаті.

Електронний цифровий підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.[[19]](#footnote-19)

Відносини, пов’язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, ЦК України, законами України «Про інформацію», «Про електронні документи та електронний документообіг» від 22 травня 2003 р. № 851‑IV, «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про телекомунікації», «Про обов’язковий примірник документів» від 9 квітня 1999 р. № 595-ХІV, «Про Національний архівний фонд та архівні установи» від 24 грудня 1993 р. № 3814-ХІІ, а також іншими нормативно-правовими актами.

*Електронний документ* – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа.

Склад та порядок розміщення обов’язкових реквізитів електронних документів визначається законодавством. *Обов’язковий реквізит електронного документа* – обов’язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили.

Електронний підпис є обов’язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб’єктами електронного документообігу.Накладанням електронного підпису завершується створення електронного документа. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

*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.

Електронний документообіг здійснюється відповідно до законодавства України або на підставі договорів, що визначають взаємовідносини суб’єктів електронного документообігу. Використання електронного документа в цивільних відносинах здійснюється згідно із загальними вимогами вчинення правочинів, встановлених цивільним законодавством. При зберіганні електронних документів обов’язкове додержання таких вимог:

– інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

– має бути забезпечена можливість відновлення електронного документа в тому форматі, у якому він був створений, відправлений або одержаний;

– у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять інформацію, яка є власністю держави, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства. Особи, винні в порушенні законодавства про електронні документи та електронний документообіг, несуть відповідальність згідно з законами України.

Отже, сучасний документообіг викликав необхідність введення нового виду документа – електронного, у якому інформація представлена у формі електронних даних, включаючи відповідні реквізити, у тому числі й електронний підпис. Значення електронного підпису як посвідчення, що покликане підтвердити цілісність документа, а також необхідність ідентифікації особи, яка його підписала, зберігається.[[20]](#footnote-20)

**Література:**

1. Про електронний цифровий підпис: закон України від 22 трав. 2003 р. № 852-IV// Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276. – Редакція від 4 лют. 2009 р.
2. Про електронні документи та електронний документо­обіг: закон України від 22 трав. 2003 р. № 851-IV//Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275. – Редакція від 24 черв. 2005 р.
3. Про затвердження Положення про державний контрольза станом технічного захисту інформації [Електронний ресурс]: наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 16 трав. 2007 р. № 87. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>? nreg=z0785-07. – Редакція від 27 січ. 2009 р.
4. Про захист інформації в інформаційно-телекомунікацій­нихсистемах: закон України від 5 лип. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286. – Редакція від 30 квіт. 2009 р.
5. Про Положення про технічний захист інформації в Україні [Електронний ресурс]: указ Президента України від 27 верес. 1999 р. № 1229/99. – Режим доступу: <http://zakon>. rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1229%2F99. – Редакція від 4 трав. 2008 р.
6. Про телекомунікації: закон України від 18 листоп. 2003 р. № 1280-IV// Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155. – Редакція від 27 січ. 2011 р.
7. Антонюк А. О. Основи захисту інформації в автоматизованих системах: навч. посіб. / А. О. Антонюк. – К.: Академія, 2003. – 242 с.
8. Домарев В. В. Защита информации и безопасностькомпьютерных систем / В. В. Домарев. – К.: DiaSoft, 1999. – 453 с.

Гавловський В. Д. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) / В. Д. Гавловський // Правове, нормативне та метрологічне забезпечення систем захисту інформації в автоматизованих системах України. – К.: ЕКМР, 2000. – С. 50–53.

*Тема № 4.* «Загрози інформаційній безпеці»

(Питання до самостійної роботи)

1. Класифікація загроз інформаційній безпеці.
2. Ієрархічна класифікація загроз інформаційній безпеці.
3. Джерела загроз інформаційній безпеці.
4. Методи і засоби забезпечення інформаційної безпеки: основні принципи, система забезпечення, основні фактори і способи.

Тема № 5 «Юридична відповідальність за порушення правових норм в сфері інформаційної безпеки»

**( до самостійного опрацювання)**

1. Поняття і види юридичної відповідальності за порушення правових норм в сфері інформаційної безпеки.

Кримінальна відповідальність за порушення правових норм в сфері інформаційної безпеки.

1. Адміністративна відповідальність за порушення правових норм в сфері інформаційної безпеки.
2. Особливості юридичної відповідальності за порушення правових норм інформаційної безпеки в галузі трудових норм і цивільно-правових відносин.
3. ***Поняття та види юридичної відповідальності за порушення правових норм в сфері інформаційної безпеки***

Юридична відповідальність – це важлива міра захисту інтересів особистості, суспільства і держави.

 Найбільш розповсюджена класифікація юридичної відповідальності за галузевою належністю. Види юридичної відповідальності співпадають з видами правопорушень. Співвідношення правопорушень і юридичної відповідальності показані на рис. 1.

|  |  |
| --- | --- |
|  | Види правопорушень |
|  |
|  Проступок Злочини |
|  Цивільний | Дисциплінарний | Адміністративний |  | Кримінальні |
|  |  |  |  |  |
| Види юридичної відповідальності |
|  |
| Цивільна | Дисциплінарна | Адміністративна |  | Кримінальна |

Рис. 1. Співвідношення видів правопорушень і юридичної відповідальності

Зазначені види правопорушень і юридична відповідальність є характерними і для галузі інформаційної безпеки – для захисту конфіденційної інформації, що обробляється в АСОД (автоматизовані системи обробки даних).

Відповідно, у зв’язку із глобальною комп’ютеризацією інформаційних процесів особливу увагу необхідно приділяти правопорушенням стосовно конфіденційної інформації, яка обробляється в АСОД.

При визначенні характеристик правопорушень інформаційної безпеки враховуються:

– властивості правопорушень, що розглядаються;

– залежність діянь від об’єктивних і суб’єктивних ознак злочинів ,що вчиняються в сфері інформаційної безпеки;

– ситуаційна безпека вчинення правопорушень інформаційної безпеки;

– залежність вирішення завдань попередження правопорушень інформаційної безпеки від заходів правового регулювання діяльності в різних сферах (економіки, зовнішньої політики, воєнній сфері тощо);

– наявність різних форм власності та ін..

1. ***Кримінальна відповідальність за порушення правових норм в сфері інформаційної безпеки***

 Кримінальний кодекс України визначає склад злочинів, предметом яких є державна таємниця. Так, кримінально-правові норми, спрямовані на захист державної таємниці, містяться у розд. І «Злочини проти основ національної безпеки України», до якого включені ст. 111 «Державна зрада» та ст. 114 «Шпигунство», а також у розд. ХІV «Злочини у сфері охорони державної таємниці, недоторканності кордонів, забезпечення призову та мобілізації», до якого входять ст. 328 «Розголошення державної таємниці» і ст. 329 «Втрата документів, що містять державну таємницю».

 Винні в розголошенні даних досудового слідства несуть кримінальну відповідальність за ст. 387 КК України.

 Кримінальним кодексом передбачена відповідальність за злочинні дії, що пов’язані з порушенням вимог охорони комерційної таємниці: незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231), розголошення комерційної або банківської таємниці (ст. 232). Адвокати, винні в розголошенні конфіденційних відомостей,щостановлять адвокатську таємницю, несуть дисциплінарну відповідальність, а в разі розголошення ними без дозволу слідчого або прокурора даних попереднього слідства – і кримінальну відповідальність (ст. 387 КК України).

 Зокрема, кримінальна відповідальність визначається ст. 132 «Розголошення відомостей про проведення медичного огляду на виявлення зараженням вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби», ст. 140 «Неналежне виконання професійних обов’язків медичним або фармацевтичним працівником», ст. 145 «Незаконне розголошення лікарської таємниці».

 Особи, винні у порушенні законодавства про психіатричну допомогу, несуть відповідальність згідно з законами України (ст. 33 Закону України «Про психіатричну допомогу»).

 У ст. 80 «Основ законодавства України про охорону здоров’я» вказується, що особи, винні в порушенні законодавства про охорону здоров’я, несуть цивільну, адміністративну або кримінальну відповідальність згідно із законодавством.

1. ***Адміністративна відповідальність за порушення правових норм в сфері інформаційної безпеки***

Кодекс України про адміністративні правопорушення (далі – КУпАП) передбачає адміністративну відповідальність за порушення законодавства про державну таємницю (ст. 212–2), а саме:

1) недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

2) засекречування інформації:

* про стан довкілля, про якість харчових продуктів і предметів побуту;
* про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;
* про стан здоров’я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти та культури населення;
* про факти порушень прав і свобод людини і громадянина; про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;
* іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, не може бути засекречена;

3) безпідставне засекречування інформації;

4) надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;

5) порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;

6) невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;

7) провадження діяльності, пов’язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов’язаних із державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею;

8) недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними;

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності.

 Кримінально-процесуальний кодекс (далі – КПК) відносить зазначені вище злочини до підслідності Служби безпеки України.

 Адміністративна відповідальність за порушення, що пов’язані з комерційною таємницею, встановлюється за отримання, використання, розголошення комерційної таємниці ст. 164-3 КУпАП.

1. ***Особливості юридичної відповідальності за порушення правових норм інформаційної безпеки в сфері трудових норм і цивільно-правових відносин***

Законом України «Про захист від недобросовісної конкуренції» від 7 червня 1996 р. № 236/96-ВР передбачена відповідальність:

* статтею 16 – за неправомірне збирання комерційної таємниці, яким уважається добування протиправним способом відомостей, що відповідно до законодавства України становлять комерційну таємницю, якщо це завдало чи могло завдати шкоди суб’єкту господарювання;
* статтею 17 – за розголошення комерційної таємниці, яким є ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до чинного законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв’язку з виконанням службових обов’язків, якщо це завдало чи могло завдати шкоди господарюючому суб’єкту господарювання;
* статтею 18 – за схилення до розголошення комерційної таємниці, яким є спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв’язку з виконанням службових обов’язків відомості, що відповідно до законодавства України становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди господарюючому суб’єкту господарювання;
* статтею 19 – за неправомірне використанням комерційної таємниці, яким є впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи відомостей, що становлять відповідно до законодавства України комерційну таємницю.

Правові гарантії захисту особистої інформації встановлені і ЦК України, у якому зазаначається:

* негативна інформація, поширена про особу, уважається недостовірною, якщо особа, яка її поширила, не доведе протилежного (ч. 3 ст. 277);
* якщо особисте немайнове право фізичної особи порушене в газеті, книзі, кінофільмі, теле-, радіопередачі тощо, які готуються до випуску у світ, суд може заборонити розповсюдження відповідної інформації; якщо особисте немайнове право фізичної особи порушене в номері (випуску) газети, книзі, кінофільмі, теле-, радіопередачі тощо, які випущені у світ, суд може заборонити (припинити) їх розповсюдження до усунення цього порушення, а якщо усунення порушення неможливе, вилучити тираж газети, книги тощо з метою його знищення (ст. 278);
* ім’я фізичної особи, яка затримана, підозрюється чи обвинувачується у вчиненні злочину, або особи, яка вчинила адміністративне правопорушення, може бути використане (обнародуване) лише в разі набрання законної сили обвинувальним вироком суду щодо неї або винесення постанови у справі про адміністративне правопорушення та в інших випадках, передбачених законом (ч. 4 ст. 296);
* 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; фізична особа, яка поширює інформацію, зобов’язана переконатися в її достовірності; фізична особа, яка поширює інформацію, отриману з офіційних джерел (інформація органів державної влади, органів місцевого самоврядування, звіти, стенограми тощо), не зобов’язана перевіряти її достовірність та не несе відповідальності в разі її спростування; фізична особа, яка поширює інформацію, отриману з офіційних джерел, зобов’язана робити посилання на таке джерело (ст. 302).

Одним із основних видів правопорушень щодо програм­ного забезпечення є контрафакція, різновидом якої є відтворення, розповсюдження та використання програмного забезпечення без дозволу власника авторських прав на ці твори (комп’ютерне піратство).

За формами порушення авторських прав, що зустріча­ються в процесі придбання та використання комп’ютерних програм, можна виділити наступні:

* придбання контрафактних примірників комп’ютерних програм, виготовлених, наприклад, шляхом запису програм на магнітні або оптичні диски та їх розповсюдження за цінами, що значно нижчі за оригінальні примірники;
* придбання комп’ютерної техніки з попередньо встанов­леним на жорсткі диски таких комп’ютерів неліцензійним програмним забезпеченням; створення в організації контрафактних примірників про­грам як шляхом запису на магнітні диски, так і шляхом вста­новлення на жорсткі диски персональних комп’ютерів в об’ємі, що перевищує кількість примірників комп’ютерних програм, дозволену правовласником за умовами договору щодо розпо­рядження майновими правами інтелектуальної власності.

Використання комп’ютерної програми без відповідного дозволу (ліцензії) автора, невиконання умов договору є пору­шенням авторських прав і може бути підставою для при­тягнення особи-порушника до наступних видів відповідаль­ності згідно з чинним законодавством України: цивільно-правової (майнової) – ст. 431 ЦК та ст. 52 Закону України «Про авторське право і суміжні права»; кримінальної – ст. 176 КК України.

 У зв’язку із цим до КУпАП були внесені зміни: спочатку включено ст. 51-2, якою передбачено відповідальність за порушення права на об’єкт права інтелектуальної власності, а потім ст. 164-9, якою передбачено відповідальність за незаконне розповсюдження примір­ників аудіовізуальних творів, фонограм, відеограм, комп’ютерних програм, баз даних. Право інтелектуальної власності – суб’єктне право, а це означає, що завдання адміністративного розслідування у справах за ст. 51-2 КУпАП необхідно виконувати в повному обсязі і вживати всіх заходів для встановлення суб’єкта права, повідомляти останнього про порушення його права та долучати відповідну інформацію до матеріалів справи.

Використання комп’ютерної програми без відповідного дозволу (ліцензії) автора, невиконання умов договору є порушенням авторських прав і може бути підставою для притягнення особи-порушника до наступних видів відповідальності згідно з чинним законодавством України:

* цивільно-правової (майнової) – ст. 431 ЦК та ст. 52 Закону України «Про авторське право і суміжні права»;
* адміністративної – ст. 51-2 КУпАП;
* кримінальної – ст. 176 КК України.

Сьогодні у судовій практиці розгляду даної категорії справ існують такі проблеми, як неправильна кваліфікація дій правопорушників та неоперативність розгляду справ. Так, судді не розмежовують незаконне використання та не­законне розповсюдження об’єктів інтелектуальної власності. Наприклад, за незаконне використання, комп’ютерної програми помилково притягають до адміністративної відповідальності за ст. 164-9 КУпАП та, навпаки, за наявності фактунезаконного розповсюдження (шляхом продажу) примірниківкомп’ютерних програм, баз даних притягують до адміністра­тивної відповідальності за ст. 51‑2 КУпАП.

 Під час розгляду справ щодо неправомірного використан­ня комп’ютерних програм не всі судді враховують, що важливою є оперативність, оскільки відповідно до п. 7 ст. 247 КУпАП, закінчення на момент розгляду справи про адмініс­тративне правопорушення строків, передбачених ст. 38 КУпАП(два місяці), є обставиною, що виключає провадження в такій справі, і, як наслідок, справа має бути закрита, а вилучена контрафактна продукція повернена власнику.

 Під час розгляду справ про правопорушення у сфері інтелектуальної власності судді, вирішуючи питання про притягнення правопорушника до адміністративної відповідальності та накладення адміністративного стягнення, мають одночасно вирішувати й питання про відшкодування винним майнової шкоди за завдані суб’єкту права протиправними діями збитки. У такому разі в постанові суду суддя має зазначити розмір шкоди, що підлягає стягненню, порядок і строк її відшкодування. Розмір спричинених збитків має істотне зна­чення і для правильної кваліфікації дій правопорушника, розмежування адміністративної та кримінальної відповідальності.

 Так, ст. 431 ЦК встановлює, що порушення права інтелектуальної власності, у тому числі невизнання цього права чи посягання на нього, тягне за собою відповідальність, встановлену цим Кодексом, іншим законом чи договором. З цього визначення випливає, що порушення права інтелектуальної власності можливе як у формі дій (посягання на право інтелектуальної власності), так і у формі бездіяльності (невизнання права інтелектуальної власності). При цьому порушником права інтелектуальної власності може бути фізична або юридична особа.

 **Література:**

1. Кодекс України про адміністративні правопорушення [Електронний ресурс]: станом на 15 берез. 2011 р. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80731-10.
2. Кримінальний кодекс України [Електронний ресурс]: станом на 8 берез. 2011 р. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14.
3. Основи законодавства України про охорону здоров’я: закон України від 19 листоп. 1992 р. № 2801-ХІІ //Відомості Верховної Ради України. – 1993. – № 4. – Ст. 19. – Редакція від 13 жовт. 2010 р.
4. Цивільний кодекс України [Електронний ресурс]: станом на 10 квіт. 2011 р. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=435-15.
5. Про авторське право і суміжні права: закон України від 23 груд. 1993 р. № 3792-ХІІ // Відомості Верховної Ради України. – 1994. – № 13. – Ст. 64. – Редакція від 9 трав. 2011 р.
6. Петренко С. Правовий захист програмного забезпечення / С. Петренко // Право України. – 2003. – № 6. – С. 62–65.

**Практичні завдання:**

***Задача № 1***

У телепередачі «Смачна їжа» ведучий Соцков, демонструючи приготування блюд, цілеспрямовано звертав увагу телеглядачів на декілька продуктів, що представляються по сюжету передачі. При цьому він постійно згадував харчовий концентрат «Том» — одну з дуже смачних сучасних добавок.

Проглядання цієї передачі викликало у фірми «Турист» живий інтерес до продукту «Том», який вона купила для продовольчого постачання туристичної компанії. Проте після вживання харчовогопродукту клієнтами і його аналізу незалежними експертами було відмічено, що рекламовані по телебаченню смакові якості «Тома» явно не відповідають тим характеристикам, про які говорив ведучий Соцков в передачі. Деякі клієнти фірми, одержуючи продукт «Том» як приправу, одержали алергічні розлади і ці неприємні факти були зафіксовані лікарями.

В результаті керівництво фірми «Турист» охарактеризувало дії Соцкова як приховану і недостовірну рекламу і звернулося з позовом до суду до телевізійної компанії, зажадавши від неї компенсацію морального збитку і відшкодування шкоди, заподіяної здоров'ю своїх клієнтів.

*Як необхідно кваліфікувати дії Соцкова і чи правомірні вимоги фірми «Турист»?*

*Відповідь*

*Дивіться Закон «Про рекламу»*

***№ 2***

Адміністрація Енської області в цілях недопущення публікації неперевіреної інформації про стан справ в області і, бажаючи підсилити контроль 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, прийнятого адміністрацією Енської області.*

*Відповідь*

*Дивіться Конституцію України; Закон України «Про друковані засоби масової інформації (пресу) в Україні».*

***Задача № 3***

Журналісти молодіжного відділу газети «Голос» підготували підбірку листів читачів, велика частина яких розділяла погляди легально діючих в країні лівих політичних партій. Цю підбірку планували опублікувати окремим додатком до газети і вже направили її в друкарню.

Проте директор друкарні Хватков відмовився друкувати вказаний додаток до газети. 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 в місцеві Ради.

*Чи відповідають закону офіційне звернення голови адміністрації і рішення самого Хваткова?*

*Відповідь*

*Дивіться Конституцію України, Закон України «Про друковані засоби масової інформації (пресу) в Україні».*

***Задача № 4***

На закритому хімічному підприємстві, розташованому у межі міста і що знаходиться в близькості від державного кордону, в результаті аварії відбувся викид шкідливих речовин в атмосферу. Обласна адміністрація вжила необхідні заходи по евакуації громадян із заражених місць і запобіганню витоку небажаної інформації про аварію. При цьому вона заборонила керівництву підприємства передавати ЗМІ і фахівцям інформацію про масштаби аварії і відомості, які стосуються життя населених пунктів, що входять в зону 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, Закон України «Про друковані засоби масової інформації (пресу) в Україні», 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 6 липня 1999 року)*

**Задача № 5**

В кінці року по телебаченню повідомили, що всі борги по зарплаті працівникам бюджетної сфери погашені. В той же час в деяких районах Енської області вчителі оголосили страйк у зв'язку з невиплатою заробітної платні за останні чотири місяці. Журналіст Воронцов звернувся в адміністрацію 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, Закон України «Про інформацію», Закон України «Про друковані засоби масової інформації (пресу) в Україні»*

**Задача №6**

Хімічний комбінат м. Енська здійснив викид отруйних речовин в річку Дністер. Міські власті, одержавши від санепідемслужби міста відповідну інформацію, не оповістили громадян про небезпеку. В результаті купання в річці діти — п'ять хлопчиків і одна дівчинка — одержали серйозні шкірні захворювання.

*Хто повинен нести відповідальність за приховання даної інформації?*

*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 6 липня 1999 року), Кримінальний кодекс України.*

**Задача №7**

Головний редактор філіалу іноземного журналу «Екологія» дав завдання журналісту зібрати дані для статті про стан води у місцевій річці. Журналіст звернувся до державного науково-дослідного інституту зі зразками води для експертизи. Дані експертизи показали значний вміст шкідливих речовин. На питання про підприємства, які займаються дослідами з цими речовинами журналіст дізнався, що досліди проводить цей науково-дослідний інститут. На запит про надання інформації було відмовлено, мотивуючи тим, що така інформація є комерційною таємницею. Тоді 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 провідного спеціаліста архіву, де за окрему плату йому допомогли знайти інформацію стосовно шкідливих речовин, виявлених в річці, дані про грошові перекази на проведення дослідів з 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, в 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 6 липня 1999 року), Закон України «Про інформацію», Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», Закон України «Про друковані засоби масової інформації (пресу) в Україні»*

**Задача №8**

26 липня громадянин Сидоров П.В., який проживає за адресою: м. Барханськ, вул. Леніна 2/55, звернувся до органів виконавчої влади м. Костишів із запитом про надання йому можливості ознайомлення з усіма документами, що стосуються діяльності міської влади та особисто мера Нікіфорова С.І. м. Костишів у питаннях ремонту стадіону «Ротор». Актуальність цього питання виникла після офіційної заяви Нікіфорова про те, що він бере під свій особистий контроль будівельні роботи на стадіоні. Цю заяву мер зробив 20 липня по місцевому телебаченню.

30 липня громадянину Сидорову зателефонувала секретар Нікіфорова та повідомила про відмову у наданні даних, що цікавлять Сидорова, через те що він не є мешканцем м. Костишів.

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

*Відповідь*

*Дивіться Конституцію України, Закон України «Про інформацію», Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації*

1. Див.: Рассолов М. М. Информационное право / М. М. Рассолов. – М. : Юристъ, 1999. – С. 41. [↑](#footnote-ref-1)
2. Див.: Про затвердження Зводу відомостей, що становлять державну таємницю [Електронний ресурс]: наказ Служби безпеки України від 12 серп. 2005 р. № 440. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0902-05. [↑](#footnote-ref-2)
3. *Рівень таємності відомостей*, віднесених до Зводу, залежить від змісту цих відомостей та від конкретного об’єкта, інформацію щодо якого ці відомості розкривають. Державну таємницю можуть становити відомості, що не перелічені у Зводі, – випадки міжнародного передання секретної інформації. Відповідно до ст. 3 Закону «Про державну таємницю», передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. [↑](#footnote-ref-3)
4. Англомовний тлумачний юридичний словник визначає *juscogens* як «обов’язкову норму міжнародного права, від виконання якої жодна нація не може себе звільнити або не може бути звільнена іншою нацією». *Термін juscogens* застосовують для позначення певних «базових принципів міжнародного права». [↑](#footnote-ref-4)
5. Підставою для передачі є міжнародний договір України, згода на обов’язковість якого надана Верховною Радою України, або мотивоване розпорядження Президента України. Дозвіл на передачу секретної інформації відповідно до цього Положення оформляється Службою безпеки України за наявності зобов’язань або письмових гарантій іноземної держави щодо забезпечення охорони секретної інформації, у тому числі недопущення її надання третій стороні. [↑](#footnote-ref-5)
6. Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, радіотеплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок. Комунікаційне обладнання іноземного виробництва, яке використовується в мережах зв’язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв’язку та змістом повідомлень, які пересилаються. [↑](#footnote-ref-6)
7. Див.: Про затвердження Концепції технічного захисту інформації в Україні [Електронний ресурс]: постанова Кабінету Міністрів України від 8 жовт. 1997 р. № 1126. – Режим доступу: http://zakon.rada.gov.ua/cgi–bin/laws/mair.cgi?nreg= 1126-97-%EF/. [↑](#footnote-ref-7)
8. Організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації, порядок контролю в цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами. [↑](#footnote-ref-8)
9. Засоби КЗІ повинні розроблятися з урахуванням можливих загроз з боку середовища, у якому передбачається їх застосування. Розробник повинен передбачити організаційно-технічні заходи щодо захисту від несанкціонованого доступу, контролю цілісності програмного забезпечення засобу КЗІ, забезпечення надійного механізму тестування засобу КЗІ на правильність функціонування, а також обов’язкового блокування роботи засобу КЗІ у разі виявлення порушень. У засобах КЗІ повинні використовуватися криптоалгоритми та криптопротоколи, які є державними стандартами України або рекомендовані Департаментом. Для розробки засобів КЗІ використовується тільки ліцензійне програмне забезпечення. [↑](#footnote-ref-9)
10. Звичайно користувач апаратних засобів криптографічного захисту інформації не має доступу до змісту запам’ятовувальних елементів, що зберігають мікропрограми керування пристроєм, алгоритм функціонування пристрою змінюється тільки їх розробником або виробником. [↑](#footnote-ref-10)
11. Телекомунікації (електрозв’язок) – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах.

 Телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

 Технічні засоби телекомунікацій – обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж. [↑](#footnote-ref-11)
12. Телекомунікації є невід’ємною частиною виробничої та соціальної інфраструктури України і призначені для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах.

Основними принципами діяльності у сфері телекомунікацій є доступ споживачів до загальнодоступних телекомунікаційних послуг, які необхідні їм для задоволення власних потреб, участі в політичному, економічному та громадському житті. [↑](#footnote-ref-12)
13. Охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України.Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом. [↑](#footnote-ref-13)
14. Призначені для оприлюднення телефонні довідники, у тому числі електронні версії та бази даних інформаційно-довідкових служб, можуть містити інформацію про прізвище, ім’я, по батькові, найменування, адресу та номер телефону абонента в разі, якщо в договорі про надання телекомунікаційних послуг міститься згода споживача на опублікування такої інформації. Під час автоматизованої обробки інформації про абонентів оператор телекомунікацій забезпечує її захист відповідно до закону. Споживач має право на безоплатне вилучення відомостей про нього повністю або частково з електронних версій баз даних інформаційно-довідкових служб. [↑](#footnote-ref-14)
15. Це зафіксовано в модельному законі Комісії ООН з міжнародного торговельного права про електронну комерцію, схваленому Резолюцією Генеральної асамблеї ООН від 16 грудня 1996 р. № А/31/628. Основним принципом використання електронного цифрового підпису є те, що повідомлення даних з таким підписом повинно розглядатися як еквівалент «паперового» документа з власноручним підписом.

 *Електронний цифровий підпис* не є прямим аналогом власноручного підпису і пов’язаний із певною технологією, що допускає специфічні умови і методики його застосування. Якщо обіг звичайного паперового документа пов’язаний із діяльністю двох сторін, то в разі застосування електронного цифрового підпису необхідною є третя сторона – особа, яка користується довірою і може засвідчити вимогу однієї або двох сторін, що підпис було згенеровано особою, зазначеною в документі як людина, котра його підписала. Сукупність таких гарантів повинна становити інфраструктуру центрів сертифікації «відкритих ключів», головне завдання яких полягає в тому, щоб гарантувати новому учаснику електронного документообігу, що наявні в нього копії «відкритих ключів» інших учасників, котрі він використовує для перевірки їхніх підписів, належать їм. [↑](#footnote-ref-15)
16. Захист інформації визначається як забезпечення виконання постачальниками послуг із сертифікації та державними органами, відповідальними за акредитацію чи нагляд, вимог, передбачених Директивою Європейського парламенту та Ради про захист осіб від втручання у зв’язку із обробленням особистої інформації та вільним переміщенням такої інформації від 24 жовтня 1995 р. № 95/46/ЄС. Директива Європейського парламенту та Ради про систему електронних підписів, що застосовуються в межах Співтовариства від 13 грудня 1999 р. № 1999/93 ЄС сприяє використанню підписів та їх юридичному визнанню, закладаючи правову основу для використання електронних підписів і певних послуг сертифікації з метою забезпечення належного функціонування внутрішнього ринку, а також містить вимоги до безпечних засобів створення підпису з метою забезпечення функціонування вдосконалених електронних підписів. [↑](#footnote-ref-16)
17. *Засіб електронного цифрового підпису*– програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису. *Надійний засіб електронного цифрового підпису* – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється в порядку, визначеному законодавством. [↑](#footnote-ref-17)
18. Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом. Важливим напрямом регулювання відносин у сфері використання цифрового підпису є визначення умов признання рівнозначності цифрового підпису і власноручного підпису. [↑](#footnote-ref-18)
19. Захист прав споживачів послуг електронного цифрового підпису, а також механізм реалізації захисту цих прав регулюються законами «Про електронний цифровий підпис» та «Про захист прав споживачів». У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, на електронний документ накладається ще один електронний цифровий підпис юридичної особи, спеціально призначений для цього.

 Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності визначається Кабінетом Міністрів України. Порядок застосування цифрового підпису в банківській діяльності визначається Національним банком України. [↑](#footnote-ref-19)
20. Хоча електронний цифровий підпис не залежить від навичок особи, при його безпосередньому виконанні також можуть виникнути певні проблеми, зокрема йдеться про можливість ненавмисного викривлення через незвичні умови виконання та навмисне викривлення з метою подальшої відмови від підпису, а тому перед законодавцем стоять питання необхідності удосконалення наявних та розроблення нових способів захисту такої інформації від несанкціонованого доступу. [↑](#footnote-ref-20)