**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**
**Харківський національний університет внутрішніх справ**
**Кафедра правоохоронної діяльності та поліціїстики**
**Факультет № 6**

# ТЕКСТ ЛЕКЦІЇ

**з навчальної дисципліни «ІНФОРМАЦІЙНЕ ПРАВО»** обов'язкових компонент освітньої програми першого (бакалаврського) рівня вищої освіти

**262 Правоохоронна діяльність**

**на тему : Правове регулювання відносин в сфері технічної інформації та інформації в інформаційно-телекомунікаційних системах.**

**Харків 2023**

**ЗАТВЕРДЖЕНО**
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30 серпня 2023 року № 7

**СХВАЛЕНО**
Вченою радою факультету № 6
Протокол від 25 серпня 2023 року № 7

**ПОГОДЖЕНО**
Секцією Науково-методичної ради
ХНУВС з юридичних дисциплін
Протокол від 29 серпня 2023 року № 7

Розглянуто на засіданні кафедри правоохоронної діяльності та поліціїстики
Протокол від 18 серпня 2023 року № 8

**Розробники:**
1. Завідувач кафедри правоохоронної діяльності та поліціїстики, кандидат юридичних наук, професор Панова Ірина Вікторівна.

**Рецензенти:**
1. Заступник начальника відділення поліції №3 Харківського районного управління поліції №1 ГУНП в Харківській області, доктор, снс Прокопенко О.Ю.
2. Професор кафедри адміністративного права та процесу факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор, заслужений діяч науки і техніки України Комзюк А.Т.

## План лекції

1. Законодавство України про захист інформації в інформаційно-телекомунікаційних системах.
2. Поняття інформаційних систем та його технологій
3. Інформаційно-телекомунікаційні системи. Обробка інформації, несанкціонований доступ, витік інформації.
4. Відносини між суб'єктами в процесі обробки інформації в інформаційно-телекомунікаційній системі.
5 Відповідальність за порушення законодавства про захист інформації в інформаційно-телекомунікаційних системах.
6. Формування концепції захисту інформації в конкретній інформаційно-телекомунікаційній системі.
7. Державна політика у створення та збільшення використання інформаційних систем, інформаційних технологій і засобів забезпечення.

## Література


1. Конституція України : від 28 черв. 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141. // URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
2. Про захист персональних даних : закон України від 1 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481. // URL: https://zakon.rada.gov.ua/laws/show/2297-17
3. Про захист суспільної моралі : закон України від 20 листоп. 2003 р. № 1296- IV // Відомості Верховної Ради України. – 2004. – № 14. – Ст. 192. // URL: https://zakon.rada.gov.ua/laws/show/1296-15
4. Про інформаційні агентства : закон України від 28 лют. 1995 р. № 74/95-ВР // Відомості Верховної Ради України. – 1995. – № 13. – Ст. 83. // URL: https://zakon.rada.gov.ua/laws/show/74/95-вр
5. Про інформацію : закон України від 2 жовт. 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650. // URL: https://zakon.rada.gov.ua/laws/show/2657-12
6. Про Концепцію Національної програми інформатизації : закон України від 4 лют. 1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 182. // URL: https://zakon.rada.gov.ua/laws/show/75/98-вр
7. Про бібліотеки і бібліотечну справу : закон України від 27 січн. 1995 № 32/95-ВР // Відомості Верховної Ради. – 1995. – № 7. – ст.45. // URL: https://zakon.rada.gov.ua/laws/show/32/95-вр
8. Про Національний архівний фонд і архівні установи : закон України від 24 груд. 1993 № 3814-XII //Відомості Верховної Ради України. – 1994. – № 15. – ст.86. . // URL: https://zakon.rada.gov.ua/laws/show/3814-12
9. Про науково-технічну інформацію: закон України від 25 червн. 1993

№ 3322-XII // Відомості Верховної Ради України. – 1993. – № 33. – ст.345. // URL: https://zakon.rada.gov.ua/laws/show/3322-12
10. Про державну таємницю : закон України від 21.01.1994 № 3855-XII // Відомості Верховної Ради України. – 1994. – №16. – С. 93. // URL: https://zakon.rada.gov.ua/laws/show/3855-12
11. Про захист інформації в інформаційно-телекомунікаційних системах : закон України від 05 лип. 1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – ст.286. // URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
12. Про рекламу : закон України від 3 лип. 1996 р. № 270/96-ВР // Відомості Верховної Ради України. – 1996. – № 39. – Ст. 181. // URL: https://zakon.rada.gov.ua/laws/show/270/96-вр
13. Про доступ до публічної інформації : закон України від 13 січ. 2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314. // URL: https://zakon.rada.gov.ua/laws/show/2939-17
14. Про Доктрину інформаційної безпеки України : Указ Президента України від 25 лютого 2017 року № 47/2017 // Урядовий кур'єр від 28.02.2017. № 38. // URL: https://zakon.rada.gov.ua/laws/show/47/2017

**Основна література:**

1. Інформаційне насильство та безпека: світоглядно-правові аспекти. Дзьобань О.П., Пилипчук В.Г. / За заг. ред. проф. В.Г. Пилипчука. – Харків: Майдан, 2011. – 244 с.
2. Марущак А. І. Інформаційне право України : підручник / А. І. Марущак. – К. : Дакор, 2011. – 456 с.
3. Інформаційна взаємодія у місцевому самоврядуванні: перспективи правового регулювання Дубняк М.В. : монографія – Київ: Видавничий дім «АртЕк». – 2019. – 190 с.
4. Основи інформаційного права України : навч. посіб. – 2-ге вид., перероб. і доп. Рекомендовано МОН / Цимбалюк В. С., Павловський В. Д. – К., 2009. – 414 с.
5. Інформаційне право та інформаційне законодавство Брижко В.М., Фурашев В.М. : наукове видання. – (НДІІП НАПрН України). Київ: Видавничий дім "АртЕК", 2020. 288 с.
6. Брижко В. М. Методологічні та правові засади упорядкування інформаційних відносин : монографія / Брижко Валерій Михайлович. – К. : ПанТОТ, 2009. – 415 с.
7. Горбулін В. П. Проблеми захисту інформаційного простору України : монографія / В. П. Горбулін, М. М. Биченок. – К. : Інтертехнологія, 2009. – 136 с.
8. Становлення і розвиток системи стратегічних комунікацій сектору безпеки і оборони України Пилипчук В. Г., Компанцева Л. Ф., Кудінов С. С., Доронін І. М., Дзьобань О. П., Акульшин О. В., Заруба О. Г.; за заг. ред. В. Г. Пилипчука: монографія – К. : ТОВ «Видавничий дім «АртЕк», 2018. – 272 с.

**Додаткова література:**

1. Панова І.В. Фактори, що впливають на утворення системи інформаційного права та формування її змісту // Інформація і право. 2018. № 3 (26). С. 9-15.
2. Панова І.В. Сучасні проблеми цифровізації військового обліку в Україні // Проблеми сучасної поліцеїстики : тези доп. III наук.-практ. конф. (м. Вінниця, 11 трав. 2023 р.) / МВС України, Харків. нац. ун-т внут. справ, Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2023. – 208 с. – С. 52-56. https://dspace.univd.edu.ua/items/53e4a11d-7784-47ec-8140-1c250b37af2e
3. Панова І.В., Шевцова А.С. Національна поліція України як суб'єкт формування і реалізації політики інформаційної безпеки України // Проблеми сучасної поліцеїстики : тези доп. II наук.-практ. конф. (м. Харків, 20 квіт. 2022 р.) / МВС України, Харків. нац. ун-т внут. справ, Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2022. – 208 с. – С. 281-283. https://dspace.univd.edu.ua/server/api/core/bitstreams/cd87cc48-6e4f-497a-a782-d3a76ce14332/content
4. Панова І.В., Шевцова А.С. Засоби забезпечення інформаційної безпеки України// Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. X Міжнар. наук.-практ. конф., присвяч. 27-й річниці створення Харків. нац. ун-ту внутр. справ (м. Харків, 19 листоп. 2021 р.).–Харків: ХНУВС, 2021.–С. 72-74 https://dspace.univd.edu.ua/items/c216c142-4cdd-427c-927c-f3b9dee6e6c0
5. Щодо окремих питань визначення стандартів кібербезпеки при підготовці працівників для кіберполіції Підготовка охоронців правопорядку в Харкові (1917–2017 рр.): зб. наук. ст. і тез доп. на наук.-практ. конф. до 100-річчя підготовки охоронців правопорядку в Харкові (м. Харків, 25 листоп. 2017 р.)/МВС України, Харків. нац. ун-т внутр. справ.–Харків, 2017.–340 с. https://dspace.univd.edu.ua/items/7230016d-744b-497c-8abf-3e2fde902571

**Інформаційні ресурси в Інтернеті**

1. Офіційний сайт Верховної Ради України https://iportal.rada.gov.ua/
2. Офіційний сайт Кабінету Міністрів України https://www.kmu.gov.ua/
3. Офіційний сайт Судова влада України https://court.gov.ua/
4. Офіційний сайт МВС України www.mvs.gov.ua.
5. Офіційний сайт Верховного Суду України http://www.viaduk.net/clients/vsu/vsu.nsf/
6. Єдиний державний реєстр судових рішень http://www.reyestr.court.gov.ua/
7. Національна бібліотека України ім. В.І. Вернадського http://www.nbuv.gov.ua/
8. Офіційний сайт Харківського національного університету внутрішніх справ http://univd.edu.ua/
9. Харківська державна наукова бібліотека ім. В.Г. Короленко http://korolenko.kharkov.com/
10. Юридична бібліотека http://pravo.biz.ua/

11. сайт Національного інституту стратегічних досліджень. – http://www.niss.gov.ua

## 1. Законодавство України про захист інформації в інформаційно-телекомунікаційних системах

Інноваційна спрямованість сучасної економічної діяльності, інтеграція до глобальних процесів розвитку інформаційного суспільства потребує відповідного правового забезпечення.

На сьогодні дослідження науковців спрямовуються саме на роз криття новітніх інформаційних процесів та їх правової регламентації. Не є винятком і питання правового регулювання захисту інформації в інформаційно-телекомунікаційних системах.

Наразі відносини, що виникають з приводу захисту інформації в інформаційно-телекомунікаційних системах, регулюються **Законом України "Про захист інформації в автоматизованих системах"** від 05.07.94 р. (нова редакція Закону **"Про захист інформації в інформаційно-телекомунікаційних системах"** від 31 травня 2005 року № 2594-ГУ, набрала чинності з 1 січня 2006 року). Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі система). Дія зазначеного Закону поширюється на будь-яку інформацію, що обробляється в автоматизованих системах.

Відносини, що виникають з приводу захисту інформації в інформаційно-телекомунікаційних системах, також частково регулюються **Законом України "Про електронні документи та електронний документообіг"** від 22.05.2003 р. Предметом правового регулювання даного Закону є відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

На сьогодні питання захисту інформації в інформаційно-телекомунікаційних системах окрім Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та інших законів регулюються також низкою підзаконних нормативно-правових актів.

Кабінет Міністрів України Постановою від 13 березня 2002 р. № 281 уповноважив Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (Законом України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23 лютого 2006 року на базі Департаменту спеціальних телекомунікаційних систем та захисту інформації та відповідних підрозділів Служби безпеки України утворено Державну службу спеціального зв'язку та захисту інформації України) здійснювати управління захистом інформації в автоматизованих системах відповідно до Закону України "Про захист інформації в автоматизованих системах".

Так, наприклад, *Кабінет Міністрів України Постановою від 2 серпня 1996 р. № 898 "Про створення Єдиної державної автоматизованої паспортної системи"* започаткував створення Єдиної державної автоматизованої паспортної системи (далі - Система), яка забезпечуватиме видачу громадянам

паспортів, що оформлюватимуться за єдиною технологією, та облік громадян за місцем проживання із застосуванням комп'ютерної мережі на єдиних принципах їх ідентифікації (із використанням особистих (ідентифікаційних) номерів громадян, відцифрованого образу осіб і біометричної ідентифікації) і взаємодії з базами даних інших інформаційних систем (як вітчизняних, так і іноземних). Передбачалося, що Система входитиме складовою частиною до Державного реєстру фізичних осіб.

Постановою Кабінету Міністрів України від 29 квітня 2004 р. № 573 було затверджено *Положення про Головний обчислювальний центр Єдиної державної автоматизованої паспортної системи.* Зазначеним Положенням зокрема визначалося, що основними завданнями Головного обчислювального центру є серед інших "впровадження комплексної системи захисту інформації Єдиної державної автоматизованої паспортної системи і здійснення постійного контролю за дотриманням у ній інформаційної безпеки" .

Постанова Кабінету Міністрів України від 16 лютого 1998 р. № 180 *"Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах"* також регулювала відносини щодо обігу інформації (яка становить державну таємницю) в автоматизованих системах.

Постанова Кабінету Міністрів України від 8 червня 1998 р. № 832 визначала комплекс заходів щодо поетапного впровадження у Пенсійному фонді автоматизованого персоніфікованого обліку відомостей у системі загальнообов'язкового державного пенсійного страхування.

Пам'ятаємо також про створення і функціонування у Центральній виборчій комісії автоматизованої інформаційної системи "Вибори", яка застосовувалась у процесі підготовки і проведення виборів Президента України, народних депутатів України.

Питання функціонування конкретних автоматизованих систем у органах державної влади, як правило, визначаються відомчими нормативно-правовими актами.

Так, наприклад, у Міністерстві фінансів України розроблено Положення про роботу із засобами обчислювальної техніки та про доступ до інформаційних ресурсів Міністерства фінансів України (додаток до наказу Міністерства фінансів України від 01.04.2003 р. № 248).

Наказом МВС України від 02.09.98 р. № 659 затверджено *Інструкцію про створення єдиної автоматизованої системи номерного обліку вогнепальної (стрілецької) зброї,* яка зберігається й використовується в МВС, на об'єктах дозвільної системи та перебуває в особистому користуванні громадян.

## 2. Поняття інформаційних систем та його технологій

Основними джерелами правовим регулюванням відносин у галузі створення застосування автоматизованих інформаційних систем, інформаційних технологій засобів зв'язку й телекомунікацій є нормативно-правова база України.

**До інформаційних систем** належить і автоматизовані інформаційні системи різного виду.

Передусім це Інтернет, і навіть автоматизовані системи управління (АСУ), автоматизовані системи обробки даних (АСОД), автоматизовані системи науково-технічної інформації (АСНТИ) тощо., банки даних, бази знань, експертні системи, інформаційно-обчислювальні системи, інформаційно-телекомунікаційні системи та мережі, системи зв'язку й телекомунікації, і навіть кошти забезпечення цих систем і технологій.

**Основні технічні засоби** — кошти обчислювальної техніки,копировально-множительная техніка, оргтехніка, засоби зв'язку і телекомунікацій, і ін.

**Програмні засоби** — операційні системи, прикладні програми, програмні кошти телекомунікації, інші програмні кошти.

**Лингвистические засоби** — словники, тезауруси, класифікатори, інші лінгвістичні кошти, організаційно-правові кошти — нормативні правові норми й правові акти, нормативно-технічні документи, становища, статути, посадові інструкції.

*Класифікація інформаційних технологій і засобів по забезпеченню:*

*1)* Автоматизированние інформаційні системи, їх мережі : банки даних, бази даних, бази знань, експертні системи, автоматизовані системи управління, системи автоматизованого проектування, автоматизовані системи обробки даних, автоматизовані системи науково-технічної інформації, інформаційно-обчислювальні системи, інформаційні мережі.

*2)* Технічні засоби: кошти обчислювальної техніки,копировально-множительная техніка, оргтехніка, засоби зв'язку, кошти телекомунікації, інші технічні засоби.

*3)* Програмні засоби: операційні системи, прикладні програми

*4)* Лингвистические засоби: словники, тезауруси, класифікатори

*5)* Организационно-правовие кошти: становище, статут, порядок реалізації функцій і завдань, посадові інструкції, порядок застосування, користування системою, нормативно-технічні документи

*6)* Технологічне забезпечення: інформаційні технології, інструкції, правила суб'єктів у сфері можна розділити на дві групи: а) суб'єкти, організуючі і здійснюють розробку інформаційних систем, інформаційних технологій і коштів на свою забезпечення; б) суб'єкти, експлуатуючі перелічені об'єкти.

Як суб'єктів, що організують і виконують розробку інформаційних систем, виступають замовники і розробники. Це — органи структурі державної влади, юридичні і особи — організації та підприємства, фахівці. Суб'єктами, що експлуатують інформаційні системи, інформаційні технології, є органи структурі державної влади, їх підрозділи, юридичні і особи. Одне з найважливіших напрямів діяльності суб'єктів у цій галузі повинні прагнути бути формування та розвиток програмно-технічної частини інформаційної інфраструктури сучасного інформаційного суспільства. Під впливом інформаційної інфраструктурою у разі розуміється організована сукупність коштів обчислювальної техніки, зв'язку й телекомунікацій, і навіть масової

інформації та інформаційних ресурсів, забезпечує ефективну і якісну реалізацію інформаційних процесів — процесів виробництва, збору, накопичення, зберігання, пошуку, поширення та споживання інформації задоволення потреб особистості, суспільства, держави. Сьогодні це найчастіше називають «російський фрагмент Інтернет». У програмно-технічної частини інформаційної інфраструктури мають відбитися заходи, пов'язані зі створенням і застосуванням коштів обчислювальної техніки, зв'язку й телекомунікацій, ні з плеканням якого і розвитком інформаційних мереж у Україні із виходом транскордонні інформаційні сіті й Інтернет. Держава визначає умови та вимоги за такими з основних питань:

розвиток (виробництва і видів використання українських програмно-технічних коштів — коштів обчислювальної техніки, зв'язку й телекомунікацій, їхню конкурентоздатність на світовий рівень;

зарубіжних засобів обчислювальної техніки, зв'язку й телекомунікацій з урахуванням захисту державних інтересів;

створення нформаційних мереж з допомогою державного бюджету та взагалі приватних вкладень, іноземних інвестицій за умови державного контролю над збереженням інформаційну безпеку України;

інтеграція інформаційних мереж глобальні транскордонними інформаційними мережами, насамперед Інтернет.

## 3. Інформаційно-телекомунікаційні системи. Обробка інформації, несанкціонований доступ, витік інформації

Розуміння основних понять, що застосовуються у сфері захисту інформації в інформаційно-телекомунікаційних системах, дає можливість не лише правильно аналізувати суб'єктно-об'єктний склад відповідних правовідносин, а й дозволяє правильно використовувати їх під час усної відповіді і виконання практичних завдань студентами та слухачами. **Законом України "Про захист інформації в інформаційно-телекомунікаційних системах"** даються такі визначення основних понять:

блокування інформації в системі — дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації — результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

власник інформації — фізична або юридична особа, якій належить право власності на інформаці власник системи — фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі — отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі — діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі — дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система — організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система — сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації — взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі — фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації — вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/віднов-лення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі — дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі — виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі — несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі — умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації — вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлений витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Доповнює перелік основних термінів у сфері захисту інформації в інформаційно-телекомунікаційних системах *Наказ ДСТЗІ СБ України 24 грудня 2001 р. № 76, яким затверджено Порядок захисту державних шформаційних ресурсів в автоматизованих системах.*

## 4. Відносини між суб'єктами в процесі обробки інформації в інформаційно-телекомунікаційній системі

Аналіз відносин, що виникають між суб'єктами в процесі обробки інформації в інформаційно-телекомунікаційних системах, дає можливість розкрити їх специфіку.

**Об'єктами захисту** в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

**Суб'єктами відносин,** пов'язаних із захистом інформації в системах, є:

- власники інформації;
- власники системи;
- користувачі;

- уповноважений орган у сфері захисту інформації в системах (Державна служба спеціального зв'язку та захисту інформації України).

На підставі укладеного договору або за дорученням власник інформації може надати право розпоряджатися інформацією іншій фізичній або юридичній особі — розпоряднику інформації.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі — розпоряднику системи.

Статтею 4 *Закону України "Про захист інформації в інформаційно-телекомунікаційних системах"* визначені загальні підстави доступу до інформації в системі: "порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом".

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі Відносини між власником системи та користувачем полягають у тому, що власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

*Відносини між власниками систем* базуються на тому, що власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням **комплексної системи захисту інформації з підтвердженою відповідністю.** Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, 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.

*Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.*

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога Щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації.

Вимоги до забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої передбачена законом, встановлюються Кабінетом Міністрів України.

Обов'язки уповноваженого органу у сфері захисту інформації в системах виконує центральний орган виконавчої влади у сфері криптографічного та технічного захисту інформації (Державна служба спеціального зв'язку та захисту інформації України).

**Уповноважений орган у сфері захисту інформації в системах:**

- розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;
- визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;
- здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Державні органи в межах своїх повноважень за погодженням з уповноваженим органом у сфері захисту інформації встановлюють особливості захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

## 5. Відповідальність за порушення законодавства про захист інформації в інформаційно-телекомунікаційних системах

Особи, винні в порушенні порядку і правил захисту оброблюваної в ІТС інформації, несуть дисциплінарну, адміністративну, кримінальну чи матеріальну відповідальність згідно з чинним законодавством України.

Зупинимося на окремих складах правопорушень у сфері захисту інформації в АС.

*Кодекс України про адміністративні правопорушення було доповнено Законом України "Про внесення змін до деяких законодавчих актів України від 11 травня 2004 року"* № 1703-ІУ статтею 212-6 "Здійснення незаконного доступу до інформації в автоматизованих системах".

Цією статтею передбачена адміністративна відповідальність за "здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах". Санкція за дане правопорушення - накладення штрафу від п'яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої Та сама дія, вчинена особою, яку протягом року було піддано адміністративному стягненню за порушення, передбачене в частині першій статті 212-6, - тягне за собою накладення штрафу від десяти до двадцяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу.

*Законом України "Про внесення змін до Кримінального та Кримінально-процесуального кодексів України* від 23 грудня 2004 року № 2289-ІУ статті 361, 361-2, 362, 363, 363-1 Кримінального кодексу України (КК України) були викладені у новій редакції. Передбачені даними статтями склади злочинів містять об'єкт, що безпосередньо стосується захисту інформації в АС.

*Стаття 361 КК України "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку"* передбачає кримінальну відповідальність за "несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації". За скоєння такого злочину передбачається санкція у вигляді штрафу від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеження волі на строк від двох до п'яти років, або позбавлення волі на строк до трьох років, з

позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи Додатковими кваліфікуючими ознаками даного злочину є вчинення його повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду. Такі діяння (дії) караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Стаття 361-2 КК України *"Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації"* передбачає, що "несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, — караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, — караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи". Стаття 362 КК України "Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї" передбачає кримінальну відповідальність за несанкціоновані зміну, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї. Санкція за скоєння даного злочину - штраф від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

"Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право

доступу до такої інформації, — караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

Дії, передбачені частиною першою або другою статті 362 КК України, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи". Стаття 363 КК України "Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється передбачає, що "порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк".

Стаття 363-1 КК України *"Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку"* передбачає кримінальну відповідальність за "умисне масове розповсюдження по відомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку". Санкція - штраф від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років.

"Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, — караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи".

Згідно зі статтею 18 Закону України "Про захист інформації в автоматизованих системах", шкода, заподіяна суб'єктам відносин, що виникають під час захисту інформації в АС (власникам інформації чи уповноваженим ними особам; власникам АС чи уповноваженим ними особам; користувачам інформації; користувачам АС), внаслідок незаконного створення

перешкод для доступу до інформації, витоку чи втрати інформації в АС, відшкодовується особами, яких визнано винними в цьому.

## 6. Формування концепції захисту інформації в конкретній інформаційно-телекомунікаційній системі

**Нормативні документи, що визначають особливості захисту інформації в конкретній автоматизованій системі,** мають розроблятися на підставі і з урахуванням положень таких державних стандартів:

НД ТЗІ 1.1-002-99. Загальних положень щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджених наказом ДСТСЗІ від 28.04.99 № 22 "Про затвердження і введення в дію нормативних документів";

НД ТЗІ 2.5-005-99. Класифікації автоматизованих систем і стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу, затвердженої наказом ДСТСЗІ від 28.04.99 №22;

НД ТЗІ 2.5-004-99. Критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджених наказом ДСТСЗІ від 28.04.99 № 22;

НД ТЗІ 1.1-003-99. Термінології в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затвердженої наказом ДСТСЗІ від 28.04.99 № 2

Згідно з НД ТЗІ 2.5-005-99. Класифікацією автоматизованих систем і стандартних профілів захищеності оброблюваної інформації від несанкціонованого доступу автоматизовані системи розподіляють на три класи: клас "1" - одномашинний однокористувачевий комплекс; клас "2" - локалізований багатомашинний багатокористува-чевий комплекс; клас "З" - розподілений машинний багатокористувачевий комплекс, у якому передання інформації здійснюється через незахищене середовище (глобальну мережу).

*Прикладом індивідуального нормотворення у сфері захисту інформації в АС* може бути Комплексна система захисту інформації в автоматизованій системі Міністерства та Інструкція користувача автоматизованої системи 3 класу, які затверджені Наказом Міністерства економіки та з питань європейської інтеграції України від 23.04.2002 р. № 121 "Про заходи щодо захисту конфіденційної і відкритої інформації, що циркулює в автоматизованій системі Міністерства". У зазначених документах використано принцип, який є актуальним не лише для Міністерства економіки та з питань європейської інтеграції України, а й для інших органів державної влади. Зокрема, зазначається, що широке застосування програмно-технічних обчислювальних засобів імпортного походження при приєднані їх до Інтернету принципово унеможливлює здійснити надійний захист інформації, що належить державі. У таких умовах забезпечення конфіденційності, цілісності і доступності інформації можливе лише в разі фізичного відокремлення автоматизованої системи, де циркулює інформація, яка потребує захисту, від системи, яка приєднана до Інтернету.

## 7. Державна політика у створення та збільшення використання інформаційних систем, інформаційних технологій і засобів забезпечення

Законом України «Про інформацію» визначена державна політика у створення застосування автоматизованих інформаційних систем, засобів зв'язку й телекомунікацій: створення й розвиток регіональних інформаційних систем та мереж, забезпечення їх сумісності і взаємодії єдиному інформаційний простір України;

сприяння формування ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів на своє забезпечення;

забезпечення національної стратегії безпеки у сфері інформатизації, і навіть забезпечення реалізації прав громадян, організацій умовах інформатизації;

формування та здійснення єдиної науково-технічної й промислової політики у сфері інформатизації з урахуванням сучасного світового рівня розвитку інформаційних технологій;

підтримка проектів і програм інформатизації;

створення й удосконалення системи залучення інвестицій і механізму стимулювання розробки й реалізації проектів інформатизації;

розвиток законодавства надають у цій галузі.

Усі види виробництва інформаційних систем та мереж, технологій і коштів на свою забезпечення становлять спеціальну галузь економічної діяльності, розвиток визначається державної науково-технічної й промислової політикою інформатизації. Державні і недержавні організації, і навіть громадяни мають рівних прав розробці і виробництво інформаційних систем, технологій і засобів на своє забезпечення. Держава створює умови щодо проведення науково-дослідницьких і дослідно-конструкторських робіт у царині розробки і виробництва інформаційних систем, технологій і коштів на свою забезпечення. Уряд України визначає пріоритетні напрямки розвитку інформатизації й встановлює порядок фінансування. Розробка і експлуатація федеральних інформаційних систем фінансуються із засобів федерального бюджету за статті витрат «Інформатика» («Інформаційне забезпечення»). Органи державної статистики разом із Міністерством зв'язку України встановлюють правила обліку, і аналізу становища галузі економічної діяльності, розвиток визначається державної науково-технічної й промислової політикою інформатизації.