

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 : Інформаційна безпека.

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. Загальна характеристика державної політики в інформаційній сфері України
2. Концепція державної інформаційної політики
3. Інформаційна безпека та її завдання
4. Проблеми забезпечення інформаційної безпеки

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. – (НДІП 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 поліцейстики : 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 поліцейської : 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 внут. 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 внут. 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://portal.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. Загальна характеристика державної політики в інформаційній сфері України

Об'єктивно категорія «інформаційна безпека» виникла з появою **засобів інформаційних комунікацій** між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завданий збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між всіма елементами соціуму.

Поняття *інформаційної безпеки* можна розглядати у декількох ракурсах. По-перше, це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави.

Під **інформаційним середовищем** розуміють сферу діяльності суб'єктів, пов'язану із створенням, обробленням й споживанням інформації.

По-друге, **інформаційна безпека** – це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість рішень і дій, що приймаються.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Інформаційна безпека держави — стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека організації — цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Інформаційна безпека особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Об'єктами інформаційної безпеки можуть бути: свідомість, психіка людини; інформаційні системи різного масштабу й різного призначення. До

соціальних об'єктів інформаційної безпеки відносять особистість, колектив, державу, суспільство, світове товариство.

До **суб'єктів інформаційної безпеки** належать: держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями щодо забезпечення інформаційної безпеки відповідно до законодавства.

1. Види інформаційної безпеки.

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

Інформаційна безпека держави характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки.

2. Загрози інформаційній безпеці.

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєвоважливим інтересам особистості, суспільства й держави в інформаційній сфері. Основні загрози інформаційній безпеці поділяють на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Фактори загроз за видовою ознакою поділяються на політичні, економічні і організаційно-технічні.

Явища та процеси природного й штучного походження, що породжують інформаційні загрози, називають *дестабілізуючими факторами*.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так й організації і їхні об'єднання. Особливу групу джерел складають інформаційні системи та засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості

або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна подати у вигляді міждержавних і внутрішньодержавних.

До *внутрішньодержавних* дестабілізуючих факторів відносять: правовий вакуум у більшості питань забезпечення інформаційної безпеки; порушення законодавства з питань інформаційної безпеки; політичні конфлікти; відмови, збої, технічні помилки інформаційних систем (засобів); природні явища, що ускладнюють передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

3. Методи й засоби забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки – це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства й держави в інформації.

Державна система забезпечення інформаційної безпеки країни являє собою організаційне об'єднання державних органів, а також сил і засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади.

Форми й способи забезпечення інформаційної безпеки утворюють інструмент, за допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань щодо захисту життєво важливих інтересів особистості, суспільства й держави. Формами забезпечення інформаційної безпеки є: інформаційний патронат, інформаційна кооперація, інформаційне протиборство.

Інформаційний патронат – це форма забезпечення інформаційної безпеки фізичних та юридичних осіб з боку держави. При цьому інформаційне забезпечення містить збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхнє оброблення, обмін інформацією між органами управління й силами та засобами системи інформаційної безпеки. Інформаційний захист здійснюється шляхом ухвалення певних законопроектів, здійснення судового захисту, проведення оперативних заходів силами й засобами інформаційної безпеки.

Інформаційна кооперація – форма забезпечення інформаційної безпеки рівноправних суб'єктів інформаційного процесу (фізичних, юридичних, міжнародних), який містить сукупність взаємоузгоджених дій цих суб'єктів. Такі дії спрямовані на одержання відомостей про дестабілізуючі фактори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами й засобами.

Для розв'язання конфліктів різного масштабу останнім часом все частіше використовується інформаційна сфера, яка породжує таке явище, як **інформаційне протиборство**, що характеризується, з одного боку, впливом на системи добування, оброблення, поширення та зберігання інформації

противника, а з іншого – застосуванням заходів захисту своїх подібних систем від деструктивного й керуючого впливу. Інформаційне протиборство здійснюється між різноманітними видами соціальних суб'єктів (особистостей, суспільств, держав), проте цілий ряд таких конфліктних взаємодій має певні відносно стійкі ознаки, які в сукупності утворюють окремі форми протиборства – інформаційну війну, інформаційний тероризм, інформаційну злочинність.

Інформаційна війна – це явище, при якому здійснюється комплексний вплив на інформаційну сферу противника, який має метою створення умов для ведення «бойових дій» (інформаційна боротьба) або виступає як самостійний фактор, який змушує конфліктуючу державу відмовитись від намічених політичних, економічних або інших цілей.

Інформаційна війна припускає використання широкого спектру сил і засобів, за допомогою яких здійснюються взаємозв'язані заходи щодо деструктивного впливу на інформаційну сферу противника. Отже, інформаційна війна – це комплекс заходів та операцій, спрямованих на забезпечення інформаційної переваги над потенційним або реальним противником.

Інформаційний тероризм – це дії окремих осіб або їхніх груп щодо дезорганізації роботи автоматизованих систем і мереж зв'язку, що створюють небезпеку життю людей, спричиняють значні матеріальні збитки або інші суспільно небезпечні наслідки, а також загроза здійснення вказаних дій, якщо вони відбуваються з метою порушення суспільної безпеки, залякування населення або здійснення впливу на прийняття рішень органами влади. До кібертероризму відносять також деструктивні дії щодо інформаційних систем, які створюють умови для проведення актів тероризму.

На відміну від війни для тероризму характерна початкова нерівність конфронтуючих сторін, що обумовлює прагнення більш слабкої сторони використати такі методи й способи, за допомогою яких противникові завдають найбільших збитків при витраті мінімуму своїх сил і засобів, а також здійснюють сильний психологічний вплив. Об'єктом тероризму є не ті, хто став жертвами, а ті, хто залишився живими. Метою тероризму є не вбивство, а залякування й деморалізація живих. Інформаційна сфера дає великі можливості для цього. За її допомогою можна поширювати ідеї тероризму, залучати до своєї діяльності нових учасників, інформаційно й психологічно впливати на широкі маси людей.

Інформаційна злочинність здійснюється як з використанням інформаційно-комп'ютерних, так й інформаційно-психологічних методів впливу – наклепу, образи, поширення недостовірної інформації тощо. Адміністративний і кримінальний кодекси України містять перелік злочинів, які можуть здійснюватися в інформаційній сфері.

Перелічені вище форми інформаційного протиборства тісно пов'язані між собою. Однією з функцій інформаційного протиборства є забезпечення інформаційної безпеки, яка досягається здійсненням певних пасивних або активних заходів.

Пасивне забезпечення інформаційної безпеки передбачає реагування на наявні загрози, його спрямовано на безпосередню протидію акціям, що є деструктивними відносно соціальної системи.

Активне забезпечення інформаційної безпеки спрямовано на завчасне виявлення й попередження загроз. Це може досягатися шляхом проведення заходів щодо з'ясування планів, цілей, сил і засобів конфронтуючої соціальної системи, а також застосування протидії деструктивним акціям на етапі їхньої підготовки.

Звідси, **Інформаційна безпека держави** — це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

Відповідно до законодавства України поняття "інформаційна безпека" має таке визначення:

"стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації." [2]

4. Виокремлюють три рівня забезпечення інформаційної безпеки:

- **рівень особи** (формування раціонального, критичного мислення на основі принципів свободи вибору);
- **суспільний рівень** (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);
- **державний рівень** (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам)є

2. Концепція державної інформаційної політики

Досі не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки.

Протягом 2002-2010 рр. було три спроби ухвали концепцію державної інформаційної політики - 2002, 2009 та 2010 року. 11 січня 2011 року черговий проект концепції прийняли у першому читанні за основу закону і направили на доопрацювання Комітету Верховної Ради України з питань свободи слова та інформації.

Загрози національній безпеці в інформаційній сфері. Однією з

основних загроз інформаційній безпеці ЗУ "Про основи національної безпеки" називає "намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації". До інших загроз віднесено:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави. ^[5]

В Доктрині інформаційної безпеки України, підписаній Президентом в липні 2009 р., серед всього виділено наступні **загрози інформаційній безпеці країни**:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;
- деструктивні інформаційні впливи, які спрямовані на підриг конституційного ладу, суверенітету, територіальної цілісності і недоторканності України;
- прояви сепаратизму в засобах масової інформації, а також у мережі Інтернет, за етнічною, мовною, релігійною та іншими ознаками. ^[6]

Діяльність Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки - при Національній Раді безпеки і оборони (РНБО) діє Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки. До основних її завдань, зокрема, належить аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики.

Важливу роль в забезпеченні інформаційної безпеки відіграють **Укази Президента України**

23 квітня 2008 р. Президент України своїм наказом № 377/2008 ввів в дію рішення РНБО "Про невідкладні заходи щодо забезпечення інформаційної безпеки України". Відповідно до цього указу уряд, зокрема, мав:

- розробити і внести у шестимісячний строк на розгляд Верховної Ради України проект Концепції національної інформаційної політики, яка визначатиме основні напрями, засади і принципи національної політики, механізми її реалізації та пріоритети розвитку інформаційної сфери;
- затвердити державну програму формування позитивного іміджу України;
- виділити фінансування на інформаційно-роз'яснювальну діяльність культурно-інформаційних центрів при закордонних дипломатичних установах України, розширити мережу таких центрів;

- затвердити заходи щодо розширення вітчизняного мовлення на території інших держав іноземними мовами;
- вжити невідкладних заходів щодо забезпечення присутності програм вітчизняних телерадіоорганізацій у багатоканальних мережах інших держав.

Результатом виконання цього указу стало, зокрема, створення РНБО Доктрини інформаційної безпеки України - сукупності основних офіційних поглядів на мету, задачі, принципи й основні напрямки забезпечення інформаційної безпеки держави. Віктор Ющенко затвердив її у липні 2009 р. В підготовці і обговоренні документу було задіяно понад 30 органів державної влади, наукових установ, враховано понад 200 конкретних пропозицій, у тому числі від представників громадських організацій, експертного середовища. В ньому сказано, що в інформаційній сфері України вирізняються такі **життєво важливі інтереси 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.

В цьому ж було документі визначено **принципи забезпечення інформаційної безпеки України**:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;
- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним;
- пріоритетність національної інформаційної продукції.

3. Інформаційна безпека та її завдання

Інформаційна безпека має на увазі під собою забезпечення захисту інформації і інфраструктури, що здійснює її підтримку від будь-якого випадкового або ж зловмисного втручання, в результаті якого може бути нанесений утрата інформації в цілому, її безпосереднім власникам і інфраструктурі, що підтримує її зберігання і існування. Інформаційна безпека

виконує завдання, пов'язані з прогнозуванням і запобіганням можливим діям подібного роду, а також зводить до мінімуму можливий збиток.

Інформаційна безпека і можливі загрози її забезпеченню.

Дії, які так або інакше загрожують збереженню, що допускають нанесення збитків інформаційній безпеці підрозділяються на певні категорії.

1. Дії, які здійснюють користувачі, авторизовані в системі. Ця категорія включає:

- зловмисні дії користувача з метою крадіжки або повного або часткового знищення даних, що є на сервері або робочій станції компанії;
- пошкодження наявних даних як результат прояву необережності, халатності у діях користувача.

2. "Електронне" втручання - дії хакерів. До категорії хакерів прийнято відносити людей, активно задіяних в здійсненні комп'ютерних злочинів, як на професійному рівні, так і на рівні простої людської цікавості. До подібних способів дії відносять:

- незаконне проникнення в захищені комп'ютерні мережі;
- здійснення DOS-атак.

Несанкціоноване проникнення ззовні в захищену мережу тієї або іншої компанії може здійснюватися з метою нанесення збитку (знищення, підміна наявних даних), крадіжка інформації, що відноситься до розряду конфіденційною з подальшим її незаконним використанням, розпорядження мережевою інфраструктурою компанії як методом для здійснення атак на інші мережеві вузли, крадіжка грошових коштів з рахунків компанії або окремих користувачів і ін.

Атаки категорії DOS ("Denial of Service") здійснюються ззовні і направлені на мережеві вузли тієї або іншої компанії, які відповідають за її безпечне, ефективне і стабільне функціонування (поштовий, файловий сервер). Зловмисниками організовується масова відправка яких-небудь даних на вибрані вузли, що викликає їх перевантаження, тим самим, виводячи з працездатного стану на деякий час. Подібні атаки можуть обернутися для постраждалої компанії різними порушеннями в здійсненні безперервних бізнес-процесів, втратою клієнтів, а також втратою репутації.

3. Комп'ютерні віруси.

Комп'ютерні віруси, так само, як і деякі інші шкідливі програми відносяться до окремої категорії способів електронної дії з подальшим нанесенням збитку. Дані засоби дії є реальною загрозою для ведення сучасного бізнесу, що має на увазі широке використання комп'ютерних мереж, електронної пошти і Інтернету в цілому. Так, "вдале" проникнення шкідливої програми (вірусу) в корпоративні мережеві вузли тягне за собою не тільки виведенням їх із стану стабільного функціонування, але і велику втрату часу, втрату наявних даних, зокрема не виключена можливість крадіжки конфіденційної інформації і прямих розкрадань грошових коштів з рахунків. Програма-вірус, яка проникла і залишилася непоміченою в корпоративній мережі дає можливість здійснення зловмисниками повного або ж часткового контролю над всією діяльністю компанії, що ведеться в електронному вигляді.

4. Спам.

Якщо ще кілька років тому спам був всього лише незначним по масштабах, дратівливим чинником, то в даний час технології спаму представляють достатньо серйозну загрозу для забезпечення інформаційної безпеки:

- так, основним каналом для ефективного і швидкого розповсюдження спаму і інших шкідливих програм в даний час стала електронна пошта;
- на перегляд спаму йде достатньо велика кількість часу, а подальше видалення численних повідомлень може викликати відчуття дискомфорту співробітників на психологічному рівні;
- спам може виступати одним з основних методів реалізації різних шахрайських схем, жертвами яких можуть ставати як приватні, так і юридичні особи;
- великий ризик видалення потрібної кореспонденції разом із спамом, що може привести до різного роду неприємним наслідкам; при цьому така небезпека зростає, якщо вдаватися до використання недосконалих поштових фільтрів для виявлення і відсіювання спаму.

5. "Природні" загрози.

В категорію "природних" загроз відносять різні зовнішні чинники. Так, причиною втрати інформаційної безпеки може виступити крадіжка інформаційних носіїв, форс-мажорні обставини, неправильний спосіб зберігання інформації і ін.

4. Проблеми забезпечення інформаційної безпеки

Розвиток держави як відкритої соціальної системи неможливий без забезпечення її безпеки в усіх сферах, що відносяться до державної компетенції. Через те важливою особливістю соціальної форми розвитку є якнайтісніший зв'язок та взаємозалежність між розвитком і безпекою як двома сторонами загального процесу функціонування соціальної системи. Нерозривність відносин функції розвитку та безпеки пояснюється, передусім, принциповою єдністю всіх процесів людської діяльності, поділ котрих на окремі сфери, галузі, напрямки є досить умовний. Через це безпека не може бути як відокремлений об'єкт вивчення – вона може бути своєрідним специфічним аспектом вивчення різних сторін стану та розвитку відкритої соціальної системи, якою є держава. Порівняно з розвитком безпека вторинна, однак це зовсім не применшує її ролі та значення в об'єктивній дійсності.

Вагомість функцій безпеки пояснюється тим, що вона активно впливає на формування напрямків і можливі рівні розвитку в тій чи іншій сфері життєдіяльності. Чимало завдань, що їх розв'язує кожна держава у сфері суспільного розвитку та забезпечення належного рівня безпеки, часто близькі та схожі. Крім того, оскільки безпека забезпечується всією сукупною міццю держави, природно, що чим розвинутіша країна загалом, тим більше в неї можливостей для забезпечення своєї безпеки. Тим часом за своєю суттю та

змістом завдання розвитку і забезпечення безпеки зазвичай мають прямо протилежну спрямованість. Розвиток органічно потребує постійного розширення, оновлення, інновацій в різних сферах життя. Безпека ж вимагає стабілізації існуючого становища, обмеження новацій, особливо ризикованих, (що було, напр., продемонстровано у відомий брежнєвський період застою).

Звичайно, абсолютної безпеки, якщо розглядати її як стан відсутності загроз і небезпек, бути не може, оскільки цілком ізолювати державу, суспільство та індивідів від негативного впливу загрозливих чинників та забезпечити їхнє безконфліктне співіснування просто не реально. Однак підвищити ступінь їхньої безпеки до рівня, що гарантує ненасильницький їхній розвиток та виключає можливість заподіяння серйозної шкоди, цілком можливо. Більшість науковців тлумачить термін „безпека” як стан захищеності життєво важливих інтересів держави, суспільства та особистості, передусім, від зовнішніх і внутрішніх загроз. Що таке „життєво важливі інтереси”? Це сукупність потреб, задоволення яких надійно забезпечує існування та можливості прогресивного розвитку держави, суспільства, індивіда. Таке сприйняття поняття “безпека” практично збігається з терміном “національна безпека” (або “державна безпека”).

Взагалі безпека в триаді „державна – суспільство – особистість” – не якесь модне запозичення з арсеналу сучасної політології воно широко вживалося ще в XIX столітті, хоч сьогодні набуло значно ширшого тлумачення. Дійсно, національна безпека – це досить складна багаторівнева функціональна система, в якій безперервно відбуваються процеси взаємодії та протиборства життєво важливих інтересів держави, суспільства та особистості із загрозами цим інтересам – як внутрішніми, так і зовнішніми. Як цільова функція цієї системи виступає міра захищеності цих інтересів від загроз. Щодо поняття “інформаційна безпека”, то воно має двоїстий вимір: з одного боку, це одна зі складових національної безпеки (нарівні з політичною, економічною, військовою та іншими), з іншого – невід’ємний компонент згаданих вище складових.

Зважаючи на міждисциплінарне використання терміну “інформаційна безпека”, в науковому середовищі існує чимало його визначень. Так, лише в нормативних документах і в науковій літературі їх налічується кілька десятків. Так, норма ч.І ст.17 Конституції України встановлює, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу». В даному контексті інформаційна безпека розглядається на одному рівні з такими невід’ємними атрибутами державності, як суверенітет і територіальна цілісність. Хоча потрібно зазначити, що ці явища не є однопорядковими. Всі аспекти національної безпеки, в тому числі і інформаційна, ґрунтуються на такому явищі, як державний суверенітет.

Саме державний суверенітет, «політико – юридична властивість державної влади, яка означає її верховенство та повноту всередині країни, незалежність і рівноправність ззовні», надає можливість та права відповідним органам державної влади здійснювати конкретні заходи щодо захисту

інформаційної безпеки. Декларація про державний суверенітет України визначає державний суверенітет України як «верховенство, самостійність, повноту і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах».

Оскільки йдеться про інформаційну безпеку як складову національної безпеки, то її джерелом потрібно вважати не лише суверенітет держави, а й суверенітет народу та нації як суб'єктів інформаційних відносин. Аналіз проблеми інформаційної безпеки неодмінно ставить питання, яке багато в чому є ключовим: чи існує окремий вид суверенітету - інформаційний? У Законі України «Про інформацію» така дефініція є, але чіткого тлумачення її змісту немає. Так, ст.53 цього закону «Інформаційний суверенітет» хоча і встановлює, що «основою інформаційного суверенітету України є національні інформаційні ресурси», але змісту самого поняття інформаційного суверенітету не розкриває. До інформаційних ресурсів України, згідно з нормами ст. 53 Закону «Про інформацію», входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Таким чином, у рамках Закону «Про інформацію» інформаційний суверенітет переважно розглядається як невід'ємне право держави формувати та розпоряджатися інформаційними ресурсами, які перебувають в її власності відповідно до національного та міжнародного законодавства. Але варто зазначити, що в такому випадку мова йде не про суверенітет, а про реалізацію права власності держави на певні види майна та майнових прав. Але ми маємо підстави говорити про тенденцію в законотворчій діяльності, спрямовану на визнання існування такого специфічного явища, як інформаційний суверенітет. Ще в 1999 р. постановою Верховної Ради України «Про проект закону України про інформаційний суверенітет і інформаційну безпеку України» Комітету Верховної Ради України з питань свободи слова та інформації запропоновано доопрацювати проект Закону України про інформаційний суверенітет.

На сьогоднішній день до Верховної Ради внесено цілий ряд проектів Закону про інформаційний суверенітет та інформаційну безпеку, які мають певні відмінності в підходах до розгляду проблеми інформаційного суверенітету. Ясна річ, у нормативно - правовому акті, який буде прийнято, цілком можуть бути використані зовсім інші погляди, але, на нашу думку, ці проекти являють цінність для аналізу самої проблеми та визначення існуючих сучасних підходів до її вирішення. Важливим міжнародно-правовим актом, що визначив баланс особистих прав та компетенції держави в сфері інформаційних відносин, є Європейська конвенція про захист прав і основних свобод людини. Стаття 10 цієї конвенції закріплює право людини на свободу виявлення поглядів, що, зокрема, включає свободу дотримуватися своїх поглядів, одержувати і поширювати інформацію та ідеї без втручання держави і незалежно від кордонів. Однак разом з тим нормами цієї статті визначається значний обсяг компетенції держави щодо регулювання інформаційних правовідносин.

До компетенції держави, зокрема, віднесено право вимагати ліцензування радіомовлення, телебачення або кінопідприємств (ч.1 ст.10). Крім того, підкреслюється, що здійснення інформаційних свобод людини пов'язане з правами та обов'язками і тому може бути предметом встановлених законом формальностей, умов, обмежень і покарань. Згідно з ч.2 ст.10 названої конвенції подібні законодавчі обмеження і покарання є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням або злочинам, для захисту здоров'я і моралі, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Водночас ч.2. ст.10 цієї конвенції прямо вказує ще на одну важливу рису діяльності держави по регулюванню інформаційних відносин, а саме те, що в демократичному суспільстві прийнятне лише регулювання порядку реалізації людиною своїх інформаційних прав і свобод шляхом встановлення відповідних правових норм, а не шляхом забезпечення державної власності на основні інформаційні ресурси або проведенням єдиної інформаційної політики, оскільки останні випадки вже межують з неправомірним обмеженням з боку держави принципу свободи інформації.