Методи захисту інформації в телекомунікаційних системах

Лекція № 2

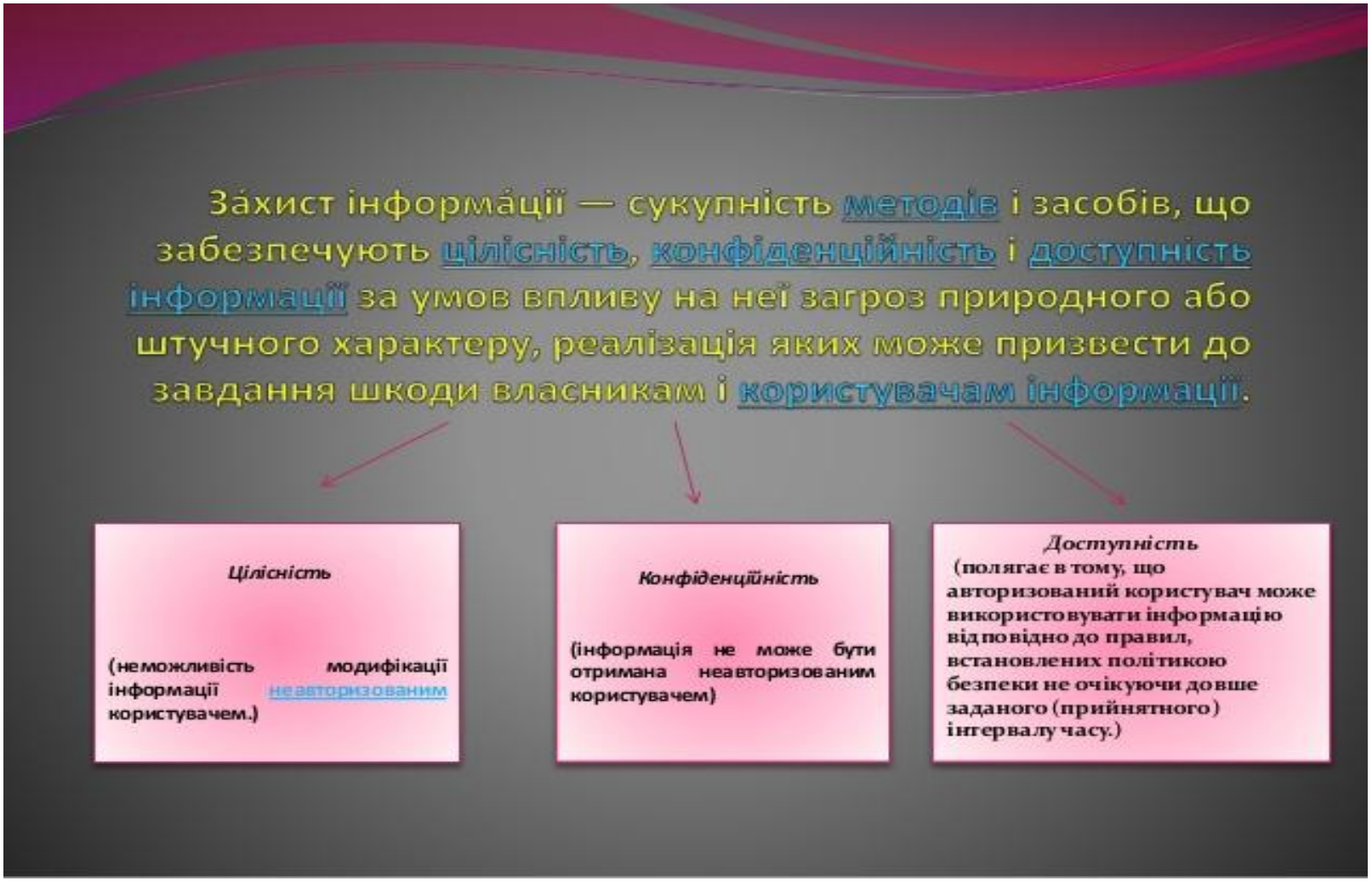
Доцент, к.т.н. Золотарьов Вадим Анатолійович

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

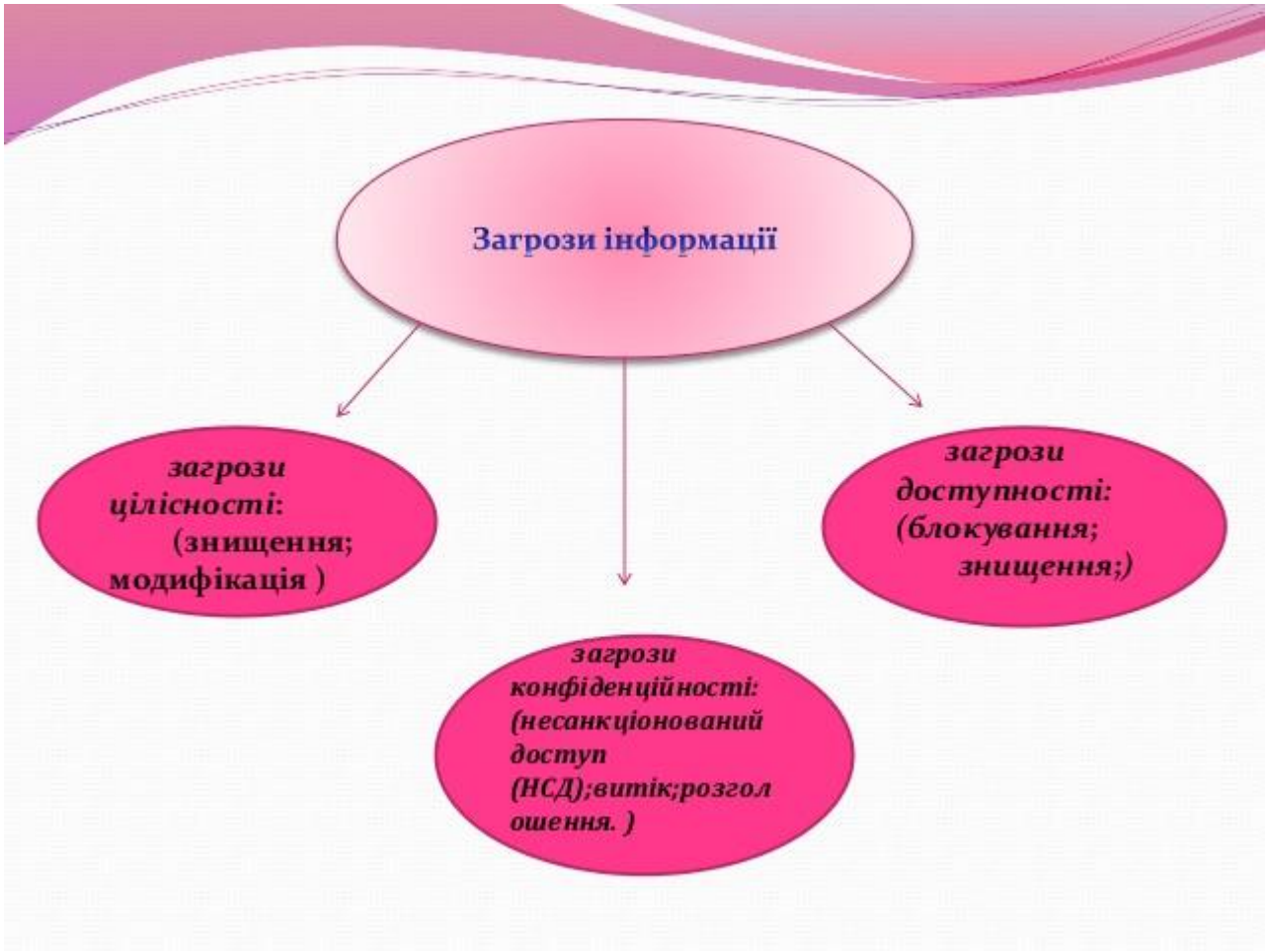
Питання 2.1

КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua



ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua


Загрози інформації
загрози цілісності: (знищення; модифікація)
загрози конфіденційності: (несанкціонований доступ (НСД);витік;розголошення.)
загрози доступності: (блокування; знищення;)

Базова тріада інформаційної безпеки CIA-triad [ЦРУ, 1980]

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Конфіденційність (Confidentiality)

- Таємність інформації як властивість бути доступною тільки певній авторизова

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Цілісність (Integrity)

- Під цілісністю інформації розуміють її правильність, повноту та вичерпаність

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Доступність (Availability)

- Властивість інформації бути щомиті доступною та наданою у повне розпорядження певній авторизованій осс

Гексада (шістка) інформаційної безпеки - Parkerian Hexad 2002

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Передбачуваність, авторизація Possession

- Можна гарантовано стверджувати, що певні операції та заходи можуть бути однозначно присвоєні, підпорядковані чи належати певній особі

Корисність (Utility)

- Дані повинні бути використовуваними (корисними), а не такими, що зашифровані та не можуть бути розшифровані через відсутність ключа

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Автентифікація, довіра (Autentificity)

- Означає достовірність (автентичність) інформації, або особи інформаційного обміну

Питання 2.2

ОСНОВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Складові інформаційної безпеки

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

«Піраміда» організації системи захисту інформації в сучасних ІТКС

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Види захисту інформації

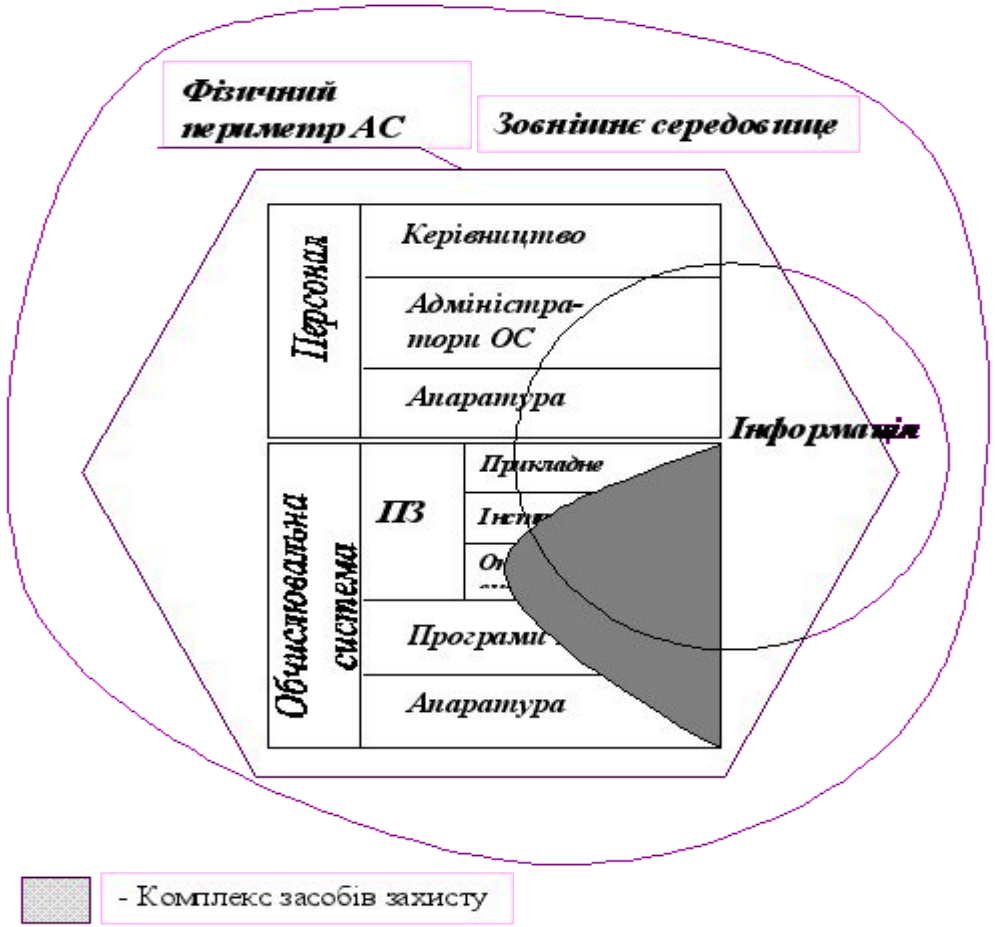
Технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, смарт-карти тощо)

Інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

Криптографічний — попереджує доступ за допомогою математичних перетворень повідомлення (ІП)

Організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

Комплекс захисту інформації в інформаційно-телекомунікаційній системі



ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Питання 2.3

НОРМАТИВНО-ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЇ

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Нормативно-правовий захист інформації

- Фундамент побудови всієї інформаційної безпеки підприємства, організації, установи.
- *Право* – це сукупність установлених чи санкціонованих державою загальнообов'язкових правил поведінки (норм), дотримання яких забезпечується методами державного впливу.
- Правовий елемент інформаційного захисту складають законодавчі засоби захисту інформації, які є множиною нормативно-правових актів (конвенції, закони, укази, постанови, нормативні документи тощо), що діють у державі і забезпечують юридичну підтримку для розв'язання задач захисту інформації.

Нормативна база інформаційної безпеки

- Регулює взаємовідносини між суб'єктами інформаційної безпеки
- Нормативно забезпечує дії суб'єктів інформаційної безпеки на всіх рівнях
- Встановлює застосування різних методів і засобів забезпечення інформаційної безпеки

Розвиток законодавчої бази в області інформаційної безпеки йде по п'ятьох основних напрямах:

- захист відомостей, що складають державну таємницю;
- захист конфіденційної інформації;
- захист авторського права у сфері інформатизації;
- захист права на доступ до інформації
- Захист персональних даних

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Види інформації за режимом доступу

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Закони України про захист інформації (dstszi.gov.ua)

- "Про Державну службу спеціального зв'язку та захисту інформації України"
- "Про захист інформації в інформаційно-телекомунікаційних системах"
- "Про Національну систему конфіденційного зв'язку"
- "Про інформацію"
- "Про телекомунікації"
- "Про радіочастотний ресурс України"

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Закони України про захист інформації

- "Про Дисциплінарний статут Державної служби спеціального зв'язку та захисту інформації України"
- "Про державну таємницю"
- "Про ліцензування певних видів господарської діяльності"
- "Про електронні документи та електронний документообіг"
- "Про наукову і науково-технічну експертизу"
- "Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання"
- "Про ратифікацію Статуту і Конвенції міжнародного союзу електрозв'язку"
- «Про електронний цифровий підпис», від 22.05.2003 № 852-IV
- «Про електроні документи та електронний документообіг», від 22.05.2003 № 851-IV
- «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», від 05.04.2007 № 877-V

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Закони України про захист інформації

- «Про інформацію», від 02.10.1992 № 2657-XII
- «Про захист персональних даних», від 01.06.2010 № 2297-VI
- «Про доступ до публічної інформації», від 13.01.2011 № 2939-VI
- «Про захист інформації в інформаційно-телекомунікаційних системах», від 05.07.1994 № 80/94-ВР

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Укази Президента України про захист інформації

- від 22.05.1998 № 505 "Про Положення про порядок здійснення криптографічного захисту інформації в Україні«
- від 27.09.1999 № 1229 "Про Положення про технічний захист інформації в Україні"

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Державні стандарти України в галузі захисту інформації

- Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96
- Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Закон України «Про інформацію»

- регулює відносини щодо створення, збирання,
одержання, зберігання, використання, поширення, охорони, захисту інформації.

З А К О Н У К Р А Ї Н И
“|Про інформацію”

{ Вводиться в дію Постановою ВР N 2658-XII (2658-12) від 02.10.92, ВВР, 1992, N 48, ст.651 }

Даний Закон закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності.

Грунтуючись на Декларації про державний суверенітет України та Акті проголошення її незалежності, Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації.

http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

З А К О Н У К Р А Ї Н И
Про державну таємницю

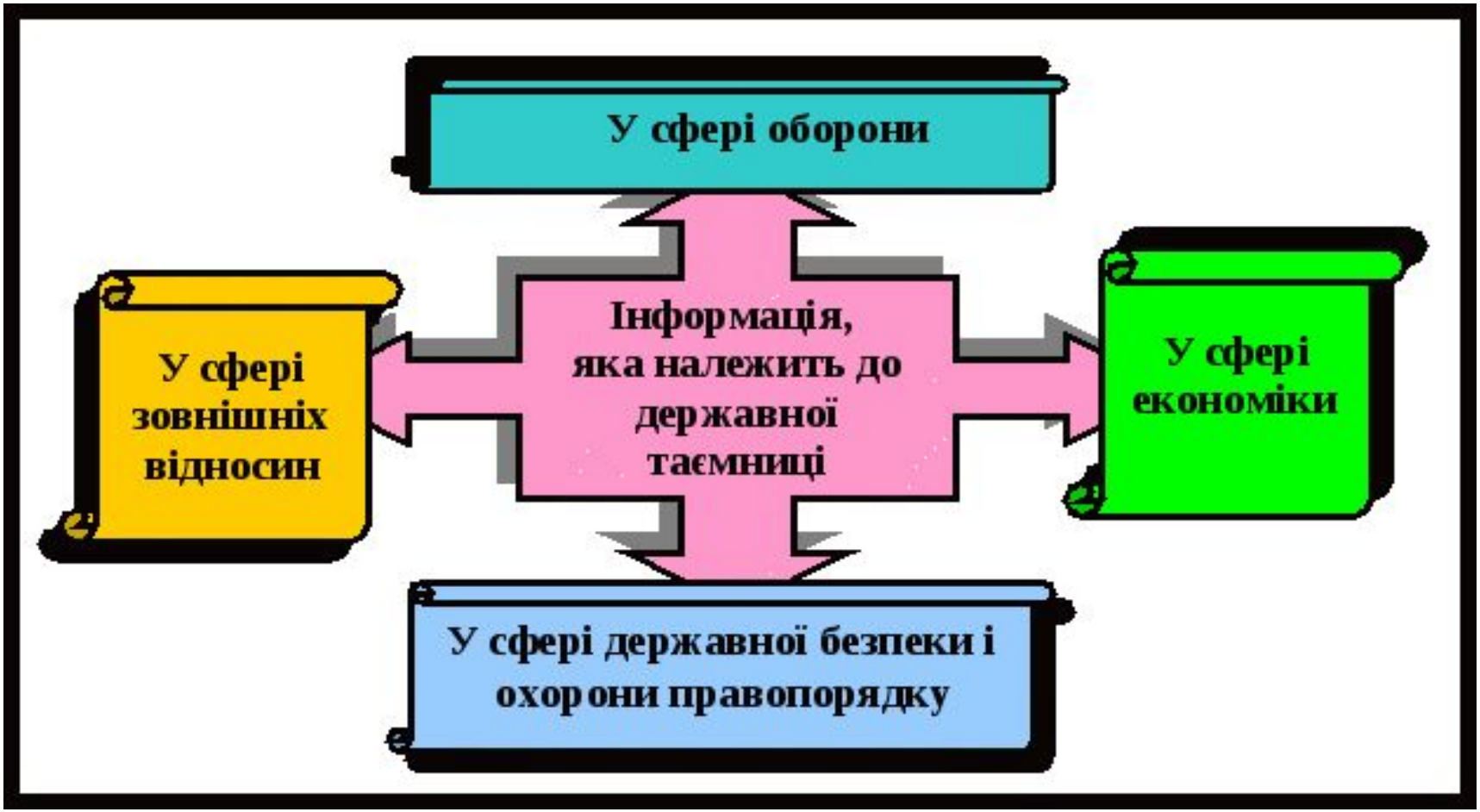
- регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

державна таємниця (секретна інформація)

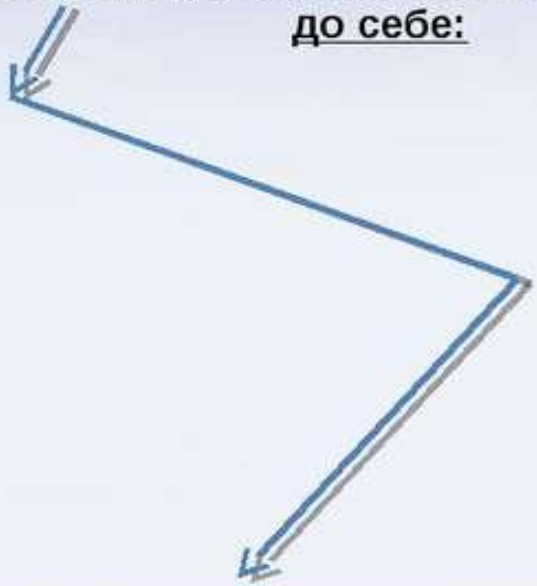
- вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою

Інформація, яка належить до державної таємниці



ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Охорона державної таємниці включає до себе:



комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативних заходів, спрямованих на запобігання розголошенню інформації, що становить державну таємницю.

віднесення інформації до державної таємниці

- процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього;

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

гриф секретності

- реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Допуск до державної таємниці

- оформлення права громадянина на доступ до секретної інформації

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

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, в якому зведено переліки відомостей, що згідно з рішеннями державних
експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах;

Приклад допуску до державної таємниці

Р О З П О Р Я Д Ж Е Н Н Я
ПРЕЗИДЕНТА УКРАЇНИ

Про надання громадянці Грузії Гонгадзе О.Т.
доступу до державної таємниці

Відповідно до статті 27 Закону України "Про державну таємницю" (3855-12) на підставі пропозиції Ради національної безпеки і оборони України:
Надати громадянці Грузії ГОНГАДЗЕ Олександрі Теодорівні доступ до інформації, яка міститься у матеріалах кримінальної справи по факту вбивства Гонгадзе Георгія Руслановича і віднесена до державної таємниці за висновком державного експерта з питань таємниць В. Євдокимова від 6 березня 2006 року N 340.

Президент України В.ЮЩЕНКО
м. Київ, 3 [illegible]вня 2006 року
N 64/2006-рп

RPDIPPP

категорія режиму секретності

- категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

матеріальні носії секретної інформації

- матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

охорона державної таємниці

- комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальни

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

режим секретності

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

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

розсекречування матеріальних носіїв секретної інформації

- зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

ступінь секретності ("особливої важливості", "цілком таємно", "таємно")

- категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

Інформація, що може бути віднесена до державної таємниці

- про систему урядового та спеціального зв'язку;
- про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;
- про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;
- про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;
- про організацію, зміст, стан і плани розвитку технічного
  захисту секретної інформації;

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Не відноситься до державної таємниці інформація:

- про стан довкілля, про якість харчових продуктів і предметів побуту, про вплив товару (роботи, послуги) на життя та здоров’я людини;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан
правопорядку, освіти і культури населення;
- про факти порушень прав і свобод людини і громадянина; про незаконні дії державних органів, органів місцевого самоврядування та їх посадових і службових осіб;
- інша інформація, доступ до якої відповідно до законів та міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, не може бути обмежено.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Форми допуску до державної таємниці:

- форма 1 - для роботи з секретною інформацією, що має ступені секретності "особливої важливості", "цілком таємно" та "таємно";
- форма 2 - для роботи з секретною інформацією, що має ступені секретності "цілком таємно" та "таємно";
- форма 3 - для роботи з секретною інформацією, що має ступінь секретності "таємно",

Форми допуску до таємної інформації

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Службовою інформацією є інформація, що міститься в:

- документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію;
- доповідних записках;
- рекомендаціях якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;
- інформація, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

- виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;
- розголошення інформації може завдати істотної шкоди цим інтересам;
- шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Нормативно-правове регулювання комерційної таємниці в Україні здійснюється Цивільним кодексом України від 16 січня 2003 р.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

У статті 505 «Поняття комерційної таємниці» якого закріплено

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

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

У статті 505 Цивільного кодексу

- «комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці»

Згідно до постанови Кабінету Міністрів України від 09 серпня 1993 року № 611 «Про перелік відомостей, що не становлять комерційної таємниці»

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;
- документи про сплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, що відповідно до чинного законодавства підлягають оголошенню.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

відомості, які можуть бути віднесені до комерційної таємниці, наприклад, підприємства, повинні мати наступні ознаки

- не містити державної таємниці;
- не наносити шкоди інтересам суспільства;
- відноситись до виробничої діяльності підприємства;
- мати дієву або потенційну комерційну цінність та створювати переваги в конкурентній боротьбі;
- мати обмеження в доступі тощо


Заходи по забезпеченню конфіденційності комерційної таємниці
Внутрішні
Зовнішні
Правові
1. Прийняття положення по забезпеченню цілісності КТ
2. Укладання договорів про повну матеріальну відповідальність.
3. Прийом розписок про нерозголошення КТ і попередження про відповідальність за розголошення таємниці.
4. Включення положень про КТ в комерційні угоди .
1.Створення спец. режиму секретних підрозділів
2.Розробка дозволяючої системи доступу до інформації.
3.Введення відповідної маркіровки документів та ін. носіїв інформації.
4.Організація секретного діловодства.
5.Призначення відповідального за збереження конфіденційності.
Технічні
1.Виявлення можливих джерел витоку інформації.
2.Придбання і монтаж спеціалізованої апаратури і програмних продуктів для захисту інформації.
3.Проведення регулярних оперативних заходів по технічному захисту і пошуку каналів витоку інформації.
Психологічні
1.Проведення роз'яснювальної роботи з персоналом, партнерами і клієнтами.
2.Створення сприятливої атмосфери в колективі.
3.Проведення регулярних перевірок (гласних і негласних) з виявлення не надійних осіб.

Закон України

Про телекомунікації

2004 р.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Закон України «Про телекомунікації»

- Встановлює правову основу діяльності у сфері телекомунікацій.
- Закон 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.

Закон України “Про телекомунікації” визначає, що

- інформаційна безпека телекомунікаційних мереж - здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Закон України “Про телекомунікації” визначає, що

- сталість телекомунікаційної мережі - властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників;

ЗУ "Про телекомунікації" стаття 9.

Охорона таємниці телефонних розмов, телеграфної та іншої кореспонденції, безпека телекомунікацій

1. Охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією) та законами України.
2. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом.
3. 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.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 34. Захист інформації про споживача

- 1. 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.

Стаття 34. Захист інформації про споживача

- 2. 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.

Стаття 34. Захист інформації про споживача

3. Інформація про споживача та про телекомунікаційні послуги, що він отримав, може надаватись у випадках і в порядку, визначених законом. В інших випадках зазначена інформація може поширюватися
лише за наявності письмової згоди споживача.

Стаття 39. Обов'язки операторів і провайдерів телекомунікацій

1. Оператори телекомунікацій зобов'язані:

… 17) вживати заходів для недопущення несанкціонованого доступу до телекомунікаційних мереж та інформації, що передається цими мережами;

Стаття 39. Обов'язки операторів і провайдерів телекомунікацій

. Оператори телекомунікацій зобов’язані за власні кошти
встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення.
Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

З А К О Н У К Р А Ї Н И
“Про захист інформації в інформаційно-телекомунікаційних системах”

(Відомості Верховної Ради (ВВР), 1994, № 31, ст.286)

(Вводиться в дію Постановою ВР № 81/94-ВР від 05.07.94, ВВР, 1994, № 31, ст.287)

Метою цього Закону є встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації.

Дія Закону поширюється на будь-яку інформацію, що обробляється в автоматизованих системах.

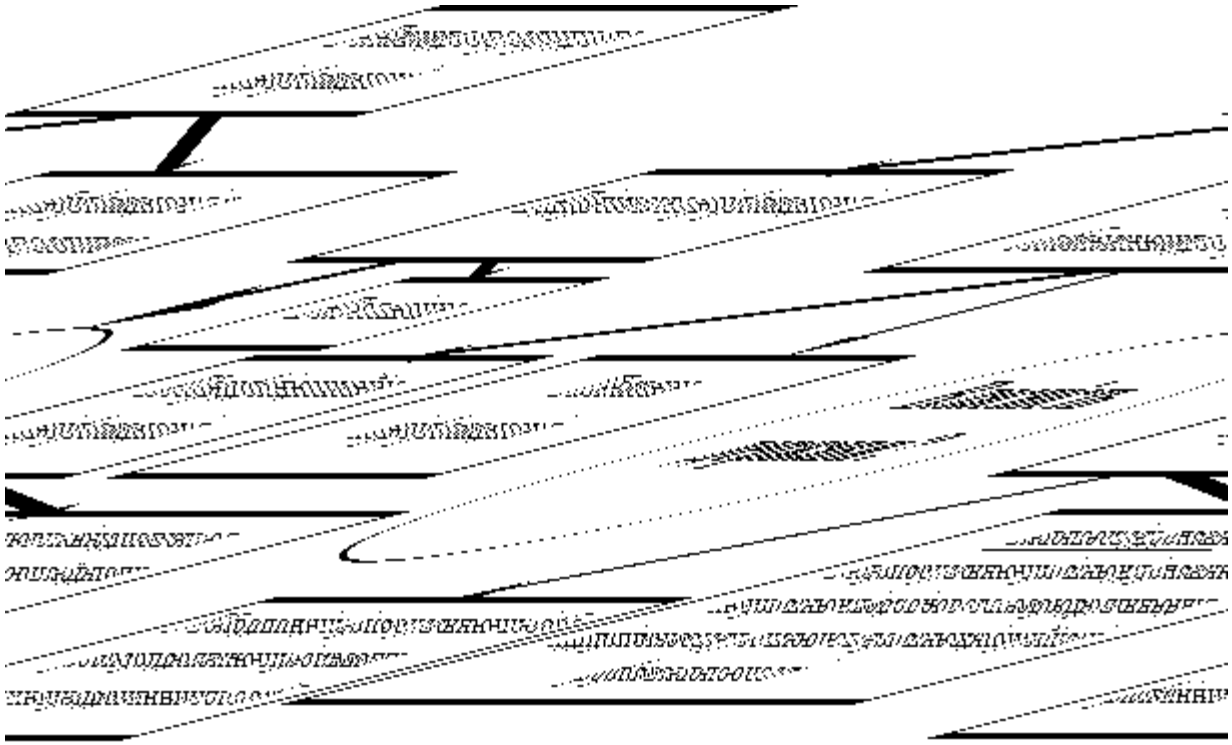
http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Інформація з обмеженим доступом

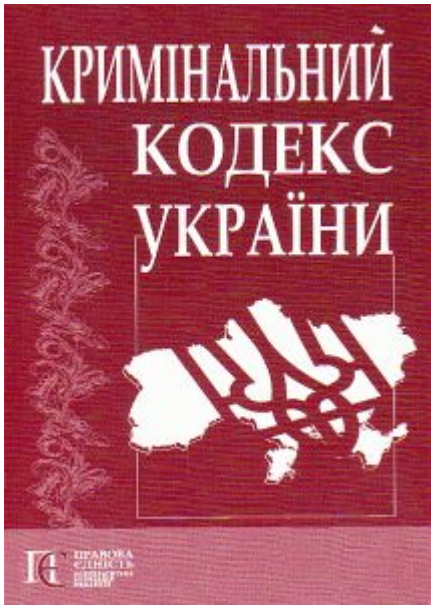
ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Класифікація інформації з обмеженим доступом



ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

2.2 Кримінальний кодекс України про захист інформації



ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 111. Державна зрада

1. Державна зрада, тобто діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в умовах воєнного стану або в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України, - карається позбавленням волі на строк від десяти до п'ятнадцяти років.

2. Звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їх представників ніяких дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 114. Шпигунство

1. Передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або
особою без громадянства, -
караються позбавленням волі на строк від восьми до п'ятнадцяти років.
2. Звільняється від кримінальної відповідальності особа, яка припинила діяльність, передбачену частиною першою цієї статті, та
добровільно повідомила органи державної влади про вчинене, якщо
внаслідок цього і вжитих заходів було відвернено заподіяння шкоди
інтересам України.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції,що передаються засобами зв'язку або через комп'ютер

1. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами
зв'язку або через комп'ютер, -
караються штрафом від п'ятдесяти до ста неоподатковуваних
мінімумів доходів громадян або виправними роботами на строк до
двох років, або обмеженням волі до трьох років.
2. Ті самі дії, вчинені щодо державних чи громадських діячів
або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації, -
караються позбавленням волі на строк від трьох до семи років.

Стаття 176. Порушення авторського права і суміжних прав

1. Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, а так само незаконне відтворення, розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, або інше умисне порушення авторського права і суміжних прав, якщо це завдало матеріальної шкоди у значному розмірі, -
караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.
2. Ті самі дії, якщо вони вчинені повторно, або за попередньою змовою групою осіб, або завдали матеріальної шкоди у великому розмірі, - караються штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п'яти
років, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.
3. Дії, передбачені частинами першою або другою цієї статті, вчинені службовою особою з використанням службового становища або організованою групою, або якщо вони завдали матеріальної шкоди в особливо великому розмірі, - караються штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого та з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувалися для їх виготовлення.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 182. Порушення недоторканності приватного життя

Незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації, -

караються штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років,

або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

ХНУРЕ, факультет ІПК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 200. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення

1. Підробка документів на переказ, платіжних карток чи інших
засобів доступу до банківських рахунків, а так само придбання,
зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ чи платіжних карток або їх використання чи збут -
карається штрафом від п'ятисот до тисячі неоподатковуваних
мінімумів доходів громадян або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою
групою осіб, -
караються позбавленням волі на строк від двох до п'яти років.

Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю

Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, -
караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 232. Розголошення комерційної або банківської таємниці

Умисне розголошення комерційної або банківської таємниці без
згоди її власника особою, якій ця таємниця відома у зв'язку з
професійною або службовою діяльністю, якщо воно вчинене з
корисливих чи інших особистих мотивів і завдало істотної шкоди
суб'єкту господарської діяльності, -
карається штрафом від двохсот до п'ятисот неоподатковуваних
мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 232-1. Незаконне використання інсайдерської інформації

- Умисне незаконне розголошення, передача або надання доступу до інсайдерської інформації, а так само надання з використанням такої інформації рекомендацій стосовно придбання або відчуження цінних паперів чи похідних (деривативів), якщо це призвело до отримання особою, яка вчинила зазначені дії, чи третіми особами необґрунтованого прибутку в значному розмірі, або уникнення учасником фондового ринку чи третіми особами значних збитків, або якщо це заподіяло значну шкоду охоронюваним законом правам, свободам та інтересам окремих громадян або державним чи громадським інтересам, або інтересам юридичних осіб, - караються штрафом від семисот п'ятдесяти до двох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років або без такого.

Стаття 328. Розголошення державної таємниці

1. Розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства - карається позбавленням волі на строк від двох до п'яти років
з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.
2. Те саме діяння, якщо воно спричинило тяжкі наслідки, - карається позбавленням волі на строк від п'яти до восьми років.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 329. Втрата документів, що містять державну таємницю

1. Втрата документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони
були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації
або предметами, -
карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.
2. Те саме діяння, якщо воно спричинило тяжкі наслідки, -
карається позбавленням волі на строк від двох до п'яти років.

Стаття 330. Передача або збирання відомостей, що становлять конфіденційну інформацію,яка знаходиться у володінні держави

1. Передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам економічних, науково-технічних або інших відомостей, що становлять
конфіденційну інформацію, яка знаходиться у володінні держави, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної
зради або шпигунства, -
караються обмеженням волі на строк до трьох років або позбавленням волі на строк від двох до п'яти років, з позбавленням
права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.
2. Ті самі дії, вчинені з корисливих мотивів, або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб, -
караються позбавленням волі на строк від чотирьох до восьми років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

Стаття 359. Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації

1. Незаконне придбання або збут спеціальних технічних засобів негласного отримання інформації, а також незаконне їх використання -
караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк.
2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, -
караються позбавленням волі на строк від чотирьох до семи років.
3. Дії, передбачені частиною першою або другою цієї статті, вчинені організованою групою або якщо вони заподіяли істотну шкоду
охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, -
караються позбавленням волі на строк від семи до десяти років}

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 360. Умисне пошкодження ліній зв'язку

Умисне пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, якщо воно спричинило тимчасове припинення зв'язку, -
карається штрафом від ста до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до одного року, або обмеженням волі на строк до двох років.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. 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, - карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.
2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади 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.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.
2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 361-2. 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

1. 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.
2. 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. 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

1. Несанкціоновані зміна, 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, - караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за
допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.
2. 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.
3. Дії, передбачені частиною першою або другою цієї статті, 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 а ися певною
діяльніс до трьох р ків та з конфіскацією програмних або технічних засобів, за допомог у здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Стаття 363. 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

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.

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів),
автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового
розповсюдження повідомлень електрозв'язку

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -
карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох
років.
2. 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.

Захист інформації в управлінні персоналом та економіці праці

Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI (*далі* — Закон № 2297) набув чинності 1 січня 2011 року.

Цей Закон регулює відносини, пов'язані із захистом персональних даних фізичних осіб під час їх обробки.

Дія Закону не поширюється на діяльність зі створення баз персональних даних (БПД) та обробки персональних даних у цих базах:

– фізичною особою — виключно для непрофесійних особистих чи побутових потреб;

– журналістом — у зв'язку з виконанням ним службових чи професійних обов'язків;

– професійним творчим працівником — для здійснення творчої діяльності.

СУБ'ЄКТИ, СТОСОВНО ЯКИХ ЗДІЙСНЮЄТЬСЯ ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ **такими суб'єктами є:**

– громадяни;

– наймані працівники;

– посадові особи;

– платники податків та зборів;

– клієнти;

– абоненти;

– пацієнти;

– пасажири,

– суб'єкти відносин у сфері страхування;

– суб'єкти фінансових відносин;

– суб'єкти відносин у сфері реклами,

– члени політичних партій / громадських / релігійних організацій;

– вихованці закладів освіти (учні, студенти, абітурієнти, курсанти, слухачі, випускники та інші);

– інші фізичні особи, які подають власні персональні дані при реалізації своїх прав чи обов'язків.

ПЕРСОНАЛЬНІ ДАНІ, ЩО ОБРОБЛЯЮТЬСЯ

- ідентифікаційні дані (ім'я, адреса, телефон тощо);
- паспортні дані;
- особисті відомості (вік, стать, сімейний стан тощо);
- склад сім'ї;
- освіта;
- професія, спеціальність, кваліфікація;
- біометричні дані (зріст, вага, особливі прикмети тощо);
- психологічні дані (особистість, характер тощо);
- житлові умови; спосіб життя, життєві інтереси та захоплення;
- споживчі звички;
- фінансова інформація;
- електронні ідентифікаційні дані (трафік, IP-адреса тощо);
- електронні дані про локалізацію (GSM, GPS тощо);
- запис зображень (фото, відео);
- звукозапис;
- інші персональні дані.

БАЗА ПЕРСОНАЛЬНИХ ДАНИХ

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

Таким чином, відомості про працівників, відображені в кадрових документах, зокрема про вік, дату і місце народження, місце проживання, ідентифікаційний номер, соціальний статус, пільги відповідно до закону (одинокі матері, жінки з дітьми віком до трьох років чи іншого віку дітей, «чорнобильці», неповнолітні, пенсіонери тощо) з точки зору Закону № 2297 вважаються персональними даними, які у своїй сукупності складають БПД або її частину.

«ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Я, _____,
(прізвище, ім'я та по батькові)
що народився/лась «___» _____ 19__ року, паспорт серії ____ № _____, виданий «___» _____ ___ року РВ УМВС України в _____, шляхом підписання цього тексту, відповідно до Закону України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, надаю Товариству з обмеженою відповідальністю «Мрія» згоду на збір та обробку моїх особистих персональних даних у картотеках та/або за допомогою інформаційно-телекомунікаційної системи бази персональних даних «Персонал» з метою ведення кадрового діловодства, підготовки відповідно до вимог законодавства статистичної, адміністративної та іншої звітної інформації з питань персоналу, а також внутрішніх документів підприємства з питань реалізації визначених законодавством України, статутом, колективним договором та іншими нормативними документами ТОВ «Мрія» прав та обов'язків працівника і роботодавця у сфері трудових правовідносин та соціального захисту.
Обсяг моїх персональних даних, які оброблятимуться в базі персональних даних «Персонал», визначається підприємством відповідно до вимог законодавства України або за погодженням зі мною у разі необхідності обробки додаткової інформації, подання якої працівником роботодавцю не передбачено законодавством України.
Передача моїх персональних даних третім особам здійснюється підприємством лише у випадках, передбачених законодавством України.
Передача моїх персональних даних третім особам у випадках, не передбачених законодавством України, здійснюється лише за моєю згодою.
Зобов'язуюсь при зміні моїх персональних даних, якими є: паспортні дані, у т. ч. громадянство, особисті відомості (родинний стан, склад сім'ї, номери телефонів тощо), місце проживання фактичне та за державною реєстрацією, освіта, професія, спеціальність, кваліфікація, відомості про військовий облік, дані про стан здоров'я в межах, визначених законодавством про працю, дані, що підтверджують право працівника на встановлені законодавством пільги, дані про житлові умови, у разі перебування мене на квартирному обліку підприємства, надавати у найкоротший термін відповідальній особі кадрового підрозділу *(Управлінню кадрів, Департаменту по роботі з персоналом, менеджеру з персоналу тощо)* та/або бухгалтерії підприємства уточнену інформацію та подавати оригінали відповідних документів для внесення моїх нових особистих даних до бази персональних даних «Персонал».

«__» _____ ____ року _____ (_____)».
(підпис) (прізвище та ініціали)
Відповідальна особа кадрового підрозділу перевіряє правильність та достовірність заповнення працівником згоди на збір та обробку персональних даних і посвідчує її написом нижченаведеного змісту та печаткою кадрового підрозділу:
«Особу та підпис _____,
(прізвище, ім'я та по батькові працівника)
достовірність заповнення інформації, зазначеної у згоді на збір та обробку персональних даних, перевірено.
Відповідальна особа: _____ _____ (_____)
(посада) (підпис) (прізвище та ініціали)
М. П.»

Домашнє завдання

- Зайти на сайт Державної служби зв'язку та захисту інформації України
- В «Розширеному пошуку» обрати «Нормативно-правова база»
- Проробити наступні Закони України про захист інформації
- Проробити проект «Концепції інформаційної безпеки України»

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua