МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

**ДОНЕЦЬКИЙ ЮРИДИЧНИЙ ІНСТИТУТ
ЛУГАНСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ
ВНУТРІШНІХ СПРАВ**

Т.В. ФІЛІПЕНКО

В.В. КАЛАЙДА

ІНФОРМАЦІЙНА БЕЗПЕКА

НАУКОВО-ПРАКТИЧНИЙ ПОСІБНИК

Донецьк - 2007 р.

УДК: 351.746:007(075.8)
ББК: 676.404.3я7
Ф 53/К 17

Рекомендовано до друку вченою радою Донецького юридичного інституту Луганського державного університету внутрішніх справ (протокол № 6 від 29 червня 2006 р.)

Філіпенко Т.В., Калайда В.В.
Інформаційна безпека: науково-практичний посібник. – Донецьк: ДЮІ ЛДУВС, 2007. – 168 с.

Рецензенти:

Рижков Е.В. – кандидат юридичних наук, доцент, начальник кафедри оперативно-розшукової діяльності Донецького юридичного інституту Луганського державного університету внутрішніх справ
Ткаченко О.Г. – кандидат економічних наук, доцент кафедри менеджменту зовнішньоекономічної діяльності Донецького державного університету управління.
Костюченко О.П. – начальник відділу фінансових ресурсів та економіки Донецького юридичного інституту Луганського державного університету внутрішніх справ

У науково-практичному посібнику розглянуто поняття та види інформації, складові інформаційної безпеки та засоби її забезпечення.

Науково-практичний посібник призначено для викладачів, ад'юнктів, аспірантів, курсантів, студентів, працівників підприємницьких структур і органів контролю, а також усіх тих, хто цікавиться питаннями інформаційної безпеки.

В научно-практическом пособии рассмотрены понятие и виды информации, составляющие информационной безопасности и способы ее обеспечения.

Научно-практическое пособие предназначено для преподавателей, адъюнктов, аспирантов, курсантов, студентов, работников предпринимательских структур и органов контроля, а также всех тех, кто интересуется вопросами информационной безопасности.

ISBN 978-966-8950-24-5

ЗМІСТ

Вступ

Швидкий розвиток процесів автоматизації, проникнення комп'ютерів в усі сфери сучасного життя спричинили, крім безсумнівних переваг, появу цілого ряду специфічних проблем. Однією з таких проблем стала необхідність забезпечення ефективного захисту інформації та засобів її обробки.

Безліч способів доступу до інформації, значна кількість кваліфікованих фахівців, широке використання в суспільному виробництві спеціальних технічних засобів дозволяють зловмиснику практично в будь-який момент і в будь-якому місці здійснювати дії, що представляють загрозу інформаційній безпеці як у локальному, так і в глобальному масштабах. У наш час людство переживає бурхливий розвиток комп'ютеризації всіх сфер життя. Це надає нові можливості розвитку національних економік. Поширення інформаційних технологій має і свій негативний аспект: це відкриває шлях до антисоціальної та злочинної поведінки. Комп'ютерні системи містять в собі нові, та дуже досконалі можливості для невідомих раніше правопорушень, а також для вчинення традиційних злочинів, але нетрадиційними засобами.

Крім того, що комп'ютерні злочини наносять великі економічні збитки, суспільство стає більш залежним від роботи комп'ютеризованих систем у різноманітних сферах суспільного життя – від керування рухом літаків і поїздів до медичного обслуговування та національної безпеки. Іноді, навіть невеличкий збій у функціонуванні таких систем може призвести до реальної загрози життю людей. Стрімке зростання глобальних комп'ютерних мереж, а також можливість підключення до них через звичайні телефонні лінії посилюють можливості їх використання для кримінальної діяльності.

У порівнянні з іншими країнами, національна безпека України поки що залежить від комп'ютерних мереж значно менше. На сьогодні, в Україні стикаються з комп'ютерними злочинами, в основному, у фінансово-кредитній сфері. Але у недалекому майбутньому такі злочини можуть призвести до глобальних катастроф – екологічних, транспортних тощо. Введення сучасної

системи управління повітряним рухом, поширення телекомунікаційної мережі, впровадження системи електронних платежів, використання комп'ютерів у діяльності правоохоронних органів та керуванні військами значно розширили сферу діяльності зловмисників.

Рішення проблеми забезпечення інформаційної безпеки припускає комплекс заходів держави, таких як розробка системи класифікації, документування інформації та способів захисту, регулювання доступу до даних, встановлення відповідальності за порушення інформаційної безпеки.

Підготовлений науково практичний посібник спрямований на:

- одержання базових знань з інформаційної безпеки з метою подальшого їх використання в процесі здійснення професійної діяльності;
- придбання практичних навичок по використанню цих знань у процесі повсякденної праці на підприємстві та в ОВС (перш за все при виявленні, попередженні, документуванні та розкритті злочинів в сфері інформаційних технологій).

1. Основні положення інформаційної безпеки

Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної й інших складових національної безпеки України. Фахівці в області інформаційних технологій єдині в думці, що, як у свій час досягнення ядерної фізики викликали небезпеку ядерної війни, так і поширення інформатизації (комп'ютеризації) стало джерелом дуже широкого кола загроз суспільству, державі й людині.

Важливим системоутворюючим поняттям в сфері міжнародного інформаційного співробітництва є «інформаційна безпека», яка є складовою національної безпеки держави.

Так, у проекті Закону України «Про інформаційний суверенітет та інформаційну безпеку України» визначено: «Інформаційна безпека України – це захищеність життєво важливих інтересів суспільства, держави та особи, за якої виключається заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення інформації, забороненої чи обмеженої для поширення законами України».

Інформаційна безпека – категорія що має декілька змістових аспектів: соціологічний, соціально-політичний, соціально-психологічний, військовий, юридичний. У юридичному аспекті вона має декілька змістів: як галузь суспільних відносин, що знаходить вираз у відповідних правових нормах; як галузь наукових знань (наукова дисципліна); як навчальна дисципліна. Інформаційна безпека, як категорія, може вживатися у поєднанні з іншими категоріями: інформаційна безпека людини, інформаційна безпека громади, інформаційна безпека юридичної особи, інформаційна безпека суспільства, інформаційна безпека країни, інформаційна безпека світового співтовариства тощо. Категорія інформаційна безпека в системі правових норм України знайшла відображення у статті 17 Конституції України.

Інформаційна безпека – це соціальні відносини щодо охорони та захисту інформаційних потреб та інтересів людини, суспільства, держави, від можливих загроз природного, техногенного, соціогенного змісту.

Інформаційна безпека України – захист суверенітету України, забезпечення її інформаційної безпеки є найважливішими функціями держави, справою всього українського народу.[1]

Інформаційна безпека України включає вжиття комплексних заходів щодо захисту свого інформаційного простору та входження України в світовий інформаційний простір; виявлення та усунення причин інформаційної дискримінації України; усунення негативних чинників порушення інформаційного простору, інформаційної експансії з боку інших держав; розробка і впровадження необхідних засобів та режимів отримання, зберігання, поширення та використання суспільно значущої інформації, створення розвиненої інфраструктури в інформаційній сфері.

Інформаційна безпека – невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну та телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни.

Інформаційна безпека щодо інформатизації знаходить правовий вираз в комплексі нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації і профілактики вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо.[2]

---

[1] Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст.17.

[2] Про Концепцію Національної програми інформатизації: Закон України від 04.02.98 № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст.182.

В науковій літературі існують альтернативні визначення інформаційної безпеки:[3]

1. Інформаційна безпека людини, суспільства, держави – це стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної) за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки та дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів.
2. Інформаційна безпека – єдність концептуальних, теоретичних і технічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, соціальної, військової, економічної, духовної та ін.), а також сфер формування, циркулювання, накопичення та використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління у всіх різновидах діяльності тощо).
3. Інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства та держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації.

У «Концепції національної безпеки України» інформаційна безпека розглядається як стан захищеності національних інтересів України в інформаційній сфері, за якою не допускається або зводиться до мінімуму завдання шкоди особі, суспільству, державі.[4]

Для всебічного обґрунтування понять «інформаційна безпека» і «безпека інформаційної сфери» та визначення функціональних напрямів діяльності

---

[3] Рубан В.Я. Інформаційна безпека України: сутність та проблеми. //Стратегічна панорама, 1998. – № 3-4. – С.170.

[4] Концепція національної безпеки України: Постанова Верховної Ради України від 16.01.97 № 3/97-ВР // Відомості Верховної Ради України. – 1997. – 10. – Ст.85.

держави доцільно визначити зміст інформаційних загроз, для усунення або послаблення дії яких створюється система інформаційної безпеки. Це важливо як для створення загальної системи захисту національних інформаційних ресурсів, так і в процесі міжнародного інформаційного співробітництва.

Інформаційну загрозу можна визначити, як:

1) такий інформаційний вплив (внутрішній чи зовнішній), при якому створюється потенційна чи актуальна (реальна) небезпека зміни напрямку або темпів прогресивного розвитку країни, суспільства й індивідів;

2) небезпеку завдання шкоди життєво важливим інтересам особистості, суспільства та країни через інформаційний вплив на свідомість, підсвідомість, інформаційні ресурси, інфосферу машино-технічних систем та інші об'єкти інформаційної структури країни.

Враховуючи наведене вище, основними об'єктами інформаційного впливу (дії інформаційних загроз) можуть бути усі об'єкти єдиного інформаційного простору України, тобто інформаційні ресурси, організаційні структури, що забезпечують функціонування інформаційного простору, інформаційно–телекомунікаційні системи мережі, інформаційно-телекомунікаційні технології, системи засобів масової інформації.

Таким чином, поняття «інформаційна безпека» доцільно формулювати з урахуванням всіх системоутворюючих складових. Справді, заподіяння шкоди через неповноту, невчасність і недостовірність інформації є суттєвою інформаційною загрозою, однак її навряд чи можна назвати головною. Тому не можна погодитися з авторами проекту Закону України «Про інформаційний суверенітет та інформаційну безпеку України» та проекту «Концепції (Основи державної політики) інформаційної безпеки України», які ставлять саме цю загрозу на перше місце. Крім зазначеного вище, необхідно забезпечити насамперед інформаційну безпеку в основних сферах життєдіяльності особи, суспільства та держави, пов'язаних з економікою, наукою, техносферою, обороною, державним управлінням, захистом усіх об'єктів інформаційного простору.

Враховуючи вищевикладене, доцільно законодавчо визначити інформаційну безпеку як комплекс системних превентивних заходів з надання гарантій захисту життєво важливих інтересів особистості, суспільства від негативних інформаційних впливів тощо, а також спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз. При цьому безпека інформаційної сфери, тобто сфери, де створюється, накопичується, зберігається, поширюється та використовується інформація, повинна розглядатися як складова загальної системи інформаційної безпеки країни.

Побудова законодавчої бази у сфері інформації, метою якої є створення оптимальних умов користування усіма можливостями національного та глобального інформаційного простору без ризику завдання шкоди особистості, суспільству та державі, неможлива без законодавчо встановленого режиму доступу до інформаційних джерел України як в межах держави, так і за її кордонами.

Характерними рисами сьогодення є реформування економіки України за участю іноземного капіталу, розвиток міжнародного співробітництва, вільного пересування іноземців по всій території України, широке коло об'єктів для іноземних інспекцій, глобалізація інформаційного простору тощо. Все це створює реальні загрози для відпливу відомостей, що містять державну таємницю та іншу інформацію з обмеженим доступом.

Розгляд проблеми правового режиму інформації у всіх наукових дослідженнях розпочинається з обґрунтування складової цієї системи, пов'язаної з правом людини на інформацію. Це право закріплено в нормах міжнародного права. Таке право встановлено і в Конституції України: «Кожен має право вільно збирати, зберігати, використовувати та поширювати інформацію усно, письмово або в інший спосіб – на свій вибір».[5] У цій статті встановлені й певні обмеження: «Здійснення цих прав може бути обмежене законом і в інтересах національної безпеки, територіальної цілісності або

[5] Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

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».

В Україні поняття «правовий режим інформації» на рівні законодавства не визначено. Чинне законодавство містить лише окремі фрагменти визначення правового режиму інформації з обмеженим доступом (крім державної і банківської таємниці), а саме: службової, військової, комерційної, медичної, дорадчої кімнати, страхування, нотаріальних дій, а також конфіденційної інформації, яка є власністю або знаходиться у володінні, користуванні або розпорядженні окремих фізичних і юридичних осіб, тобто конфіденційної інформації, фрагменти правового режиму якої визначені конституційними правовими нормами та Законом України «Про інформацію».[6]

В Україні поширена практика встановлення обмежень до певних видів інформації, що підлягає захисту, на рівні підзаконних актів, хоча це суперечить як Конституції України, так і вимогам Європейського Союзу, набути асоційованого членства в якому прагне Україна. Стандарти ЄС та конституційна правова норма вважають дійсними лише обмеження доступу до будь-якої інформації тільки у разі їх встановлення на рівні національних законів.

Чинним законодавством України проголошено створення загальної системи охорони інформації, але лише Закон України «Про державну таємницю» містить комплекс правових норм, котрі встановлюють правовий режим інформації, що становить державну таємницю (перелік відповідної інформації, порядок її віднесення до категорії таємної, зміст режиму доступу, організаційно-правові заходи щодо охорони, здійснення прав власності на таку інформацію та її носії, компетенцію суб'єктів України щодо встановлення правового режиму відомостей, віднесених до державної таємниці,

[6] Про інформацію: Закон України від 2 жовтня 1992 року №2651-XII //Відомості Верховної Ради України. – 1992. – № 48. – ст.ст. 28, 30, 38.

відповідальність за порушення вимог чинного законодавства про державну таємницю).[7]

Причини недосконалості систем інформаційної безпеки:

- інформація як матеріальна цінність у порівнянні з будь-якою іншою матеріальною цінністю відносно просто копіюється, модернізується і руйнується;
- широкомасштабний розвиток і впровадження обчислювальної техніки і телекомунікаційних систем у рамках територіально розподіленої мережі, перехід на цій основі до безпаперової технології (електронним документам), збільшення обсягів і структурованості оброблюваної інформації, розширення кола її користувачів приводить до ускладнення можливості контролю та запобігання несанкціонованого одержання та використання інформації.

Концепція безпеки повинна в загальному вигляді відповідати на три базових питання: що захищати? від чого (кого) захищати? як захищати?

З питанням «що захищати» пов'язане поняття «об'єкт захисту». По сформованій міжнародній практиці об'єктами захисту з урахуванням їх пріоритету є: людина; інформація; матеріальні цінності.

Тому проблема безпеки містить у собі:

- фізичну безпеку, під якою розуміється забезпечення захисту від зазіхань на життя людей;
- матеріальну безпеку, що забезпечує збереження матеріальних цінностей.

Таким чином, **інформаційна безпека** – це здатність держави, суспільства, соціальної групи, людини:

- **по-перше**, забезпечити захист соціального інтелекту й інформаційного ресурсу, оптимальне соціальне інфосередовище з метою підтримки життєдіяльності та життєздатності, а також стійкого функціонування та розвитку соціуму;

[7] Про державну таємницю: Закон України від 21.01.94 №3855-XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

- **по-друге**, протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на індивідуальну та суспільну свідомість і психіку людей, а також на комп'ютерні мережі й інші технічні джерела інформації;
- **по-третє**, виробляти особистісні та групові навички й уміння безпомилкового поводження;
- **по-четверте**, підтримувати постійну готовність до адекватної відповіді в інформаційному протиборстві, ким би воно не було нав'язане.

Розглядаючи питання інформаційної безпеки необхідно звернути увагу на основні напрями діяльності з метою її забезпечення:

Перший – розвиток науково-практичних основ інформаційної безпеки;

Другий – розвиток законодавчої та нормативно-правової бази забезпечення інформаційної безпеки. Визначення порядку розробки законодавчих і нормативно-правових актів, а також механізмів практичної реалізації прийнятого законодавства;

Третій – удосконалення організації форм і методів запобігання та нейтралізації загроз інформаційній безпеці;

Четвертий – розвиток сучасних методів забезпечення інформаційної безпеки.

З метою ефективного забезпечення безпеки інформації потрібно створення розвинутого методологічного базису, що дозволяє вирішити наступні комплексні задачі:

- створити систему органів, відповідальних за безпеку інформації;
- розробити теоретико-методологічні основи забезпечення безпеки інформації;
- вирішити проблему керування захистом інформації і її автоматизації;
- створити нормативно-правову базу, що регламентує рішення всіх задач забезпечення безпеки інформації;
- налагодити виробництво засобів захисту інформації;
- організувати підготовку фахівців із захисту інформації;
- підготувати нормативно-методичну базу з метою проведення робіт із

забезпечення захисту інформації.

Інформація є головним об'єктом захисту, але необхідно вирішити яку інформацію треба захищати та що таке інформація. Закон України від 2 жовтня 1992 р. «Про інформацію» визначає, що **інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі**.[8]

Цікавою представляється думка Орлова П.І. наведена в науково-практичному посібнику «Інформація та інформатизація: Нормативно-правове забезпечення»:[9]

1. Точне і повне, але кінцеве визначення інформації не уявляється можливим.
2. Робочим визначенням визнаємо інформацію як вторинну властивість речі-носія, що за своєю актуалізацією змінює приймачем його склад або поведінку в мірі, не зводимої до обміну між ними тільки енергією та матерією.
3. Інформація сьогодні – це інструментальна цінність. Визнання її в такій якості дозволяє визначити її цінність як споживчу вартість тієї внутрішньої цінності, яка врешті решт досягається через отримання даної інформації.
4. Цінність інформації найбільш адекватно визначається не ***a priori***, але ***a posteriori*** – ринковими процесами (менш адекватно, але більш оперативно-уявно їх моделюючими досвідченими експертами).
5. Мета захисту інформації як інструментальної цінності полягає в тому, щоб її законний власник отримував за її допомогою бажану, врешті решт, внутрішню цінність.
6. Захист інформації-можливості здійснюється через захист її джерела або носія та середовища їх існування. Цей рівень захисту має своїм завданням запобігти суттєвому перекручуванню, повному руйнуванню або підміні інформації.

---

[8] Про інформацію: Закон України від 02.10.92 № 2651-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

[9] Орлов П.І. Інформація та інформатизація: Нормативно-правове забезпечення: Науково-практичний посібник. – Харків: Вид-во Ун-ту внутр. справ, 2000. – С.37.

7. Актуалізація інформації-можливості здійснюється шляхом захисту приймача або тих засобів, за допомогою котрих інформація переводиться із можливості до дійсності. Цей рівень захисту за своєю суттю направлений на зберігання конфіденційності інформації. Однак він важливий і для запобігання суттєвому перекручуванню, повному руйнуванню або підміні інформації.
8. Захист інформації-дійсності може бути здійснено законодавчими засобами, наприклад, через патентування. В цьому випадку вводиться норма закону, яка забороняє використовування неконфіденційної інформації тим, хто не має на це права.
9. Збиток від суттєвого перекручування, руйнування інформації, дезінформації або від втрати конфіденційності, а також від використовування інформації тим, хто не має на це права, визначається споживчою вартістю тієї внутрішньої цінності, яку втрачає внаслідок цього законний власник інформації.

Інформація може бути відкритою або з обмеженим доступом. Згідно зі ст. 30 Закону «Про інформацію» інформація з обмеженим доступом поділяється на конфіденційну і таємну.[10]

Конфіденційна – інформація що знаходиться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюється за їх бажанням.

Таємна – інформація, що містить відомості, розголошення яких завдає шкоди особі, суспільству та державі.

Інформація щодо діяльності та фінансового стану підприємства, яка стала відомою банку в процесі обслуговування та взаємовідносин з ним, чи третіми особами при наданні банківських послуг і розголошення якої може завдати матеріальної чи моральної шкоди відповідно до ст. 60 Закону України від 7 грудня 2000 р. «Про банки і банківську діяльність» є **банківською**

[10] Про інформацію: Закон України від 02.10.92 № 2651-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

таємницею.[11]

Для належного захисту інформації необхідно обмежити до неї доступ. Обмеження доступу полягає у зменшенні кола осіб, яким відома закрита інформація. Йдеться не лише про встановлення всіляких комп'ютерних паролів, замикання документів у сейфі та знищення чернеток.

Організація системи захисту інформації починається з визначення переліку відомостей, які є комерційною таємницею та конфіденційною інформацією. Керівник підприємства має затвердити наказом положення про комерційну таємницю та про конфіденційну інформацію на підприємстві, в якому надати перелік таких відомостей, і зазначити, що нерозголошення комерційної таємниці та конфіденційної інформації входить до трудових обов'язків працівників, та визначити відповідальність за невиконання цих обов'язків.

До того ж велику увагу треба приділяти інформації, яку отримують сторонні особи. Існує поняття **інсайдерської інформації**, тобто інформації, якою володіють інсайдери – особи, які не працюють на підприємстві, але володіють закритою інформацією про це підприємство. Так, інсайдерами є колишні топ-менеджери – особи, які займали керівну посаду на підприємстві (начальник відділу, головний бухгалтер, заступник директора тощо), акціонери, ділові партнери, співробітники юридичних, аудиторських і консалтингових фірм, які надають послуги підприємству.

Покарання за розголошення конфіденційної інформації передбачено лише ст. 164-3 КоАП. Однак власник конфіденційної інформації може самостійно встановити відповідальність за її розголошення. Відповідальність працівника є дисциплінарною – догана, звільнення (на підставі ст. 147 КЗпП).

Під **інформаційною загрозою розуміється потенційне порушення безпеки, чи ступінь імовірності виникнення такого явища (події), наслідком якого можуть бути небажані впливи на інформацію.**

---

[11] Про банки і банківську діяльність: Закон України від 07.12.2000 р. № 2121- III // Відомості Верховної Ради України. – 2001. – № 5-6. – Ст. 30.

Загрози інформації циркулюючої в інформаційній системі залежать від її структури та конфігурації, технології обробки інформації в ній, стану навколишнього фізичного середовища, а також дій персоналу. З безлічі способів класифікації загроз інформації найбільш загальною (базовою) є класифікація за результатами можливого впливу на інформацію: загрози порушення **конфіденційності**; загрози порушення **цілісності**; загрози порушення **доступу до інформації**.

Загрози конфіденційності спрямовані на розголошення конфіденційної чи секретної інформації. При реалізації цих загроз інформація стає відомою особам, що не повинні мати до неї доступ.

Загрози цілісності інформації спрямовані на її зміну чи перекручування, що приводить до порушення її якості чи повного знищення. Цілісність інформації може бути порушена навмисне, а також у результаті об'єктивних впливів з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації, комп'ютерних мереж і систем телекомунікацій.

Загрози доступу до інформації (відмова в обслуговуванні) спрямовані на створення таких ситуацій, коли визначені навмисні дії знижують працездатність інформаційної системи (ІС) або блокують доступ до деяких її ресурсів.

Джерелами названих вище загроз інформації можуть бути люди, апаратно-програмні засоби та середовище, що оточує ІС і її компоненти, що можуть впливати на інформацію ззовні (зовнішні джерела загроз) чи знаходитися у середині інформаційної системи (внутрішні джерела загроз).

До **зовнішніх джерел** відносяться: діяльність розвідувальних і спеціальних служб; діяльність різних політичних, військових, фінансових і інших економічних структур, спрямована проти інтересів держави; злочинні дії окремих груп, формувань і фізичних осіб.

До **внутрішніх джерел** відносяться: протизаконна діяльність різних структур, угруповань і окремих осіб в галузі використання інформації з метою приховання правопорушень, нанесення збитків законним інтересам інших

юридичних чи фізичних осіб; порушення встановлених правил збору, обробки та передачі інформації.

Іншими формами загроз безпеки інформації є:

- витік інформації по технічних каналах;
- розкрадання, знищення, перекручування, підробка, блокування, затримка, копіювання інформації в результаті несанкціонованого доступу до носіїв чи засобів її обробки, передачі та збереження;
- розкрадання, знищення власне носіїв інформації.

По природі походження джерела загроз можуть бути природними та штучними.

Природні – це загрози, викликані впливами на інформаційну систему і її елементи фізичних процесів чи стихійних природних явищ, що не залежать від людини.

Штучні – це загрози інформаційній системі, викликані діяльністю людини. Серед них, виходячи з мотивацій дій (безвідповідальність, самоствердження, цікавість, корисливий інтерес і т.д.) можна виділити:

- **ненавмисні** (випадкові) – загрози, викликані помилками в апаратно-програмному забезпеченні та діях персоналу;
- **навмисні** загрози – задумані (заборонені) дії людей, що спрямовані на порушення конфіденційності чи цілісності, доступу до інформації.

Поширена також класифікація інформаційних загроз по характеру, типам і способам їх реалізації.

По **характеру реалізації** загрози інформації поділяють на **пасивні** (без порушення цілісності інформаційної системи і будь-якого впливу на її елементи) і **активні**, здійснювані шляхом прямого чи непрямого контакту джерела загроз з елементами інформаційної системи за допомогою будь-якого впливу.

До **основних типів реалізації загроз** відносяться: стихійні лиха; злочинні дії; побічні явища; відмовлення, збої, помилки елементів інформаційної системи.

Більш непередбаченими з погляду загрози захищеності інформації та, як наслідок, менш пророблениими є заходи щодо запобігання злочинним діям і побічним явищам. **До побічних явищ** відносяться: електромагнітні випромінювання пристроїв ІС; паразитні наведення; зовнішні електромагнітні випромінювання; вібрація; зовнішні атмосферні умови. **До злочинних дій** у загальному випадку відносять такі категорії порушень безпеки як розкрадання, підміна, підключення, поломка (ушкодження), диверсія.

Злочинні дії можуть здійснюватися безвідносно до обробки інформації чи в процесі її обробки, з доступом до елементів інформаційної системи чи без нього, активно чи пасивно (тобто зі зміною стану чи без системи).

У залежності від цього основні типи злочинних загроз інформації в інформаційних системах можна класифікувати в такий спосіб:

- безвідносно до обробки інформації та без доступу зловмисника до елементів інформаційної системи: підслуховування розмов; використання оптичних, візуальних чи акустичних засобів;
- у процесі обробки без доступу зловмисника до елементів інформаційної системи: електромагнітні випромінювання; паразитні наведення; зовнішнє електромагнітне випромінювання; підключення апаратури, що реєструє;
- безвідносно до обробки інформації з доступом зловмисника до елементів інформаційної системи, але без зміни останніх: копіювання магнітних чи інших носіїв, вихідних чи інших документів; крадіжка виробничих відходів;
- у процесі обробки з доступом зловмисника до елементів інформаційної системи, але без зміни останніх: копіювання інформації в процесі обробки; маскування під зареєстрованого користувача; використання недоліків мов програмування, програмних пасток, недоліків операційних систем і вірусів;
- безвідносно до обробки інформації з доступом зловмисника до елементів інформаційної системи зі зміною останніх: підміна машинних носіїв, вихідних документів, апаратури, елементів програм, елементів баз даних, розкрадання носіїв і документів; включення в програми «троянських коней»,

«бомб» і т.п.; читання залишкової інформації в ЗУ після виконання санкціонованих запитів;

- у процесі обробки з доступом зловмисника до елементів інформаційної системи зі зміною останніх;
- незаконне підключення до апаратури та ліній зв'язку, зняття інформації на шинах живлення.

По **способах реалізації загрози** можуть здійснюватися: по технічних каналах; по каналах спеціального впливу; несанкціонованим доступом.

Найбільш розповсюдженим способом реалізації інформаційних загроз є **несанкціонований доступ (НСД),** тобто доступ суб'єкта до об'єкта (наприклад, користувача до інформації, інформаційному ресурсу, елементів інформаційної системи) у порушення встановлених у ІС правил розмежування доступу.

До основних способів несанкціонованого доступу відносяться:

- безпосереднє звертання до об'єктів доступу;
- створення програмних і технічних засобів, що виконують звертання до об'єктів доступу в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє здійснити НСД;
- впровадження в інформаційну систему програмних чи технічних механізмів, що порушують її штатну структуру та функцію елементів.

Технічна чи програмна реалізація способів несанкціонованого доступу до елементів інформаційної системи заснована на наступних **методах: переривання; перехоплення; модифікація; підробка (фальсифікація).**

Спробу реалізувати кожну з перерахованих вище загроз інформації називають **атакою**. Успішність атаки може приводити до втрати інформацією однієї з критичних особливостей (конфіденційності, цілісності чи доступу до інформації).

Наступні ознаки можуть свідчити про наявність уразливих місць в інформаційній безпеці:

1. Не розроблено положень про захист інформації чи вони не дотримуються.

2. Не призначений відповідальний за інформаційну безпеку.
3. Паролі пишуться на комп'ютерних терміналах, містяться в загальнодоступних місцях, ними поділяються з іншими, чи вони з'являються на комп'ютерному екрані при їхньому введенні.
4. Віддалені термінали та мікрокомп'ютери знаходяться без догляду в робочі та неробочі часи. Дані відображаються на комп'ютерних екранах, залишених без догляду.
5. Не існує обмежень на доступ до інформації, чи на характер її використання. Усі користувачі мають доступ до всієї інформації та можуть використовувати усі функції системи.
6. Не ведуться системні журнали, і не зберігається інформація про те, хто та з якою метою використовує комп'ютер.
7. Зміни в програми можуть вноситися без попереднього затвердження керівництвом.
8. Відсутня документація чи вона не дозволяє розуміти звіти, що надходять, і формули, по яких виходять результати, модифікувати програми, готувати дані для введення, виправляти помилки, робити оцінку мір захисту та розуміти самі дані – їхні джерела, формат збереження, взаємозв'язок.
9. Робляться численні спроби ввійти в систему з неправильними паролями.
10. Дані, що вводяться, не перевіряються на коректність чи точність, при їхній перевірці багато даних відкидається через помилки в них; потрібно внести багато виправлень у даних, не ведуться записи в журналах про зроблені транзакції.
10. Мають місце виходи з ладу системи, що приносять великі збитки.
11. Не проводиться аналіз інформації, обробленої в комп'ютері, з метою визначення необхідного для неї рівня безпеки.

Виходячи з вищезазначеного можна зробити висновок, що інформаційній безпеці приділяється недостатньо уваги. Хоча політика безпеки й існує, більшість людей вважає, що насправді вона не потрібна.

2. Наслідки злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж

Дослідження й аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розподілити на випадкові і навмисні. Навмисні загрози можуть бути виконані шляхом довготривалої масованої атаки несанкціонованими втручаннями або вірусами.

Наслідки, до яких призводить реалізація загроз: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, коректну за формою і змістом, але яка має інше, значення), ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути різною: від невинних жартів до відчутних втрат, що в деяких випадках складають загрозу національній безпеці країни. Попередження наведених наслідків в автоматизованій системі і є основною метою створення системи безпеки інформації. Для створення засобів захисту інформації необхідно визначити природу загроз, форми і шляхи їх можливого **вияву і здійснення**.[12]

У юридичній літературі пропонується наступна загальна класифікація можливих наслідків злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж.[13]

1. Порушення функцій:

а) тимчасові порушення, котрі призводять до плутанини в графіках роботи, розкладі тих чи інших дій і т.д.;

б) недоступність системи для користувачів;

в) пошкодження апаратури (деякі практичні спеціалісти вважають, що пошкоджень апаратури, коли це стосується незаконного доступу, не буває);

г) пошкодження програмного забезпечення.

2. Втрати значних ресурсів – грошей, речей, обладнання, інформації.

---

[12] Голубєв В.О., Юрченко О.М. Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту / Під редакцією д.ю.н. Снігерьова О.П. та д.т.н. Вертузаєва М.С. – Запоріжжя: ВЦ «Павел», 1998. – С. 36.

[13] Батурин Ю.М. Проблемы компьютерного права. – М.: Юрид. лит., 1991. С. 134-135.

3. Втрата монопольного використання, яка обумовлена тим, що певна інформація цінна для власника лише доти, допоки він є її монопольним володарем.

4. Порушення прав (авторських, суміжних, патентних, винахідницьких і т.д.).

Як однобоко і неправильно в будь-якому новому явищі вбачати лише позитивне, так і високі технології мають бути оцінені з точки зору тієї шкоди, якої вони можуть завдати, адже вони відкривають нові можливості для всіх, і для злочинців також. Як свідчить історія розвитку світового науково-технічного прогресу, будь-яка технічна новація, зокрема в галузі засобів комунікації, неминуче притягувала до себе людей, які намагалися й намагаються використати її для злочину.

Комп'ютеризація породила новий вид злочинів. Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки грошових коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем – ось далеко не повний перелік комп'ютерних злочинів. При цьому слід зазначити, що загальна кількість зловживань у сфері комп'ютерних технологій та розмір завданих при цьому збитків неухильно зростають.

Цей факт можна пояснити декількома факторами:

- високою динамічністю та масовістю впровадження у багатьох сферах людської діяльності різноманітних інформаційних технологій та процесів, що базуються на використанні засобів обчислювальної техніки;

- різким розширенням кола спеціалістів у галузі комп'ютерних технологій, підвищенням їх кваліфікації;

- недосконалістю законодавчої бази у сфері інформаційних відносин та інформаційної безпеки;

- недосконалістю чи відсутністю технічних засобів забезпечення інформаційної безпеки у конкретних інформаційних технологіях;

- низьким ступенем розкриття злочинів.

Це, в свою чергу, викликало потребу осмислення комп’ютерної злочинності як соціального явища та напрацювання відповідних методик боротьби з нею, в тому числі виявлення і розслідування злочинів, що вчиняються з використанням комп’ютерних технологій.

Зусилля щодо створення системи боротьби з комп’ютерними злочинами концентруються у кількох напрямах:

- створення законодавчого забезпечення боротьби з комп'ютерними злочинами;

- розробка захищених інформаційних технологій;

- розробка засобів захисту з метою модернізації існуючих інформаційних технологій.

Кошти, що потрібні для вирішення цих завдань, дуже великі, і з кожним роком їх потрібно все більше. Обсяг виробництва засобів фізичного контролю та захисту ЕОМ тільки у США має такі розміри і темпи росту: від 1,8 млрд. дол. в 1990 р. до 5 млрд. дол. у 2000 р. Однак витрати на ці цілі все одно значно менші за можливі збитки.

Адекватне реагування на зміни в суспільних відносинах у результаті інформаційних процесів знайшло відображення в нормативних актах Ради Європи (їх більше 100), резолюціях, конвенціях, рекомендаціях і директивах Європарламенту і Євросоюзу. Конкретне відображення процесів інформатизації виражається в правовому просторі, нормативних та етичних нормах суб’єктів інформаційних відносин усіх розвинених країн світу.

Не дивлячись на економічні труднощі, український сегмент мережі Інтернет розвивається динамічно (за оцінками спеціалістів у середньому за кожні шість місяців кількість хостів у сегменті UA збільшується в 1,7 разів), що значно перевищує середній темп росту мережі Інтернет у цілому. За кількістю

провайдерів послуг Інтернет Україна знаходиться на першому місці серед країн Східної Європи.[14]

Україна, інтегруючись у світове співтовариство, за роки незалежності здійснила стрибок у єдиний світовий інформаційний простір у багатьох сферах суспільного життя. Наприклад, створення єдиної загальнодержавної системи електронних платежів під егідою Національного банку України, рівних якій немає в країнах СНД, є певним досягненням держави, сприяє укріпленню її суверенітету, економічній безпеці, здатності краще протистояти загальносвітовим і регіональним потрясінням.

Вводяться інформаційні технології мережі Інтернет, створюються інші транснаціональні, національні, багатопрофільні чи вузькоспеціалізовані інформаційні мережі. Зараз важко уявити перспективну сферу суспільної діяльності, в якій би не використовувалися сучасні комп'ютери, локальні і глобальні комп'ютерні мережі, програмні комплекси від найпростіших до найвищого рівня складності.

При цьому надзвичайну стурбованість у спеціалістів викликає загрозливий розрив між рівнем втілення інформаційних комп'ютерних технологій і рівнем засобів їх правового, організаційно-технологічного захисту. Адже за оцінками експертів ООН, збитки від комп'ютерних злочинів у світі вже перевищили 1 трлн. дол. США.

Інститут Комп'ютерної безпеки (CSI) (Сан-Франциско) опублікував у 2003 році результати дослідження загроз кіберзлочинності та статистику кібератак. Кількість серйозних інцидентів, пов'язаних із комп'ютерною безпекою, виявилася приблизно однаковою в 2002 і 2001 роках. Як і раніше, найбільших збитків завдається в результаті викрадення цінної інформації – 70 млн. дол. США. На другому місці – атаки «Відмова в обслуговуванні» (Denial of Service). Причому у 2002 році втрати від подібних дій хакерів склали 65,6 млн. дол. США.

---

[14] Виталий Балюк. Украинский сегмент сети Internet сегодня. – http://boy.dlab.kiev.ua/PRJ/B_Intt/Main/Addon/Lib/anal_ukr/htm

Фінансові втрати від злочинів, пов’язаних із викраденням конфіденційної інформації, з початку 2003 р. склали 70195900 дол. США (у 2002 р. – 170827000 дол. США).

Викривлення даних у мережі спричинило збиток у сумі 5158500 дол. США (у 2002 р. – 15134000 дол. США).

Несанкціоноване перехоплення інформації без її зміни в телекомунікаційних мережах – 76000 дол. США (у 2002 р. – 346000 дол. США).

Проникнення в мережу сторонніх осіб – 2754400 дол. США (у 2002 р. – 13055000 дол. США).

Порушення роботи мережі санкціонованими користувачами – 11767200 дол. США (у 2002 р. – 50099000 дол. США).

Шахрайство – 10186400 дол. США (у 2002 р. – 115753000 дол. США).

Атаки типу «Відмова в обслуговуванні» (Denial of Service) – 18370500 дол. США (у 2002 р. – 65643300 дол. США).

Розповсюдження вірусів – 27382340 дол. США (у 2002 р. – 49979000 дол. США).

Несанкціонований доступ до інформації всередині мережі – 4063000 дол. США (у 2002 р. – 4503000 дол. США).

Шахрайство з телекомунікаційними ресурсами – 7015000 дол. США (у 2002 р. – 6015000 дол. США).

Активне прослуховування телефонних розмов - 705000 дол. США (у 2002 р. подібних злочинів не зареєстровано).

Крадіжка ноутбуків – 6830500 дол. США (у 2002 р. – 11766500 дол. США).

Загальні ж фінансові втрати від комп’ютерної злочинності склали 201797340 дол. США (у 2002 р. – 455848000 дол. США).

Якщо порівнювати традиційні злочини і комп’ютерні, то останні відрізняються, перш за все, феноменом розповсюдження у часі та просторі, місцем та суб’єктом посягання. Інакше кажучи, щоб вкрасти гроші, немає потреби проникати в сховище банку, перетинати кордони, долати системи

охорони і сигналізації. Досить мати комп'ютер, вихідну інформацію стосовно доступу та захисту електронних систем банку, набір хакерських програм і досвід такої роботи.

Інший важливий аспект комп'ютерних злочинів – це феномен безликості інформації. Такі традиційні ознаки криміналістичної експертизи, як почерк, відбитки пальців та ін. – в електронних імпульсах комп'ютера безликі.

Ще одна специфіка комп'ютерних злочинів – феномен інструментарію комп'ютерних посягань. На відміну від традиційних способів злочину (зброя, ніж і т.д.) інструментарій комп'ютерних злочинів – різноманітні програмні засоби комп'ютерних втручань.

На увагу заслуговує техніко-технологічний спосіб скоєння злочину. Суть його – злочинне порушення функціонування інформаційних систем, обумовлене впливом на їх вразливі компоненти. І, хоча цей вид злочину суттєво відрізняється від традиційних терористичних злочинів, наслідки за своєю трагічністю можуть бути подібними до великих техногенних катастроф.

Стан інформаційно-телекомунікаційних систем і рівень їх захисту є одним із найважливіших факторів, що впливає на інформаційну безпеку держави. Економічні збитки від комп'ютерних злочинів сьогодні стоять на одному рівні з перевагами, здобутими від впровадження електронно-обчислювальних машин у практику, а соціальні та моральні втрати взагалі не підлягають оцінці.[15]

Далі наведемо деякі приклади шахрайства зі всього світу.

У 2005 році у світі було зареєстровано більше 130 великих витоків інформації з приватних баз даних. Зокрема, були скопійовані дані групи ABN Amro Mortgage Group, автомобільної корпорації Ford Motor, підрозділу компанії Wal-Mart Sam's Club, мережі готелів Marriott International і багатьох інших. Зловмисники скопіювали інформацію про більш ніж 55 млн. американських громадян, насамперед номери кредитних карток і карток

[15] Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. – Запоріжжя: ГУ «ЗІДМУ», 2003. – С. 34.

соціального страхування. Держказначейство США заявило, що фінансові втрати від розкрадання баз даних корпорацій і інших комп'ютерних злочинів у 2004 році склали понад 105 млрд. дол. США. Остаточний розмір збитку від дій комп'ютерних піратів у 2005 році ще не визначений.

У Міністерстві внутрішньої безпеки США не виключають, що в 2006 році випадки крадіжок конфіденційної інформації почастішають. Крім того, на думку американських чиновників, у 2006 році може бути зафіксована рекордна кількість фінансових шахрайств із використанням приватної інформації, вилученої з корпоративних баз даних.

У червні 2005 року компанія Master Card International оголосила про те, що хакери одержали доступ до рахунків 40 млн. власників пластикових карток, у тому числі 13,9 млн. карт Master Card Master Card (включаючи Maestro і Master Card International), 22 млн. карт Visa, а також 4 млн. карт American Express і Discover.

У Master Card International вважають, що провина лежить на компанії Card System Solutions, що опікується обробкою платежів. Імовірно, причина втрати даних полягає в недосконалості системи безпеки, що виявилася нездатною протистояти вірусу. Card System Solutions побічно визнала себе винною, заявивши, що приступила до удосконалення своєї системи безпеки. Імовірніше за все, виявилися розкриті чи продані файли транзакцій. Хакери мали можливість одержати доступ до номерів кредитних карт. Цікаво, що сам епізод відбувався наприкінці травня, тобто постраждалі компанії ховали цю інформацію приблизно місяць.

Водночас були втрачені дані клієнтів Citigroup. 6 червня компанія Citi Financial, роздрібне відділення Citigroup, повідомила про втрату даних 3,9 млн. своїх американських клієнтів. Конфіденційна інформація містила їх імена, номери соціального страхування, дані про операції й отримані кредити. Провина лежить на компанії-перевізнику United Parcel Service, що втратила електронні стрічки з даними вкладників під час перевезення в кредитне бюро Experian у штаті Техас. Цікаво, що в цьому випадку компанія не ховала втрату

інформації, а сама довго не могла її знайти. Дані були відправлені з Нью-Джерсі в Техас 2 травня. Лише 20 травня одержувач Experian усвідомив, що зведення до нього не дійшли. Топ-менеджери Citigroup були проінформовані про зникнення 24 травня, але тільки 27 травня служба безпеки банку розпочала розслідування. Довідавшись про те, що трапилося, Citigroup завірила громадськість, що дані не потраплять до зловмисників. Однак паралельно CitiFinancial приступила до розсилання повідомлень усім 3,9 млн. своїх клієнтів, пропонуючи їм способи захисту від можливих шахрайств.

На відвідувачах порносайтів нью-йоркське злочинне угрупування, відоме як родина Гамбіно, заробило біля 200 млн. дол. Мафіозі були причетні до функціонування ряду платних порнографічних інтернет-сторінок, де й організували пастку. Відвідувачам сайтів пропонувався нібито безкоштовний перегляд, але за умови введення реквізитів банківської картки, з якої ділки Гамбіно знімали проти волі відвідувачів досить кругленькі суми. Американська Феміда засудила головних винуватців афери до 10 років.

Багато довірливих громадян США стали жертвами так званих «нігерійських листів». Співробітниця американської фірми перейнялася цією аферою настільки, що за раз перерахувала віртуальному партнеру 2,1 млн. дол. США з рахунків роботодавця. Схема обману виглядала так: потенційній жертві надсилався електронний лист нібито впливового африканського чиновника, що пропонував заробити на корупційній схемі в Нігерії. За перерахування в один з американських банків 18 млн. дол. (іноді фігурувала інша цифра) подільник африканця повинен був одержати щедрий хабар у 25%. От тільки треба було підкинути африканському ділку трохи грошей, нібито на хабарі нігерійським чиновникам. Деякі жертви нігерійського розсилання не шкодували і власних грошових заощаджень. Правоохоронці кілька років шукали шахраїв, і деяких таки вдалося посадити за грати – «нігерійців» засуджено до 5 років позбавлення волі.

У Європі досить поширена практика клонування фальшивих сайтів. Швейцарські шахраї заробили 3,9 млрд. дол. за допомогою 29

псевдокорпоративних сайтів, через які продавали повітря під виглядом цінних паперів. Потенційні інвестори були впевнені, що мають справу з авторитетними компаніями, й охоче перераховували гроші фальсифікаторам корпоративних web-сторінок в надії вигідно придбати акції.

Легендою пострадянського хакерства залишається Володимир Левін, що вкрав з американського City Bank 10 млн. дол. Свою діяльність пітерський кібер-гангстер розпочав у часи, коли комп'ютери були в офісах заможних і престижних компаній, а Інтернет і електронна пошта здавалися незбагненною вигадкою high-tech. У 1994 році у Москві вже була відкрита філія відомого City Bank, і Володимир Левін вирішив піддати транснаціональний банк іспиту на міцність. Він досить швидко знайшов ключі до електронної системи захисту банку та почав незаконні транзакції. Але з украдених десяти мільйонів молодий петербуржець перевів у реальні гроші тільки 400 тис. дол., інше ФБР встигла повернути City Bank після арешту Левіна. Сам зловмисник одержав 3 роки американських «таборів».[16]

У червні 2004 р. співробітники компанії російського оператора мобільного зв'язку «Вимпелком» (торгова марка «Білайн») знайшли в Інтернеті сайт, що надавав платні послуги, серед яких була інформація про вхідні та вихідні дзвінки плюс персональні дані будь-яких запитаних абонентів стільникових мереж «Білайн». Природно, що одержати ці зведення поза судовим порядком можна лише незаконним шляхом. Усі зведення були передані в розпорядження до МВС Росії, що здійснило контрольну закупівлю, затримало підозрюваного та простежило ланцюжок передачі інформації аж до джерела витоку. У результаті, 29 листопада 2004 р. було заарештовано шість осіб, троє з яких виявилися співробітниками самої компанії «Вимпелком». Цілком можливо, що співробітники МТС і Мегафона теж були членами банди, але офіційного підтвердження цієї версії немає. Всім арештованим були пред'явлені обвинувачення за статтями КК Російської Федерації, що передбачають до 5 років позбавлення волі. Незважаючи на те, що про вирок

[16] Випадки з життя // Контракти. – 2006. – №14. – С. 52-53.

суду офіційної інформації немає, сценарій розвитку подій є тим виключенням, коли постраждала компанія та правоохоронні органи спрацювали бездоганно.

У лютому 2005 року у продаж надійшла база даних Центрального банку РФ. У ній містилася інформація про платежі, проведені банками через розрахунково-касові центри Центробанку із квітня 2003 року по вересень 2004 року Інцидент отримав широкий суспільний резонанс, тому що вкрадена інформація могла бути використана в нечесній конкурентній боротьбі. Депутати Держдуми попросили Генпрокуратуру розібратися. У той же час сам Центробанк провів внутрішнє розслідування обставин витоку.

Однак вже в травні на ринках з'явилася нова даних Центробанку, що містить інформацію за IV квартал 2004 року. Зокрема, розповсюджена база дозволяла ознайомитися з деталями продажу з аукціону основного видобувного підприємства Юкоса «Юганскнефтегаза». Центробанк знову провів внутрішнє розслідування. Генпрокуратура зайнялася перевіркою обставин витоку за запитом Держдуми, нарешті, за неофіційними даними, до справи підключилася ФСБ. Результати всіх цих розслідувань не відомі. У жовтні 2005 г. Владимир Бабкін, заступник начальника Управління безпеки та захисту інформації Московського головного територіального управління Банку Росії, повідомив на прес-конференції, що канал витоку інформації з Центробанку перекритий, однак джерело витоку так і не назвав.

У жовтні 2005 року в Інтернеті з'явилася база даних одного з найбільших реєстраторів Росії – компанії «Нікойл». Вона веде реєстри акціонерів таких гігантів, як Лукойл, МТС, Скайлінк і ще декількох сотень корпорацій національного масштабу. Оголошення про продаж бази з'явилося 23 жовтня на форумі ресурсу www.zahvat.ru у розділі «Ворожі поглинання». Актуальність пропонованої бази – 1 серпня, а початкова ціна – 12 тис. дол.

Утім, топ-менеджмент компанії-реєстратора заперечує можливість витоку конфіденційної інформації. За словами гендиректора компанії Максима Калініна, внутрішнє розслідування показало, що продавці бази даних володіють, швидше за все, лише компіляцією зведень, що були у відкритому

доступі, а також деякими даними, переданими Нікойлом правоохоронним і податковим органам. Керівник реєстраційної компанії не виключає, що оголошення про продаж бази може бути спробою скомпроментувати реєстратора.

Двоє луганських хакерів імітували торгівлю у всесвітній мережі нібито від імені інтернет-аукціону «eBay» і заробили на цьому 150 тис. дол. США. Для більшої переконливості комбінатори залучили до своїх махінацій співробітників одного з луганських банків – так шахраї одержали можливість відкрити рахунок у США, на якому й акумулювали гроші, отримані з аукціонів. Через підставних осіб хакери знімали гроші з рахунка та за допомогою Western Union відправляли їх до України. От тільки товарів, придбаних нібито на «eBay», довірливі покупці не одержували. Діяльність електронних шахраїв перервав Інтерпол разом із СБУ.

Як бачимо, збитки та втрати від комп'ютерних злочинів дуже великі. Розглянемо, як проводиться робота з протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж в Донецькій області.

У 2005 році на території області знаходилося понад 8,5 тис. об'єктів інтелектуальної власності, з них близько 250 комп'ютерних фірм, понад 240 суб'єктів господарювання, що займались поширенням аудіо-, відеопродукції та програмного забезпечення.

Співробітниками УДСБЕЗ УМВС України в Донецькій області за 2004 рік виявлено 40 злочинів (21 особа) у сфері інтелектуальної власності, а за 2005 рік вже 50 злочинів (тільки 6 осіб). У сфері високих технологій простежується тенденція до зменшення виявлених злочинів та осіб, що їх скоїли. Але показники «збиток» та «відшкодування» свідчать, що фінансові втрати кожен рік зростають у абсолютному значенні, а відшкодовувати їх стає дедалі складніше (Таблиця 1).

Таблиця 1

Результати роботи УДСБЕЗ УМВС України в Донецькій області за 2004-2005 рр.

Показники	Всього в області			У тому числі за напрямками					
				Інтелект. власність			*Високі технології*		
	2004	2005	Зміни	2004	2005	Зміни	2004	2005	Зміни
Виявлено злочинів:	2858	2535	-323	40	50	+10	101	84	-17
З них кваліфіковано:	1984	1941	-43	19	17	-2	68	69	+1
-середньої важкості;	828	794	-34	19	17	-2	33	21	-12
-важких;	940	926	-14				31	35	+4
-особливо важких	216	221	+5				4	13	+9
Виявлено осіб	1308	868	-440	21	6	-15	5	1	-4
З них кваліфіковано:	812	592	-220	7	1	-6	3	1	-2
-середньої важкості;	319	226	-93	7	1	-6	2	1	-1
-важких;	419	299	-120						
-особливо важких	74	67	-7						
Направлено матеріалів до суду	2085	1526	-559	24	7	-17	69	51	-18
З них кваліфіковано:	1463	1168	-295	11		-11	51	48	-3
-середньої важкості;	606	59	-147	11		-11	31	14	-17
-важких;	728	577	-151				16	23	+7
-особливо важких	129	132	+3				4	11	+7
Притягнуто осіб до крім. відповідальності	1112	801	-311	16	5	-11	5		-5
З них кваліфіковано:	745	555	-190	6		-6	5		-5
-середньої важкості;	277	198	-79	6		-6	3		-3
-важких;	395	294	-101				2		-2
-особливо важких	73	63	-10						
Збиток, тис.грн.	162862	312385	+149523	2256	4718	+2462	2840	11274	+8434
Відшкодування, тис.грн.	22684	34307	+11626	925	920	-5	1153	240	-913

Якщо зробити простий аналіз змін показників, наведених у таблиці 1 з боку їх питомої ваги за напрямками, можна побачити, що питома вага кількості виявлених злочинів за ці роки змінилася не суттєво. У той же час питома кількість збитків від виявлених зловживань у сфері високих технологій зменшилася в 2005 році на 4,2%, але в 2004 році питома кількість збитків майже вдвічі перевищувала питому кількість виявлених злочинів.[17]

Увагу привертає незначна кількість (з тенденцією до зменшення) виявлення осіб, направлених матеріалів до суду, притягнутих до відповідальності осіб та реального відшкодування збитків (Таблиця 2).

Таблиця 2

Аналіз змін показників роботи УДСБЕЗ УМВС України в Донецькій області за 2004-2005 рр.

Показники	**Всього в області**			**Питома кількість за напрямками**					
				Інтелект. власність			*Високі технології*		
	2004	2005	Зміни	2004	2005	Зміни	2004	2005	Зміни
Виявлено злочинів:	2858	2535	-323	1,4%	1,97%	+0,57%	3,53%	3,31%	-0,2%
Виявлено осіб	1308	868	-440	1,6%	0,7%	-0,9%	0,38%	0,12%	-0,26%
Направлено матеріалів до суду	2085	1526	-559	1,15%	0,46%	-0,69%	3,31%	3,34%	+0,03%
Притягнуто осіб до крім. відпові-дальності	1112	801	-311	1,44%	0,62%	-0,82%	0,45%	--	-0,45%
Збиток, тис.грн.	162862	312385	+149523	1,39%	1,5%	+0,11%	6,9%	2,7%	-4,2%
Відшко-дування, тис.грн.	22684	34307	+11626	4,08%	2,68%	-1,4%	5,08%	0,7%	-4,38%

Наведені показники свідчать про значні труднощі правоохоронців у виявленні, запобіганні, документуванні та розкритті злочинів у сфері інформаційних технологій. Саме тому надзвичайно важливо з’ясувати основні принципи інформаційної безпеки.

[17] За даними УДСБЕЗ УМВС України в Донецькій області.

3. Інформаційна система як об’єкт захисту

Інформаційна система (ІС) – організаційно-технічна система, що реалізує інформаційні технології та включає апаратне, програмне й інші види забезпечення, а також відповідний персонал.

Під інформаційною системою можна також розуміти автоматизовану систему, призначену для організації, збереження, поповнення, підтримки та надання користувачам інформації відповідно до їх запитів.

Метою будь-якої інформаційної системи, незалежно від області її застосування, програмного чи апаратного забезпечення, є надання повної, достовірної та своєчасної інформації.

Інформаційні системи можна поділити на дві основні групи: **системи інформаційного забезпечення** та системи, що мають **самостійне цільове призначення** та область застосування.

Системи (чи підсистеми) інформаційного забезпечення входять до складу будь-якої ІС. Вони – найважливіші компоненти систем, що розвиваються інтенсивно в теперішній час інтегральної автоматизації виробничих систем, систем автоматизованого проектування, автоматизованих систем наукових досліджень і інші.

До числа самостійних ІС належать інформаційно-пошукові (ІПС), інформаційно-довідкові (ІДС) і інформаційно-керуючі системи. Інформаційно-пошукові й інформаційно-довідкові системи призначені для збереження та надання користувачу інформації (фактографічних записів, текстів, документів і т.і.) відповідно з деякими характеристиками, що формально задаються.

Для ІПС і ІДС характерні два етапи функціонування:

- збір і збереження інформації;
- пошук і видача інформації користувачу.

Рух інформації в таких системах здійснюється по замкнутому колу від джерела до споживача.

Залежно від режиму організації пошуку ІПС і ІДС можуть бути розділені

на документальні, бібліографічні, бібліотечні, фактографічні.

Документальними називають інформаційно-пошукові системи, у яких реалізується пошук в інформаційному фонді ІПС документів чи текстів відповідно до отриманого запиту з наступним наданням користувачу цих документів чи їхніх копій. Вся обробка отриманої інформації в документальних ІПС здійснюється користувачем.

Залежно від того, по яким збереженим документам чи по їхнім описам (вторинним документам) здійснюється пошук, документальні ІПС поділяють на системи з бібліотечним чи з **бібліографічним** пошуком. У першому випадку пошук ведеться в інформаційному фонді, що містить первинні документи, у другому – в інформаційному фонді вторинних документів.

Фактографічні інформаційно-пошукові системи реалізують пошук і видачу фактів, текстів, документів, що містять зведення, що можуть задовольнити запит користувача, що надійшов. У цьому випадку здійснюється пошук не якогось конкретного документа, а сукупності зведень по даному запиту, що зберігаються в інформаційному фонді ІПС чи ІСС. Відзначимо, що основною відмінністю фактографічних інформаційно-пошукових систем від документальних є те, що ці системи видають користувачу не який-небудь раніше введений документ, а вже в тому чи іншому ступені оброблену інформацію.

Під **інформаційними процесами** розуміється сукупність взаємозалежних і взаємообумовлених процесів виявлення, аналізу, введення та добору інформації, її передачі й обробки, збереження, пошуку, видачі та прийняття рішень і т.д.

Крім того, ІС характеризують:

- наявність прямих, зворотних, багатоканальних і розгалужених зв’язків, а також процесів керування;
- складність, що розуміється як принципова неможливість повною мірою, без додаткових умов і обмежень, мати адекватний формалізований опис;

- достаток різноманітних складових інформаційного процесу, розподілених у просторі, що безупинно переміняють один одного в часі.

Обробка інформації ІС – будь-яка сукупність операцій (прийом, збір, нагромадження, збереження, перетворення, відображення, видача і т.п.), здійснюваних над інформацією (зведеннями, даними) з використанням технічних засобів ІС.

Специфічним для ІС є поняття структури, що розкриває схему зв'язків і взаємодії між елементами.

Фізична структура ІС – це схема зв'язків фізичних елементів, таких, як технічні засоби, апаратура вузлів, власне вузли, обчислювальна техніка, встановлювана в них. До основних компонентів фізичної структури можна віднести вузли, канали та лінії зв'язку.

Логічна структура ІС визначає принципи встановлення зв'язків, алгоритми організації процесів і керування ними, логіку функціонування програмних засобів. У загальному вигляді вона визначає з'єднання та взаємодію двох принципово різних по призначенню та функціям складових частин архітектури ІС: безлічі автономних інформаційних підсистем (вузлів) і безлічі засобів їхнього зв'язку та взаємодії (фізичних засобів з'єднань).

Узагальнена геометрична модель фізичної структури ІС визначає **топологічну структуру** ІС.

Більш конкретний склад апаратно-програмних засобів і схема їхніх зв'язків називається також **конфігурацією** ІС.

Під **архітектурою ІС** розуміють погодженість усіляких структур ІС. Так, при деякій логічній структурі, що відповідає прийнятій архітектурі ІС, може бути побудовано безліч фізичних структур, що впливають на властивості та можливості системи. У свою чергу, логічна структура ІС у достатній мірі визначає властивості архітектури ІС у цілому.

Інформаційний вузол – це технічна чи організаційно-технічна система визначеної складності, що здійснює ті чи інші задані процеси (наприклад,

обробка та накопичення інформації, що надходить, розподіл по каналах і ін.).

Вузли, в яких інформація виходить за межі системи чи надходить у систему, називають кінцевими пунктами. Тут установлюються технічні засоби, що називають терміналами («абонентськими» пунктами).

Внутрішні мережні вузли – це звичайно транзитні чи в загальному випадку комунікаційні зв'язні вузли. З'єднання окремих інформаційних вузлів здійснюється за допомогою різних каналів зв'язку (провідних, безпровідних, комбінованих).

ІС можна розділити на системи великих масштабів (глобальні), середніх (регіональні чи зональні) і малих (місцеві чи локальні).

У залежності від рівня розвитку архітектури можна виділити:

- **комунікаційні системи,** тобто такі, у яких застосовані засоби розраховані на забезпечення зв'язку та здійснення обміну інформацією між територіально розділеними користувачами та терміналами;
- **інформаційно-обчислювальні системи** (ІОС), що надають по запитах окремих користувачів і систем ті чи інші інформаційні, обчислювальні ресурси та послуги.

Відомі два основних методи розподілу інформації – комутація та селекція.

Комутація здійснюється двома способами: комутацією каналів, чи повідомлень пакетів.

Селекція ґрунтується на обраному методі доступу взаємодіючих систем до зв'язку. Вона широко застосовується в локальних ІОС.

Види послуг, наданих ІС:

- встановлення зв'язку;
- передача даних;
- телеобробка;
- доступ до розподілених баз даних та ін.

Ресурси ІС – усі компоненти ІС, її апаратне та програмне забезпечення. Поняття ресурсу може бути поширено на інші компоненти ІС – процедури,

протоколи, структури що керують і т.д. Отже, поняття ресурсу визначається в широкому змісті.

Залежно від виду засобів, методів і алгоритмів керування можна виділити ІС з централізованим і розподіленим керуванням. При цьому можуть виконуватися як тверді (фіксовані), так і гнучкі (адаптивні) алгоритми керування ІС, що враховують численні фактори.

Об'єднання мереж здійснюється або через загальний вузол, або шляхом створення спеціальних каналів, що з'єднують вузли однієї системи з вузлами іншої. Якщо мережа може бути з'єднана з іншими, то вона називається відкритою, якщо не може чи не повинна з'єднуватися, то – закритою. Закритість системи (чи її частини) для деякої категорії користувачів є одним із способів захисту інформаційних і обчислювальних ресурсів системи.

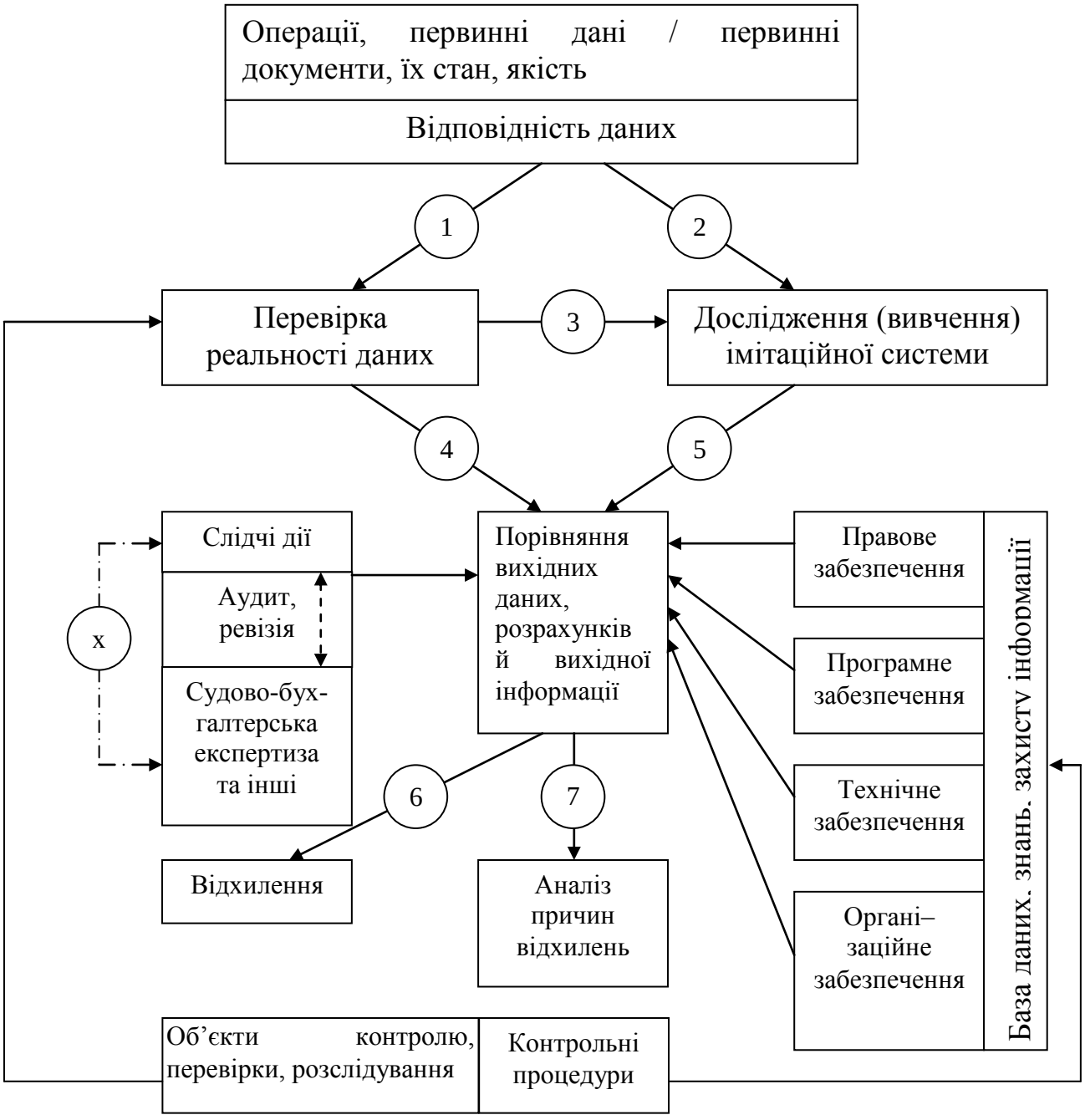
За функціонально-цільовим і прикладним призначенням існуючі ІС можна розділити на дві групи: загального користування і спеціального призначення.

ІС загального користування призначені для різних сфер застосування незалежно від конкретного змісту даних, оброблюваних у ІС. Засоби, структура та функціональні можливості таких ІС виявляються однаковими для багатьох випадків застосування та забезпечують широкий діапазон послуг.

ІС спеціального призначення використовуються з метою рішення задач у визначеній предметній чи відомчій області.

При проектуванні й аналізі ІС істотне значення має топологічна структура ІС, тобто схематично представлені дані про безліч фізичних елементів системи, їхньому розподілі та зв'язках.

Рис. 3.1. Загальна послідовність перевірки стану цілісності комп'ютерної інформації[18]



Примітка: для спрямованості перевірки визначеність (послідовність) дій:

а) установлена;

б) не установлена (передбачається постійна дія, використання);

в) при необхідності (x – умовний розрив);

г) використання матеріалів, ознайомлення з ними.

[18] Лазуренко В.И., Филипенко Т.В. Правовое обеспечение экономической безопасности предприятий. Научно-практические рекомендации. – Донецк: ДЮИ МВД при ДонНУ, 2004. – С. 73.

Можна виділити три ієрархічних класи автоматизованих систем, вимоги до системи захисту яких істотно розрізняються.

Клас 1 – одномашинний однокористувальницький комплекс, що обробляє інформацію однієї чи декількох категорій конфіденційності.

Суттєві особливості:

- у кожен момент часу з комплексом може працювати один користувач, хоча в загальному випадку допущених до роботи користувачів може бути більше, але вони усі мають однакове право доступу до інформації;
- використані технічні засоби (носії інформації та засоби їх застосування) з погляду захищеності відносяться до однієї категорії.

Наприклад, автономна персональна ЕОМ чи локальна робоча станція (ЛРС), доступ до якої контролюється з використанням організаційних заходів.

Клас 2 – локалізований багатомашинний багатокористувальницький комплекс, що обробляє інформацію різних категорій конфіденційності. Істотна відмінність від попереднього класу – наявність користувачів з різними правами доступу до ресурсів і розходження використовуваних технічних засобів захисту. Наприклад, локальна інформаційно-обчислювальна мережа (ЛІОМ).

Клас 3 – розподілений багатомашинний багатокористувальницький комплекс, що обробляє інформацію різних категорій конфіденційності.

Суттєва відмінність від попереднього класу - необхідність передачі інформації через незахищене зовнішнє середовище чи у загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Наприклад, глобальна мережа чи територіально розподілена інформаційно-обчислювальна мережа (РІОМ)

Під лінейно-розподіленою системою мається на увазі персональна ЕОМ за умови, що вона не підключена до каналів передачі даних. Основою сучасних ІС, як правило, є територіально розподілені комп'ютерні системи (обчислювальні мережі) інтенсивно взаємодіючі. Основу апаратних (технічних) засобів таких систем складають ЕОМ (групи ЕОМ), периферійні, допоміжні пристрої та засоби зв'язку, що сполучаються з ЕОМ. Склад програмних засобів

визначається можливостями ЕОМ і характером задач, розв’язуваних при обробці інформації.

З безлічі компонентів ІС розглянемо наступні об’єкти, що у свою чергу можуть бути розбиті на відповідні складові елементи:

- локальна мережа;
- канали та засоби зв’язку;
- вузли комутації;
- умовний кабінет керівника (або будь-яке інше приміщення, де для обробки інформації використовуються різні технічні засоби);
- робоче місце вилученого (легального) користувача системи;
- робоче місце стороннього користувача (потенційного зловмисника);
- носії інформації (магнітні, оптичні й ін.);
- друкуюча чи розмножувальна техніка;
- окремі ПК і робочі станції (термінали);
- користувачі (звичайні люди).

Основу технічних засобів ІС складає звичайно ЕОМ високої продуктивності. Комплекс засобів збору та видачі інформації виконує функції зв’язку та спілкування між ІС і зовнішнім середовищем – окремими користувачами, технологічними процесами, іншими ІС і т.д.

Зв’язок і передачу інформації в ІС забезпечує пристрій комутації (комутаційний центр).

Визначальне значення для організації ефективного функціонування ІС має її програмне забезпечення.

Для формування повного представлення про **системи захисту** інформації доцільно розглянути **їхні основні складові**, а саме:

- законодавча, нормативно-методична та наукова база;
- структура та задачі органів (підрозділів), що здійснюють комплексний захист інформації;
- організаційно-технічні та режимні міри;

- програмно-технічні методи та засоби захисту інформації.

Нормативні документи, що визначають порядок захисту ІС повинні задовольняти наступним вимогам:

- відповідати структурі, цілям і задачам ІС;
- описувати загальну програму забезпечення безпеки мережі, включаючи питання експлуатації і удосконалення;
- перелічувати можливі погрози інформації та канали її витоку, результати оцінки небезпек і захисні міри, що рекомендуються;
- визначати відповідальних за впровадження й експлуатацію всіх засобів захисту;
- визначати права й обов'язки користувачів, причому таким способом, щоб цей документ можна було використовувати в суді при порушенні правил безпеки.

Перш ніж приступити до розробки документів, що визначають порядок захисту інформації, потрібно провести оцінку загроз, визначити інформаційні ресурси, що доцільно захищати в першу чергу, подумати, що необхідно при забезпеченні їхньої безпеки. Правила повинні ґрунтуватися на здоровому глузді.

Доцільно звернути увагу на наступні питання:

- приналежність інформації (про інформацію зобов'язаний піклуватися той, кому вона належить);
- визначення важливості інформації (поки не визначена значимість інформації, не слід очікувати проявів належного відношення до неї);
- значення таємності;
- як користувачі хотіли б захищати таємність інформації? Чи потрібна вона їм узагалі? Якщо право на зберігання таємниці буде визнано у вашій організації, то чи може вона виробити такі правила, що забезпечували б права користувачів на захист інформації?

Для організації та забезпечення ефективного функціонування СЗІ повинні бути розроблені документи, що визначають порядок і правила забезпечення

безпеки інформації при її обробці в ІС, а також документи, що визначають права й обов'язки користувачів при роботі з електронними документами юридичного характеру (договір про організацію обміну електронними документами).

Організаційно-технічні та режимні заходи.

До таких заходів захисту можна віднести організаційно-технічні й організаційно-правові заходи, здійснювані в процесі створення й експлуатації системи обробки та передачі даних фірмі чи банку з метою забезпечення захисту інформації.

Наскільки важливі організаційно-режимні заходи в загальному арсеналі засобів захисту, говорить вже хоча б той факт, що жодна ІС не може функціонувати без участі обслуговуючого персоналу. Крім того, організаційно-режимні заходи охоплюють усі структурні елементи системи захисту на всіх етапах їхнього життєвого циклу: будівництво приміщень, проектування системи, монтаж і налагодження устаткування, іспити та перевірка в експлуатації апаратури, оргтехніки, засобів обробки та передачі даних.

З одного боку, ці міри повинні бути спрямовані на забезпечення правильності функціонування механізмів захисту та виконуватися адміністратором безпеки системи. З іншого боку, керівництво фірми повинне регламентувати правила обробки та захисту інформації, а також установити міру відповідальності за порушення цих правил.

Організаційно-режимні заходи захисту базуються на законодавчих і нормативних документах з безпеки інформації.

Вони повинні охоплювати всі основні шляхи збереження інформаційних ресурсів:

- обмеження фізичного доступу до об'єктів обробки та збереження інформації та реалізацію режимних мір;
- обмеження можливості перехоплення інформації внаслідок існування електромагнітного поля;
- обмеження доступу до інформаційних ресурсів і інших елементів системи

обробки даних шляхом установлення правил розмежування доступу, криптографічне закриття каналів передачі даних, виявлення та знищення «закладок»;

- створення твердих копій, важливих з погляду втрати масивів даних;
- проведення профілактичних чи інших мір від упровадження «вірусів»;
- внесення необхідних змін і доповнень в усі організаційно-розпорядницькі документи (положення про підрозділи, обов'язок посадових осіб, інструкції користувачів системи і т.п.) з питань забезпечення безпеки програмно-інформаційних ресурсів ІС і дії у випадку виникнення кризових ситуацій;
- оформлення юридичних документів (договору, наказів і розпоряджень керівництва організації) з питань регламентації відносин з користувачами (клієнтами), що працюють в автоматизованій системі, між учасниками інформаційного обміну та третьою стороною (арбітраж, третейський суд) про правила розгляду суперечок, пов'язаних із застосуванням електронного підпису;
- створення науково-технічних і методологічних основ захисту ІС;
- виключення можливості таємного проникнення в приміщення, установки апаратури, що прослуховує і т.п.;
- перевірка та сертифікація використаних у ІС технічних і програмних засобів на предмет визначення заходів щодо їхнього захисту від витоку по каналах побічних електромагнітних випромінювань і наведень;
- визначення порядку призначення, зміни, затвердження та надання конкретним посадовим особам необхідних повноважень з доступу до ресурсів системи;
- розробка правил керування доступом до ресурсів системи, визначення переліку задач, розв'язуваних структурними підрозділами організації з використанням ІС, а також використаних при їхньому рішенні режимів обробки та доступу до даних;
- визначення переліку файлів і баз даних, що містять зведення, що

складають комерційну та службову таємницю, а також вимоги до рівнів їхньої захищеності від несанкціонованого доступу при передачі, збереженні й обробці в ІС;

- виявлення найбільш ймовірних загроз для даної ІС, виявлення уразливих місць процесу обробки інформації та каналів доступу до неї;
- оцінка можливого збитку, викликаного порушенням безпеки інформації, розробка адекватних вимог з основних напрямків захисту;
- організація надійного перепускного режиму;
- визначення порядку обліку, видачі, використання та збереження зйомних магнітних носіїв інформації, що містять еталонні чи резервні копії програм і масивів інформації, архівні дані і т.п.;
- організація обліку, збереження, використання та знищення документів і носіїв із закритою інформацією;
- організація та контроль за дотриманням усіма посадовими особами вимог по забезпеченню безпеки обробки інформації;
- визначення переліку необхідних заходів із забезпечення безупинної роботи ІС у критичних ситуаціях, що виникають у результаті несанкціонованого доступу, збоїв і відмовлень СВТ, помилок у програмах і діях персоналу, стихійних лих і т.п.;
- контроль функціонування та керування використовуваними засобами захисту;
- явний і прихований контроль за роботою персоналу системи;
- контроль за реалізацією обраних мір захисту в процесі проектування, розробки, введення в експлуатацію і функціонування ІС;
- періодичний аналіз стану й оцінка ефективності мір захисту інформації;
- розподіл реквізитів розмежування доступу (паролів, ключів шифрування і т.п.);
- аналіз системних журналів, вживання заходів по виявлених порушеннях правил роботи;

- складання правил розмежування доступу користувачів до інформації;
- періодичне, з залученням сторонніх фахівців, здійснення аналізу стану й оцінки ефективності мір і застосованих засобів захисту. На основі отриманої від такого аналізу інформації вживати необхідних заходів з удосконалення системи захисту;
- розгляд і затвердження всіх змін в устаткуванні ІС, перевірка їх на задоволення вимогам захисту, документальне відображення змін і т.п.;
- перевірка прийнятих на роботу, навчання їх правилам роботи з інформацією, ознайомлення з мірами відповідальності за порушення правил захисту, навчання, створення умов, при яких персоналу було б невигідно порушувати свої обов'язки.

Захищеною називається ІС, у якій реалізовані механізми виконання правил, що задовольняють встановленому на основі аналізу загроз переліку вимог по захисту інформації та компонентів цієї ІС. При цьому механізми виконання зазначених правил найчастіше реалізуються у вигляді **системи захисту інформації (СЗІ).**

Під СЗІ розуміється сукупність механізмів захисту, що реалізують встановлені правила, що задовольняють зазначеним вимогам.

Системи захисту інформації являють собою діючі в єдиній сукупності законодавчі, організаційні, технічні й інші засоби, що забезпечують захист важливої інформації від усіх виявлених загроз і можливих каналів витоку.

За сучасних умов, спостерігається цілеспрямований усебічний вплив на інформаційні ресурси, тому в складі ІС необхідно передбачити комплексну систему захисту інформації, у яку повинні бути включені:

- структурні органи (з визначеною ієрархією), що здійснюють розробку нормативних і керівних документів по забезпеченню захисту інформації і контроль їх виконання;
- сукупність різних методів (фізичних, організаційних, криптографічних і ін.) і засобів (програмних, апаратних, апаратно-програмних), що здійснюють всеосяжний захист апаратного та

програмного забезпечення інформаційних систем, а також безпеку та контроль самих систем захисту.

Недоліки у захисті можуть бути значною мірою усунуті, якщо при проектуванні враховувати наступні **основні принципи побудови системи захисту:**

1.Простота механізму захисту.

2.Сталість захисту.

3.Всеосяжність контролю.

4.Нетаємність.

5.Ідентифікація.

6.Поділ повноважень.

7.Мінімізація повноважень.

8. Надійність.

9. Максимальна відособленість механізму.

10. Захист пам’яті.

11. Зручність для користувачів.

12. Контроль доступу на підставі авторизації користувача по його фізичному ключу й особистому PIN-коду.

13. Авторизація.

14. Звітність.

15. Виконання тільки тих команд операційної системи, що не можуть пошкодити операційне середовище та результат контролю попередньої аутентифікації.

16. Наявність механізму захисту інформації, що циркулює в локальній і розподіленій мережі. Даний механізм захищає від атак несанкціонованих і несумлінних користувачів:

- несанкціоноване читання інформації;
- модифікація, що зберігається та циркулює в мережі інформації;
- нав’язування інформації;
- відмовлення від авторства переданої інформації.

17. Системний підхід до захисту інформації.

18. Можливість нарощування.

19. Комплексний підхід.

20. Адекватність.

21. Мінімізація привілеїв у доступі.

22. Повнота контролю.

23. Караність порушень.

24. Економічність механізму.

25. Системність.

26. Спеціалізованість.

27. Неформальність.

28. Гнучкість системи захисту.

29. Безперервність захисту.

Розвиток підходів до побудови системи захисту інформації відбувається під впливом перерахованих принципів.

5. Програмні та апаратно-технічні заходи забезпечення захисту інформації.

Раніше не усвідомлювалося, що користувачі інформаційних систем можуть самі припускати різні ненавмисні помилки та ставати предметом різних зловживань. Сьогодні, коли така велика концентрація масивів інформації, відсутність елементарного контролю за її збереженням та відносно низький рівень надійності технічних засобів викликають тривогу.

Механізми захисту процесів, процедур і програм обробки даних повинні контролювати доступ до об'єктів інформаційних систем, особливо інформаційних. Діапазон вимог до цих механізмів захисту має на увазі з одного боку, повну ізоляцію виконуваної програми від інших програм, а з іншого боку – дозвіл їхньої взаємодії та спільного використання.

Програмне забезпечення стає джерелом уразливості сучасних інформаційних систем, що породжує нову проблему – забезпечення технологічної безпеки програмних засобів. Небезпека порушення функцій програмного забезпечення складних обчислювальних систем пов'язана з можливістю внесення в програмні засоби навмисних дефектів, іменованих «програмними закладками», що використовуються з метою цілеспрямованого прихованого впливу на технічну чи інформаційну систему.

Шкідливі комп'ютерні програми та їх негативні наслідки.

Існують шкідливі програми від яких, як і від вірусів, необхідно з особливою старанністю очищати свої комп'ютерні системи. Це так називані **«програмні закладки»**, що можуть виконувати хоча б одну з перерахованих нижче дій:

- вносити довільні перекручування в коди програм, що знаходяться в оперативній пам'яті комп'ютера (програмна закладка першого типу);
- переносити фрагменти інформації з одних областей оперативної чи зовнішньої пам'яті комп'ютера в інші (програмна закладка другого типу);

- спотворювати виведену на зовнішні комп’ютерні пристрої чи в канал зв’язку інформацію, отриману в результаті роботи інших програм (програмна закладка третього типу).

Програмні закладки можна класифікувати ще й з методу їхнього впровадження в комп’ютерну систему:

- програмно-апаратні закладки, асоційовані з апаратними засобами комп’ютера (їхнім середовищем, як правило, є BIOS – набір програм, записаних у вигляді машинного коду в постійному запам’ятовуючому пристрої – ПЗУ);
- завантажувальні закладки, асоційовані з програмами початкового завантаження, що розташовуються в завантажувальних секторах (з цих секторів у процесі виконання початкового завантаження комп’ютер зчитує програму, що бере на себе керування для наступного завантаження самої операційної системи);
- драйверні закладки, асоційовані з драйверами (файлами, у яких міститься інформація, необхідна операційній системі для керування підключеними до комп’ютера периферійними пристроями);
- прикладні закладки, асоційовані з прикладним програмним забезпеченням загального призначення (текстові редактори, утиліти, антивірусні монітори та програмні оболонки);
- закладки асоційовані з програмними модулями, що виконуються, утримують код цієї закладки (найчастіше ці модулі являють собою пакетні файли, тобто файли, що складаються з команд операційної системи, виконуваних одна за одною, якби їх набирали на клавіатурі комп’ютера);
- закладки-імітатори, інтерфейс яких збігається з інтерфейсом деяких службових програм, що вимагають уведення конфіденційної інформації (паролів, криптографічних ключів, номерів кредитних карток);

- замасковані закладки, що маскуються під програмні засоби оптимізації роботи комп'ютера (файлові архіватори, дискові відеофрагментатори) чи під програми ігрового та розважального призначення.

Існують три основні групи деструктивних дій, що можуть здійснюватися програмними закладками:

- копіювання інформації користувача комп'ютерної системи (паролів, криптографічних ключів, кодів доступу, конфіденційних електронних документів), що знаходиться в оперативній чи зовнішній пам'яті цієї системи або в пам'яті іншої комп'ютерної системи, підключеної до неї через локальну чи глобальну комп'ютерну мережу;
- зміна алгоритмів функціонування системних, прикладних і службових програм (наприклад, внесення змін у програму розмежування доступу може привести до того, що вона дозволить вхід у систему усім без винятку користувачам поза залежністю від правильності введеного пароля);
- нав'язування визначених режимів роботи (наприклад, блокування запису на диск при видаленні інформації, при цьому інформація, яку потрібно видалити, не знищується та може бути згодом скопійована хакером).

У всіх програмних закладок (незалежно від методу їхнього впровадження в комп'ютерну систему, терміну їхнього перебування в оперативній пам'яті та призначення) **є одна важлива загальна риса**: вони обов'язково виконують операцію запису в оперативну чи зовнішню пам'ять системи. **При відсутності даної операції ніякого негативного впливу програмна закладка зробити не може.** Зрозуміло, що з метою цілеспрямованого впливу вона повинна виконувати й операцію читання, інакше в ній може бути реалізована тільки функція руйнування (наприклад, видалення чи заміна інформації у визначених секторах твердого диску).

Моделі впливу програмних закладок на комп'ютери:

Перехоплення – програмна закладка впроваджується в постійний запам'ятовуючий пристрій, системне чи прикладне програмне забезпечення та

зберігає всю чи обрану інформацію, що вводиться з зовнішніх пристроїв комп'ютерної системи чи виведену на ці пристрої, у схованій області пам'яті локальної чи віддаленої комп'ютерної системи. Ця модель може бути ефективно використана при атаці на захищену операційну систему Windows NT.

Перекручування – програмна закладка змінює інформацію, що записується в пам'ять комп'ютерної системи в результаті роботи програм, або допускає чи ініціює виникнення помилкових ситуацій у комп'ютерній системі.

Задача захисту від програмних закладок може розглядатися в трьох принципово різних варіантах:

- не допустити впровадження програмної закладки в комп'ютерну систему;
- виявити впроваджену програмну закладку;
- вилучити впроваджену програмну закладку.

Універсальним засобом захисту від упровадження програмних закладок є створення **ізольованого** комп'ютера. Комп'ютер називається ізольованим, якщо виконані наступні умови:

- у ньому встановлена система BIOS, не утримуюча програмних закладок;
- операційна система перевірена на наявність у ній закладок;
- достеменно встановлена незмінність BIOS і операційної системи для даного сеансу;
- на комп'ютері не запускалося та не запускається ніяких інших програм, крім вже перевірених в минулому на присутність у них закладок;
- виключено запуск перевірених програм у будь-яких інших умовах, крім перерахованих вище, тобто поза ізольованим комп'ютером.

Використання програмних засобів захисту інформації.

Програмні засоби захисту – це сукупність алгоритмів і програм, що забезпечують розмежування доступу та неможливість несанкціонованого використання інформації.

Підсистема захисту від несанкціонованого доступу (НСД) – використовується з метою забезпечення аутентифікації користувачів ІС, контролю їхнього доступу до ресурсів ІС і розмежування повноважень, обліку дій користувачів і запобігання несанкціонованого доступу до робочих станцій. Підсистема захисту від НСД у значній мірі використовує функції захисту штатного ПЗ.

Функції підсистеми складаються з:

- ідентифікації і аутентифікації користувача (суб'єкта) при вході до системи;
- ідентифікації ресурсів (об'єктів);
- розмежуванні доступу користувачів до ресурсів у рамках виборчої чи мандатної політики безпеки;
- реєстрації;
- запобіганні повторного використання об'єктів.

Автентифікація користувачів.

Ідентифікація – засіб визначення:

а) тотожності особи за сукупністю її загальних та окремих даних;

б) повноважень користувача системи за допомогою пароля.

Після ідентифікації звичайно здійснюється автентифікація.

Під автентифікацією розуміється шлях встановлення вірогідності інформації, пред'явленої користувачем (суб'єктом) у разі звернення його до системи та відкриття йому доступу, якщо він має на це право.

Під авторизацією (санкціонуванням) мається на увазі керування рівнями та засобами доступу до різних об'єктів та ресурсів системи залежно від ідентифікатора та пароля користувача.

Метод парольного захисту та його модифікації.

Законність запиту користувача визначається згідно до паролю, що представляє собою, як правило, рядок знаків. Метод паролів вважається досить слабким, тому що пароль може стати об'єктом розкрадання, перехоплення,

перебору, угадування. Однак простота методу стимулює пошук шляхів його посилення.

З метою підвищення ефективності парольного захисту рекомендується:

- вибирати пароль довжиною більше 6 символів, уникаючи розповсюджених, слів, що легко угадуються, імен, дат і т.п.;
- використовувати спеціальні символи;
- паролі, що зберігаються на сервері, шифрувати за допомогою однобічної функції;
- файл паролів розміщати в області, що особливо захищається, запам'ятовуючому пристрої ЕОМ, закритої для читання користувачами;
- границі між суміжними паролями маскуються;
- коментарі файлу паролів варто зберігати окремо від файлу;
- періодично змінювати паролі;
- передбачити можливість примусової зміни паролів з боку системи через визначений проміжок часу;
- використовувати кілька користувальницьких паролів: наприклад, власне пароль, персональний ідентифікатор, пароль для блокування/розблокування апаратури при короткочасній відсутності і т.п.

Криптографічні методи забезпечення інформаційної безпеки.

Під **криптологією** (від грецького kruptos – таємний і logos – повідомлення) розуміється наука про безпеку (таємність) зв'язку.

Криптологія поділяється на дві частини: криптографію (шифрування) та криптоаналіз. **Криптограф** намагається знайти методи забезпечення таємності й автентичності (дійсності) повідомлень. **Криптоаналітик** намагається виконати зворотну задачу: розкрити шифротекст чи підробити його так, щоб він був прийнятий як справжній.

Криптографічними засобами захисту називаються спеціальні методи та засоби перетворення інформації, у результаті яких маскується її зміст.

Основними видами криптографічного закриття є шифрування та кодування даних, що захищаються. При цьому **шифрування** – такий вид

закриття, при якому самостійному перетворенню піддається кожен символ даних, що закривається*;* при **кодуванні** дані, що захищаються, поділяються на блоки, що мають значення, і кожен такий блок заміняється цифровим, буквеним чи комбінованим кодом.

Основними методами є шифрування, цифровий підпис і імітозахист повідомлень.

Шифрування повідомлень дозволяє перетворити вихідне повідомлення (відкритий текст) до виду, що не читається; результат перетворення називають шифротекстом.

Цифровий підпис забезпечує:

- аутентифікацію джерела даних;
- цілісність повідомлення;
- юридичну значимість повідомлення.

Імітозахист повідомлень складається у формуванні контрольної суми (імітовставки, коду автентифікації повідомлення) по криптоалгоритму, що додається до повідомлення. **Імітозахист забезпечує** – цілісність повідомлення у відповідності з властивостями контрольної суми.

Основні проблеми тестування програмного забезпечення:

- відсутність загальноприйнятої номенклатури показників якості;
- неможливість проведення натурних іспитів програм на всій безлічі вихідних даних;
- низька вірогідність і недостатність інформації для одержання оцінок показників якості та недоліки засобів виміру метрик програм, відсутність обґрунтованих вимог у числовому вираженні при перевірці;
- відсутність можливості інтерпретації одержаних метрик і оцінок показників якості програм.

У даний час з метою виявлення «програмних закладок» і «програмних дефектів» можуть бути запропоновані тільки дорогі методи контролю вихідних текстів програм у сполученні з методами математичного моделювання процесів функціонування інформаційної системи.

Технічні методи та засоби захисту інформації.

Сутність апаратного чи схемного захисту полягає в тому, що в пристроях ЕОМ та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації, наприклад схеми контролю інформації на достовірність, що здійснює контроль за правильністю передачі інформації між різними пристроями ЕОМ, а також екранують пристрої, що локалізують електромагнітні випромінювання.

Лише комплексне використання різних захисних заходів може забезпечити надійний захист, тому що кожен прийом чи метод має свої слабкі та сильні сторони.

6. Правове забезпечення захисту інформації

6.1. Основи правового регулювання захисту інформації в Україні

З метою з'ясування сутності захисту інформації в автоматизованих системах, як правового явища (як інституції права), слід визначити його місце в системі права та правознавства.

З точки зору теорії критичної маси норм права в теорії соціальних систем, на межі галузей права виник синтетичний міжгалузевий комплексний гіперінститут права – інформаційне право. Системоутворюючим цього інституту права в нашій країні виступає Закон України від 2 жовтня 1992 року «Про інформацію».[19]

Однією із складових інформаційного права є субінститут права (підінститут, підсистема, система другого порядку) – захист інформації в автоматизованих системах. Системоутворюючим якого є Закон України від 5 липня 1994 року «Про захист інформації в автоматизованих системах».[20] Метою цього Закону є встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України та 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.

З метою з'ясування сутності захисту інформації в автоматизованих системах, як інституції правовідносин, визначимося у провідних її категоріях. Деякі з них подаються у законодавстві. Серед них – визначення категорії

---

[19] Про інформацію: Закон України від 02.10.92 №2651-XII //Відомості Верховної Ради України. – 1992. – № 48. – ст. 650.

[20] Про захист інформації в автоматизованих системах: Закон України від 05.07.94 №80/94-ВР // Відомості Верховної Ради України. – 1994. – №31 – ст.286.

«захист інформації» (ч. 4 ст. 1 Закону України «Про захист інформації в автоматизованих системах»).

Захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованій системі та осіб, які користуються інформацією.

У Законі також подається визначення ряду категорій, які можна розглядати як об’єкти суспільних інформаційних відносин:

- **автоматизована система** (АС) – система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв’язку), а також методи та процедури, програмне забезпечення;
- **інформація в АС –** сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення;
- **обробка інформації –** вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюється за допомогою технічних і програмних засобів, включаючи обмін каналами передачі даних.

Захист інформації – це суспільні відносини щодо визначення, створення та підтримання в належному стані комплексної системи організаційно-управлінських, організаційно-технічних та організаційно-правових заходів та засобів, які здійснюються відповідними суб’єктами інформаційних відносин для запобігання заподіянню і усуненню шкоди інтересам власника інформації чи автоматизованої системи та правомірних користувачів інформацією.

Автоматизована (комп'ютерна) інформаційна система (АС) – це комплекс електронно-обчислювальних технічних і програмно-математичних засобів, за допомогою яких здійснюється автоматизована обробка та передача інформації, до складу якої також входять методи та процедури забезпечення функціонування цієї системи в конкретно визначеній (предметній) соціальній сфері.

АС є підсистемою (системою другого порядку) в конкретно визначеній (предметній) соціальній системі (організації, системі першого порядку), її суспільних інформаційних відносин.

Інформація в АС – відповідним чином упорядкована у результаті аналітико-синтетичної обробки множини даних, відомостей, знань, у тому числі – комп'ютерних програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення.

Обробка інформації – відповідним чином упорядкована множина операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою комп'ютерних (електронно-обчислювальних) технічних і програмно-математичних засобів (комп'ютерних програм), включаючи обмін каналами передачі даних (зв'язку).

Важливою складовою захисту інформації в АС є з'ясування змісту категорій «загроза інформаційній безпеці» та «способи (види) заподіяння шкоди». З метою з'ясування їх сутності зазначимо, що ці категорії розглядаються нами як ідентичні. Виходячи зі змісту Закону України «Про захист інформації в автоматизованих системах» можна надати таке визначення соціогенних загроз інформаційній безпеці в умовах застосування АС:

- **порушення роботи АС –** дії або обставини, які призводять до спотворення процесу обробки інформації;
- **несанкціонований доступ –** доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу;
- **підроблення інформації –** навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС;
- **блокування інформації –** дії, наслідком яких є припинення доступу до інформації;
- **витік інформації –** результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

- **втрата інформації –** результат дії, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.

У ст. 5 Закону України «Про захист інформації в автоматизованих системах» вживаються такі категорії, які можна вважати також загрозами інформаційній безпеці:

- навмисні чи ненавмисні втрати інформації;
- знищення інформації;
- спотворення інформації;
- інші неправомірні дії.

6.2. Відомчі нормативні акти з питань захисту інформації

У відповідності з законодавством уповноважений Кабінетом Міністрів України орган виконавчої влади здійснює управління захистом інформації шляхом:

- проведення єдиної технічної політики щодо захисту інформації;
- розроблення концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій щодо захисту інформації в АС;
- затвердження порядку організації, функціонування та контролю за виконанням заходів, спрямованих на захист оброблюваної в АС інформації, яка є власністю держави, а також рекомендацій щодо захисту інформації – власності юридичних та фізичних осіб;
- організації випробувань і сертифікації засобів захисту інформації в АС, в якій здійснюється обробка інформації, яка є власністю держави;
- створення відповідних структур для захисту інформації в АС;
- проведення атестації сертифікаційних органів, центрів і лабораторій, видачі ліцензії на право проведення сервісних робіт в галузі захисту інформації в АС;

- здійснення контролю захищеності оброблюваної в АС інформації, яка є власністю держави;
- визначення порядку доступу осіб і організацій зарубіжних держав до інформації в АС, яка є власністю держави, або до інформації – власності фізичних та юридичних осіб, щодо поширення і використання якої державою встановлено обмеження.

На законодавчому рівні визначається, що міністерства, відомства та інші центральні органи державної виконавчої влади забезпечують вирішення питань захисту інформації в АС у межах своїх повноважень (ст. 14 Закону України «Про захист інформації в автоматизованих системах»). Зазначене положення повинно знаходити відображення у відповідних нормах Положень міністерств, відомств та інших центральних органів виконавчої влади.

Для здійснення захисту визначаються спеціальні функціональні організаційні структури – служби захисту інформації в АС. Зокрема у державних установах та організаціях можуть створюватись підрозділи, служби, які організують роботу, пов’язану із захистом інформації, підтримкою рівня захисту інформації в АС і несуть відповідальність за ефективність захисту інформації відповідно до вимог законодавства (ст. 15 Закону України «Про захист інформації в автоматизованих системах»). Зазначимо, що ця норма носить не імперативний (обов’язковий) характер, а рекомендаційний. Зі змісту цієї норми в поєднанні з іншими нормами Закону «Про захист інформації в автоматизованих системах» випливає, що захист інформації в АС є обов’язковою функцією, проте необов’язково під цю функцію може створюватися окрема функціональна організаційна структура. Ця функція може бути складовою іншої організаційної структури, тобто виконуватися у поєднанні з іншими функціями.

Важливим аспектом організаційних заходів щодо захисту інформації в АС є фінансування робіт. Законодавець визначає загальне положення, щодо фінансування робіт, пов’язаних із захистом інформації, яка обробляється в АС, здійснюється власником АС.

Враховуючи те, що на рівні юридичних норм врегулювати всі відносини щодо захисту інформації в автоматизованих системах неможливо, в нормативних актах спеціально визначаються основні принципи, за якими формується та проводиться державна політика України у сфері захисту інформації.

З аналізу нормативно-правових актів України випливає, що державна політика у сфері захисту інформації визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень зазначених в законодавстві та положень Концепції технічного захисту інформації, а також програм розвитку захисту інформації та окремих проектів.

Основними напрямками державної політики у сфері захисту інформації є:

- нормативно-правове забезпечення;
- удосконалення чинних та розроблення і прийняття нових нормативних документів з питань технічного захисту інформації;
- організаційне забезпечення;
- науково-технічна та виробнича діяльність.

6.3. Особливості застосування нормативних актів з питань захисту інформації у діяльності ОВС

У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності і т. і. Тому Конституція України **забезпечення інформаційної безпеки** відносить **до найважливіших функцій держави.**

З огляду на зазначене, варто зупинитися на одному з найважливіших аспектів забезпечення належного захисту інформаційної безпеки – на координації діяльності державних органів, приватного сектору, громадських організацій та окремих громадян. Згідно зі ст. 17 Конституції України забезпечення інформаційної безпеки – справа всього українського народу.

Одну з найнебезпечніших загроз національній безпеці України в інформаційній сфері становить так звана «комп'ютерна злочинність». Як показують дослідження Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю, рівень загрози буде зростати пропорційно розширенню використання нових інформаційних технологій в управлінні, бізнесі, торгівлі. Загрози можуть бути як зовнішніми, так і внутрішніми. Слід зазначити, що у зв'язку з поширенням використання в Україні глобальної комп'ютерної мережі Інтернет та з приєднанням до міжнародних систем телекомунікацій нових країн, підвищенням інтелектуального рівня зловмисників зовнішня загроза постійно зростатиме.

Через Інтернет хакери мають несанкціонований доступ до комп'ютерної інформації, а для проведення безподаткових фінансових операцій, «відмивання брудних» коштів через електронні банківські системи глобальна мережа створює принципово нові умови, які у повному обсязі використовують кримінальні структури. Тому вже сьогодні необхідною є відповідна координація зусиль щодо забезпечення протидії цьому виду правопорушень.

На сьогодні найгострішою проблемою залишається створення Міжвідомчого центру боротьби з комп'ютерною злочинністю (МЦБКЗ), в якому необхідно організувати контактний пункт для отримання повідомлень про «кіберзлочини» та надання оперативної допомоги жертвам зловмисників, а також організувати лабораторію для проведення комп'ютерних експертиз. Центр може стати місцем для організації семінарів, практикумів у системі підготовки суддів, прокурорів, слідчих. Якщо сьогодні на створення та функціонування МЦБКЗ не буде виділено достатніх фінансово-матеріальних

ресурсів, то у недалекому майбутньому втрати економіки держави від комп'ютерної злочинності виявляться набагато більшими.

6.4. Напрямки вдосконалення нормативно-правової бази з питань захисту інформації

Важливою складовою інформаційного права є формування в ньому вчення про правопорушення у сфері інформаційних відносин щодо захисту інформації на принципі гармонізації норм з галузевими нормами конституційного, адміністративного, цивільного, трудового та кримінального права.

Невизначеність законодавця в цьому напрямку, знайшла відображення у Законах України «Про інформацію», «Про захист інформації в автоматизованих системах» новому чинному Кримінальному кодексі України (2001 р.) – ст.361-363 та деяких інших, де визначено диспозиції правопорушень, але чітко не визначена, а в деяких зовсім відсутня відповідальність за них в адміністративно-правовому, цивільно-правовому та кримінально-правовому аспектах.

У проблематиці вдосконалення нормативно-правової бази з питань захисту інформації особлива увага повинна звертатися на виявлення та дослідження недоліків як вітчизняних, так і зарубіжних правовідносин, їх регулювання для уникнення помилок у правотворчій та правозастосовній діяльності в Україні. Мета досліджень – запобігання негативним для суспільства наслідкам інформатизації та комп'ютеризації, попередження поширенню правопорушень, проступків, злочинів, що вчиняються з використанням сучасних інформаційних технологій. Особливе місце повинно відводитися дослідженню кримінологічних, адміністративно-правових, цивільно-правових, трудових, кримінально-правових та криміналістичних аспектів такого негативного для суспільства явища, як комп'ютерна злочинність.

Один з важливих аспектів є проблематика державного правотворення. Правотворча діяльність найкраще повинна здійснюватися на таких основоположних принципах наукового забезпечення:

- формування концепції інформаційного законодавства України;
- системний та комплексний підходи у вирішенні проблем правотворчості;
- фундаментальне та прикладне теоретичне обґрунтування новацій (понять, категорій тощо);
- узагальнення і використання досвіду зарубіжних країн;
- залучення широкого кола вітчизняних фахівців до розробки проектів законодавчих та підзаконних актів в галузі інформаційного права України.

Звичайно, що національне інформаційне законодавство повинно стати на шлях систематизації через кодифікацію – створення системоутворюючого його кодексу. Цей Кодекс повинен буде розвивати визначені в Конституції України положення інформаційних відносин, в тому числі щодо інформаційної безпеки людини, суспільства, нації, держави. Він повинен:

- об’єднати, гармонізувати та розвивати норми та принципи суспільних відносин, що визначені в законодавстві України;
- враховувати ратифіковані Україною нормативні акти (угоди, конвенції) міжнародного права;
- легалізувати позитивні звичаї в сфері інформаційних відносин та норми суспільної моралі, загальнолюдські цінності, визначені Організацією Об’єднаних Націй в її Статуті, Декларації прав людини та інших загальноприйнятих міждержавних нормативних актах, які сьогодні виступають в ролі стандартів, за якими визначається цивілізованість не тільки окремої країни, але й світового співтовариства в цілому.

Майбутній Кодекс України про інформацію має на меті об’єднати в одному законодавчому акті регулювання провідних суспільних відносин, об’єктом яких є інформація, незалежно від форми, способу чи технології її прояву у суспільних відносинах. Це дозволяє, у разі виникнення необхідності публічно правового урегулювання нових суспільних відносин щодо інформації,

агрегувати юридичні формулювання їх у Кодекс через внесення в нього на рівні законів змін і доповнень без породження нових системоутворюючих законодавчих актів.

6.5. Аналіз зарубіжного досвіду правового забезпечення захисту інформації

За кордоном розробка правових мір боротьби з комп'ютерною злочинністю вже має свою історію. Так наприклад, у США федеральний «комп'ютерний» закон діє вже з 1984 року, у Данії – з липня 1985 року, у Канаді – з грудня 1985 року, у Португалії – з 1982 року. Прийняття відповідних норм карного права здійснене в Німеччині з серпня 1986 року. Ведуться роботи з удосконалення національного законодавства по боротьбі з комп'ютерними злочинами і в інших країнах.

З метою уніфікації національних законодавств 13 вересня 1989 року на засіданні Комітету міністрів Європейської Ради був вироблений список правопорушень, рекомендований країнам-учасницям ЄС для розробки єдиної карної стратегії по розробці законодавства, зв'язаного з комп'ютерними злочинами. У повному обсязі він містить у собі так звані Мінімальний і Необов'язковий списки порушень.

«Мінімальний список порушень» містить вісім видів комп'ютерних злочинів, склад яких визначений у документі, озаглавленому як «Керівництво Інтерполу по комп'ютерній злочинності».

Коротко розглянемо їхній склад.

А. Комп'ютерне шахрайство.

Уведення, зміна чи стирання, ушкодження даних ЕОМ чи програм ЕОМ, чи інше втручання в хід обробки даних, що впливає на результат обробки даних таким чином, що служить причиною економічних утрат чи викликає стан утрати майна іншої людини з наміром незаконного поліпшення економічного

становища для себе чи іншої людини (чи як альтернатива: з наміром до незаконного позбавлення цієї людини його майна).

B. Підробка комп'ютерної інформації.

Несанкціоноване стирання, ушкодження, чи погіршення, придушення даних ЕОМ чи програм ЕОМ, чи інше втручання в хід обробки даних різними способами, чи створення таких умов, що будуть, відповідно до національного закону, складати таке правопорушення, як підробка, у традиційному змісті такого порушення.

C. Ушкодження даних ЕОМ чи програм ЕОМ.

Несанкціоноване стирання, ушкодження, чи погіршення даних ЕОМ чи програм ЕОМ.

D. Комп'ютерний саботаж

Уведення, зміна, стирання, ушкодження даних ЕОМ чи програм ЕОМ, чи втручання в системи ЕОМ з наміром перешкоджати функціонуванню комп'ютера чи системи передачі даних.

E. Несанкціонований доступ.

Несанкціонований доступ до системи ЕОМ через мережу з порушенням засобів захисту.

F. Несанкціоноване перехоплення даних.

Несанкціоноване перехоплення за допомогою технічних засобів зв'язку як у межах комп'ютера чи системи мережі, так і ззовні.

G. Несанкціоноване використання захищених комп'ютерних програм.

Незаконне відтворення чи поширення зв'язків із програмою ЕОМ, що захищена відповідно до закону.

H. Несанкціоноване відтворення схем.

Несанкціоноване відтворення схемних рішень, захищених відповідно до закону про напівпровідникові вироби (програми), чи комерційна експлуатація, чи незаконне імпортування з тією ж метою схеми напівпровідникового виробу як продукту, зробленого з використанням даних схем.

«Необов’язковий список» містить у собі чотири види комп’ютерних злочинів.

A. Зміна даних ЕОМ чи програм ЕОМ.

Незаконна зміна даних ЕОМ чи програм ЕОМ.

B. Комп’ютерне шпигунство.

Придбання з використанням незаконних засобів чи шляхом несанкціонованого розкриття, пересилання чи використання торгових чи комерційних секретів за допомогою подібних методів чи інших незаконних засобів, з тим чи іншим наміром, що наносить економічний збиток людині шляхом доступу до його секретів, чи дозволяють одержати незаконну економічну перевагу для себе чи іншої людини.

C. Недозволене використання ЕОМ.

Використання системи ЕОМ чи комп’ютерної мережі без відповідного дозволу є злочинним, коли воно:

- інкримінується в умовах великого ризику втрат, викликаних невідомою особою, що використовує систему чи наносить шкоду системі її функціонуванню;
- інкримінується невідомій особі, що має намір завдати шкоду, і використовує для цього систему чи особі, яка завдає шкоду системі, її функціонуванню;
- застосовується у випадку, коли губиться інформація за допомогою невідомого автора, що використовував дану систему чи завдав шкоду системі, її функціонуванню.

D. Недозволене використання захищеної програми ЕОМ.

Використання без дозволу захищеної програми ЕОМ чи її незаконне відтворення з наміром виправити програму таким чином, щоб викликати незаконну економічну вигоду для себе чи іншої людини, чи заподіяти шкоду законному власнику даної програми.

У Німецькому карному законодавстві не має статті, що передбачає покарання за здійснення дій, що відповідають пункту «C. Недозволене

використання ЕОМ» «Необов'язкового списку порушень» Європейської Ради. Породження функціональних втрат шляхом несанкціонованого використання мережі передачі даних за рахунок постраждалої сторони не є злочином, якщо злочинний намір полягає в тому, щоб викликати утрату власної переваги.

З огляду на важливість гармонізації законодавства держав – членів Європейської Ради, у Нідерландах був створений національний комітет у складі представників уряду та ділових кіл, що провів дослідження масштабів і видів комп'ютерних злочинів, а також розглянув правові аспекти боротьби з цим видом злочинності. Як відзначалося в звіті комітету виду комп'ютерних злочинів, що фігурують у переліку Європейської Ради лише частково підпадають під існуюче законодавство Нідерландів. Комп'ютерне шахрайство, підробки, копіювання програм власне кажучи є лише різновидом злочинів, що підпадають під статті кримінального кодексу. Вивід з ладу комп'ютерної системи також вважається кримінально карним діянням. Однак, за винятком деяких випадків, по існуючому зараз законодавству акти зловживання, що мають метою перешкоджати функціонуванню комп'ютерної системи чи негативним образом уплинути на цілісність збереженої інформації, поки ще не переслідується законом.

Законопроект про комп'ютерну злочинність, винесений на розгляд нідерландського парламенту, містить ряд нових статей, що гарантують судове переслідування та більш суворі санкції. При дослідженні було вивчено кілька реальних справ із прив'язкою до чинного законодавства, що привело до наступних висновків.

У відповідності зі ст. 350 навмисне ушкодження комп'ютерних даних буде розглядатися як карний злочин. Це положення буде поширюватися і на збиток, заподіюваний комп'ютерним вірусом. Однак у зв'язку з тим, що способи поширення вірусів специфічні і тимчасові відрізки між уведенням вірусу і його впливом на систему дуже розтягнуті, буде важко довести навмисність з боку зловмисника нанести утрату визначеному комп'ютеру чи даним.

У відповідності зі ст. 138 несанкціонований доступ до чиєїсь комп'ютерної системи також буде трактуватися як карне діяння, однак у ділових колах дотримуються думки, що стаття повинна «працювати» тільки в тих випадках, коли має місце порушення мір безпеки.

Формулювання міри покарання, передбаченої в ст. 232 за підробку чи незаконне використання чеків, кредитних карток чи інших цінних паперів, може утруднити одержання доказів здійснення такого злочину. На відміну від статті 225 у новій статті відсутня належна чіткість визначення намірів зловмисника.

Ні в існуючих законах, ні в розглянутому законопроекті виробництво і збереження комп'ютерних програм, що є явно підробленими та призначених з метою використання сторонніми особами, не вважається кримінально карними актами. Таким чином, найчастіше буде неможливо довести зв'язок між правопорушником і впливом використовуваної їм програми на комп'ютерну систему потерпілого. Більш того, по існуючому положенню, судові влади не мають повноважень як на вилучення, так і знищення таких програм.

Комп'ютерне законодавство Сполучених Штатів Америки багато в чому відрізняється від аналогічного законодавства країн-членів Європейської Ради. Розробкою комп'ютерних правових норм у США займаються три галузі державної влади – законодавча, виконавча і судова.

Законодавча влада, що включає в себе конгрес і законодавчі установи п'ятидесятьох штатів США, створює в основному правові акти декларативного характеру. Наприклад, конгрес може прийняти законопроект про необхідність забезпечення безпеки конфіденційної інформації, що міститься в базах даних державних установ.

Виконавча влада, до якої відноситься адміністрація президента і відомства, розробляє та видає розпорядження з виконання законів, прийнятих легіслатурами. Наприклад, Міністерство торгівлі може випустити директиву, що встановлює критерії для визначення конфіденційності економічної інформації та вимоги до її захисту.

Судова влада забезпечує виконання прийнятих законів, проводить слухання по спірних питаннях, розглядає апеляції, трактує значення підзаконних актів, розробляє у виняткових випадках додаткові розпорядження. Після того як рішення прийняті (а в деяких випадках задоволені апеляції), вони стають обов'язковими в юридично схожих ситуаціях з прецеденту.

Федеральний уряд керується наступними цілями в області боротьби з комп'ютерними злочинами:

- моніторинг масштабу проблеми;
- установа програм підготовки персоналу;
- сприяння ефективному співробітництву урядових агентств і управлінь;
- розробка плану міжнародного реагування;
- висування законодавчих припущень.

В даний час у юриспруденції США немає загального поняття комп'ютерного злочину. Однією з причин цього є швидка зміна технології. Наприклад, у 1979 році у виданому Міністерством юстиції США Кримінальному Кодексі поняття комп'ютерного злочину поділялося на три категорії:

- Зловживання комп'ютером – ряд заходів з використанням комп'ютера з метою отримування вигоди, що нанесли чи могли нанести збиток.
- Пряме незаконне використання комп'ютерів у здійсненні злочину.
- Будь-яка незаконна дія, для успішного здійснення якої необхідне знання комп'ютерної технології.

Однак значне збільшення числа терміналів і впровадження нових технологій за останнім часом позбавили дані тези визначеності. Очевидно, що будь-який розвиток комп'ютерної технології повинний адекватно відображатися законодавством.

Таким чином, навіть короткий і далеко не повний огляд законодавства деяких ведучих країн у сфері боротьби з комп'ютерною злочинністю показує всю глибину і складність проблем, що нам готує науково-технічний прогрес.

7. Криміналістична характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку – це вчинені, як правило, умисно або з необережності суспільно небезпечні діяння (дії або бездіяльність), що посягають на відносини у сфері обробки інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах і мережах електрозв'язку, права власності фізичних та юридичних осіб на інформацію і доступу до неї.

Суб'єктами відносин, пов'язаних з обробкою інформації в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, є: 1) власники інформації чи уповноважені ними особи; 2) власники технічних засобів автоматизованої обробки чи уповноважені ними особи; 3) користувачі інформації; 4) користувачі технічних засобів автоматизованої обробки.

Родовим об'єктом злочинів, передбачених розділом XVI Особливої частини КК України, є врегульовані законом суспільні відносини забезпечення безпеки автоматизованої обробки інформації.

Додатковими обов'язковими об'єктами вказаних злочинів є відносини власності на інформацію, яка обробляється в електронно-обчислювальних машинах (компёютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, а також право користувачів на доступ до зазначеної інформації та користування нею.

Предметом злочинів у сфері є:

1) інформація, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку;

2) технічні засоби автоматизованої обробки та захисту інформації (елементи електронно-обчислювальних машин (компютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку).

Як предмет злочину, інформація, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, має притаманні ознаки фізичного, економічного та юридичного характеру.

Інформація матеріалізується в носіях інформації, якими можуть бути фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах.

Носіями інформації в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку виступають тверді фізичні об'єкти (жорсткі диски, дискети, компакт-диски тощо), сигнали (у каналах зв'язку), поля (оперативна пам'ять ЕОМ та її периферійних пристроїв).

Носії інформації можуть бути вилучені з володіння законного власника або пошкоджені чи знищені. Інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах, зберігається на носіях такої інформації у формі даних.

Правова охорона інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, зумовлена не статусом цієї інформації як об'єкта власності, а її змістом, споживчою цінністю, здатністю задовольняти інформаційні потреби.

Інформація є чужою для винного (не перебуває у власності чи законному володінні винного), належить на праві власності іншому суб'єкту власності. Суб'єкти права власності на інформацію визначаються авторським правом або договірними відносинами. Власник інформації, уповноважені ним на те особи визначають користувачів належної йому інформації та встановлюють їх повноваження.

Власник інформації – фізична або юридична особа, яка реалізує повноваження володіння, користування та розпорядження інформацією у обсязі, наданому законодавством.

Володар інформації – фізична або юридична особа, яка реалізує повноваження володіння, користування та розпорядження інформацією у обсязі, встановленому власником інформації.

Розпорядник інформації – фізична або юридична особа, яка має право розпорядження інформацією за угодою з її власником або за його дорученням.

Користувач (споживач) інформації – фізична або юридична особа, яка звертається до власника, володаря або розпорядника інформації за отриманням необхідних йому інформаційних продуктів або можливості користування засобів інформаційного обміну та користується ними.

Інформація, яка обробляється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах, терезках електрозв’язку являє, собою сукупність усіх даних і програм, які використовуються в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах, передаються мережами електрозв’язку незалежно від засобу їх фізичного та логічного представлення.

Дані – інформація у формі, придатній для автоматизованої обробки (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації) її засобами обчислювальної техніки (автоматичними засобами).

Програма – послідовність інструкцій, команд для здійснення певного процесу, яка надається в такій формі, що вона може бути виконана електронно-обчислювальною машиною (комп’ютером) або може бути перетворена в таку форму.

Комп'ютерна програма – об'єктивна форма представлення сукупності даних та команд, призначених для функціонування ЕОМ та інших комп'ютерних пристроїв з метою одержання певного результату.

Загальне програмне забезпечення автоматизованої системи – частина програмного забезпечення автоматизованої системи (операційна система, драйвери тощо), призначена для організації обчислювального процесу.

Операційна система – організована певним чином сукупність керівних та оброблювальних програм, що забезпечують найекономніший розподіл ресурсів обчислювальної системи та виконання програм. Драйвер –додаткова до операційної системи програма, що виконує функцію зв'язку операційної системи з зовнішнім пристроєм. Функційне програмне забезпечення – частина програмного забезпечення автоматизованої системи, що реалізує функції автоматизованої системи.

Системні програмні засоби – програмні засоби, що не залежать від прикладних програмних засобів і підтримують їх роботу.

Прикладні програмні засоби – програмні засоби призначені для виконання прикладної задачі.

Прикладна програма – програма, що призначена для розв'язання задачі або класу задач в певній області застосування систем оброблення даних.

Електронно-обчислювальна машина (ЕОМ, комп'ютер) це сукупність технічних засобів та системного програмного забезпечення, яка створює можливість проведення оброблення інформації та отримання результату в необхідній формі. Крім того, відповідно державних стандартів, **комп'ютер** – функційний пристрій, що складається з одного або кількох взаємопов'язаних центральних процесорів і периферійних пристроїв і може виконувати обчислення без участі людини. Комп'ютер, призначений для обслуговування одного користувача, що характеризується невеликими габаритами, підвищеною надійністю, простотою зміни конфігурації та розвинутими засобами діалогу є персональним комп'ютером. Він відзначається також «автономністю».

Автоматизована система – система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення. Державні стандарти визначають автоматизованими

організаційно-технічні системи, що складаються із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність.

Комп'ютерна мережа – сукупність територіально розосереджених систем оброблення даних, засобів і (чи) систем зв'язку і пересилання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів. Мережа обчислювальних машин – система сполучених між собою комунікаційними засобами ЕОМ різної продуктивності та конфігурації.

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

Мережа електрозв'язку загального користування – мережа електрозв'язку, що експлуатується операторами для забезпечення потреб у послугах електрозв'язку всіх споживачів.

Основними компонентами ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку є правове, організаційне, програмне, інформаційне, лінгвістичне та технічне забезпечення, їх персонал та користувачі.

Правове забезпечення – сукупність норм, що регламентують правові взаємини при функціонуванні ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку та юридичний статус результатів їх функціонування.

Організаційне забезпечення – сукупність документів, що установлюють організаційну структуру, права та обов'язки персоналу і користувачів при експлуатації ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

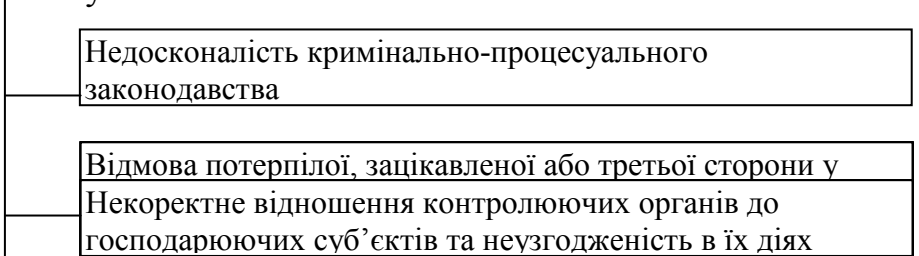


Рис. 7.1. Фактори негативного впливу на процес виявлення та розслідування комп'ютерних злочинів[21]

[21] Лазуренко В.И., Филипенко Т.В. Правовое обеспечение экономической безопасности предприятий. Научно-практические рекомендации. – Донецк: ДЮИ МВД при ДонНУ, 2004. – С. 93.

Програмне забезпечення – сукупність програм, процедур, правил та документації, що стосуються функціонування ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

Інформаційне забезпечення – інформаційна база ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку і засоби її організації та реалізації.

Лінгвістичне забезпечення – тезауруси та мовні засоби опису і маніпулювання даними, використувані в ЕОМ (комп'ютерах), автоматизованих системах та комп'ютерних мережах і мережах електрозв'язку. Тезаурус – словник найменувань понять та їх класифікаційних зв'язків, призначений для єдиного уніфікованого та формалізованого подання інформації в автоматизованій системі.

Технічне забезпечення – сукупність технічних та комунікаційних засобів, що використовуються під час функціонування ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

Персонал автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – фізичні особи, яких власник автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або уповноважена ним особа чи розпорядник визначили для здійснення функцій управління та обслуговування автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (програмісти, оператори ЕОМ, адміністратори мереж, працівники, які займаються обслуговуванням та ремонтом тощо).

Користувач ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – будь-яка фізична або юридична особа, яка має право використання ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку за угодою із їх власником або розпорядником.

Власник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку–- фізична або юридична особа, яка реалізує повноваження володіння, користування та розпорядження ЕОМ

(комп'ютерами), автоматизованими системами, комп'ютерними мережами чи мережами електрозв'язку у обсязі, наданому законодавством.

Розпорядник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – фізична або юридична особа, яка має право розпоряджатися ЕОМ (комп'ютерами), автоматизованими системами, комп'ютерними мережами чи мережами електрозв'язку за угодою з її власником або за його дорученням.

Власник або розпорядник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'зку дає користувачам можливість доступу до інформації, що в них обробляється, згідно з повноваженнями, встановленими власником інформації.

Власник або розпорядник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку регламентує порядок взаємодії користувачів з ними за погодженням з власником інформації.

Об'єктивна сторона злочинів у сфері використання ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку полягає в:

- несанкціонованому втручанні у роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'зку;

- створенні з метою використання, розповсюдження або збуту, а також розповсюдженні або збуті 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;

- несанкціонованому збуті або розповсюдженні 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;

- несанкціонованих діях з інформацією, яка оброблюється у ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку;

- порушенні 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;

- умисному масовому розповсюдженні повідомлень електрозв'язку, здійснене без попередньої згоди адресатів.

Характерною особливістю усіх розглянутих посягань є те, що всі вони вчиняються шляхом активних дій. 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 може вчинятися шляхом бездії.

Суб'єктом злочинів, передбачених статтями **361-363[1]** КК України, може бути фізична осудна особа, яка досягла 16-річного віку. Суб'єкт окремих злочинів – спеціальний. Ним може бути:

1) особа, яка не має право доступу до певної інформації, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку або до технічних засобів її автоматизованої обробки (ст. 361);

2) особа, яка має право доступу до інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації у зв'язку із займаною посадою або спеціальними повноваженнями (ст. 362);

- неслужбова особа, яка відноситься до персоналу автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, тобто працівників, які перебувають у трудових відносинах з власником технічних засобів (уповноваженою ним особою чи розпорядником) та визначена для здійснення

функцій управління та обслуговування ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363).

Суб'єктом злочину передбаченого ст. 363 КК України може бути також будь-яка інша особа, яка відповідно до своїх трудових, службових обов'язків або на основі відповідної угоди з власником ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку виконує роботу, пов'язану з їх експлуатацією і зобов'язана при її виконанні дотримуватись встановлених правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також порядку та правила захисту інформації, яка в них оброблюється.

Суб'єктивна сторона злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку характеризується прямим умислом і як правило корисливим мотивом. Лише діяння передбачене ст. 363 КК України може вчинятися як умисно, так і через необережність.

Ознаками кваліфікованих видів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є вчинення таких діянь: 1) повторно; 2) за попередньою змовою групою осіб; 3) із заподіянням значної шкоди.

Повторністю злочинів визнається вчинення особою двох або більше злочинів, передбачених відповідною статтею розділу XVI КК України або її частиною. Повторність відсутня при вчиненні продовжуваного злочину, який складається з двох або більше тотожних діянь, об'єднаних єдиним злочинним наміром.

Зміст другої кваліфікуючої ознаки визначається відповідно положень ч. 2 ст. 28 КК України. Злочин визнається вчиненим за попередньою змовою групою осіб, якщо його спільно вчинили декілька суб'єктів злочину (двоє або більше), які заздалегідь (до моменту виконання об'єктивної сторони злочину), домовилися (дійшли згоди) про спільне його вчинення. Домовленість стосується спільності вчинення злочину, а саме: узгодження об'єкта злочину,

його характеру, місця, часу, способу вчинення, змісту виконуваних функцій тощо.

Поняття значної шкоди є оціночною ознакою і потребує вирішення у кожному конкретному випадку з урахуванням всіх обставин справи та розміру завданих матеріальних збитків.

Значною шкодою у статтях **361-363[1]**, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка **в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян**.

Примітка. Необхідно враховувати, що коли норми законів містять посилання на неоподатковуваний мінімум, то для цілей їх застосування використовується сума у розмірі 17 гривень. Але це не стосується норм адміністративного та кримінального законодавства у частині кваліфікації злочинів або правопорушень, для яких сума неоподатковуваного мінімуму встановлюється на рівні податкової соціальної пільги, визначеної Законом України «Про податок з доходів фізичних осіб».

Відповідно вказаного Закону на перехідний період встановлено наступні розміри податкової соціальної пільги:

-у 2005 році – у розмірі 50% суми податкової соціальної пільги, визначеної у розмірі, що дорівнює одній мінімальній заробітній платі (у розрахунку на місяць), встановленій законом на 1 січня звітного податкового року;

-у 2006 році – у розмірі 80% суми податкової соціальної пільги, визначеної у розмірі, що дорівнює одній мінімальній заробітній платі (у розрахунку на місяць), встановленій законом на 1 січня звітного податкового року;

-у 2007 році – у розмірі 100% суми податкової соціальної пільги, визначеної у розмірі, що дорівнює одній мінімальній заробітній платі (у розрахунку на місяць), встановленій законом на 1 січня звітного податкового року.

Законом України «Про Державний бюджет України на 2005 рік» з 1 січня 2005 року розмір мінімальної заробітної плати встановлено у розмірі 262 гривні на місяць, а з 1 грудня 2005 року - 282 гривні на місяць.

Законом України «Про Державний бюджет України на 2006 рік»(ст. 82) розмір мінімальної заробітної плати встановлено: з 1 січня – 350 гривні на місяць; з 1 липня – 375 гривні на місяць; з 1 грудня – 400 гривні на місяць.

Законом України «Про Державний бюджет України на 2007 рік»(ст. 76) розмір мінімальної заробітної плати встановлено: з 1 січня – 400 гривні на місяць; з 1 липня – 420 гривні на місяць; з 1 грудня – 450 гривні на місяць.

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, спотворенню 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.

Примітка. Значною шкодою у статтях 361-363[1], якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

1. Об'єктом злочину є встановлений порядок обробки інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах та передавання її каналами електрозв'язку.

Під обробкою інформації розуміється вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних.

Предметом злочину є інформація, яка обробляється в електронно-обчислювальних, машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, мережах електрозв'язку – сукупність усіх даних і програм, які використовуються в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, передаються мережами електрозв'язку незалежно від засобу їх фізичного та логічного представлення.

Інформація матеріалізується в носіях інформації. Носіями інформації можуть бути фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах.

Носіями інформації в ЕМО (комп'ютерів) автоматизованих систем, комп'ютерних мереж: чи мереж електрозв'язку виступають тверді фізичні об'єкти (дискети, компакт-диски, жорсткі диски, стрімерні стрічки, пристрої з флеш-пам'ттю тощо), сигнали (у каналах зв'язку), поля (оперативна пам'ять ЕОМ та її периферійних пристроїв).

2. З об'єктивної сторони злочин характеризується сукупністю трьох ознак: 1) діяння – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 2) суспільно небезпечні наслідки у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки

інформації або порушення встановленого порядку її маршрутизації; 3) причинний зв'язок між зазначеними діянням і наслідками.

Обов'язковою ознакою об'єктивної сторони є несанкціонованість втручання. Санкціонованим вважається втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку з дозволу власника, а також уповноважених власником осіб або службових осіб на яких покладено забезпечення їх нормальної роботи.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку може проявлятися у наступних діяннях:

- вчинений умисно, без наявності права на це, доступ до інформації (несанкціонований доступ), яка в них обробляється, пов'язаний з подоланням програмних, технічних чи організаційних заходів захисту;

- вчинений умисно, без наявності права на це, вплив на інформацію (несанкціонований вплив).

Доступ – звернення для отримання даних.

Метод доступу – сукупність засобів та угод, за допомогою яких реалізується заданий вид доступу до них. Доступ у більшості випадків здійснюється за паролем, але можуть бути використані і спеціальні технічні прилади для ідентифікації користувача (наприклад магнітні карти). На об'єктах телекомунікацій, а також в окремих структурних підрозділах операторів, провайдерів телекомунікацій, де передається, обробляється або зберігається інформація з обмеженим доступом, що є власністю держави, встановлюється спеціальний режим доступу відповідно до законодавства.

Для отримання необхідних інформаційних продуктів та їх використання користувач інформації повинен звертатися за дозволом до власника інформації, її володаря або розпорядника.

Несанкціонований доступ – доступ до інформації, що здійснюється з порушенням встановлених в автоматизованій системі правил розмежування

доступу, які регламентують доступ користувачів до інформації, на яку вони мають право. Несанкціонований доступ може бути здійсненим двома способами:

- безпосереднє проникнення в заборонену зону, приміщення де оброблюється інформація тощо;

- опосередковано – віддалений доступ з використанням програмних та технічних засобів для подолання захисту.

Обов'язковою ознакою цього посягання має бути те, що винний, здійснюючи несанкціонований доступ, долає заходи безпеки певної комп'ютерної системи чи телекомунікаційної мережі. Захист інформації (запобігання вільному доступу до інформації, усунення технічних каналів її витоку тощо) в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах та мережах електрозв'язку забезпечується комплексом організаційних, програмних і технічних заходів.

Подолання захисту може проявлятися у зламі паролів, кодів доступу тощо. Спосіб подолання зазначених заходів безпеки не матиме значення для кваліфікації, звичайно, якщо сам по собі не буде містити ознак іншого складу злочину (наприклад, знищення програмних або технічних засобів). Злочинними наслідками несанкціонованого доступу є виток інформації.

Витік інформації – результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї. Як процес, витік інформації являє собою неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

Несанкціонований вплив – вплив на інформацію, що здійснюється з порушенням методів та процедур автоматизованої обробки інформації. Вплив на інформацію, її носії та засоби захисту з метою порушення цілісності інформації, її втрати або витоку, може здійснюватися шляхом формування сигналів, полів, середовищ і блоків програм. Підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації може здійснюватись через програмні чи технічні

засоби автоматизованої обробки інформації або засоби передавання її каналами зв'язку.

Технічні засоби автоматизованої обробки інформації – сукупність апаратних і комунікаційних засобів, носіїв даних та допоміжних матеріалів, що забезпечують автоматизовану обробку інформації в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах та передавання її каналами електрозв'язку.

Засоби апаратні – це сукупність пристроїв, що використовуються для оброблення даних.

Засоби комунікаційні (мережа) – сукупність ліній пересилання даних та комутаційних пристроїв, що дозволяє здійснювати взаємне сполучення прикінцевого обладнання.

Під методами та процедурами необхідно розуміти методи оброблення інформації та відповідні дії персоналу.

Злочин, по перше, вважається закінченим з моменту настання хоча б одного із зазначених наслідків: 1) виток інформації; 2) втрата інформації; 3) підробка інформації; 4) блокування інформації; 5) спотворення процесу обробки інформації; 6) порушення встановленого порядку маршрутизації інформації.

Втрата інформації – результат дій, внаслідок яких інформація в автоматизованих системах перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.

Підробка інформації – результат навмисних дій, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в автоматизованих системах.

Блокування інформації – результат дій, наслідком яких є унеможливлення (припинення) санкціонованого доступу до інформації.

Спотворення процесу обробки інформації – результат дій, наслідком яких є порушення визначеного алгоритму виконання програм обробки інформації.

Обробка інформації – вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних.

Порушення встановленого порядку маршрутизації інформації – результат дій, наслідком яких є зміна визначеного маршруту передавання або приймання інформації каналами зв'язку.

Канал електрозв'язку – сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і які характеризуються смугою частот та/або швидкістю передачі.

Фізичне знищення або пошкодження ЕОМ (комп'ютерів), інших технічних засобів автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, якщо умисел винного було спрямовано саме на це, кваліфікується за ст. 194 КК України («Умисне знищення або пошкодження майна»).

Факт перегляду інформації за результатом несанкціонованого доступу кваліфікується за ст. 361 у разі настання наслідку – витоку інформації з обмеженим доступом. Одержання несанкціонованого доступу правопорушником у більшості випадків блокує інформацію (або інформаційну послугу) призначену для законного користувача (наприклад, несанкціонований доступ до мережі Інтернет з використанням чужих паролів). В інших випадках, коли дії особи хоч і пов'язані з несанкціонованим доступом, але не спричинили суспільно-небезпечних наслідків, це можна кваліфікувати, в залежності від обставин, як готування до вчинення іншого умисного злочину – усунення перешкод, інше умисне створення умов для вчинення злочину (ст. 14 КК України) або замах на злочин – якщо злочин не було доведено до кінця з причин, що не залежали від її волі (ст. 15 КК України).

У випадку коли несанкціоноване втручання виступає способом вчинення іншого умисного злочину, а технічні засоби використовуються в якості

знаряддя для досягнення злочинної мети, вчинене винним кваліфікується по сукупності злочинів.

3. Суб'єкт злочину – загальний. Це фізична особа, яка не має права доступу до певної інформації, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку або до технічних засобів і автоматизованої обробки.

Якщо особа має право доступу до інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, то її дії кваліфікуються за ст. 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») або ст. 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») КК України.

4. Суб'єктивна сторона злочину характеризується умисною виною. Злочинні дії при подоланні програмного та технічного захисту для отримання несанкціонованого доступу можуть бути вчинені лише з прямим умислом, тоді як ставлення винного до наслідків несанкціонованих дій у роботу ЕОМ (комп'ютерів) може характеризуватись як прямим так і непрямим умислом.

Особа, яка здатна втрутитись у роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'терних мереж чи мереж електрозв'язку має відповідні знання, вміння та навички. Вона:

- усвідомлює соціальну небезпечність несанкціонованого втручання, його протиправність;

- передбачає наслідки у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації;

- бажає або свідомо припускає настання цих наслідків, ставиться до їх

настання байдуже.

Мотив переважно корисливий, але можливі – помста, хуліганство, підрив репутації, приховування іншого злочину тощо.

5. Кваліфікуючими ознаками (ч. 2 ст. 361) злочину є вчинення його: 1) повторно; 2) за попередньою змовою групою осіб; 3) заподіяння ним значної шкоди.

Повторністю злочинів визнається вчинення двох або більше злочинів, передбачених цією статтею або її частиною.

Питання значної шкоди є питанням факту і потребує вирішення у кожному конкретному випадку з урахуванням всіх обставин справи. Значною шкодою у статтях 361-363[1], якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

СТАТТЯ 361[i]. 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.

1. Об’єктом злочину є суспільні відносини у сфері забезпечення безпеки обробки інформації в ЕОМ (комп’ютерах), автоматизованих системах, комп’ютерних мережах чи передаванні її мережами електрозв’язку.

Предметом злочину є шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку.

Під шкідливими програмними засобами необхідно розуміти створені або пристосовані комп’ютерні програми, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Переважно це різноманітні види так званих «комп’ютерних вірусів».

Шкідливі технічні засоби – це спеціально створені або пристосовані технічні пристрої, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Наприклад клоновані мобільні телефони, «вічні» телефонні картки, пристрої електромагнітного впливу тощо.

2. Об’єктивна сторона злочину полягає у: 1) створенні з метою використання, розповсюдження або збуту 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; 2) розповсюдженні або збуті 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.

Поняття несанкціонованого втручання надано у коментарі ст. 361 КК України.

Створення шкідливих засобів – це дії в результаті яких відбувається фізична матеріалізація (факт створення), шкідливого програмного засобу на носії інформації або шкідливого технічного засобу у просторових формах.

Розповсюдження шкідливих програмних і технічних засобів – безпосередня чи опосередкована пропозиція шкідливих програмних засобів іншим особам шляхом продажу, передавання, прокату, здачі в оренду, надання у борг, а також створення умов, за яких інші особи можуть здійснити доступ до них або отримати у користування з будь-якого місця і в будь-який час за власним вибором, у тому числі мережевими та іншими способами.

Передавання шкідливих програмних і технічних засобів може здійснюватися будь-яким способом на будь-яких підставах:

установки таких засобів у процесі виготовлення, ремонту, реалізації з метою подальшого використання для несанкціонованого доступу; ознайомлення інших осіб зі змістом програмних і технічних засобів.

3. Суб'єкт злочину загальний: фізична, осудна особа, яка досягла шістнадцятирічного віку.

4. Суб'єктивна сторона злочину характеризується прямим умислом, мета спеціальна. Створення шкідливих програмних чи технічних засобів, призначеними для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку є злочинним лише тоді, коли ці дії вчинено з метою використання, розповсюдження або збуту.

Особа усвідомлює, що засоби, створювані або розповсюджувані нею, є шкідливими та призначеними для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, усвідомлює суспільно небезпечний характер цього діяння, передбачає та бажає настання суспільно небезпечних наслідків.

5. Кваліфікуючою ознакою цього злочину (ч. 2 ст. 361[1]) є вчинення його: 1) повторно; 2) за попередньою змовою групою осіб; 3) якщо ним заподіяно значну шкоду.

Повторністю злочинів визнається вчинення двох або більше злочинів, передбачених цією статтею або її частиною.

Поняття значної шкоди визначено у примітці до ст. 361 КК України. Питання значної шкоди є питанням факту і потребує вирішення у кожному конкретному випадку з урахуванням всіх обставин справи. Визначення розміру значної шкоди вказано у коментарі до ст.361 КК України.

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.

1. Об’єкт злочину – встановлений порядок обігу інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації.

Предметом його є інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації.

Визначення інформації, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, надано у коментарі до ст. 361 КК України.

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну і таємну.

Конфіденціальна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов (наприклад паролі, логіни, коди доступу, інші дані, що дають право доступу тощо).

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденціальної, та встановлюють для неї систему (способи) захисту.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених Законом України «Про інформацію».

2. Об’єктивна сторона злочину полягає у несанкціонованому збуті або розповсюдженні 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.

Визначення понять електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж надано у коментарі до статті 361 КК України.

Несанкціонований збут інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації – умисне, без дозволу власника , як сплатне так і безоплатне відчуження інформації іншій особі. Такі дії можуть бути вчинені у формі продажу, дарування, тощо і з правової точки зору являють собою недійсні угоди. Несанкціонований збут інформації з обмеженим доступом для задоволення інформаційних потреб сторонніх осіб може здійснюватися шляхом:

- передачі носія інформації;
- пересилання інформації каналами зв’язку;
- надання доступу до інформації і змоги користуватися нею.

Несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації – умисне, без дозволу власника інформації, надання доступу до відтвореної у будь-якій матеріальній формі інформації, у тому числі мережевими та іншими способами, а також шляхом продажу, прокату, здачі в оренду, надання у борг.

Відтворення інформації – виготовлення одного або декількох екземплярів інформації (даних або програм) у будь-якій матеріальній формі, а також запис їх у оперативну пам’ять ЕОМ.

Необхідно відмітити, що відповідно Закону України «Про телекомунікації», оператори, провайдери телекомунікацій забезпечують і несуть відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

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.

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.

3. Суб'єкт злочину загальний: фізична, осудна особа, яка досягла шістнадцятирічного віку.

4. Суб'єктивна сторона злочину характеризується прямим умислом.

Винна особа усвідомлює той факт, що інформація, яка нею несанкціоновано збувається або розповсюджується, є інформація з обмеженим доступом, усвідомлює суспільно небезпечний характер цього діяння, і бажає вчинити таке діяння.

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 або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

1. Об'єктом злочину є встановлений порядок обробки інформації в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

Додатковим обов'язковим об'єктом злочину є відносини власності на інформацію, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах та комп'ютерних мережах або зберігається на носіях такої інформації.

Предметом злочину є інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації.

Визначення інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, надано у коментарі до ст. 361 КК України.

2. Об'єктивна сторона злочину полягає у вчиненні двох видів діянь: 1) несанкціонованій зміні, знищенні або блокуванні 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; 2) несанкціонованому перехопленні або копіюванні 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

Визначення понять електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж надано у загальних положеннях коментарю до розділу XVI КК України.

Носій інформації, яка призначена для обробки в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах (носій даних) - матеріальний об'єкт, призначений для запису, зчитування, накопичення, зберігання чи пересилання даних.

Як твердий носій даних може бути використано дискету, компакт-диск, жорсткий диск, пристрої зовнішньої пам'яті тощо. Носієм даних є також і поле оперативної (енергозалежної) пам'яті ЕОМ (комп'ютера) або її кінцевих

терміналів. У мережах носієм даних виступає сигнал, отриманий внаслідок накладення потоку даних на несучу частоту й придатний для пересилання каналами зв’язку.

Інформація, яка призначена для обробки в ЕОМ (комп’ютерах), автоматизованих системах чи комп’ютерних мережах (носій даних) є об’єктом права власності громадян, організацій (юридичних осіб) і держави. Інформація (як сукупність даних і програм) може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження. Власник інформації щодо об'єктів своєї власності має право здійснювати будь-які законні дії. Підставами виникнення права власності на інформацію є:

- створення інформації своїми силами і за свій рахунок (авторське право);
- договірні відносини (договір на створення інформації; договір, що містить умови переходу права власності на інформацію до іншої особи тощо).

Інформація, створена кількома громадянами або юридичними особами, є колективною власністю її творців. Порядок і правила користування такою власністю визначаються договором, укладеним між співвласниками. Інформація, створена організаціями (юридичними особами) або придбана ними іншим законним способом, є власністю цих організацій. Інформація, створена на кошти державного бюджету, є державною власністю. Інформацію, створену на правах індивідуальної власності, може бути віднесено до державної власності у випадках передачі її на зберігання у відповідні банки даних, фонди або архіви на договірній основі.

Право власності на інформацію, створену як вторинну в процесі обробки в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах, встановлюється з урахуванням норм авторського права на підставі угоди між власником вхідної інформації і користувачем ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж. Якщо такої угоди немає, то така інформація належить користувачу, який здійснив цю обробку.

Власник інформації має право призначати особу, яка здійснює володіння, використання і розпорядження інформацією, і визначати правила обробки інформації та доступ до неї, а також встановлювати інші умови щодо інформації.

Власник або розпорядник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж зобов'язаний інформувати власника і користувача інформації про властивості методів обробки інформації та межі їх використання, а власник і користувач інформації повинні підтвердити свою згоду на застосування пропонованих методів обробки та відсутність претензій.

Користувач ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж може проводити обробку інформації лише за наявності згоди на те її власника або уповноваженої ним особи, якщо ця інформація не віднесена до категорії загальнодоступної.

Без дозволу власника доступ до інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, здійснюється лише у випадках, передбачених чинним законодавством.

Несанкціонована зміна інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації – вчинені без дозволу власника інформації дії, шляхом впливу на матеріальний носій інформації, в наслідок яких змінюється первинний стан інформації (її цілісність, властивості або функції). Змінена інформація може бути повністю, частково або тимчасово непридатною для задоволення інформаційних потреб. Наприклад: реструктурування або реорганізація бази даних, видалення або додавання записів бази даних, переклад даних з однієї мови на іншу тощо.

Несанкціоноване знищення інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації - вчинені без дозволу власника інформації дії (повне або часткове видалення інформації з її носіїв), в наслідок

яких інформація перестає існувати на певному носії в повному чи обмеженому обсязі в силу втрати нею основних ознак, стає непридатною для задоволення інформаційних потреб. При цьому не має значення наявність чи відсутність копії даної інформації у потерпілого.

Несанкціоноване блокування інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації – вчинені без дозволу власника інформації дії, які унеможливлюють власнику (законному користувачу) доступ до цієї інформації або використання її за прямим призначенням.

Несанкціоноване перехоплення інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах – здійснення умисно, без дозволу власника, збирання та записування, за допомогою програмних або технічних засобів, інформації, в процесі її обробки в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах. Способи: встановлення реєстраторів інформації, відтворення стертих файлів тощо.

Несанкціоноване копіювання інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах - здійснення, без дозволу власника, переносу інформації або її частини з одного фізичного носія на інший. При переносі відбувається зчитування інформації з одного носія та її записування на інший без зміни цілісності, властивостей та функцій інформації.

Несанкціоновані перехоплення та копіювання інформації, що обробляється або зберігається в засобах обчислювальної техніки, можуть здійснюватися шляхом включення до бібліотек програм спеціальних програмних блоків, зміни програмного забезпечення та іншими засобами, у тому числі технічними. Навмисні канали витоку інформації можуть створюватися відповідним формуванням (перетворенням) полів або середовищ їх поширення з метою забезпечення сприятливих умов для витоку інформації.

Ненавмисні канали витоку інформації можуть утворюватися в результаті виникнення полів і середовищ їх поширення.

Злочин вважається закінченим з моменту настання для власників інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, одного з наступних наслідків, передбачених ст. 362 КК України: несанкціонованої зміни інформації, несанкціонованого знищення інформації, несанкціонованого блокування інформації або витоку інформації.

Умисний вплив на інформацію з метою порушення її цілісності та на її носії може також здійснюватися шляхом формування сигналів, полів, середовищ і блоків програм.

3. Суб'єкт злочину спеціальний. Це осудна особа, яка досягла шістнадцятирічного віку і має право доступу до інформації, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації у зв'язку із займаною посадою або спеціальними повноваженнями.

Доступ до інформації, яка зберігається, обробляється і передається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, здійснюється лише згідно з правилами розмежування доступу, встановленими власником такої інформації чи уповноваженою ним особою.

Користувачі інформації визначаються власником інформації або уповноваженою ним особою, ними ж встановлюються їх повноваження.

4. Суб'єктивна сторона злочину характеризується умисною формою вини.

Винна особа усвідомлює, що несанкціоноване втручання вчиняє зміну, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи

комп’ютерних мережах або зберігається на носіях такої інформації, чи перехоплення або копіювання такої інформації, та бажає вчинення таких дій.

6. Кваліфікуючими ознаками злочину є вчинення злочину: 1) повторно; 2) за попередньою змовою групою осіб; 3) із заподіянням значної шкоди.

Повторністю злочинів визнається вчинення двох або більше злочинів, передбачених цією статтею або її частиною.

Поняття значної шкоди визначено у примітці до ст. 361 КК України. Питання значної шкоди є питанням факту і потребує вирішення у кожному конкретному випадку з урахуванням всіх обставин справи. Визначення розміру значної шкоди вказано у загальних положеннях коментарю до розділу XVI КК України.

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.

1. Суспільна небезпека злочину полягає у створенні передумов для несанкціонованого втручання у процес автоматизованої обробки інформації та несанкціонованих дій з інформацією, порушенні прав суб’єктів інформаційних чи телекомунікаційних відносин.

Об’єктом злочину є встановлений порядок нормального функціонування ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, та порядок захисту інформації, яка в них оброблюється.

Предметом злочину є інформація, програмні та технічні засоби ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку експлуатація і захист яких доручені винній особі.

2. Об’єктивну сторону злочину характеризує сукупність трьох ознак: 1) діяння – 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; 2) суспільно небезпечні наслідки у вигляді заподіяння значної шкоди суб’єктам інформаційних чи телекомунікаційних відносин; 3) причинний зв’язок між діянням і суспільно небезпечними наслідками.

Диспозиція ст. 363 КК України є бланкетною. У кожному випадку вчинення такого діяння має бути встановлено які конкретно нормативні акти порушено винним. **Відсутність на підприємстві**, в установі чи організації таких **правил експлуатації** автоматизованих ЕОМ, їх систем чи комп’ютерних мереж, порядку і правил захисту інформації, яка в них оброблюється, **виключає наявність в діяннях особи складу злочину, передбаченого ст. 363 КК України.**

Під експлуатацією ЕОМ (комп’ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку розуміють всі види діяльності, необхідні для забезпечення їх належного та ефективного використання (функціонування).

Правила експлуатації ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку можна поділити на:

- технічні правила експлуатації, які встановлюють технічні норми використання певних технічних засобів (інструкції по експлуатації, технічні вимоги, технічні стандарти та регламенти тощо);

- організаційні правила експлуатації, які нормативно закріплюють вимоги до персоналу та користувачів при користуванні технічними засобами та їх обслуговуванні (закони, укази, постанови, відомчі накази, посадові інструкції, функціональні обов’язки тощо).

Порушення правил експлуатації встановлених виробником позбавляє власника технічних засобів лише права на гарантійне обслуговування.

Вимоги державних і галузевих стандартів, інших нормативних документів щодо технічних засобів інформатизації та телекомунікацій є обов'язковими для персоналу всіх автоматизованих систем, операторів, провайдерів телекомунікацій.

Порядок та умови використання діючих трубопроводів, кабельних каналів, колекторів, веж, антен та інших пристроїв особами, яким вони не належать, встановлюються договором з їх власником.

Умовами застосування технічних засобів телекомунікацій є їх відповідність стандартам і технічним регламентам. Технічні засоби телекомунікацій повинні мати виданий у встановленому законодавством порядку документ про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій.

Захист інформації в ЕОМ (комп’ютерах), автоматизованих системах, комп’ютерних мережах чи мережах електрозв’язку забезпечується шляхом:

- дотримання суб’єктами правових відносин норм, вимог та правил організаційного і технічного характеру щодо захисту оброблюваної інформації;

- використання засобів обчислювальної техніки, програмного забезпечення, засобів зв’язку і автоматизованих систем в цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо захисту інформації (мають відповідний сертифікат);

- перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв’язку і автоматизованих систем в цілому встановленим вимогам щодо захисту інформації (сертифікація засобів обчислювальної техніки, засобів зв’язку і автоматизованих систем);

- здійснення контролю щодо захисту інформації. Власник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку повинен забезпечити захист інформації згідно з вимогами і правилами, що обумовлюються угодою з власником інформації або уповноваженою ним особою, та зобов'язаний повідомити його про всі факти порушення її захисту. Згідно з укладеною угодою власник інформації або уповноважені ним особи мають право здійснювати контроль за дотриманням вимог щодо захисту інформації та забороняти чи зупиняти обробку інформації у разі порушення цих вимог.

Власник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку не несе відповідальності за шкоду, заподіяну власнику інформації, якщо при цьому не було порушено встановлені власником інформації правила її захисту.

Оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічні та організаційні заходи із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Якщо інформація є власністю держави або належить до державної таємниці чи окремих видів інформації, захист яких гарантується державою, то власник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку повинен забезпечити захист інформації згідно з вимогами і правилами, що їх визначає уповноважений Кабінетом Міністрів України орган.

Вимоги і правила щодо захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, встановлюються державним органом, уповноваженим Кабінетом Міністрів України. Ці вимоги і правила є обов'язковими для власників електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, де така інформація обробляється, і

мають рекомендаційний характер для інших суб'єктів права власності на інформацію.

Державна політика технічного захисту інформації формується згідно із законодавством і реалізується Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України у взаємодії з органами, щодо яких здійснюється ТЗІ.

Інформація, яка є власністю інших суб'єктів, може оброблятися у електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах за розсудом власника інформації. Власник інформації може звернутися до органів сертифікації з клопотанням про проведення аналізу можливостей електронно-обчислювальних машин (комп'ютерів), автоматизованих систем щодо належного захисту його інформації та одержання відповідних консультацій.

Власник або розпорядник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку повинен інформувати власника і користувача інформації про властивості методів обробки інформації та межі їх використання, а власник і користувач інформації повинні підтвердити свою згоду на застосування пропонованих методів обробки та відсутність претензій.

Розпорядник ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку в обов'язковому порядку інформує власника інформації про технічні можливості захисту інформації в його автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, типові правила, встановлені для персоналу.

Персоналу оператора, провайдера телекомунікацій, відповідно Закону України «Про телекомунікації» забороняється брати участь у страйках, якщо такі дії призводять до припинення функціонування мереж телекомунікацій чи надання телекомунікаційних послуг, що створює перешкоди для забезпечення національної безпеки, охорони здоров'я, прав і свобод людини.

Відповідальність за ст.363 КК України настає лише у разі, якщо особа була не лише зобов'язана, а й мала реальну можливість виконати належним

чином встановлені правила експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також порядку і правил захисту інформації, яка в них оброблюється.

Поняття значної шкоди дано у примітці до ст. 361 КК України. Питання значної шкоди є питанням факту і потребує вирішення у кожному конкретному випадку з урахуванням всіх обставин справи. Визначення розміру значної шкоди вказано у коментарі до ст.361 КК України.

Між порушенням і наслідками у вигляді заподіяння значної шкоди суб'єктам інформаційних чи телекомунікаційних відносин має існувати причинний зв'язок – значна шкода суб'єктам інформаційних чи телекомунікаційних відносин заподіюється в результаті порушення встановлених правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, або порядку чи правил захисту інформації, яка в них оброблюється.

Це може проявитися у порушенні цілісності та взаємодії мереж телекомунікацій, інформаційної безпеки ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, електромагнітної сумісності радіоелектронних засобів, ускладнення чи унеможливлення надання інформаційних чи телекомунікаційних послуг споживачам.

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 може бути здійснене як шляхом певних дій, так і шляхом бездіяльності.

Склад злочину є матеріальним: злочин вважається закінченим з моменту настання суспільно небезпечних наслідків у вигляді заподіяння значної шкоди суб'єктам інформаційних чи телекомунікаційних відносин.

Якщо ж метою винної особи було знищення саме технічних засобів захисту інформації, вчинене за наявності підстав кваліфікується відповідно до ст. 194 КК України «Умисне знищення або пошкодження майна».

3. Суб’єкт злочину спеціальний. Ним може бути неслужбова особа, яка відноситься до персоналу автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, тобто працівників, які перебувають у трудових відносинах з власником технічних засобів (уповноваженою ним особою чи розпорядником) та визначені для здійснення функцій управління та обслуговування ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку.

Вказана особа відповідно до вимог нормативно-правових актів, своїх трудових, службових обов’язків, посадової інструкції або на основі відповідної угоди з власником ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку виконує роботу, пов’язану із забезпеченням їх належного та ефективного використання (функціонування), і зобов’язана при її виконанні дотримуватись встановлених правил експлуатації ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, а також порядку та правил захисту інформації, яка в них обробляється.

Невиконання або неналежне виконання службовою особою своїх обов’язків через несумлінне ставлення до них, у тому числі пов’язаних з експлуатацією ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, а також захистом інформації, яка в них обробляється, кваліфікується за ст. 367 КК України «Службова недбалість».

4. Суб’єктивна сторона злочину характеризується змішаною формою вини, яка передбачає умисне порушення існуючих 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, та необережне ставлення суб’єкту до суспільно небезпечних наслідків у вигляді заподіяння значної шкоди.

Умисне сприяння особою, яка відповідає за експлуатацію ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, заподіянню суспільно небезпечних наслідків у вигляді значної

шкоди суб’єктам інформаційних чи телекомунікаційних відносин, є співучастю у вчиненні відповідного злочину і потребує кваліфікації за відповідною статтею Особливої частини КК України.

СТАТТЯ 363[i]. 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 електрозв’язку, які є власністю винної особи.

1. Об’єктом злочину є нормальна робота ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку по забезпеченню інформаційних та телекомунікаційних потреб користувачів.

Предметом злочину є програмні та технічні засоби ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку.

2. З об’єктивної сторони злочин характеризується сукупністю трьох ознак: 1) діяння – масове розповсюдження повідомлень електрозв’язку, здійснене без попередньої згоди адресатів; 2) суспільно небезпечні наслідки у вигляді порушення або припинення роботи електронно-обчислювальних машин

(комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) причинний зв'язок між зазначеними діяннями і наслідками.

Повідомленням (в теорії інформатизації та теорії зв'язку) є впорядковані серії символів, призначені для пересилання інформації.

Повідомлення електрозв'язку – інформація в електронній формі, призначена для обробки в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, яка передається засобами телекомунікаційного зв'язку. Повідомлення електрозв'язку зберігаються на засобах збереження інформації у вигляді файла.

Повідомлення електрозв'язку, які розповсюджуються без попередньої згоди адресатів, серед користувачів інформаційних послуг отримали назву «спам» (spam).

Ознаками «спаму» є:

1) повідомлення направляються адресату, який не висловив (явно чи не явно) бажання отримати таке (такі) повідомлення;

2) повідомлення мають нав'язливий, небажаний для адресата характер (не має значення – комерційна це реклама чи просто корисна на думку відправника інформація);

3) повідомлення розсилаються масово. Масовість досягається розсилкою протягом короткого часу повідомлень на значну кількість адрес (наприклад, при розсилці повідомлень на 1000 чи більше адрес) або численних повідомлень одному адресату (наприклад, при розсилці 1000 чи більше однакових повідомлень на одну адресу).

Переважна більшість «спаму» розповсюджується електронною поштою (e-mail) – листуванням у формі повідомлень, що пересилаються між терміналами користувачів через комп'ютерну мережу. Але також, як «спам» визнаються аналогічні повідомлення, що розповсюджуються в телеконференціях (newsgroups), по каналам чату (IRC, ICQ), по SMS, по факсу.

Розповсюдження повідомлень електрозв'язку – будь-які дії, за допомогою яких забезпечується переміщення інформації у вигляді даних з

використанням телекомунікаційних мереж від джерела даних в один чи кілька пунктів призначення.

Перевантаження ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку та їх ресурсів при обробці надмірного обсягу повідомлень електрозв'язку призводить до порушення (зміни режиму роботи) або припинення їх роботи. Боротьба зі «спамом» відволікає значні ресурси провайдерів на блокування та фільтрацію сумнівних поштових повідомлень. Адресат також несе матеріальні збитки – оплачує час з'єднання з Інтернетом при обробці «спаму» (або обсяг трафіку). Внаслідок перевантаження може виникнути фізичне порушення окремих елементів ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, нестабільність їх живлення, порушення температурного режиму тощо.

Порушення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – стан об'єкту при якому, при умові збереження фізичної цілісності технічних засобів, погіршилися його експлуатаційні характеристики, що унеможливлює нормальне його функціонування. Наприклад: збій у процесі обробки інформації, відображення невірної інформації, самостійне перезавантажування тощо.

Припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – стан об'єкту при якому він протягом тривалого часу не здатен виконувати задані функції по задоволенню інформаційних та комунікаційних потреб користувачів. Наприклад: відмова роботи обладнання, роз'єднання лінії тощо.

При встановлені умислу на втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку необхідно кваліфікувати за ст. 361 КК України.

Злочин вважається закінченим з моменту настання суспільно небезпечних наслідків у вигляді заподіяння значної шкоди суб'єктам інформаційних та телекомунікаційних відносин при тимчасовому припиненні роботи ЕОМ

(комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порушенні процесу автоматизованої обробки інформації через опрацювання масово надісланих повідомлень електрозв'язку.

Тривалість порушення або припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку не має значення. Значення має факт спричинення суб'єктам інформаційних та телекомунікаційних відносин значної шкоди.

Фізична цілісність та недоторканність технічних засобів автоматизованої обробки інформації охороняється іншими кримінально-правовими нормами, зокрема тими, які передбачають відповідальність за посягання на власність (наприклад ст.ст. 188, 194 КК України). Умисне пошкодження ліній електрозв'язку або споруд чи обладнання, які входять до їх складу іншими способами кваліфікується за ст. 360 КК України «Умисне пошкодження ліній зв'язку».

3. Суб'єкт злочину загальний: фізична, осудна особа, яка досягла шістнадцятирічного віку.

4. Суб'єктивна сторона злочину може характеризуватись як умисною так і необережною формою вини.

Ставлення винного до діяння є завжди умисним.

Ставлення винного до наслідків у вигляді порушення або припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку може характеризуватись як прямим (особа уявляє характер шкідливих наслідків, усвідомлює їх соціальну значимість та причинно-наслідкову залежність) так і непрямим умислом (особа усвідомлювала соціальну небезпечність діяння, його протиправність, свідомо припускала настання цих наслідків), або необережністю (особа передбачала можливість настання суспільно небезпечних наслідків, але легковажно розраховувала на їх відвернення, або не передбачала можливість настання суспільно небезпечних наслідків, хоча повинна була і могла їх передбачити).

5. Кваліфікуючою ознакою цього злочину (ч. 2 ст. 363[і]) є вчинення його: 1) повторно; 2) за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду.

Повторністю злочинів визнається вчинення двох або більше злочинів, передбачених цією статтею або її частиною. Повторність відсутня при вчиненні продовжуваного злочину, який складається з двох або більше тотожних діянь, об'єднаних єдиним злочинним наміром.

Поняття значної шкоди визначено у примітці до ст. 361 КК України. Питання значної шкоди є питанням факту і потребує вирішення у кожному конкретному випадку з урахуванням всіх обставин справи. Визначення розміру значної шкоди вказано у коментарі до ст.361 КК України.

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

А

Абонент - споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Абонент локальної обчислювальної мережі (абонент ЛОМ) - пристрій, програма чи ЕОМ, під'єднані до локальної обчислювальної мережі, які мають свою мережеву адресу (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Автентифікація - шлях встановлення вірогідності інформації, пред'явленої користувачем у разі звернення його до системи та відкриття йому доступу, якщо він має на це право (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Автоматизована обробка включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних і/або арифметичних операцій з цими даними, змінення, знищення, вибірка або поширення даних (Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру, М.Страсбург, 28 січня 1981 року).

Автоматизована система (АС) - 1. система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах"); 2. організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів)

діяльності людей та персоналу, що здійснює цю діяльність (відповідно ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення)

Автоматизована система оброблення інформації -сукупність технічних та програмних засобів, методів оброблення інформації й дій персоналу, що забезпечують виконання автоматизованого оброблення інформації (ДСТУ. 2226-93 Автоматизовані системи. Терміни і визначення).

Автоматизоване оброблення даних - оброблення даних технічними та програмними засобами з участю людини (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення).

Авторизація - керування рівнями та засобами доступу до різних об'єктів та ресурсів системи залежно від ідентифікатора і пароля користувача (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Адміністратор безпеки - посадова особа, відповідальна за виконання заходів щодо забезпечення захисту ЛОМ від несанкціонованого втручання (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Адміністратор системи - особа або група осіб, що мають повне уявлення про функціональну та програмно-апаратну структуру інформаційної системи і контролюють її проектування та використання (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Адміністрування адресного простору українського сегмента мережі Інтернет - включає комплекс організаційно-технічних заходів, необхідних для забезпечення функціонування технічних засобів підтримки адресування, у тому числі серверів доменних назв українського сегмента мережі Інтернет, реєстру домену в координації з міжнародною системою адміністрування мережі Інтернет, спрямованих на систематизацію та оптимізацію використання, обліку та адміністрування доменів другого рівня, а також створення умов для

використання простору доменних імен на принципах рівного доступу, захисту прав споживачів послуг Інтернет та вільної конкуренції (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Адреса мережі Інтернет - визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Аналіз трафіка - дослідження інформації шляхом спостереження потоків трафіка (наявність і відсутність пересилання даних, кількість блоків даних, напрямок пересилання тощо) (ДСТУ 2230-93. Взаємозв'язок відкритих систем. Базова еталонна модель. Терміни та визначення).

Б

База даних (компіляція даних) - 1. сукупність творів, даних або будь-якої іншої незалежної інформації у повільній формі, в тому числі - електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп'ютера) чи інших засобів (Закон України "Про авторське право і суміжні права" №3792-XII від 23 грудня 1993 року в редакції Закону № 2627-Ш від 11 липня 2001 року); 2. іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області (Закон України № 74/98-ВР від 4 лютого 1998 року "Про Національну програму інформатизації"); 3. незалежна від прикладних програм сукупність даних, що організована за певними правилами, які передбачають загальні принципи описання, зберігання і маніпулювання даними (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи"); 4. пойменована структурована сукупність даних, що відносяться до конкретної предметної галузі (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

База інформаційна АС - сукупність упорядкованої інформації, використовуваної при функціонуванні АС (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Банк даних - система програмно-апаратних, мовних і організаційних засобів, призначених для централізованого накопичення і колективного використання даних, а також самі дані, які зберігаються в базах даних (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Безпека даних автоматизованої системи (безпека даних АС) - властивість організації доступу до даних, що забезпечує їх захист від несанкціонованого використання, навмисного чи ненавмисного спотворення або руйнування (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Безпека інформації - 1. захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи зруйнування даних (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи"); 2. захищеність пристроїв, процесів, програм, середовища та даних, яка забезпечує цілісність інформації, що обробляється, зберігається й пересилається (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Безпека мережі - заходи, які забезпечують захист ЛОМ від несанкціонованого втручання в її роботу чи спроб порушення нормальної роботи її елементів (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ) - електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів

закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру (Закон України № 1280-1V від 18 листопада 2003 року "Про телекомунікації").

Блокування - непрацездатність ресурсу мережі, яка виникає внаслідок одночасних вимог користувачів ресурсу мережі на використання цього ресурсу, що перевищують його пропускну здатність (ДСТУ 2617-94. Електрозв'язок. Мережі та канали передавання даних. Терміни та визначення).

Блокування інформації - 1. дії, наслідком яких є припинення доступу до інформації (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах); 2. унеможливлення санкціонованого доступу до інформації (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення).

В

Введення даних - 1. процес внесення даних до системи оброблення даних чи до будь-якої з її частин для оброблення і, можливо, зберігання (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення); 2. процес занесення даних у пристрої обчислювальної машини (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Взаємоз'єднання телекомунікаційних мереж - встановлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватись інформацією (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Виведення даних - 1. процес продуктування даних будь-яким пристроєм обчислювальної машини (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення); 2. процес, під час якого система оброблення даних чи будь-яка з її частин пересилає дані за межі цієї системи або її частини (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення).

Використання інформації - це задоволення інформаційних потреб громадян, юридичних осіб і держави (Закон України №2657-ХП від 2 жовтня 1992 року "Про інформацію" //Відомості Верховної Ради 1992, № 48, ст. 650).

Витік інформації - 1. результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах"); 2. неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання. (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення).

Відтворення - виготовлення одного або більше примірників твору, відеограми, фонограми в будь-якій матеріальній формі, а також їх запис для тимчасового чи постійного зберігання в електронній (у тому числі цифровій), оптичній або іншій формі, яку може зчитувати комп'ютер (Закон України "Про авторське право і суміжні права" №3792-XII від 23 грудня 1993 року в редакції Закону № 2627-III від 11 липня 2001 року).

Візуалізація (відображення даних) - подання даних у вигляді, який робить їх доступними для безпосереднього сприйняття органами зору людини (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Внутрішньобанківська платіжна система (ВПС) - програмно-технічний комплекс із власними засобами захисту інформації, який експлуатується комерційним банком та його філіями і використовується для здійснення розрахунків між учасниками цієї системи, а також забезпечує взаємодію з СЕП, у тому числі з ІПС. Транспортні потреби системи можуть забезпечуватися системою електронної пошти Національного банку України (система ЕП), власними чи загального користування засобами телекомунікації тощо (Постанова Національного банку України № 621 від 27 грудня 1999 року "Про затвердження Інструкції про міжбанківські розрахунки в Україні").

Втрата інформації - дія, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в

повному чи обмеженому обсязі (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах).

Вузол системи - функціонально та територіальне завершена програмно-апаратна частина системи (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Д

Дані - 1. інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки (Закон України № . 1280-IV від 18.11. 2003 "Про телекомунікації" //Урядовий кур'єр №4 від 24.12.2003); 2. інформація, яка подана у формі, придатній для її оброблення електронними засобами (Закон України № 851-IV від 22 травня 2003 року "Про електронні документи та електронний документообіг"); 3. інформація, яка передається мережею передачі даних незалежно від способу її фізичного та логічного представлення (Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 76 від 24.12.2001 "Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах"); 4. інформація, подана у формалізованому вигляді, придатному для пересилання, інтерпретування чи оброблення за участю людини або автоматичними засобами (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення); 5. інформація, подана у формалізованому вигляді, придатному для зберігання, оброблення, пересилання й інтерпретації користувачами, прикладними процесами чи технічними засобами (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Дані про рух інформації - будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, яка складала частину ланцюгу комунікації, і які зазначають походження, кінцевий пункт, шлях, час, дату, розмір і тривалість

інформації або тип основної послуги (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Джерело даних - функційний пристрій, що формує дані для пересилання (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Джерело інформації - частина комунікаційної системи, яка породжує повідомлення (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Джерело повідомлення - частина системи зв'язку, яка видає оригінал повідомлення (ДСТУ 2396-94. Системи оброблення інформації. Теорія інформації. Терміни і визначення).

Диск жорсткий - жорсткий незмінний металевий диск, покритий магнітним матеріалом і використовуваний як носій інформації великої ємності (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Дискета - гнучкий диск, покритий магнітним матеріалом, що використовується як змінний носій інформації невеликої ємності (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Дистанційне оброблення даних - оброблення даних, за якими деякі функції введення-виведення виконуються пристроями, зв'язаними з комп'ютерною системою за допомогою засобів пересилання даних (ДСТУ 2400-94. Розподілене оброблення даних. Терміни і визначення).

Доступ - звернення для отримання даних (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Доступ до даних -- надання процесу оброблення даних порції даних або прийняття від нього порції даних за допомогою послідовності операцій пошуку, зчитування і (чи) записування даних (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Доступ до інформації (ДДІ) - можливість одержання, оброблення інформації та (чи) порушення її цілісності (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення).

Доступність - властивість інформації бути захищеною від несанкціонованого блокування (Указ Президента України № 1229/99 від 27

вересня 1999 року "Про Положення про технічний захист інформації в Україні").

Драйвер - додаткова до операційної системи програма, що виконує функцію зв'язку операційної системи з зовнішнім пристроєм (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Дублювання даних - копіювання даних таким чином, що фізична форма результату ідентична формі оригіналу, включаючи тип носія (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Е

Електрозв'язок - 1. див. "телекомунікації" (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації"); 2. будь-яке передавання, випромінювання або приймання знаків, сигналів, письмового тексту, зображення та звуків чи повідомлень будь-якого роду провідною, радіо, оптичною чи іншою електромагнітною системою (Постанова Кабінету Міністрів України № 803 від 12 жовтня 1995 року "Про затвердження Національної таблиці розподілу смуг радіочастот України").

Електронна пошта - листування у формі повідомлень, що пересилаються між терміналами користувачів через комп'ютерну мережу (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Електронний підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних (Закон України N 852-IV від 22 травня 2003 року "Про електронний цифровий підпис").

Електронний документ - 1. документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (Закон України № 851-IV від 22 травня 2003 року "Про електронні документи та електронний документообіг"); 2. документ, інформація в якому представлена у формі електронних даних, включаючи відповідні реквізити документа, в тому

числі і електронний цифровий підпис, який може бути сформований, переданий, збережений і перетворений електронними засобами у візуальну форму чи на папері (Закон України № 2346-Ш від 5 квітня 2001 року "Про платіжні системи та переказ грошей в Україні").

Електронний документообіг (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів (Закон України № 851-IV від 22 травня 2003 року "Про електронні документи та електронний документообіг").

Електронний обмін повідомленнями - формування, пересилання, зберігання та пошук тексту, графічних чи звукових даних електронними способами (ДОТУ 2227-93. Автоматизована установа. Терміни і визначення).

Електронний цифровий підпис - 1. вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа (Закон України № 852-IV від 22 травня 2003 року "Про електронний цифровий підпис"); 2. сукупність даних, отримана за допомогою криптографічного перетворення вмісту електронного документа, яка дає змогу підтвердити його цілісність та ідентифікувати особу, яка його підписала (Закон України № 2346-Ш від 5 квітня 2001 року "Про платіжні системи та переказ грошей в Україні").

Електронні засоби захисту - програмно-технічні засоби, які забезпечують захист електронних документів від несанкціонованого доступу та спотворення на етапі передавання цих документів електронною поштою (Наказ Агентства з питань банкрутства № 96 від 6 листопада 1999 року "Про затвердження Положення про порядок формування та ведення єдиної бази

даних про підприємства, щодо яких порушено провадження у справі про банкрутство").

Електронні міжбанківські розрахунки - міжбанківські розрахунки із застосуванням електронних засобів приймання, оброблення, передавання та захисту інформації про рух коштів (Постанова Національного банку України № 621 від 27 грудня 1999 року "Про затвердження Інструкції про міжбанківські розрахунки в Україні").

З

Забезпечення організаційне автоматизованої системи (забезпечення організаційне АС) - сукупність документів, що установлюють організаційну структуру, права та обов'язки персоналу і користувачів при експлуатації АС. (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Забезпечення програмне автоматизованої системи (забезпечення програмне АС) - сукупність програм, процедур, правил та документації, що стосуються функціонування АС (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Забезпечення технічне автоматизованої системи (забезпечення технічне АС) - сукупність технічних та комунікаційних засобів, що використовуються під час функціонування АС (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Загальне програмне забезпечення АС – частина програмного забезпечення АС (операційна система, драйвери тощо), призначена для організації обчислювального процесу (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Загроза для інформації - витік, можливість блокування або порушення цілісності інформації. Примітка. Загроза для інформації може здійснюватися під час застосування технічних засобів чи технологій, недосконалих щодо захисту інформації (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення).

Закладний пристрій (закладка) - потай встановлюваний технічний засіб, який створює загрозу для інформації (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення).

Записування даних - процес занесення даних у запам'ятовувальний пристрій чи носій даних (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису (Закон України № 852-IV від 22 травня 2003 року "Про електронний цифровий підпис").

Засоби апаратні - сукупність пристроїв, що використовується для оброблення даних (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Засоби інформатизації - електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій (Закон України № 74/98-ВР від 4 лютого 1998 року "Про Національну програму інформатизації").

Засоби комунікаційні (мережа) - сукупність ліній пересилання даних та комунікаційних пристроїв, що дозволяє здійснювати взаємне сполучення прикінцевого обладнання (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Засоби технічні автоматизованої системи (засоби технічні АС) - сукупність апаратних і комунікаційних засобів, носіїв та допоміжних матеріалів, що забезпечують реалізацію функцій АС (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Захист - засіб обмеження доступу до використання всієї обчислювальної системи чи її частини. (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Захист даних - організаційні, програмні й технічні методи та засоби, спрямовані на реалізацію обмежень доступ до даних, установлених для типів даних у системі оброблення даних. (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Захист інформації - 1. сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах); 2. заходи, спрямовані на збереження інформації від небажаних наслідків дій, що навмисно або випадково призводять до модифікації. розкриття чи руйнування даних.(Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Зберігання інформації - це забезпечення належного стану інформації та її матеріальних носіїв.(Закон України №2657-XII від 2 жовтня 1992 року "Про інформацію").

Зберігання даних - режим роботи запам'ятовувального пристрою після запису даних, що забезпечує можливість їх подальшого зчитування в довільний момент часу (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Збирання даних - процес ідентифікації, відбору й накопичення даних, що підлягають обробленню (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Здавання у майновий найм - передача права користування і (або) володіння оригіналом чи примірником твору, фонограми, відеограми на певний строк з метою одержання прямої чи опосередкованої комерційної вигоди (Закон України "Про авторське право і суміжні права" №3792-ХП від 23 грудня 1993 року в редакції Закону № 2627-111 від 11 липня 2001 року).

Зловживання пристроями - а) виробництво, продаж, придбання для використання, розповсюдження або надання для використання іншим чином: пристроїв, включаючи комп'ютерні програми, створених або адаптованих для

вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 Конвенції; .комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до комп'ютерної системи з наміром її використання для вчинення незаконного доступу, нелегального перехоплення, протиправного втручання в комп'ютерні дані чи комп'ютерну систему; в) володіння одним із предметів, зазначених у попередньому пункті з наміром його використання для вчинення незаконного доступу, нелегального перехоплення, протиправного втручання в комп'ютерні дані чи комп'ютерну систему(Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Злочини у сфері комп'ютерної інформації - кримінальне каране діяння, предметом посягання якого є комп'ютерна інформація (Угода про співробітництво держав-учасників Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації, м.Мінськ, 1 червня 2001 року).

Зовнішня завада - завада обчислювальній машині, джерело якої не е частиною обчислювальної машини (ДСТУ 2668-94. Системи оброблення інформації. Безвідмовність, обслуговування та готовність. Терміни та визначення).

Зчитування даних - процес отримання даних із запам'ятовувального пристрою, з носія даних чи з інших джерел (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

І

Ідентифікація - засіб встановлення: а) тотожності особи за сукупністю її загальних та окремих даних; б) повноважень користувача системи за допомогою пароля (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Інтерактивний режим - режим взаємодії користувача з обчислювальною системою, при якому система здійснює приймання, оброблення і видачу повідомлень в реальному масштабі часу (Постанова Кабінету Міністрів

України № 40 від 20 січня 1997 р. "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Інтернет - всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами (Закон України № 1280-TV від 18 листопада 2003 року "Про телекомунікації").

Інтерфейс - сукупність програмно-апаратних засобів, призначених для здійснення функцій обміну інформацією між різноманітними пристроями в обчислювальних машинах, системах і мережах (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 р. "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Інформатизація - сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які .побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки (Закон України № 74/98-ВР від 4 лютого 1998 року "Про Національну програму інформатизації").

Інформаційна безпека телекомунікаційних мереж - здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації (Закон України № 1280-1V від 18 листопада 2003 року "Про телекомунікації").

Інформаційна послуга - 1. це здійснення у визначеній законом формі інформаційної діяльності по доведенню інформаційної продукції до споживачів з метою задоволення їх інформаційних потреб (Закон України №2657-XII від 2 жовтня 1992 року "Про інформацію"); 2. дії суб'єктів щодо забезпечення споживачів інформаційними продуктами (Закон України № 74/98-ВР від 4 лютого 1998 року "Про Національну програму інформатизації").

Інформаційна продукція - це матеріалізований результат інформаційної діяльності, призначений для задоволення інформаційних потреб громадян, державних органів, підприємств, установ і організацій (Закон України №2657-XII від 2 жовтня 1992 року "Про інформацію").

Інформаційна система - 1. система оброблення даних засобами накопичення, зберігання, обновлення та їх пошуку і відображення (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи"); 2. автоматизована система, комп'ютерна мережа або система зв'язку (Указ Президента України № 1229/99 від 27 вересня 1999 року "Про Положення про технічний захист інформації в Україні"; спільний наказ Державного комітету з питань регуляторної політики та підприємництва, Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 89/67 від 29 грудня 2000 року "Про затвердження Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації").

Інформаційна система загального доступу - сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних (Закон України № 12 80-1V від 18 листопада 2003 року "Про телекомунікації").

Інформаційна технологія - цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування (Закон України № 74/98-ВР від 4 лютого 1998 року "Про Національну програму інформатизації").

Інформаційне забезпечення автоматизованої системи - інформаційна база автоматизованої системи і засоби її організації та реалізації (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Інформаційне повідомлення - інформація в електронній формі, призначена для використання в програмно-технічних комплексах інформаційно-обчислювальної мережі Національного банку України (крім СЕП), що має визначений формат і технологію обробки згідно з вимогами відповідного програмно-технічного комплексу, передається засобами телекомунікаційного зв'язку та зберігається на зовнішніх засобах збереження інформації у вигляді файла (Постанова Національного банку України № 621 від 27 грудня 1999 року "Про затвердження Інструкції про міжбанківські розрахунки в Україні").

Інформаційний продукт (продукція) - документована інформація, яка підготовлена і призначена для задоволення потреб користувачів (Закон України № 74/98-ВР від 4 лютого 1998 року "Про Національну програму інформатизації").

Інформаційний ресурс - сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) (Закон України № 74/98-ВР від 4 лютого 1998 року "Про Національну програму інформатизації").

Інформаційний ринок - система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг (Закон України № 3322-XII від 25 червня 1993 року "Про науково-технічну інформацію").

Інформаційно-аналітична система - автоматизована інформаційна система, призначена для аналізу і синтезу з деякого первісного масиву даних, що зберігаються в ній, нової інформації, яка в явному вигляді відсутня в первісному масиві (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Інформаційно-телекомунікаційна система - організаційно-технічна сукупність, що складається з автоматизованої системи та мережі передачі даних (Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 76 від 24 грудня 2001 року "Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах").

Інформація - 1. документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі (Відповідно Закону України № 2657-ХП від 2 жовтня 1992 року "Про інформацію"); 2. відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб (Закон України № 1280-1V від 18.11.2003 "Про телекомунікації"); 3. відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості (Закон України № 2210-ИИ від 11 січня 2001 року "Про захист економічної конкуренції"); 4. сукупність відомостей, знань і повідомлень про об'єкти, явища і процеси (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Інформація (для процесу оброблення даних) - будь-які знання про предмети, факти, поняття і т.ін. проблемної сфери, якими обмінюються користувачі системи оброблення даних (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення).

Інформація в автоматизованих системах - сукупність усіх даних і програм, які використовуються в автоматизованих системах незалежно від засобу їх фізичного та логічного представлення (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах").

Інформація вихідна автоматизованої системи (інформація вихідна АС) - інформація, отримувана в результаті виконання функцій АС (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Інформація вхідна автоматизованої системи (інформація вхідна АС) - інформація, що надходить до АС у вигляді документів, повідомлень сигналів та є необхідною для виконання функцій АС (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Інформація з обмеженим доступом - інформація, права доступу до якої обмежено встановленими правовими нормами і (чи) правилами (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення).

К

Канал електрозв'язку - сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і який характеризується смугою частот та/або швидкістю передачі (Закон України № 1280-1V від 18 листопада 2003 року "Про телекомунікації").

Канал зв'язку - засоби двостороннього обміну даними як сукупність апаратури закінчення ланки даних та лінії пересилання даних (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Керування доступом - заборона несанкціонованого користування ресурсом, включаючи заборону користування ресурсом недозволеними способами (ДСТУ 2230-93. Взаємозв'язок відкритих систем. Базова еталонна модель. Терміни і визначення).

Кінцеве обладнання - обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Кінцевий користувач - людина, пристрій, програма або комп'ютерна система, що використовують комп'ютерну мережу для опрацювання даних та

обміну інформацією (ДСТУ 2400-94. Розподілене оброблення даних. Терміни і визначення).

Клієнт - комп'ютер, що користується послугами іншого комп'ютера, який в цьому випадку називається сервером (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Клієнт-серверна технологія - технологія оброблення даних, за якої клієнт-комп'ютер звертається за необхідними даними до головного комп'ютера (сервера), при цьому власне оброблення даних може виконуватися як на клієнтському, так і серверному комп'ютері (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Кодування даних - конвертування даних за допомогою коду із забезпеченням можливості зворотного перетворення їх до початкового вигляду (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Комп'ютер - 1. електронна цифрова обчислювальна машина (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення); 2. функційний пристрій, що складається з одного або кількох взаємопов'язаних центральних процесорів і периферійних пристроїв і може виконувати обчислення без участі людини (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення).

Комп'ютерна мережа - 1. сукупність територіальне розосереджених систем оброблення даних, засобів і (чи) систем зв'язку і пересилання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення); 2. мережа, в одного або кількох вузлах якої як ресурс оброблення даних містяться комп'ютери (ДСТУ 2400-94. Розподілене оброблення даних. Терміни і визначення).

Комп'ютерна система - 1. будь-який пристрій або група взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, у відповідності до певної програми, виконує автоматичну обробку даних (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року); 2. комп'ютер з підключеними до нього зовнішніми пристроями та системними програмними засобами (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Комп'ютерні дані - будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті (Указ Президента України № 1229/99 від 27 вересня 1999 року "Про Положення про технічний захист інформації в Україні").

Комп'ютерна інформація - інформація, яка знаходиться у пам'яті комп'ютера, на машинних або інших носіях у формі, доступної сприйняттю ЕОМ, або яка передається по каналам зв'язку (Угода про співробітництво держав-учасників Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації, м.Мінськ, 1 червня 2001 року).

Комп'ютерна програма - набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) (Закон України "Про авторське право і суміжні права" №3792-XII від 23 грудня 1993 року в редакції Закону № 2627-ІП від 11 липня 2001 року).

Комп'ютерний вірус - програма, що розмножується та поширюється самочинно (ДСТУ 3396.2-97. Технічний захист інформації. Терміни і визначення).

Комунікаційні послуги - послуги зв'язку, у тому числі телекомунікаційні, забезпечення телефонного, телексного, телеграфного зв'язку, радіомовлення, електронної пошти, супутникового, факсимільного та телевізійного зв'язку, поштові послуги (Постанова Правління НБУ № 433 від 1 вересня 1999 року "Про затвердження Доповнення № 16 до Правил організації фінансової та статистичної звітності банків України). Комутація каналів - процес з'єднання двох чи більше абонентських станцій, який забезпечує монопольне використання каналу пересилання даних до його роз'єднання (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Комутація пакетів - процес пересилання частин повідомлення, поділеного на пакети, .коли канал пересилання даних зайнятий лише на час пересилання пакету; після завершення пересилання даного пакету канал звільняється для пересилання інших пакетів (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Комутація повідомлень - процес пересилання даних, що включає приймання, збереження, вибір необхідного напрямку та подальше пересилання повідомлень без порушення їх цілісності (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Конвертування даних - зміна форми подання даних без зміни їх змісту (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Конфіденціальна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов (Закон України №2657-ХП від 2 жовтня 1992 року "Про інформацію").

Конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення (Указ Президента України № 1229/99 від 27 вересня 1999 року "Про Положення про технічний захист інформації в Україні").

Конфіденційність інформації - доступність інформації тільки адресату (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Копіювання даних (копіювання) - зчитування даних з одного носія даних і запис їх на інший носій даних або в інше місце того самого носія даних без зміни початкової форми даних (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Копія документа тверда - виведений на папір чи інший аналогічний носій даних документ, оригінал якого зберігається в пам'яті комп'ютера (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Коригування даних - зміна даних, що не зачіпає їхню структуру (ДСТУ 2226-93 Автоматизовані системи. Терміни і визначення).

Користувач - будь-яка особа або будь-який об'єкт, який може пересилати команди чи повідомлення в систему оброблення даних або приймати їх від неї (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Користувач автоматизованої системи - 1. фізична або юридична особа, яка має право використання АС за угодою із розпорядником АС (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах"); 2. особа, що бере участь у функціонуванні автоматизованої системи або має право використовувати і використовує результати її функціонування (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Користувач, який пересилає - користувач ЛОМ, який виступає як джерело даних під час їх пересилання (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Л

Лінгвістичне забезпечення автоматизованої системи - тезауруси та мовні засоби опису і маніпулювання даними, використувані в автоматизованих системах (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Локальна обчислювальна мережа (ЛОМ) - система, яка забезпечує на обмеженій території один чи декілька каналів зв'язку, наданих приєднаним до неї абонентам для короткочасного монопольного користування (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

М

Маршрутизатор - блок взаємодії, який забезпечує вибір маршруту пересилання даних між кількома ЛОМ, які мають різну архітектуру чи протоколи (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Маршрутизація - функція всередині рівня, що виконує перетворення символічного імені логічного об'єкта або адреси пункту доступу до сервісу, до якого підключено логічний об'єкт, у маршрут, за яким може встановлюватися зв'язок із вказаним логічним об'єктом (ДСТУ 2230-93. Взаємозв'язок відкритих систем. Базова електронна модель. Терміни та визначення).

Машина обчислювальна персональна (комп'ютер персональний, ПОМ) - комп'ютер, призначений для обслуговування одного користувача, що характеризується невеликими габаритами, підвищеною надійністю, простотою зміни конфігурації та розвинутими засобами діалогу (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Машина обчислювальна цифрова електронна (ЕОМ) - сукупність технічних засобів та системного програмного забезпечення, яка створює можливість проведення оброблення інформації та отримання результату в

необхідній формі (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Мережа електрозв'язку загального користування - мережа електрозв'язку, що експлуатується операторами для забезпечення потреб у послугах електрозв'язку всіх споживачів (Наказ Державного комітету зв'язку та Інформатизації України № 113 від 21 червня 1999 року "Про затвердження Правил приєднання мереж електрозв'язку операторів різних форм власності до мереж електрозв'язку загального користування").

Мережа інформаційна - сукупність мережі ЕОМ і відділених реальних прикінцевих систем, що взаємодіють через мережу ЕОМ, яка забезпечує доступ прикладних процесів, розташованих в будь-якій із цих систем, до всіх її інформаційних, обчислювальних, комунікаційних ресурсів і колективне їх використання (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Мережа обчислювальних машин - система сполучених між собою комунікаційними засобами ЕОМ різної продуктивності та конфігурації (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Мережа передачі даних - організаційно-технічна система, яка складається з комплексів телекомунікаційного обладнання (вузлів комутації) та реалізує технологію інформаційного обміну з використанням первинної мережі зв'язку (Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 76 від 24 грудня 2001 року "Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах").

Метод доступу - сукупність засобів та угод, за допомогою яких реалізується заданий вид доступу до даних (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Моніторинг мережі - збір, обробка, збереження та аналіз інформації про поточний стан мережі без втручання в її функціонування (Наказ Державного комітету зв'язку та інформатизації України №19 від 14.02.2001 "Про

затвердження Положення про діяльність операторів міжміського, міжнародного зв'язку телефонної мережі загального користування України та їх взаємодію між собою").

Н

Незаконний доступ - протиправний навмисний доступ до комп'ютерної системи або її частині (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Нелегальне перехоплення - протиправне навмисне перехоплення технічними засобами, передач комп'ютерних даних, які не призначені для публічного користування, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Неправомірний доступ - несанкціоноване звернення до комп'ютерної інформації (Угода про співробітництво держав-учасників Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації, м.Мінськ, 1 червня 2001 року).

Несанкціонований доступ - 1. доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах); 2. протиправне використання програмно-технічних засобів СЕП, системи автоматизації банку, ВПС або спроба перейняття, нав'язування, підроблення чи викривлення інформації про рух коштів або службових повідомлень цих систем (Постанова Національного банку України № 621 від 27 грудня 1999 року "Про затвердження Інструкції про міжбанківські розрахунки в Україні").

Несанкціонований доступ до інформації (НДДІ) - доступ до інформації, за якого порушуються порядок його здійснення і встановлені правові норми (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення).

Несправний стан (системи); несправність - стан об'єкту, у якому він не здатний виконувати хоч би одну із своїх заданих функцій (ДСТУ 2668-94. Системи оброблення інформації. Безвідмовність, обслуговування та готовність. Терміни та визначення).

Носій даних - об'єкт, призначений для запису, зберігання, зчитування або пересилання даних (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Носій даних (у ЛОМ) - сигнал, отриманий внаслідок накладення потоку даних на несучу й придатний для пересилання крізь середовище пересилання (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Носій даних (у системах оброблення даних) - матеріальний об'єкт, призначений для запису, зчитування і зберігання даних (ДСТУ 2938-94. Системи оброблення даних. Основні понятгя. Терміни та визначення).

О

Обробка інформації - вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах").

Оброблення даних - процес виконання операцій з даними (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення): — систематичне виконання операцій над даними (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Оброблення даних автоматизоване - оброблення даних, що виконується автоматичними засобами при можливій участі людини (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Оброблення інформації - систематичне виконання операцій над інформацією (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Одержання інформації - це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою (Закон України №2657-ХП від 2 жовтня 1992 року "Про інформацію").

Оператор телекомунікацій - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Оприлюднення (розкриття публіці) твору - здійснена за згодою автора чи іншого суб'єкта авторського права і (або) суміжних прав дія, що вперше робить твір доступним для публіки шляхом опублікування, публічного виконання, публічного показу, публічної демонстрації, публічного сповіщення тощо (Закон України "Про авторське право і суміжні права" №3792-ХП від 23 грудня 1993 року в редакції Закону № 2627-ІП від 11 липня 2001 року).

Організаційне забезпечення автоматизованої системи -сукупність документів, що установлюють організаційну структуру, права та обов'язки персоналу і користувачів при експлуатації автоматизованої системи (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

П

Пакування даних - процес подання даних у компактному вигляді на носії даних за допомогою конвертування з використанням властивостей даних і носія для забезпечення можливості відновлення початкової форми даних (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Пароль - секретний код, що використовується з метою забезпечення конфіденційності інформації (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Перевантаження ЛОМ - стан ЛОМ, у якому в наслідок надмірного навантаження погіршуються її експлуатаційні характеристики (ДСТУ 2229-93.

Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Перегляд даних - систематичний аналіз даних (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Передавання даних - 1. передавання інформації у вигляді даних з використанням телекомунікаційних мереж (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації"); 2. Вид електрозв'язку з множинним доступом до каналу зв'язку на основі комутації частин інформації визначеної довжини та структури (комутації пакетів) за визначеним порядком (Наказ Державного комітету зв'язку та інформатизації України №22 від 19.02.2001 "Про затвердження змін та доповнень до Регламенту аматорського радіозв'язку України").

Переписування даних - копіювання даних з одного носія даних на інший з можливим конвертуванням даних (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Пересилання даних - процес переміщення даних між віддаленими функційними пристроями, здійснюваний за допомогою засобів зв'язку від джерела даних в один чи кілька пунктів призначення (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Пересилання даних (в обчислювальній машині) - процес переміщення даних з однієї ділянки запам'ятовувального пристрою в іншу (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Перетворення даних - модифікація форми даних за певними правилами без ґрунтовної зміни їх значення (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Персонал автоматизованої системи - 1. фізичні особи, яких власник АС або уповноважена ним особа чи розпорядник АС визначили для здійснення функцій управління та обслуговування АС (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах"); 2.

сукупність осіб, що забезпечують функціонування автоматизованої системи (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Персоналом оператора, провайдера телекомунікацій - є всі працівники, які перебувають з ним у трудових відносинах (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Персональний комп'ютер - комп'ютер, призначений переважно, для автономного використання людиною (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення).

Підробка інформації - навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах").

Підробка, пов'язана з комп'ютерами - протиправне навмисне введення, зміна, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважалися або у відповідності до них проводилися б дії, як з дійсними, незалежно від того чи можна такі дані прямо прочитати і зрозуміти, чи ні (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Повідомлення (в теорії інформатизації та теорії зв'язку) - впорядковані серії символів, призначені для пересилання інформації (ДСТУ 2396-94. Системи оброблення інформації. Теорія інформації. Терміни і визначення).

Повноваження - дозвіл абоненту ЛОМ виконувати необхідні дії (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Портативний комп'ютер - комп'ютер, розрахований на те, що його можна переносити вручну і розміщувати для роботи у більш ніж одному місці (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення).

Порушення інформації - спотворення інформації, її руйнування або знищення (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення).

Порушення роботи АС - дії або обставини, які призводять до спотворення процесу обробки інформації (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах").

Порушення цілісності інформації - спотворення інформації, її руйнування або знищення (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення).

Порушник - фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо АС та інформації в ній (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах").

Послуга електрозв'язку - продукт (результат) діяльності оператора електрозв'язку, що полягає в передаванні, прийманні та обробці інформації (споживача) (Наказ Державного комітету зв'язку та інформатизації України №19 від 14.02.2001 "Про затвердження Положення про діяльність операторів міжміського, міжнародного зв'язку телефонної мережі загального користування України та їх взаємодію між собою").

Постачальник послуг - будь-яка державна або приватна установа, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та будь-яка інша установа, яка обробляє або зберігає комп'ютерні дані від імені такої послуги або користувачів такої послуги (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Поширення інформації - це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації (Закон України №2657-XII від 2 жовтня 1992 року "Про інформацію").

Пошук даних - аналіз елементів даних з метою знаходження даних з певними властивостями (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Право власності на інформацію - це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією (Закон України №2657-XII від 2 жовтня 1992 року "Про інформацію").

Правове забезпечення автоматизованої системи - сукупність норм, що регламентують правові взаємини при функціонуванні автоматизованої системи та юридичний статус результатів її функціонування (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Прикладна програма - програма, що призначена для розв'язання задачі або класу задач в певній області застосування систем оброблення даних (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Прикладні програмні засоби - програмні засоби призначені для виконання прикладної задачі (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Провайдер телекомунікацій - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації" //Урядовий кур'єр №4 від 24.12.2003).

Проводовий електрозв'язок - передавання і приймання інформації із застосуванням проводових ліній з металевими або волоконнооптичними жилами (Закон України № 1280-1V від 18 листопада 2003 року "Про телекомунікації" //Урядовий кур'єр №4 від 24.12.2003).

Програма - послідовність команд для здійснення процесу, яка надається в такій формі, що вона може бути виконана електронним комп'ютером або

може бути перетворена в таку форму (Постанова Кабінету Міністрів України № 302 від 12 березня 1996 року "Про затвердження Положення про порядок контролю за експортом, імпортом і транзитом товарів, що стосуються ядерної діяльності та можуть бути використані у створенні ядерної зброї").

Програмна закладка - потай впроваджена програма, яка створює загрозу для інформації, що міститься у комп'ютері (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення).

Програмне забезпечення автоматизованої системи - сукупність програм, процедур, правил та документації, що стосуються функціонування автоматизованої системи (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Програмний засіб - взаємопов'язана сукупність програм, і процедур правил, документації та даних, що належить до функціонування обчислювальної системи (ДСТУ 2844-94. Програмні засоби ЕОМ забезпечення якості. Технічний захист інформації. Терміни і визначення).

Програмні засоби - засоби, що складаються з програм і документації, яка стосується їх функціонування. (ДСТУ 2938-94. Системи оброблення даних. Основні поняття. Терміни та визначення).

Протиправне втручання в дані - навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Протиправне втручання в систему – навмисне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, зміни або припинення комп'ютерних даних (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Протокол - 1. набір семантичних і синтаксичних правил, що визначають поведінку функціональних блоків під час передачі даних (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи"); 2. Сукупність правил, що регламентують сукупність правил і процедури обміну

даними між двома чи кількома незалежними процесами (пристроями) (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Процес оброблення даних - наперед визначений хід дій, які мають місце під час виконання програм (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Публічне сповіщення (доведення до загального відома) - передача за згодою суб'єктів авторського права і (або) суміжних прав в ефір за допомогою радіохвиль (а також лазерних променів, гамма-променів тощо), у тому числі з використанням супутників, чи передача на віддаль за допомогою проводів або будь-якого виду наземного чи підземного (підводного) кабелю (провідникового, оптоволоконного та інших видів) творів, виконань, будь-яких звуків і (або) зображень, їх записів у фонограмах і відеограмах, програм організацій мовлення тощо, коли зазначена передача може бути сприйнята необмеженою кількістю осіб у різних місцях, віддаленість яких від місця передачі є такою, що без зазначеної передачі зображення чи звуки не можуть бути сприйняті (Закон України "Про авторське право і суміжні права" №3792-ХП від 23 грудня 1993 року в редакції Закону № 2627-ІП від 11 липня 2001року).

Р

Редагування даних - підготовлення даних до дальшого оброблення (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Ресурс - елемент системи оброблення даних, необхідний під час виконання операцій (ДСТУ 2938-94. Основні поняття. Терміни та визначення).

Ресурс мережі - організаційне, інформаційне, програмне та технічне забезпечення мережі з пакетною комутацією, призначене для виконання як окремих так і всіх функцій мережі (ДСТУ 2617-94 Електрозв'язок. Мережі та канали передавання даних. Терміни та визначення).

Ресурси ЛОМ - програмне, технічне, інформаційне й організаційне забезпечення ЛОМ, призначене для виконання прикладних процесів (ДСТУ

2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Розміщення даних (розміщення) - розташування даних відповідно до певних критеріїв впорядкування (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Розповсюдження об'єктів авторського права і (або) суміжних прав - будь-яка дія, за допомогою якої об'єкти авторського права і (або) суміжних прав безпосередньо чи опосередковано пропонуються публіці, в тому числі доведення цих об'єктів до відома публіки таким чином, що її представники можуть здійснити доступ до цих об'єктів з будь-якого місця і в будь-який час за власним вибором (Закон України "Про авторське право і суміжні права" №3792-XII від 23 грудня 1993 року в редакції Закону № 2627-ІГІ від 11 липня 2001 року).

Розподіл ресурсів - призначення засобів комп'ютерної системи для виконання завдань (ДСТУ 2940-94. Керування процесами оброблення даних. Терміни та визначення).

Розпорядник АС - фізична або юридична особа, яка має право розпоряджання АС за угодою з її власником або за його дорученням (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах").

Рухомий (мобільний) зв'язок - електрозв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції (Закон України №1280-IV від 18 листопада 2003 року "Про телекомунікації").

С

Санкціонування - підтвердження права доступу до ресурсу (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Сервер - 1. комп'ютер, що надає послуги іншим комп'ютерам у мережі, які називаються клієнтами (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи"); 2. абонент ЛОМ, який обслуговує інших абонентів ЛОМ (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Сервер бази даних - програмно-апаратний комплекс, який зберігає дані та приймає й обробляє запити, що керують цими даними (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Система електронних платежів Національного банку України (СЕП) - загальнодержавна платіжна система, що забезпечує здійснення розрахунків між банківськими установами, органами державного казначейства на території України із застосуванням електронних засобів приймання, оброблення, передавання та захисту інформації (Постанова Національного банку України № 621 від 27 грудня 1999 року "Про затвердження Інструкції про міжбанківські розрахунки в Україні").

Система зв'язку - канал зв'язку разом з джерелом і приймачем інформації (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Система оброблення даних - комплекс технічних і математичних засобів, що виконує автоматизоване оброблення даних, включаючи апаратні засоби оброблення даних, методи і процедури, програмне забезпечення і відповідний персонал (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Система оброблення інформації автоматизована - сукупність технічних і програмних засобів, методів оброблення інформації й дій персоналу, що забезпечують виконання автоматизованого оброблення інформації (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Система операційна - 1. організована певним чином сукупність керівних та оброблювальних програм, що забезпечують найекономніший розподіл ресурсів обчислювальної системи та виконання програм (ДСТУ 2226-93 Автоматизовані системи. Терміни і визначення); 2. сукупність програмних засобів, призначених для автоматизованого керування виконанням програмами та надання користувачам певних послуг (ДСТУ 2938-94 Системи оброблення інформації. Основні поняття. Терміни і визначення).

Системні програмні засоби - програмні засоби, що не залежать від прикладних програмних засобів і підтримують їх роботу (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Список доступу - перелік користувачі ЛОМ, яким дозволений доступ до ресурсів ЛОМ з вказівкою наданих прав доступу (ДСТУ 2229-93. Системи оброблення даних. Локальні обчислювальні мережі. Терміни та визначення).

Споживач телекомунікаційних послуг (споживач) - юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Суб'єктами відносин, пов'язаних з обробкою інформації в АС, є: 1)власники інформації чи уповноважені ними особи; 2) власники АС чи уповноважені ними особи; 3) користувачі інформації; 4) користувачі АС (Закон України № 80/94-ВР від 5 липня 1994 року "Про захист інформації в автоматизованих системах").

Суб'єкти ринку телекомунікацій - оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Т

Тезаурус - словник найменувань, понять та їх класифікаційних зв'язків, призначений для єдиного уніфікованого та формалізованого подання

інформації в АС (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Телебачення - вид електрозв'язку, призначений для передачі змінних зображень нерухомих та рухомих об'єктів (Наказ Державного комітету зв'язку та інформатизації України №22 від 19.02.2001 "Про затвердження змін та доповнень до Регламенту аматорського радіозв'язку України").

Телеграфія - вид електрозв'язку для передавання текстової інформації з використанням сигнального коду (Наказ Державного комітету зв'язку та інформатизації України №22 від 19.02.2001 "Про затвердження змін та доповнень до Регламенту аматорського радіозв'язку України").

Телекомунікації (електрозв'язок) - передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Телекомунікаційна мережа доступу - частина телекомунікаційної мережі між пунктом закінчення телекомунікаційної мережі та найближчим вузлом (центром) комутації включно (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації"").

Телекомунікаційна мережа загального користування - телекомунікаційна мережа, доступ до якої відкрито для всіх споживачів (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Телекомунікаційна послуга (послуга) - продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Телемережі - телекомунікаційні мережі загального користування, що створюються в межах одного населеного пункту і призначаються для передавання абонентам програм радіо- та телебачення з використанням штучного спрямовуючого середовища і які можуть інтегруватися в

телекомунікаційні мережі загального користування загальнодержавного рівня (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Телефонія - вид електрозв'язку, призначений, головним чином, для обміну інформації у вигляді мови (Наказ Державного комітету зв'язку та інформатизації України №22 від 19.02.2001 "Про затвердження змін та доповнень до Регламенту аматорського радіозв'язку України").

Термінал (в автоматизованих системах) - комплекс технічних та програмних засобів (від найпростішого пристрою введення-виведення даних до комп'ютера), призначений для зв'язку користувача з обчислювальною системою чи інформаційною мережею (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Термінал (користувача) - 1. функційний пристрій для взаємодії людини (користувача чи оператора) з комп'ютером (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення); 2. периферійний пристрій введення-виведення, що забезпечує взаємодію користувача з ЕОМ (ДСТУ 2869-94. Обладнання периферійне. Терміни та визначення).

Технічна компетентність уповноваженого органу - сукупність ознак, що включають наявність належного обладнання, нормативно-методичної документації та кваліфікації персоналу цього органу, які дозволяють на професійному рівні проводити атестацію фахівців з неруйнівного контролю (Наказ Державного комітету України по нагляду за охороною праці № 126 від 23 липня 1996 року "Про зміни та доповнення до Правил атестації фахівців неруйнівного контролю").

Технічна розвідка - несанкціоноване здобуття інформації за допомогою технічних засобів та її аналіз (ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення).

Технічне забезпечення автоматизованої системи - сукупність технічних та комунікаційних засобів, що використовуються під час функціонування

автоматизованої системи (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Технічне обслуговування (системи); обслуговування - будь-яка діяльність, призначена для збереження або відновлення працездатності функційного модуля (системи) (ДСТУ 2668-94. Системи оброблення інформації. Безвідмовність, обслуговування та готовність. Терміни та визначення).

Технічний засіб обробки інформації - технічний засіб, призначений для приймання, накопичення, зберігання, пошуку, перетворення, відображення та передавання інформації каналами зв'язку (Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації № 53 від ЗО листопада 1999 року "Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації").

Технічний захист інформації - вид захисту інформації, який реалізується інженерно-технічними заходами перешкод несанкціонованому доступу до інформації та впливу на неї (Протокол №2 до Угоди між Урядом України та Урядом Грузії про співробітництво в галузі урядового зв'язку м.Тбілісі, 4 серпня 2000 року).

Технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації (Указ Президента України № 1229/99 від 27 вересня 1999 року "Про Положення про технічний захист інформації в Україні"; спільний наказ Державний комітет стандартизації, сертифікації та метрології України, Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 329/32 від 9 липень 2001 року "Про затвердження Порядку проведення робіт з сертифікації засобів забезпечення технічного захисту інформації загального призначення").

Технічний захист секретної інформації - вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та

унеможливлення блокування інформації (Закон України № 3855-XII від 21 січня 1994 року "Про державну таємницю").

Технічні засоби автоматизованої системи - сукупність апаратних і комунікаційних засобів, носіїв даних та допоміжних матеріалів, що забезпечують реалізацію функцій автоматизованої системи (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Технічні засоби захисту - технічні пристрої і (або) технологічні розробки, призначені для створення технологічної перешкоди порушенню авторського права і (або) суміжних прав при сприйнятті і (або) копіюванні захищених (закодованих) записів у фонограмах (відеограмах) і передачах організацій мовлення чи для контролю доступу до використання об'єктів авторського права і суміжних прав (Закон України "Про авторське право і суміжні права" №3792-XII від 23 грудня 1993 року в редакції Закону № 2627-IH від 11 липня 2001 року).

Технічні засоби телекомунікацій - обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації" //Урядовий кур'єр №4 від 24.12.2003).

Транзакція - одиниця роботи в системах керування базами даних, що характеризується логічною завершеністю всіх взаємодій з базою даних.(Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

Транспортна телекомунікаційна мережа - мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу (Закон України № 1280-IV від 18 листопада 2003 року "Про телекому н ікації").

Трафік - інтенсивність потоку повідомлень у мережі передачі даних (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про

затвердження Концепції створення Єдиної державної автоматизованої паспортної системи").

У

Ущільнення даних - процес скорочення обсягу даних на носії даних за допомогою кодування чи вилучення символів, що повторюються (ДСТУ 2228-93. Системи оброблення даних. Підготовлення і оброблення даних. Терміни та визначення).

Ф

Файл - сукупність зв'язаних записів, яка сприймається як єдине ціле (ДСТУ 2505-94. Організація даних. Терміни і визначення).

Фіксований зв'язок - телекомунікації, що здійснюються із застосуванням стаціонарного (нерухомого) кінцевого обладнання (Закон України № 1280-IV від 18 листопада 2003 року "Про телекомунікації").

Функційне програмне забезпечення - частина програмного забезпечення АС, що реалізує функції АС (ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення).

Функційний пристрій - сукупність технічних і (чи) програмних засобів, призначених для досягнення конкретної мети (ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення).

Функція автоматизованої системи (функція АС) - сукупність дій АС, спрямованих на досягнення певної мети (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення).

Ц

Цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення (Указ Президента України № 1229/99 від 27 вересня 1999 року "Про Положення про технічний захист інформації в Україні").

Цілісність даних - 1. умови, за яких дані зберігаються для використання згідно з призначенням, передаються та приймаються без змін і купюр (Постанова Кабінету Міністрів України № 40 від 20 січня 1997 року "Про

затвердження Концепції створення Єдиної державної автоматизованої паспортної системи"); 2. якість, яка свідчить про те, що дані не змінювались або не вилучались несанкціонованим способом (ДСТУ 2230-93. Взаємозв'язок відкритих систем. Базова еталонна модель. Терміни та визначення).

Ш

Шахрайство, пов'язане з комп'ютерами - протиправне навмисне вчинення дій, з шахрайською або нечесною метою набуття економічних переваг для себе чи іншої особи, що приводять до втрати майна іншої особи шляхом: а) будь-якого введення, зміни, знищення або приховування комп'ютерних даних; б) будь-якого втручання у функціонування комп'ютерної системи (Конвенція про кіберзлочинність, м.Будапешт, 23 листопада 2001 року).

Шкідлива програма (російськ. - вредоносная программа) -створена або існуюча програма зі спеціально внесеними змінами, яка завідомо призводить до несанкціонованого знищення, блокування, модифікації або копіюванню інформації, порушенню роботи ЕОМ, системи ЕОМ або їх мережі (Угода про співробітництво держав-учасників Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації, м.Мінськ, 1 червня 2001 року).