ЛУЦЬКИЙ МІСЬКИЙ ГОЛОВА

РОЗПОРЯДЖЕННЯ

від 06.08.2009 № 382
м. Луцьк

Про Правила роботи працівників виконавчих органів Луцької міської ради на персональних комп'ютерах, у корпоративній мережі Луцької міської ради та у мережі Інтернет

1. Затвердити Правила роботи працівників виконавчих органів Луцької міської ради на персональних комп'ютерах, у корпоративній мережі Луцької міської ради та у мережі Інтернет згідно з додатком 1.

2. Сектору консультативно-інформаційного забезпечення та автоматизованих систем управління загально-технічного відділу міської ради (Н.М.Хмель) до 25.09.2009 розробити та впровадити у виконавчих органах міської ради інформаційну систему «ІТ-сервіс».

3. Керівникам виконавчих органів міської ради здійснювати переміщення комп'ютерної техніки, умонтування або видалення окремих її комплектуючих лише з оформленням актів переміщення, модернізації комп'ютерної техніки (додатки 2, 3).

4. Контроль за виконанням розпорядження покласти на заступника міського голови, керуючого справами виконкому Іванюка М.І.

Міський голова Богдан Шиба

Виконавчий комітет Луцької міської ради Волинської області * Україна *

Матвійчук 773757

Додаток 1
до розпорядження міського голови
від 06.08.2009 № 382

ПРАВИЛА
роботи працівників виконавчих органів Луцької міської ради
на персональних комп'ютерах, у корпоративній мережі
Луцької міської ради та у мережі Інтернет

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Правила роботи працівників виконавчих органів Луцької міської ради на персональних комп'ютерах, у корпоративній мережі Луцької міської ради та у мережі Інтернет (далі – Правила, виконавчі органи та корпоративна мережа) розроблені з метою організації, формалізації та врегулювання інформаційних процесів при роботі на персональних комп'ютерах, у корпоративній мережі та мережі Інтернет, чіткої й злагодженої взаємодії працівників виконавчих органів за рахунок автоматизації процесів передачі (приймання), обробки, відображення, документування інформації.

1.2. Основні поняття та терміни, що використовуються у Правилах, мають такі визначення:

- відповідальні за інформатизацію – керівники структурних підрозділів (працівники) виконавчих органів міської ради, які згідно з посадовими інструкціями відповідальні за впровадження та супровід інформаційних систем, технологій у цих виконавчих органах;
- захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;
- інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;
- комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;
- корпоративна мережа передачі даних Луцької міської ради – це мультисервісна мережа передачі даних, яка працює відповідно до встановлених правил під єдиним управлінням власника мережі;
- локальна обчислювальна мережа (далі - ЛОМ) - це телекомунікаційна система, яка забезпечує на обмеженій території (в межах однієї установи, підрозділу) один чи декілька каналів зв'язку, наданих приєднаним до неї абонентам для короткочасного локального користування з метою передачі (приймання) та обробки інформації різноманітних типів, організації та спільного використання баз/банків даних, різноманітних програмних продуктів тощо.

1.3. У результаті впровадження Правил мають покращитися:

- регламентація діяльності працівників виконавчих органів при використанні персональних комп'ютерів;

- використання ресурсів корпоративної мережі, мережі Інтернет;

- підтримка необхідного рівня захисту інформації, її збереження і дотримання прав доступу до інформації, встановлених її власником;

- інформаційна взаємодія виконавчих органів.

2. ЗАГАЛЬНІ АСПЕКТИ РОБОТИ НА ПЕРСОНАЛЬНИХ КОМП'ЮТЕРАХ

2.1. Комп'ютерна техніка, електронна поштова скринька на офіційному домені міської ради, доступ до інформаційних систем та ресурсів міської ради надається працівникам виконавчих органів для виконання своїх службових обов'язків.

2.2. Користувач несе відповідальність за збереження комп'ютерної техніки, наданої йому у користування, згідно з договором про матеріальну відповідальність, який укладається між працівником та виконавчим органом.

2.3. Взаємодія користувачів повинна базуватися на загальноприйнятих нормах ділової етики, Етичного кодексу працівників виконавчих органів Луцької міської ради.

2.4. Всі працівники, які використовують персональні комп'ютери для виконання своїх службових обов'язків у виконавчих органах, повинні дотримуватися цих Правил і бути ознайомлені з ними під підпис в окремому журналі (форма згідно з додатком 1 до цих Правил), який зберігається у відповідальних за інформатизацію або, у разі відсутності у виконавчому органі відповідального за інформатизацію, у секторі консультативно-інформаційного забезпечення та автоматизованих систем управління загально-технічного відділу міської ради (далі – сектор АСУ).

2.5. Правила є обов'язковими також і для осіб, яким для виконання своїх службових обов'язків виконавчим органом були надані персональні комп'ютери для тимчасового використання або, які підключають свої персональні комп'ютери до локальної обчислювальної мережі виконавчого органу.

2.6. У разі виникнення будь-яких апаратних чи системних несправностей комп'ютера користувач повинен негайно припинити роботу і викликати відповідального за інформатизацію.

2.7. Відповідальні за інформатизацію здійснюють встановлення та оновлення програмного забезпечення на усіх персональних комп'ютерах відповідного виконавчого органу.

2.8. Користувачам персональних комп'ютерів забороняється:

– зберігати та запускати на персональних комп'ютерах програми комп'ютерних ігор;

– надавати можливість використання свого комп'ютера іншим користувачам, а також працівникам інших виконавчих органів, якщо це не викликано службовою необхідністю;

– використовувати комп'ютерну техніку в особистих цілях;

– надавати адресу службової скриньки електронної пошти для отримання інформації неслужбового характеру;

– вилучати, встановлювати чи змінювати будь-які апаратні компоненти комп'ютерної техніки, змінювати конфігурації існуючого програмного забезпечення;

– самостійно виконувати будь-які ремонтні та профілактичні роботи персональних комп'ютерів;

– знімати корпуси комп'ютерів, мережевих і периферійних пристроїв;

– самостійно здійснювати переміщення комп'ютерної техніки;

– вводити, обробляти та зберігати інформацію, що є державною таємницею (на персональних комп'ютерах, на яких не побудована відповідна комплексна система захисту інформації).

2.9. По закінченні робочого дня користувач повинен вимкнути персональний комп'ютер, іншу комп'ютерну техніку з мережі електроживлення (якщо інше не обумовлено технологічними вимогами).

2.10. Користувачі несуть персональну відповідальність за постійне використання антивірусних програм. Відповідальність за встановлення, належне функціонування антивірусних програм та регулярне оновлення їх баз даних покладається на відповідальних за інформатизацію.

2.11. Портативні персональні комп'ютери (notebook) можуть використовуватися працівниками, за погодженням з їх безпосередніми керівниками, для виконання своїх службових обов'язків за межами приміщень виконавчих органів.

3. ПОРЯДОК РОБОТИ З ІНФОРМАЦІЄЮ У КОРПОРАТИВНІЙ МЕРЕЖІ, ЛОМ, ІНФОРМАЦІЙНИХ СИСТЕМАХ

3.1. Порядок під'єднання до корпоративної мережі, ЛОМ, інформаційних систем

3.1.1. Сектор АСУ організовує під'єднання нових сегментів до корпоративної мережі відповідно до плану розвитку корпоративної мережі, заявок керівників виконавчих органів (форма згідно з додатком 2 до цих Правил), які подаються у паперовому вигляді або через інформаційну систему «ІТ-сервіс» сектору АСУ.

3.1.2. Під'єднання нових користувачів до інформаційних систем проводиться згідно з регламентами функціонування цих систем.

3.1.3. Під'єднання нових користувачів до ЛОМ, інформаційних систем виконавчих органів здійснюють відповідальні за інформатизацію на підставі заявок безпосередніх керівників працівників, яким необхідно організувати доступ до зазначених ресурсів. Ці заявки можуть подаватися як у паперовому вигляді, так і через інформаційну систему «ІТ-сервіс».

3.1.4. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються виконавчим органом -

власником інформації. Права доступу користувачів до корпоративної мережі на рівні каталогів та інформаційних ресурсів мережі мають визначатися у мінімальному обсязі, необхідному для виконання службових обов'язків.

3.1.5. Конфігурацію комп'ютерів для роботи в ЛОМ виконують відповідальні за інформатизацію при підключенні комп'ютерів до ЛОМ.

3.1.6. Для виконавчих органів за зверненням їх керівників до сектору АСУ на серверах міської ради для зберігання службової інформації, функціонування інформаційних систем може виділятися (за наявності технічної можливості) дисковий простір, де підтримується цілісність даних, їх безпека, резервне копіювання і розмежування прав доступу відповідно до вимог, вказаних у цих зверненнях.

3.2. Правила роботи на комп'ютерах, під'єднаних до корпоративної мережі, ЛОМ, інформаційних систем

3.2.1. Працівникам виконавчих органів забороняється самовільне підключення до ЛОМ комп'ютерів (у тому числі портативних) без відома відповідальних за інформатизацію.

3.2.2. Робота користувачів в інформаційних системах проводиться згідно з регламентами функціонування цих систем.

3.2.3. Для аутентифікації при доступі до інформаційних ресурсів ЛОМ кожен користувач зобов'язаний використовувати пароль, який має складатися не менше ніж з 8 символів. Для паролю слід використовувати поєднання таких літер, цифр, спеціальних символів, що утворюють слово, яке неможливо знайти у словнику.

3.2.4. Пароль доступу до інформаційних ресурсів ЛОМ, отриманий від відповідальних за інформатизацію, може бути змінений користувачем.

3.2.5. Користувачам персональних комп'ютерів, під'єднаних до ЛОМ, забороняється:

- працювати в ЛОМ під чужими іменами та адресами (IP та MAC) чи з реквізитами інших користувачів;
- передавати власний пароль іншим особам, включаючи відповідальних за інформатизацію;
- використовувати на мережевих комп'ютерах програми моніторингу, сканування мережі тощо без письмового дозволу керівництва виконавчих органів;
- самостійно відключати засоби автоматичного здійснення та відновлення антивірусного захисту без попереднього узгодження з відповідальним за інформатизацію;
- використовувати дисковий простір серверів для зберігання і пересилання іншим користувачам програм і даних неслужбового характеру.

3.2.6. Сектор АСУ забезпечує протоколювання роботи користувачів у корпоративній мережі, ЛОМ.

3.2.7. Користувач зобов'язаний відключати в робочий час під час грози комп'ютерну техніку і мережевий кабель.

3.3. Захист інформації у корпоративній мережі, ЛОМ, інформаційних системах

3.3.1. Об'єктами захисту у корпоративній мережі, ЛОМ, інформаційних системах є інформація, що обробляється в них, та програмне забезпечення, яке призначене для обробки цієї інформації.

3.3.2. Політика захисту інформації у корпоративній мережі формується та реалізовується сектором АСУ.

Захист інформації у корпоративній мережі складається з комплексу організаційних і технічних заходів, спрямованих на виключення або неможливість протиправних дій щодо ресурсів корпоративної мережі.

3.3.3. Для належного захисту інформації у корпоративній мережі сектор АСУ спільно з відділом оборонно-мобілізаційної і режимно-секретної роботи міської ради організовує формування комплексної системи захисту інформації.

3.3.4. Організаційні заходи щодо захисту інформації у корпоративній мережі включають:

а) організацію постійного контролю за дотриманням правил користування мережею;

б) обмеження доступу працівників у приміщення, де встановлені сервери та комутаційне обладнання;

в) контроль за структурою корпоративної мережі і припинення несанкціонованого підключення до неї;

г) інші заходи організаційного характеру.

3.3.5. Технічні заходи включають:

а) правила зміни мережевих паролів;

б) антивірусний контроль;

в) регулярне резервне копіювання інформації;

г) відслідковування запуску і припинення використання програмного забезпечення, що ускладнює або порушує належну працездатність корпоративної мережі, комп'ютерів у ній і порушує безпеку корпоративної мережі;

ґ) обмеження пропуску мережевих протоколів на маршрутизаторах відповідно до визначених у затверджених проектах потреб окремих сегментів корпоративної мережі;

д) інші заходи технічного характеру.

3.3.6. Сектор АСУ забезпечує авторизацію доступу до мережевих послуг, а також централізовану аутентифікацію користувачів, що отримали доступ у корпоративну мережу.

3.4. Зловживання у корпоративній мережі, ЛОМ, мережі Інтернет

3.4.1. До зловживань у корпоративній мережі, ЛОМ, мережі Інтернет, у першу чергу, належить діяльність, що порушує чинне законодавство України (цивільне і кримінальне), а також несанкціонований доступ до корпоративної мережі, ЛОМ.

3.4.2. До зловживань у корпоративній мережі, ЛОМ, мережі Інтернет, крім того, належать:

а) самовільна організація точок доступу у мережу по комутованих, виділених і фізичних каналах без письмового погодження з сектором АСУ;

б) спроби доступу і доступ до даних і програм, розміщених як усередині корпоративної мережі, так і за її межами осіб, що не мають на це право;

в) використання робочих місць або серверів корпоративної мережі для здійснення мережевих атак на робочі станції, сервери і мережеве обладнання корпоративної мережі або мережі Інтернет;

г) розсилання не витребуваної інформації електронною поштою (спам), листів з вказівкою чужої адреси відправника, листів загрозливого або ображаючого характеру, "mailbombing", тобто відправлення листів, що переповнюють поштову скриньку одержувача і перешкоджають отриманню нової пошти;

ґ) несанкціоноване знищення (або фальсифікація) користувачами корпоративної мережі даних і програм без погодження з їх авторами або відповідальними за інформатизацію;

д) незаплановане і необґрунтоване виробничою необхідністю завантаження корпоративної мережі;

е) відвідування сайтів «соціальних мереж», ресурсів мережі Інтернет, не пов'язаних з виконанням службових обов'язків, використання ICQ, інших аналогічних систем.

є) використання корпоративної мережі в діяльності, що суперечать законодавству України.

4. ПРАВА ТА ОБОВ'ЯЗКИ СЕКТОРУ АСУ, ВІДПОВІДАЛЬНИХ ЗА ІНФОРМАТИЗАЦІЮ ТА КОРИСТУВАЧІВ КОРПОРАТИВНОЇ МЕРЕЖІ, ЛОМ, ІНФОРМАЦІЙНИХ СИСТЕМ

4.1. Права і обов'язки сектору АСУ

4.1.1. Сектор АСУ має право:

а) у разі зловживання корпоративною мережею частково або повністю усувати порушників від користування нею;

б) видаляти програмне забезпечення, що порушує роботу корпоративної мережі;

в) давати вказівки відповідальним за інформатизацію щодо роботи корпоративної мережі, ЛОМ, які не суперечать вимогам цих Правил.

4.1.2. Сектор АСУ зобов'язаний:

а) обмежувати доступ працівників у приміщення, де встановлені сервери і комутаційне обладнання корпоративної мережі;

б) здійснювати контроль за дотриманням структури корпоративної мережі;

в) реалізовувати технічні заходи щодо:

- відстеження запуску і припинення використання програмного забезпечення, що ускладнює або порушує безпеку, належну працездатність корпоративної мережі, комп'ютерів у ній;
- налагодження політики безпеки домена.

г) вживати організаційних і технічних заходів щодо припинення спроб несанкціонованого доступу до комп'ютерів із зовнішніх мереж і з комп'ютерів корпоративної мережі, а також щодо припинення розповсюдження інформації, що заборонено чинним законодавством України.

4.2. Права і обов'язки відповідальних за інформатизацію

4.2.1. Відповідальні за інформатизацію мають право:

а) у разі зловживання працівниками виконавчих органів корпоративною мережею, ЛОМ частково або повністю усувати порушників від користування цими мережами;

б) видаляти програмне забезпечення, що порушує роботу корпоративної мережі, ЛОМ.

4.2.2. Відповідальні за інформатизацію зобов'язані:

а) дотримуватися плану адресації, встановлених правил іменування комп'ютерів, користувачів;

б) забезпечувати актуалізацію інформації про користувачів в Active Directory;

в) обмежувати доступ працівників у приміщення виконавчих органів, де встановлені сервери і комутаційне обладнання корпоративної мережі, ЛОМ;

г) реалізовувати технічні заходи щодо відстеження запуску і припинення використання програмного забезпечення, що ускладнює або порушує безпеку, нормальну працездатність ЛОМ, комп'ютерів у ній;

ґ) вживати організаційних і технічних заходів щодо припинення спроб несанкціонованого доступу до комп'ютерів із зовнішніх мереж і з комп'ютерів корпоративної мережі, ЛОМ, а також щодо припинення розповсюдження інформації, що заборонено чинним законодавством України;

д) виконувати вказівки сектору АСУ щодо роботи корпоративної мережі, які не суперечать вимогам цих Правил.

4.3. Права і обов'язки користувача

4.3.1. Користувач має право:

а) на доступ до всіх ресурсів корпоративної мережі, ЛОМ, інформаційних систем у межах компетенції та відповідно до цих Правил;

б) звертатися за довідковою інформацією і консультацією до працівників виконавчих органів, що обслуговують корпоративну мережу, ЛОМ, інформаційні системи.

4.3.2. Користувач зобов'язаний:

а) ознайомитися з цими Правилами під підпис;

б) використовувати ресурси корпоративної мережі, ЛОМ, інформаційних систем виключно в цілях, пов'язаних з виконанням службових обов'язків;

в) виконувати вимоги сектору АСУ (відповідального за інформатизацію), що не суперечать цим Правилам;

г) дотримуватись правил техніки безпеки при роботі з комп'ютерною технікою;

ґ) забезпечувати нерозголошення ідентифікаційної інформації, що використовується для доступу до ресурсів корпоративної мережі, ЛОМ, мережі Інтернет, інформаційних систем;

д) перешкоджати несанкціонованому і недобросовісному використанню ресурсів корпоративної мережі, ЛОМ, інформаційних систем;

е) користуватися антивірусними програмами;

є) негайно повідомити відповідального за інформатизацію у разі появи відомостей або підозр про факти порушення цих Правил, зокрема, про факти несанкціонованого доступу до інформації, розміщеної на його комп'ютері або якого-небудь іншого порушення;

ж) постійно удосконалювати свої знання і навички роботи з комп'ютерною технікою;

з) належно експлуатувати комп'ютерну техніку, запобігати попаданню на комп'ютерну техніку чужорідних речовин (рідин, крихт тощо).

5. ВІДПОВІДАЛЬНІСТЬ ЗА ВИКОНАННЯ ПРАВИЛ

5.1. Відповідальність завідувача сектору АСУ

5.1.1. Завідувач сектору АСУ несе відповідальність за:

а) організацію управління корпоративною мережею;

б) формування та впровадження комплексної системи захисту інформації у корпоративній мережі (спільно з відділом оборонно-мобілізаційної і режимно-секретної роботи міської ради).

5.2. Відповідальність системного адміністратора сектору АСУ

5.2.1. Системний адміністратор сектору АСУ несе відповідальність за:

а) функціонування корпоративної мережі в цілому;

б) функціонування базових сервісів корпоративної мережі;

в) порушення функціонування корпоративної мережі унаслідок некоректного управління маршрутизацією, базовими мережевими сервісами (DNS, DHCP, AD тощо).

5.2.2. Системний адміністратор сектору АСУ не несе відповідальності за:

а) інформацію, що знаходиться на комп'ютерах у ЛОМ виконавчих органів, що входять у корпоративну мережу, встановлені права доступу до комп'ютерів у ЛОМ виконавчих органів і за діяльність, що ведеться на цих комп'ютерах;

б) працездатність комп'ютерів і устаткування ЛОМ виконавчих органів, працездатність і фізичний стан ліній зв'язку і інших засобів комунікацій усередині мереж цих виконавчих органів;

в) зміст даних, що передаються через корпоративну мережу.

5.3. Відповідальність відповідальних за інформатизацію

5.3.1. Відповідальні за інформатизацію несуть відповідальність за порушення функціонування відповідних сегментів корпоративної мережі

унаслідок некоректного управління цими сегментами мережі, управління мережевими сервісами, неналежне налагодження мережевих параметрів на робочих місцях користувачів корпоративної мережі, несвоєчасне інформування сектору АСУ про зміни у маршрутизації і складі ЛОМ, про випадки зловживань у відповідних сегментах корпоративної мережі.

5.4. Відповідальність користувачів

5.4.1. Користувач несе повну відповідальність за всі дії, пов'язані з використанням персонального комп'ютера, корпоративної мережі, ЛОМ, інформаційних систем від його імені або із закріпленого за ним робочого місця, інформацію, що знаходиться на персональному комп'ютері.

5.4.2. Невиконання користувачем цих Правил є порушенням виконавської дисципліни.

5.4.3. У разі скоєння комп'ютерних злочинів застосовуються норми чинного законодавства України (додаток 3 до цих Правил).

Заступник міського голови,
керуючий справами виконкому Микола Іванюк

Виконавчий комітет Луцької міської ради Волинської області * Україна *

Додаток 1
до Правил роботи працівників виконавчих органів Луцької міської ради на персональних комп'ютерах, у корпоративній мережі Луцької міської ради та мережі Інтернет

Форма

Журнал
ознайомлення працівників

_____

(назва виконавчого органу міської ради)
з Правилами роботи працівників виконавчих органів Луцької міської ради на персональних комп'ютерах, у корпоративній мережі Луцької міської ради та у мережі Інтернет

№ з/п	Прізвище, ім'я, по батькові	Посада	Дата ознайомлення	Підпис

Додаток 2
до Правил роботи працівників виконавчих органів Луцької міської ради на персональних комп'ютерах, у корпоративній мережі Луцької міської ради та мережі Інтернет

Форма

_____
(посада, прізвище, ініціали, відповідального за інформатизацію)

Заявка
на під'єднання до корпоративної мережі
(локальної обчислювальної мережі, інформаційної системи)

Прошу під'єднати _____ до корпоративної мережі
(назва суб'єкта під'єднання)
(локальної обчислювальної мережі, інформаційної системи).

Керівник структурного
підрозділу виконавчого
органу міської ради _____
(прізвище, ініціали)

* При потребі вказується детальніша інформація щодо під'єднання.
** Заявка подається у паперовому вигляді або через інформаційну систему «ІТ-сервіс».

Додаток 3
до Правил роботи працівників виконавчих органів Луцької міської ради на персональних комп'ютерах, у корпоративній мережі Луцької міської ради та мережі Інтернет

ВИТЯГИ
з Кримінального кодексу України щодо комп'ютерних злочинів

"Стаття 176. Порушення авторського права і суміжних прав

1. Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, а так само незаконне відтворення, розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, або інше умисне порушення авторського права і суміжних прав, якщо це завдало матеріальної шкоди у значному розмірі, -

караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

2. Ті самі дії, якщо вони вчинені повторно, або за попередньою змовою групою осіб, або завдали матеріальної шкоди у великому розмірі, -

караються штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п'яти років, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення. 3. Дії, передбачені частинами першою або другою цієї статті, вчинені службовою особою з використанням службового становища або організованою групою, або якщо вони завдали матеріальної шкоди в особливо великому розмірі, -

караються штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого та з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувалися для їх виготовлення.

Примітка. У статті 176 … цього Кодексу матеріальна шкода вважається завданою в значному розмірі, якщо її розмір у двадцять і більше разів перевищує неоподатковуваний мінімум доходів громадян, у великому розмірі - якщо її розмір у двісті і більше разів перевищує неоподатковуваний мінімум доходів громадян, а завданою в особливо великому розмірі - якщо її розмір у тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 216. Незаконне виготовлення, підроблення, використання або збут незаконно виготовлених, одержаних чи підроблених марок акцизного збору чи контрольних марок

1. Незаконне виготовлення, підроблення, використання або збут незаконно виготовлених, одержаних чи підроблених марок акцизного збору або контрольних марок для маркування упаковок примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних чи голографічних захисних елементів -

караються штрафом від ста до трьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб,-

караються штрафом від трьохсот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до п'яти років з конфіскацією товарів, промаркованих підробленими марками чи голографічними захисними елементами.

Стаття 301. Ввезення, виготовлення, збут і розповсюдження порнографічних предметів

1. Ввезення в Україну творів, зображень або інших предметів порнографічного характеру з метою збуту чи розповсюдження або їх виготовлення, перевезення чи інше переміщення з тією самою метою, або їх збут чи розповсюдження, а також примушування до участі в їх створенні -

караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років, з конфіскацією порнографічних предметів та засобів їх виготовлення і розповсюдження.

2. Ті самі дії, вчинені щодо кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру, -

караються штрафом від ста до трьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на той самий строк, з конфіскацією порнографічної кіно- та відеопродукції, засобів її виготовлення і демонстрування.

3. Дії, передбачені частинами першою або другою цієї статті, якщо вони вчинені повторно або за попередньою змовою групою осіб, а також

примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, -

караються позбавленням волі на строк від трьох до семи років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією порнографічних предметів, кіно- та відеопродукції, комп'ютерних програм, засобів їх виготовлення, розповсюдження і демонстрування.

Р о з д і л XVI
ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

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

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, -

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

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.

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

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-

обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, -

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, -

караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

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

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

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Стаття 363. 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.

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

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або

припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, -

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи."

Додаток 2
до розпорядження міського голови
від 06.08.2009 № 382

АКТ
переміщення комп'ютерної техніки

Відповідно до розпорядження міського голови від "___" _____ 200__ р. №_____ (наказу, листа, доручення) обладнання, розташоване за адресою: _____

_____

переміщується за адресою: _____

_____

ПЕРЕЛІК ОБЛАДНАННЯ:

№ з/п	Назва	Інвентарний номер	Заводський номер	Кількість

Обладнання здав: _____ _____ _____
(посада) (підпис) (прізвище та ініціали)

Обладнання прийняв: _____ _____ _____
(посада) (підпис) (прізвище та ініціали)

Переміщення дозволив: _____ _____ _____
(посада) (підпис) (прізвище та ініціали)

Заступник міського голови,
керуючий справами виконкому Микола Іванюк

Виконавчий комітет Луцької міської ради Волинської області * Україна *

Додаток 3
до розпорядження міського голови
від 06.08.2009 № 382

АКТ
модернізації комп'ютерної техніки

Відповідно до розпорядження міського голови від "___" _____ 200__ р. №_____ (наказу, листа, доручення) обладнання _____,

_____
(назва та опис обладнання)

інвентарний номер _____, заводський номер _____,
розташоване за адресою: _____

_____

було доукомплектоване/розукомплектоване такими пристроями:

№ з/п	Назва пристрою	Доукомплектовано/ Розукомплектовано	Одиниця виміру	Кількість

Доукомплектацію/розукомплектацію здійснив:

_____ _____ _____
(посада) (підпис) (прізвище та ініціали)

Обладнання прийняв:

_____ _____ _____
(посада) (підпис) (прізвище та ініціали)

Доукомплектацію/
розукомплектацію дозволив: _____ _____ _____
(посада) (підпис) (прізвище та ініціали)

Виконавчий комітет Луцької міської ради Волинської області Україна

Заступник міського голови,
керуючий справами виконкому Микола Іванюк