МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДВНЗ «Ужгородський національний університет»

Фізичний факультет

Кафедра твердотільної електроніки з/с інформаційної безпеки

**НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**ЗБІРНИК ЛЕКЦІЙ - 2013**

Старший викладач: Гребенніков Вадим Вікторович

**Зміст**

1. Нормативно-правові акти з основних положень інформаційної безпеки

2. Нормативно-правові акти з інформатизації та електронного урядування

3. Нормативно-правові акти щодо захисту конфіденційної інформації

4. Нормативно-правові акти з охорони державної таємниці

5. Нормативно-правові акти щодо захисту інформації в телекомунікаційних системах

6. Нормативно-правові акти з технічного захисту інформації

7. Закони про електронний документообіг та цифровий підпис

8. Підзаконні акти щодо електронного документообігу та цифрового підпису

9. Нормативно-правові акти з ліцензування діяльності у сферах інформаційної безпеки

10. Нормативно-правові акти з державної експертизи у сферах інформаційної безпеки

**1. Нормативно-правові акти з основних положень**

**інформаційної безпеки**

Під час створення сучасної та ефективної системи забезпечення інформаційної безпеки істотного значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити усі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави й ефективно реалізовувати політику національної безпеки в інформаційній сфері.

Це означає, що всі без винятку дії щодо захисту й реалізації національних інтересів України в будь-якій сфері й на будь-якому рівні мають передусім спиратися на чинне законодавство України, підтверджувати законність функціонування системи національної безпеки. Водночас у демократичному суспільстві такі дії суб'єктів забезпечення національної безпеки повинні відповідати національному законодавству, а також загальновизнаним міжнародно-правовим нормам та бути під контролем громадськості.

З огляду на викладене законність функціонування є однією з головних вимог до системи забезпечення інформаційної безпеки. Ця законність повинна базуватися на сукупності законів і підзаконних нормативних актів, які спрямовані на створення необхідних умов для захисту національних інтересів в інформаційній та інших сферах життя країни.

Так, зокрема, наявність необхідної та достатньої нормативної бази і механізмів її реалізації та контролю дозволяє системі забезпечення національної безпеки України ефективно функціонувати в сучасних умовах.

Нормативна база інформаційної безпеки повинна виконувати три основні функції:

1. Регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність.

2. Нормативно забезпечувати дії суб'єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави.

3. Встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

Найбільш актуальним завданням у сфері забезпечення інформаційної безпеки держави на сьогодні є формування відповідних положень національного інформаційного законодавства щодо правового забезпечення діяльності в інформаційній сфері відповідних суб'єктів, у першу чергу державних органів, на які державою покладено виконання пов'язаних з цим функцій.

За роки незалежності в Україні закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було напрацьовано великий масив нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері. Акти національного законодавства, які регламентують діяльність державних органів, організацій і громадян в інформаційній сфері, встановлюють повноваження державних органів щодо забезпечення інформаційної безпеки України.

З огляду на викладене нормативну базу з національної безпеки України в інформаційній сфері доцільно розглядати з урахуванням 3-рівневої ієрархії нормативних актів: першого (вищого), другого та третього рівня НПЗІБ.

**Перший (вищий)** **рівень** визначає концептуальні положення національної безпеки України в усіх сферах її існування. Це норми Конституції України, закон України «Про основи національної безпеки України» та «Стратегія національної безпеки України», а також «Доктрина інформаційної безпеки України» (у разі прийняття). Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки.

**Другий рівень** визначає важливі положення забезпечення національної безпеки в інформаційній сфері. Це закони конститутивного напрямку: «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо.

**Третій рівень** визначає діяльність державних органів у процесі забезпечення національної безпеки в інформаційній та інших сферах. Це закони інституційного напрямку: «Про оборону України», «Про Збройні Сили України», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації», «Про міліцію», «Про прокуратуру», «Про надзвичайний стан» тощо.

У структурі нормативно-правової бази забезпечення національної безпеки України в інформаційній сфері особливе місце посідають укази та розпорядження Президента України, а також акти (постанови, декрети) Кабінету Міністрів України. Ці нормативні акти є підзаконними та видаються з метою конкретизації та підвищення якості вирішення завдань забезпечення інформаційної безпеки.

Міністерства й відомства України в межах визначеної законами компетенції та відповідальності на основі чинного законодавства про національну безпеку України, а також згідно з рішеннями Президента та Кабінету Міністрів України розробляють відомчі накази, інструкції, положення, які спрямовані на реалізацію програм захисту життєво важливих інтересів людини, суспільства, держави в інформаційній сфері.

Важливу роль у системі законодавства України з питань національної безпеки відіграють акти нормативного і директивного характеру місцевих органів влади - рішення з питань забезпечення національної безпеки (про боротьбу з наслідками стихійних лих, техногенних аварій і катастроф, з епідеміями, про підтримання громадського порядку тощо), які є обов'язковими для виконання всіма підприємствами, установами й організаціями, а також посадовими особами і громадянами на території, підпорядкованій цьому органу влади.

Значним кроком на шляху створення системи нормативно-правового регулювання забезпечення інформаційної безпеки України стало прийняття Верховною Радою України **Конституції України**. В ній, зокрема, є норми, що стосуються забезпечення інформаційної безпеки України та які є визначальними для побудови національної системи інформаційної безпеки.

Так, зокрема, згідно **статті 17** Конституції забезпечення інформаційної безпеки України є «справою всього українського народу». Згідно **статті 15** Конституції жодна ідеологія не може визнаватися державою як обов'язкова, при цьому цензура заборонена. З точки зору захисту прав людини і громадянина в інформаційній сфері найбільш знаковими є **статті 31, 32, 34** Конституції.

Згідно **статті 31** Конституції кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочину чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Згідно **статті 32** Конституції ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Згідно **статті 34** Конституції кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

У **статті 107** Конституції закріплено законність функціонування Ради національної безпеки і оборони України як координаційного органу з питань національної безпеки при Президенті України.

Захист прав людини і громадянина в інформаційній сфері закріплює також «**Цивільний кодекс україни**» (далі - Кодекс). Так, згідно **статті 285** Кодексу повнолітня фізична особа має право на достовірну та повну інформацію про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються її здоров'я.

Якщо  інформація про хворобу фізичної особи може погіршити стан її здоров'я або погіршити стан здоров'я фізичних осіб, визначених  частиною другою цієї статті, зашкодити процесові лікування, медичні працівники мають право дати неповну інформацію про стан здоров'я фізичної особи, обмежити можливість їх ознайомлення з окремими медичними документами.

Згідно **статті 286** Кодексу фізична особа має право на таємницю  про стан  свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні.

Забороняється вимагати та подавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи.

Фізична особа зобов'язана утримуватися від поширення інформації, зазначеної у частині першій цієї статті, яка стала їй відома у зв'язку з виконанням службових обов'язків або з інших джерел.

Згідно **статті 301** Кодексу фізична особа має право на збереження у таємниці  обставин свого особистого життя. Обставини особистого життя фізичної особи можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що підтверджено рішенням суду, а також за її згодою.

Згідно **статті 302** Кодексу фізична особа має право вільно збирати, зберігати, використовувати та поширювати інформацію.  Збирання, зберігання, використання та поширення інформації про особисте  життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Згідно **статті 306** Кодексу фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції.

Листи, телеграми та інші види кореспонденції можуть використовуватися, зокрема шляхом опублікування, лише за згодою особи, яка направила їх, та адресата.

Порушення таємниці кореспонденції може бути дозволено судом у випадках, встановлених законом, з метою запобігання злочинові чи під час кримінального провадження, якщо іншими способами одержати інформацію неможливо.

Згідно **статті 307** Кодексу фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку припускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру.

Фізична особа, яка погодилася на знімання її на фото-, кіно-, теле- чи відеоплівку, може вимагати припинення їх публічного показу в тій частині, яка стосується її особистого життя. Витрати, пов'язані з демонтажем виставки чи запису, відшкодовуються цією фізичною особою.

Знімання фізичної особи на фото-, кіно-, теле- чи відеоплівку, в тому числі таємне, без згоди особи може бути проведене лише у випадках, встановлених законом.

Згідно **статті 308** Кодексу фотографія, інші художні твори, на яких зображено фізичну особу, можуть бути публічно показані, відтворені, розповсюджені лише за згодою цієї особи.

Якщо фізична особа позувала автору за плату, фотографія, інший художній твір може бути публічно показаний, відтворений або розповсюджений без її згоди.

Фотографія може бути розповсюджена без дозволу фізичної особи, яка зображена на ній, якщо це викликано необхідністю захисту її інтересів або інтересів інших осіб.

Викладені положення Конституції та Кодексів України, в свою чергу, стали поштовхом до розробки всього пакета нормативно-правових актів, необхідних для ефективного забезпечення національної безпеки України в інформаційній та інших сферах її існування - зовнішньо- та внутрішньополітичній, державної безпеки, військовій та сфері безпеки державного кордону, економічній, соціальній, гуманітарній, науково-технологічній та екологічній.

У січні 1997 року Верховна Рада України схвалила «**Концепцію (основи державної політики) національної безпеки України**» (далі - Концепція). Цей документ нормативно закріпив загальні положення та принципи забезпечення національної безпеки України, національні інтереси і загрози національній безпеці, основні напрями державної політики національної безпеки, систему її забезпечення та повноваження основних суб'єктів цієї системи.

У червні 2003 року був прийнятий закон України «**Про основи національної безпеки України**», згідно з яким Концепція втратила чинність та було нормативно закріплено компетенцію та функції усіх визначених законом суб'єктів забезпечення національної безпеки України в усіх сферах, зокрема в інформаційній.

Цей Закон відповідно до п.17 першої частини статті 92 Конституції України визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності, зокрема в інформаційній сфері.

Згідно **статті 3** Закону об'єктами національної безпеки є:

- людина і громадянин - їхні конституційні права і свободи;

- суспільство - його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси;

- держава - її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Згідно **статті 4** суб'єктами забезпечення національної безпеки є:

- Президент України;

- Верховна Рада України;

- Кабінет Міністрів України;

- Рада національної безпеки і оборони України;

- міністерства та інші центральні органи виконавчої влади;

- Національний банк України;

- суди загальної юрисдикції;

- прокуратура України;

- місцеві державні адміністрації та органи місцевого самоврядування;

- Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України;

- громадяни України, об'єднання громадян.

Згідно **статті 7** Закону загрозами національній безпеці України в інформаційній сфері є:

- прояви обмеження свободи слова та доступу до публічної інформації;

- поширення засобами масової інформації культу насильства, жорстокості, порнографії;

- комп'ютерна злочинність та комп'ютерний тероризм;

- розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Згідно **статті 8** Закону основними напрямами забезпечення державної політики з питань національної безпеки в інформаційній сфері є:

- забезпечення інформаційного суверенітету України;

- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

- активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України;

- забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов’язків, за критику;

- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Повноваження суб'єктів забезпечення національної безпеки визначені у статті 9 Закону, а також у відповідних профільних законах та положеннях, що предметно регулюють правовий статус кожного з них.

Національна безпека України в інформаційній сфері забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах.

Вибір конкретних засобів і шляхів забезпечення національної безпеки України в інформаційній сфері обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Відповідно до Закону цільові настанови та керівні принципи державного будівництва в інформаційній сфері, а також напрями діяльності органів державної влади в конкретній обстановці визначаються Стратегією національної безпеки України з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України в інформаційній та інших сферах життєдіяльності.

«**Стратегія національної безпеки України**» (далі - Стратегія), затверджена Указом Президента України від 12 лютого 2007 року № 105 (в редакції [Указу Президента України](http://zakon4.rada.gov.ua/laws/show/389/2012/paran18#n18) від 8 червня 2012 року № 389) визначає загальні принципи, пріоритетні цілі, завдання і механізми захисту життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз.

Як головну мету Стратегії визначено формування сприятливих умов для забезпечення інтересів громадян, суспільства і держави, дальшого поступу України як демократичної держави зі сталою та зростаючою ринковою економікою, держави, що керується європейськими політичними й економічними цінностями, в якій повага і захист прав і законних інтересів усіх територіальних громад, суспільних верств, етнічних груп є запорукою незалежного, вільного, суверенного і демократичного розвитку єдиної України.

Згідно **п.4.3.8** Стратегії ключовими завданнями політики національної безпеки у внутрішній сфері щодо забезпечення інформаційної безпеки є:

- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

- забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;

- розробка та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав - членів ЄС, у тому числі згідно з вимогами «Конвенції про кіберзлочинність»;

- створення національної системи кібербезпеки.

Згідно **п.5.1** Стратегії досягнення її цілей потребує кардинального реформування сектору безпеки і оборони, вдосконалення механізмів правового, організаційного, кадрового, фінансового, матеріально-технічного забезпечення національної безпеки, що передбачає:

- комплексне реформування всіх складових цієї системи;

- ефективне функціонування системи забезпечення національної безпеки на всіх етапах її реформування та розвитку;

- ефективне керівництво та управління ресурсами;

- дотримання балансу ефективності функціонування та демократизації органів сектору безпеки і оборони.

Згідно **п.5.2.1** Стратегії системне вдосконалення законодавства з питань національної безпеки передбачає:

- взаємоузгодження законодавчих актів з питань національної безпеки, усунення наявних протиріч і прогалин;

- розроблення узгоджених проектів актів щодо формування єдиної державної політики національної безпеки та її реалізації у визначених законодавством сферах;

- уточнення завдань, функцій і повноважень суб'єктів забезпечення національної безпеки України, зокрема, в умовах кризових ситуацій, що загрожують національній безпеці;

- сприяння розвитку права міжнародної безпеки і спільного здобутку ЄС у галузі безпеки та їх імплементація у національне законодавство.

Інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

8 липня 2009 року Указом Президента України № 514 була затверджена «**Доктрина інформаційної безпеки України**». Основною метою реалізації положень Доктрини було створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Однак цей Указ втратив чинність на підставі Указу Президента № 504 від 6 червня 2014 року, тому на даний час Україна не має Доктрини інформаційної безпеки.

Ще одним важливим для забезпечення інформаційної безпеки України нормативним актом є Закон України «**Про інформацію**» (далі - Закон). Цим Законом закладено правові основи інформаційної діяльності, стверджено інформаційний суверенітет України, закріплене право на інформацію та на доступ до неї, визначено систему відносин і зобов'язань у цій сфері, прийняту для демократичної держави, визначено правові форми міжнародного співробітництва в галузі інформації.

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації. Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави під час одержання, використання, поширення та зберігання інформації (зокрема й використання мережі Інтернет).

У цьому Законі наведені нижче терміни вживаються в такому значенні:

- документ - матеріальний носій інформації, функціями якого є її збереження та передавання у часі та просторі;

- інформація - будь-які дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

- захист інформації - сукупність заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Згідно **статті 2** Закону основними принципами інформаційних відносин є:

- гарантованість права на інформацію;

- відкритість, доступність інформації, свобода обміну інформацією;

- достовірність і повнота інформації;

- свобода вираження поглядів і переконань;

- правомірність одержання, використання, поширення, зберігання та захисту інформації;

- захищеність особи від втручання в її особисте та сімейне життя.

Згідно **статті 3** Закону одним з основних напрямів державної інформаційної політики є забезпечення інформаційної безпеки України.

Згідно **статті 5**Закону кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Разом з тим, згідно **статті 6** Закону право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Згідно **статті 11** Закону не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Згідно **статті 20** Закону за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Згідно **статті 21** Закону інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини і громадянина;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Згідно **статті 24** Закону забороняється цензура - будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання в будь-якій іншій формі тиражуванню або поширенню інформації.

Ця заборона не поширюється на випадки, коли попереднє узгодження інформації здійснюється на підставі закону, а також у разі накладення судом заборони на поширення інформації.

Згідно **статті 28** Закону інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Згідно **статті 29** Закону інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Важливим кроком для забезпечення інформаційної безпеки України було прийняття у 2011 році Закону України «**Про доступ до публічної інформації**» (далі - Закон). Він визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес.

**Перша частина статті 6** Закону повторює **статтю 21** Закону України «Про інформацію» щодо визначення інформації з обмеженим доступом, яка може бути конфіденційною, таємною або службовою інформацією.

Згідно **другої частини статті 6** Закону обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Згідно **п’ятої частини статті 6** Закону не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. При дотриманні вимог, передбачених частиною другою цієї статті, зазначене положення не поширюється на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину.

Згідно **шостої частини статті 6** Закону не належать до інформації з обмеженим доступом відомості, зазначені у декларації про майно, доходи, витрати і зобов’язання фінансового характеру, оформленої за формою і в порядку, що встановлені Законом України «Про засади запобігання і протидії корупції».

Згідно **сьомої частини статті 6** Закону обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

**Перша частина статті 7** Закону визначає конфіденційну інформацію як таку, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Згідно **другої частини статті 7** Закону розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини.

**Перша частина статті 8** Закону визначає таємну інформацію як таку, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Згідно **першої частини статті 9** Закону до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Згідно **другої частини статті 9** Закону документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування» (ДСК). Доступ до таких документів надається відповідно до частини другої статті 6 цього Закону.

Згідно **третьої частини статті 9** Закону перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

**Види професійної таємниці згідно чинного законодавства**

1. Закон «**Про державну таємницю**» - стаття 1 - **державна таємниця** - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України.

2. **Цивільний кодекс України** - стаття 505 - **комерційна таємниця** - інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить.

3. Закон «**Про банки і банківську діяльність**» - стаття 60 «**Банківська таємниця**» - інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку.

4. Закон «**Основи законодавства України про охорону здоров'я**» - Стаття 40 «**Лікарська таємниця**» - відомості про хворобу, медичне обстеження, огляд та їх результати, інтимну та сімейну сторони життя громадянина, які стали відомі медичним працівникам під час виконання професійних обов'язків.

5. Закон «**Про нотаріат**» -стаття 8 «**Нотаріальна таємниця**» - сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо.

6. Закон «**Про адвокатуру та адвокатську діяльність**» -стаття 22 «**Адвокатська таємниця**» - інформація, що стала відома адвокату про клієнта, а також питання, з яких клієнт звертався до адвоката, зміст порад, консультацій, роз’яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності.

**Інші таємниці згідно чинного законодавства**

1. Закон «**Про телекомунікації**» - стаття 9- **таємниця телефонних розмов**, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій.

2. Закон «**Про поштовий зв'язок**» - стаття 6 - **таємниця поштових відправлень**, у тому числі листування та іншої письмової кореспонденції, електронних повідомлень, що пересилаються (передаються) засобами зв'язку.

3. Закон «**Про страхування» -** стаття 40 «**Таємниця страхування**» - конфіденційна інформація щодо діяльності та фінансового стану страхувальника - клієнта страховика, яка стала відомою йому під час взаємовідносин з клієнтом чи з третіми особами при провадженні діяльності у сфері страхування, розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

4. Закон «**Про друковані засоби масової інформації (пресу) в Україні**» - стаття 26 - **таємниця авторства** осіб, які надають інформацію журналісту, за їх проханням.

5. Закон «**Про свободу совісті та релігійні організації**» - стаття 3 - **таємниця сповіді** віруючих, відомості про життя яких одержані священнослужителями.

6. **Сімейний кодекс України** -стаття 226 «**Таємниця усиновлення**» - таємниця перебування на обліку тих, хто бажає усиновити дитину, пошуку дитини для усиновлення, подання заяви про усиновлення та її розгляду, рішення суду про усиновлення. Дитина, яка усиновлена, має право на таємницю, в тому числі і від неї самої, факту її усиновлення.

7. **Кримінальний кодекс України** - стаття 159 - порушення **таємниці голосування** під час проведення виборів або референдуму, що виявилося у розголошенні змісту волевиявлення громадянина, який взяв участь у виборах або референдумі.

**Конфіденційна інформація згідно чинного законодавства**

1. Закон «**Про захист персональних даних**» - стаття 5 - конфіденційність персональних даних.

2. Закон «**Про організацію формування та обігу кредитних історій**» - стаття 4 - конфіденційність інформації, яка складає кредитну історію особи.

3. Закон «**Про поховання та похоронну справу**» -стаття 7 - конфіденційність інформації про померлого.

**2. Нормативно-правові акти з інформатизації та електронного урядування**

З точки зору подальшого розвитку концептуальних засад нормативно-правового регулювання забезпечення інформаційної безпеки України важливим нормативним актом є Закон України «**Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки**».

Зокрема, у **п.13** «Інформаційна безпека в інформаційному суспільстві» Закону визначено:

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

Вирішення проблем інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

З метою реалізації Закону 15 травня 2013 року розпорядженням Кабінету Міністрів України № 386-р була схвалена «**Стратегія розвитку інформаційного суспільства в Україні**», яка визначає мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення, а також основні напрями, етапи і механізм реалізації цієї Стратегії з урахуванням сучасних тенденцій та особливостей розвитку України в перспективі до 2020 року.

Згідно цієї Стратегії забезпечення інформаційної безпеки у процесі використання інформаційно-комунікаційних технологій є однією з найважливіших умов успішного розвитку інформаційного суспільства.

Пріоритетами діяльності в галузі інформаційної безпеки є:

- сприяння виробництву конкурентоспроможного національного інформаційного продукту;

- сприяння вітчизняному виробництву засобів захисту інформації, створенню захищених інформаційно-телекомунікаційних систем, запровадження сучасних захищених інформаційних технологій в інтересах державного управління;

- створення ефективної системи виявлення та запобігання загрозам державних електронних інформаційних ресурсів, у тому числі щодо протидії розповсюдженню комп’ютерних вірусів, програмних і апаратних закладок, а також витоку інформації технічними каналами та за рахунок несанкціонованих дій;

- забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів України, які створюють умови для розвитку особи, стійкого функціонування суспільства і держави, захисту персональних даних та інформації, що перебуває у володінні фізичних, юридичних осіб та держави, від зовнішніх і внутрішніх інформаційних загроз, зокрема шляхом протидії комп’ютерним злочинам;

- забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та органів місцевого самоврядування, інформаційно-телекомунікаційних систем, які функціонують в інтересах управління державою, задовольняють потреби оборони та безпеки держави, кредитно-банківських та інших сфер національної економіки, систем управління об’єктами критичної інфраструктури;

- удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема кібернетичної безпеки національної критичної інфраструктури;

- впровадження захищеного механізму ідентифікації учасників електронної взаємодії;

- формування системи моніторингу безпеки інформаційних ресурсів та систем.

Базовим законом у сфері інформатизації на сучасному етапі є Закон України «**Про Національну програму інформатизації**» (далі - Закон), однією із двох головних цілей якої є забезпечення інформаційної безпеки держави.

Згідно **статті 2** Закону Національна програма інформатизації (далі - НПІ) визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Національна програма інформатизації включає:

- Концепцію Національної програми інформатизації;

- сукупність державних програм з інформатизації;

- галузеві програми та проекти інформатизації;

- регіональні програми та проекти інформатизації;

- програми та проекти інформатизації органів місцевого самоврядування.

Згідно статті 3 Закону завданням законодавства про НПІ є запровадження правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних засад регулювання процесу формування та виконання цієї Програми та окремих її завдань (проектів).

Згідно **статті 5** Закону головною метою НПІ є створення умов для забезпечення громадян, суспільства та держави своєчасною, достовірною та повною інформацією шляхом широкого використання новітніх інформаційних технологій, забезпечення інформаційної безпеки держави.

Згідно **статті 6** Закону державні органи, в межах їх компетенції, здійснюють такі функції у процесі інформатизації:

- захист авторського права на бази даних і програми, створені для потреб інформатизації та особистої інформації;

- встановлення стандартів, норм і правил використання засобів інформатизації;

- забезпечення доступу громадян та їх об'єднань до інформації державних органів та органів місцевого самоврядування, а також до інших джерел інформації;

- визначення пріоритетних напрямів інформатизації з метою подальшої її підтримки шляхом державного фінансування та пільгового оподаткування;

- інформатизацію науки, освіти, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави, пріоритетних галузей економіки;

- підтримку вітчизняного виробництва програмних і технічних засобів інформатизації;

- підтримку фундаментальних наукових досліджень для розроблення швидкісних математичних і технічних засобів обробки інформації;

- забезпечення підготовки спеціалістів з питань інформатизації та інформаційних технологій;

- організацію сертифікації програмних і технічних засобів інформатизації;

- державне регулювання цін і тарифів на використання телекомунікаційних та комп'ютерних мереж для потреб інформатизації у бюджетній сфері;

- забезпечення інформаційної безпеки держави.

У законі визначено етапи формування і виконання, порядок здійснення експертизи, механізм контролю за виконанням НПІ, замовників, науково-технічну раду та виконавців програми, їх права та обов'язки.

В свою чергу, в Законі України «**Про Концепцію Національної програми інформатизації**» (далі - Закон) важливим фактором подолання відставання України у сфері інформатизації названа ефективна державна політика інформатизації.

Окрім того, в цьому Законі закріплені принципи державної політики у сфері інформатизації, визначені основні завдання, напрями, порядок формування та виконання основних етапів програми інформатизації, очікувані результати.

Першочергові пріоритети надаються створенню нормативно-правової бази інформатизації, включаючи систему захисту авторських прав і особистої інформації, розробленню національних стандартів у галузі інформатизації; формуванню телекомунікаційної інфраструктури, перш за все оптимізації діючої мережі магістралей передачі даних, будівництву нових сучасних каналів, включаючи волоконно-оптичні та супутникові системи зв'язку; формуванню комп'ютерної мережі освіти, науки та культури як частини загальносвітової мережі Інтернет; здійсненню заходів щодо інформаційної безпеки.

Головною метою Програми інформатизації є забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Законом визначені такі основні напрями інформатизації:

1. Розроблення політики та організаційно-правове забезпечення інформатизації.

2. Формування національної інфраструктури інформатизації.

3. Інформатизація стратегічних напрямів розвитку державності, безпеки та оборони.

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

Результатом виконання Програми буде:

- комплект 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.

4. Інформатизація процесів соціально-економічного розвитку.

5. Інформатизація пріоритетних галузей економіки.

6. Інформатизація фінансової та грошової системи, державного фінансово-економічного контролю.

7. Інформатизація соціальної сфери.

8. Інформатизація в галузі екології та використання природних ресурсів.

9. Інформатизація науки, освіти і культури.

10. Міжнародне співробітництво.

Крім того, в Законі визначено також низку інших важливих положень щодо програми інформатизації в Україні, спрямованих на забезпечення інформаційної безпеки держави.

З метою реалізації на загальнодержавному та регіональному рівнях положень відповідних законів України у галузі інформатизації були прийняті відповідні постанови Кабінету Міністрів України:

- «Про затвердження Положення про формування та виконання Національної програми інформатизації» від 31 серпня 1998 року № 1352;

- «Про затвердження Порядку формування та виконання галузевої програми і проекту інформатизації" від 18 грудня 2001 року № 1702;

- «Про затвердження Порядку формування та виконання регіональної програми і проекту інформатизації» від 12 квітня 2002 року № 644.

Державне регулювання у сфері інформатизації забезпечує **Національна комісія, що здійснює державне регулювання у сфері зв`язку та інформатизації** (далі – НКРЗІ) згідно «Положення про НКРЗІ» (далі - Положення), затвердженого Указом Президента України від 23 листопада 2011 року № 1067.

Згідно п.3 Положення основними завданнями НКРЗІ є:

1) забезпечення проведення єдиної державної політики з питань державного регулювання у сфері інформатизації та розвитку інформаційного суспільства;

2) здійснення державного регулювання у сфері інформатизації, використання інфраструктури з метою максимального задоволення попиту споживачів на послуги зв'язку та інформаційні послуги, створення сприятливих умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних та інформаційно-телекомунікаційних мереж з урахуванням інтересів національної безпеки;

5) забезпечення системності, комплексності і узгодженості розвитку інформатизації та інформаційного суспільства в державі.

*Офіційний сайт НКРЗІ: http://nkrzi.gov.ua.*

Головним органом у системі центральних органів виконавчої влади, що забезпечує формування державної політики у сфері інформатизації, електронного урядування, національних електронних інформаційних ресурсів, розвитку інформаційного суспільства є **Міністерство регіонального розвитку, будівництва та житлово-комунального господарства** **України** (далі - Мінрегіон).

Мінрегіон здійснює свою діяльність згідно **«Положення про** Мінрегіон» (далі - Положення), **затвердженого п**остановою Кабінету Міністрів України від 30 квітня 2014 року № 197. Згідно вимог Положення Мінрегіон відповідно до покладених на нього завдань:

2) затверджує:

- порядок технічного забезпечення Єдиного веб-порталу та функціонування офіційних веб-сайтів органів виконавчої влади; порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи «Електронний Уряд»;

- вимоги до форматів даних електронного документообігу в органах державної влади;

- методики визначення належності бюджетних програм до сфери інформатизації; формування індикаторів розвитку інформаційного суспільства;

- нормативно-правові акти у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства;

11) подає Кабінету Міністрів України пропозиції щодо забезпечення інформатизації, електронного урядування, формування та використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства.

Для вирішення цих завдань у складі Мінрегіону було створено **Управління інформаційних технологій та електронного урядування**. Функції з реалізації державної політики у сфері інформатизації, електронного урядування, національних електронних інформаційних ресурсів, розвитку інформаційного суспільства були покладеніна **Державне агентство з питань електронного урядування**.

З 2003 року в Україні з метою запровадження єдиної системи обліку електронних інформаційних ресурсів формується **Національний реєстр електронних інформаційних ресурсів** згідно «Концепції формування системи національних електронних інформаційних ресурсів» (далі - Концепція), затвердженої розпорядженням Кабінету Міністрів України від 5 травня 2003 року № 259-р.

Згідно Концепції інформаційна безпека національних ресурсів забезпечується їх власниками шляхом створення КСЗІ з метою запобігання несанкціонованому доступу та дотримання належного рівня захисту національних ресурсів.

Реалізація державної політики щодо забезпечення безпеки національних ресурсів здійснюється згідно законодавства спеціально уповноваженим органом державного управління у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації (*Адміністрацією Держспецзв'язку*).

Національний реєстр ведеться з використанням новітніх досягнень у сфері інформаційно-телекомунікаційних технологій згідно «**Положення про Національний реєстр електронних інформаційних ресурсів**» (далі - Положення), затвердженого постановою Кабінету Міністрів України від 17 березня 2004 року № 326.

Згідно п.3 Положення Національний реєстр - це інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах.

До Національного реєстру включаються веб-сайти, бази даних і реєстри в електронній формі (далі - е-ресурси).

Згідно п.4 Положення замовником і утримувачем Національного реєстру є **Державне агентство з питань науки, інновацій та інформатизації** (далі - Держінформнауки).

Згідно п.7 Положення до Національного реєстру включаються е-ресурси органів державної влади, органів місцевого самоврядування та інших юридичних осіб публічного права, доступ до яких здійснюється через телекомунікаційні мережі загального користування. Е-ресурсів приватної форми власності включаються на добровільних засадах.

Згідно п.8 Положення До Національного реєстру не включаються е-ресурси, які містять інформацію з обмеженим доступом та інформацію, розповсюдження якої заборонене законодавством.

Згідно п.9 Положення для включення е-ресурсу до Національного реєстру власник е-ресурсу протягом 30 днів після надання користувачам доступу до нього подає адміністратору заяву за формою, встановленою Держінформнауки.

У заяві зазначаються такі обов'язкові відомості: найменування е-ресурсу, його доменне ім'я та адреса електронної пошти, умови доступу до нього, анотація та ключові слова е-ресурсу, мова, обсяг інформації (у байтах), основні дані (реквізити) власника, основні дані (реквізити) розробника, дата надання користувачам доступу до цього е-ресурсу.

*Офіційний сайт* *Національного реєстру: http://e-resurs.gov.ua.*

4 червня 2014 року постановою Кабінету Міністрів України № 255 **Держінформнауки** було перейменоване у **Державне агентство з питань електронного урядування**. Воно здійснює свою діяльність згідно **«Положення про** Державне агентство з питань електронного урядування України» (далі - Положення), **затвердженого п**остановою Кабінету Міністрів України від 1 жовтня 2014 року № 492.

#### Згідно п.4 Положення агентство відповідно до покладених на нього завдань:

4) здійснює державну реєстрацію електронних інформаційних ресурсів державних органів, органів місцевого самоврядування та інших юридичних осіб публічного права, доступ до яких здійснюється через телекомунікаційні мережі загального користування, та видає відповідні свідоцтва;

5) забезпечує в межах повноважень, передбачених законом, належне функціонування Єдиного веб-порталу Кабінету Міністрів України з можливістю інтеграції інформаційних ресурсів центральних та місцевих органів виконавчої влади, що розміщені в Інтернеті;

6) проводить моніторинг інформаційного наповнення офіційних веб-сайтів органів виконавчої влади та про його результати інформує щороку Кабінет Міністрів України;

7) координує діяльність органів виконавчої влади, пов’язану із створенням та інтеграцією електронних інформаційних систем і ресурсів в Єдиний веб-портал органів виконавчої влади та наданням інформаційних та інших послуг через електронну інформаційну систему «Електронний Уряд»;

8) координує та контролює роботи, пов’язані із створенням, веденням і забезпеченням функціонування Національного реєстру електронних інформаційних ресурсів, визначає правила користування ним;

9) розробляє вимоги до форматів даних електронного документообігу в державних органах;

11) здійснює у межах повноважень, передбачених законом, заходи щодо:

- розвитку електронного урядування;

- створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів;

- створення Національного депозитарію електронних інформаційних ресурсів;

13) створює та забезпечує функціонування автоматизованої системи «Єдине вікно подання електронної звітності»;

14) координує адміністрування адресного простору українського сегмента Інтернету;

15) забезпечує:

- функціонування системи електронної взаємодії органів виконавчої влади;

- впровадження Національної системи індикаторів розвитку інформаційного суспільства;

- проведення експертизи Національної програми інформатизації та окремих її завдань (проектів);

16) здійснює у межах повноважень, передбачених законом, заходи щодо функціонування електронного документообігу;

17) бере участь у здійсненні заходів із застосування електронного цифрового підпису;

18) визначає у межах повноважень, передбачених законом, особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

*Офіційний сайт агентства: http://dknii.gov.ua.*

12 квітня 2002 року постановою Кабінету Міністрів України № 522 був затверджений «**Порядок підключення до глобальних мереж передачі даних**» (далі - Порядок), який визначає процедуру підключення органів виконавчої влади, інших державних органів, підприємств, установ та організацій, які одержують, обробляють, поширюють і зберігають інформацію, що є об'єктом державної власності та охороняється згідно із законодавством, до глобальних мереж передачі даних, зокрема Інтернет.

У цьому Порядку поняття вживаються в такому значенні:

- абоненти - органи виконавчої влади, інші державні органи, підприємства, установи та організації, які одержують, обробляють, поширюють і зберігають інформацію, що є об'єктом державної власності та охороняється згідно із законодавством;

- сервер - сукупність апаратних і програмних засобів, призначених для обслуговування інформаційних запитів комп'ютерів абонентів у мережах передачі даних;

- Веб-сервер - сервер, призначений для відображення інформації в мережі Інтернет;

- домен - частина адресного простору в мережі Інтернет, призначена для ідентифікації комп'ютера або групи комп'ютерів. Домени поділяються на піддомени або домени нижчих рівнів.

Згідно п.4 Порядку для підключення до глобальних мереж:

- органи виконавчої влади та інші державні органи зобов'язані зареєструвати свій домен у домені .GOV.UA;

- інші абоненти зобов'язані зареєструвати свій домен у домені нижчого рівня домену .UA;

- абоненти повинні зареєструвати хоча б одну офіційну адресу електронної пошти на сервері оператора або на власному сервері.

Адреси Веб-серверів, окремих веб-сайтів та електронної пошти абонентів повинні відповідати назвам їх доменів.

 Згідно п.7 Порядку локальні обчислювальні мережі, а також окремі електронні обчислювальні машини, на яких обробляють або зберігають інформацію з обмеженим доступом, забороняється підключати до глобальних мереж.

Домен .GOV.UA призначений для обслуговування державних установ та організацій України, що здійснюють свою діяльність у відповідності до чинного законодавства України. Адміністративні питання, пов'язані з веденням домену .GOV.UA, вирішує Адміністратор домену GOV.UA.

На дания час таким Адміністратором є ТОВ «Хостмайстер» (Київ), яке було створено в 2001 році провідними українськими фахівцями у галузі Інтернет-технологій, виконує в Україні функцію адміністратора доменів .UA і .COM.UA і визначає правила розподілу адресного простору, встановлення порядку та правил реєстрації й використання доменних імен.

Згідно розроблених ТОВ «Хостмайстер» **«Правил домену GOV.UA**»(*www.gov.ua*) делегування доменних імен у домені .GOV.UA здійснюється на підставі офіційного листа на ім'я Адміністратора домену GOV.UA, виконаного на офіційному бланку державної організації-замовника з печаткою організації та за підписом її керівника.

З метою підвищення ефективності та прозорості діяльності цих органів шляхом впровадження та використання сучасних інформаційних технологій для надання інформаційних та інших послуг громадськості, забезпечення її впливу на процеси, що відбуваються у державі 4 січня 2002 року постановою Кабінету Міністрів України № 3 був затверджений «**Порядок оприлюднення в мережі Інтернет інформації про діяльність органів виконавчої влади**» (далі - Порядок).

Згідно п.2 Порядку оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади здійснюється шляхом:

- розміщення і постійного оновлення міністерствами, іншими центральними та місцевими органами виконавчої влади інформації відповідно до вимог Закону України «Про доступ до публічної інформації» та цього Порядку на офіційних веб-сайтах;

- створення Єдиного веб-порталу Кабінету Міністрів України (далі - Веб-портал), призначеного для інтеграції офіційних веб-сайтів органів виконавчої влади та розміщення інформаційних ресурсів відповідно до потреб громадян.

Інформаційне наповнення та технічне забезпечення веб-порталів:

- Верховної Ради України здійснюється згідно «**Положення про веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет**», затвердженого розпорядженням Голови Верховної Ради України від 24 травня 2001 року № 462;

- органів виконавчої влади - згідно «**Порядку інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади**» та «**Порядку функціонування веб-сайтів органів виконавчої влади**», затверджених спільним наказом Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України від 25 листопада 2002 року № 327/225, зареєстрованим в Міністерстві юстиції України 29 грудня 2002 року за № 1021/7309.

24 лютого 2003 року Кабінетом Міністрів України була прийнята постанова № 208 «**Про заходи щодо створення електронної інформаційної системи "Електронний Уряд"**», яка встановила, що:

- одним з пріоритетних завдань щодо розвитку інформаційного суспільства є надання громадянам та юридичним особам інформаційних та інших послуг шляхом використання електронної інформаційної системи «Електронний Уряд», яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з фізичними та юридичними особами на основі сучасних інформаційних технологій;

- Єдиний веб-портал органів виконавчої влади є центральною частиною електронної інформаційної системи «Електронний Уряд», призначеною для інтеграції веб-сайтів, електронних інформаційних систем та ресурсів органів виконавчої влади і надання інформаційних та інших послуг з використанням мережі Інтернет.

*Офіційний сайт Єдиного веб-порталу: www.kmu.gov.ua.*

Іншим важливим нормативно-правовим актом у зазначеній сфері є наказ Державного комітету зв'язку та інформатизації України від 15 серпня 2003 року № 149 «**Про затвердження Переліку і Порядку надання інформаційних та інших послуг з використанням електронної інформаційної системи "Електронний Уряд"**», зареєстрований в Міністерстві юстиції України 19 листопада 2003 року за № 1065/8386.

Порядок визначає процедуру надання органами виконавчої влади інформаційних та інших послуг громадянам і юридичним особам з використанням електронної інформаційної системи «Електронний Уряд».

Види інформаційні послуг, що надаються з використанням електронної інформаційної системи «Електронний Уряд», визначені в Переліку. Можливості надання органом виконавчої влади певної послуги визначаються готовністю цього органу надавати відповідну державну послугу в електронній формі та потребою громадян і юридичних осіб у такій послузі.

1 березня 2010 року було прийнято розпорядження Кабінету Міністрів України № 360-р  «**Питання реалізації пілотного проекту впровадження технологій електронного урядування**», згідно чого основним завданням пілотного проекту є визначення механізму розв'язання проблем, пов'язаних з:

- функціонуванням електронного документообігу;

- забезпеченням постійного зберігання електронних документів та інших електронних інформаційних ресурсів, а також захисту інформації;

- розробленням форматів типових електронних документів органів державної влади та органів місцевого самоврядування;

- підготовкою тимчасового регламенту електронного документообігу в органах виконавчої влади;

- впровадженням єдиних форматів та протоколів ЕЦП;

- розробленням та впровадженням програмно-апаратних засобів для забезпечення сумісності систем електронного документообігу органів державної влади;

- створенням та забезпеченням функціонування системи загальнодержавних класифікаторів і реєстрів, необхідних для підготовки електронних документів, шляхом інтеграції відповідних електронних інформаційних ресурсів;

- створенням та забезпеченням ведення національного реєстру електронних інформаційних ресурсів;

- впровадженням програмно-технічного комплексу другої черги технологічного центру центрального засвідчувального органу;

- утворенням резервного акредитованого центру сертифікації ключів для органів державної влади;

- створенням національної системи єдиного часу для синхронізації інформаційних систем із Всесвітнім координованим часом (UTC);

- впровадженням технології надання адміністративних послуг через Інтернет органами виконавчої влади і бюджетними установами в межах їх повноважень;

- створенням веб-порталу з питань підтримки розвитку електронного урядування;

- утворенням на базі державного підприємства «Державний центр інформаційних ресурсів» (далі - ДП «Держінформресурс») **Національного центру електронного урядування** (далі - НЦЕУ).

НЦЕУ - це установа, що забезпечує інформаційну підтримку органів виконавчої влади та місцевого самоврядування, фізичних і юридичних осіб щодо застосування технологій електронного урядування.

*Офіційний сайт НЦЕУ: http://nc.da-gov.adamant.ua.*

НЦЕУ є структурним підрозділом ДП «Держінформресурс» і функціонує згідно «Положення про НЦЕУ», затвердженого наказом ДП «Держінформресурс» від 3 лютого 2014 року.

*Офіційний сайт ДП «Держінформресурс»: www.dir.gov.ua.*

З метою подальшого розвитку інформаційного суспільства держави розпорядженням Кабінету Міністрів України від 5 вересня 2012 року № 634-р була схвалена «**Концепція створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів**» (далі - Концепція).

Згідно Концепції впровадження електронного урядування є важливою умовою розвитку інформаційного суспільства та становлення електронної демократії, де кожен громадянин може створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися та обмінюватися інформацією і знаннями, використовувати інформаційні технології для розширення можливостей реалізації власного потенціалу, сприяти суспільному і особистому розвитку, підвищувати якість життя та створювати умови для відкритого і прозорого державного управління.

Головною складовою електронного урядування повинна стати система електронної взаємодії державних електронних інформаційних ресурсів. Метою її створення є забезпечення електронного обслуговування осіб за принципом «єдиного вікна» із застосуванням ЕЦП. Основною умовою функціонування системи є забезпечення безпеки інформації згідно вимог законодавства про захист інформації та персональних даних.

18 липня 2012 року постановою Кабінету Міністрів України № 670 було затверджено «**Положення про систему електронної взаємодії органів виконавчої влади**» (далі - Положення), яке визначає загальні засади створення, впровадження та забезпечення функціонування системи електронної взаємодії органів виконавчої влади (далі - система).

Згідно п.2 Положення система призначена для автоматизації процесів створення, відправлення, передавання, одержання, оброблення, використання, зберігання, знищення електронних документів та копій паперових документів в електронному вигляді з використанням ЕЦП (далі - електронні документи), які не містять інформацію з обмеженим доступом, та контролю за виконанням актів Кабінету Міністрів України та інших документів.

Згідно п.4 Положення користувачами системи є відповідальні посадові особи Секретаріату Кабінету Міністрів України, міністерств, інших центральних та місцевих органів виконавчої влади.

Згідно п.5. Положення створення та функціонування системи забезпечує держатель, яким є Державне агентство з питань електронного урядування (далі - держатель системи).

Згідно п.6 Положення адміністратором системи є ДП «Держінформресурс» (далі - адміністратор системи), що належить до сфери управління Державного агентства з питань електронного урядування.

Адміністратор системи:

- створює, впроваджує та здійснює підтримку функціонування системи;

- надає користувачам захищений доступ до системи;

- забезпечує зберігання та несе відповідальність за захист інформації, яка обробляється у системі;

- здійснює інші заходи, пов'язані з функціонуванням системи.

Згідно п.7 Положення обмін інформацією в системі здійснюється за допомогою Інтернету або Національної системи конфіденційного зв'язку.

Програмно-технічні комплекси та технічні засоби системи повинні забезпечувати унеможливлення несанкціонованого знищення, блокування, порушення цілісності та режиму доступу до інформації, яка обробляється в системі.

Захист інформації в системі забезпечується шляхом здійснення організаційних та інженерно-технічних заходів з використанням програмно-технічних засобів відповідно до законодавства.

1 листопада 2012 року наказом Міністерства юстиції України № 1600/5 був затверджений «**Порядок роботи з електронними документами через систему електронної взаємодії органів виконавчої влади з використанням ЕЦП**» (далі - Порядок), зареєстрованим в Міністерстві юстиції України 5 листопада 2012 року за № 1854/22166.

Цей Порядок встановлює загальні правила створення, відправлення, передавання, одержання, оброблення, використання та зберігання електронних документів, які не містять інформацію з обмеженим доступом, Секретаріатом Кабінету Міністрів України, міністерствами, іншими центральними та місцевими органами виконавчої влади (далі - суб’єкти) через систему електронної взаємодії органів виконавчої влади (далі - Система).

Згідно розділу І Порядку «**Загальні положення**» з використанням функціональних можливостей програмного забезпечення Системи здійснюється автоматизація процесів створення, відправлення, передавання, одержання, оброблення, використання, зберігання, обліку та контролю за виконанням електронних документів, що створюються суб'єктами у процесах документообігу.

Інформація у Системі обробляється із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

Суб’єкти під час користування Системою за рішенням керівника цього суб’єкта використовують для передачі та отримання інформації мережу Інтернет або Національну систему конфіденційного зв'язку.

Згідно розділу ІІ Порядку «**Реєстрація та отримання доступу в Системі**» Адміністратором системи забезпечується реєстрація суб'єктів та їх користувачів у Системі.

Доступ користувачів до Системи забезпечується шляхом їх авторизації. Авторизація користувачів у Системі здійснюється з використанням надійних засобів ЕЦП.

Згідно розділу ІІІ Порядку «**Робота з електронними документами в Системі**» користувач для одержання інформації щодо створених суб'єктами електронних документів використовує списки вхідних і вихідних документів, сформованих Системою.

Електронний документ, що надійшов на електронну адресу суб’єкта, відхиляється у таких випадках:

- електронний документ надійшов не за адресою;

- електронний документ заражений вірусом;

- електронний документ не пройшов перевірку на цілісність;

- будь-який із накладених на електронний документ ЕЦП не пройшов перевірку на справжність.

Про реєстрацію чи відхилення електронного документа суб'єкт, що відправив документ, невідкладно повідомляється в автоматизованому режимі засобами Системи.

Згідно розділу ІV Порядку «**Зберігання документів**» документи постійного та тривалого (понад 10 років) зберігання створюються одночасно в паперовій та електронній формах.

Електронні документи, опрацювання яких у Системі закінчено та які повинні бути передані на постійне або тривале зберігання до архіву, мають бути підготовлені до передачі на архівне зберігання засобами Системи у порядку, визначеному законодавством.

20 жовтня 2011 року наказом Міністерства освіти і науки, молоді та спорту України № 1207 були затверджені «**Вимоги до форматів даних електронного документообігу в органах державної влади**» (далі - Вимоги), зареєстрованим у Міністерстві юстиції України 15 листопада 2011 року за № 1306/20044.

Згідно розділу І Вимог програмне забезпечення може бути реалізовано окремим автономним рішенням або інтегровано у внутрішню систему електронного документообігу як його складова частина.

Електронне повідомлення передається з системи електронного документообігу відправника в систему електронного документообігу одержувача у вигляді файлу.

Електронне повідомлення в цілому та його складові частини можуть бути незалежно підписані ЕЦП та (або) зашифровані.

**3. Нормативно-правові акти щодо захисту**

**конфіденційної інформації**

Важливим кроком для захисту конфіденційної інформації з урахуванням розвитку інформатизації та утворення різноманітних баз даних було прийняття у 2010 році Закону України «**Про захист персональних даних**» (далі - Закон), який регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Він поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

У цьому Законі нижченаведені терміни вживаються в такому значенні:

- персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

- суб’єкт персональних даних - фізична особа, персональні дані якої обробляються;

- обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем;

- база персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

- володілець персональних даних - фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Згідно **статті 5** Закону персональні дані є об’єктами захисту.

Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень.

Персональні дані, зазначені у декларації про майно, доходи, витрати і зобов’язання фінансового характеру, оформленій за формою і в порядку, встановленими Законом України «Про засади запобігання і протидії корупції», не належать до інформації з обмеженим доступом.

Не належать до інформації з обмеженим доступом дані про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених статтею 6 Закону України «Про доступ до публічної інформації».

Згідно **статті 6** Закону не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Згідно **статті 8** Закону суб'єкт персональних даних має право:

1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

5) пред’являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

7) на захищеність своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

8) звертатися із скаргами на обробку своїх персональних даних до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

11) відкликати згоду на обробку персональних даних;

12) знати механізм автоматичної обробки персональних даних;

13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Згідно **статті 24** Закону розпорядники персональних даних та треті особи зобов’язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

В органах державної влади, органах місцевого самоврядування, а також у розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому, який забезпечує її оприлюднення.

Структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці:

1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

2) взаємодіє з Уповноваженим та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

 Згідно **статті 25** Закону дозволяється обробка персональних даних без застосування положень цього Закону, якщо така обробка здійснюється:

1) фізичною особою виключно для особистих чи побутових потреб;

2) виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів.

Контроль за додержанням вимог законодавства про захист персональних даних здійснює Уповноважений Верховної Ради України з прав людини(далі - Уповноважений).

8 січня 2014 року наказом Уповноваженого № 1/02-14 були затверджені такі документи:

- Типовий порядок обробки персональних даних;

- Порядок здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних;

- Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.

**1. Типовий порядок обробки персональних даних** (далі - Порядок).

Розділ 3 «Захист персональних даних» Порядку визначає такі вимоги:

3.1. Володілець (розпорядник) персональних даних (далі - володілець) вживають заходів щодо захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

3.2. Володілець самостійно визначає перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки.

3.3. Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

3.4. Організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників володільця;

- визначення порядку ведення обліку операцій, пов’язаних з обробкою персональних даних суб’єкта та доступом до них;

- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;

- регулярне навчання співробітників, які працюють з персональними даними.

3.5. Володілець веде облік працівників, які мають доступ до персональних даних суб’єктів. Володілець визначає рівень доступу зазначених працівників до персональних даних суб’єктів. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб’єктів, які необхідні йому у зв’язку з виконанням своїх професійних чи службових або трудових обов’язків.

3.6. Усі інші працівники володільця мають право на повну інформацію лише стосовно власних персональних даних.

3.7. Працівники, які мають доступ до персональних даних, дають письмове зобов’язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв’язку з виконанням професійних чи службових або трудових обов’язків.

3.13. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

3.14. З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

**2. «Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації»** (далі - Порядок).

Згідно п.1.2 Порядку обробка персональних даних, що становить особливий ризик для прав і свобод суб’єктів, - це будь-які дії з персональними даними про:

- расове, етнічне та національне походження;

- політичні, релігійні або світоглядні переконання;

- членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;

- стан здоров’я;

- статеве життя;

- біометричні дані;

- генетичні дані;

- притягнення до адміністративної чи кримінальної відповідальності;

- застосування щодо особи заходів в рамках досудового розслідування;

- вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»;

- вчинення щодо особи тих чи інших видів насильства;

- місцеперебування та/або шляхи пересування особи.

Згідно п.2.1 Порядку володілець повинен повідомити Уповноваженого про обробку персональних даних, які становлять особливий ризик для прав і свобод суб’єктів персональних даних, крім випадків, якщо:

- здійснюється обробка, єдиною метою якої є ведення реєстру для надання інформації населенню, який відкритий для населення в цілому;

- обробка здійснюється громадськими об’єднаннями, політичними партіями та/або організаціями, професійними спілками, об’єднаннями роботодавців, релігійними організаціями, громадськими організаціями світоглядної спрямованості за умови, що обробка стосується виключно персональних даних членів цих об’єднань та не передається без їх згоди;

- обробка необхідна для реалізації прав та виконання обов’язків володільця персональних даних у сфері трудових правовідносин відповідно до закону.

*Офіційний сайт Уповноваженого: www.ombudsman.gov.ua.*

Закон України «**Про організацію формування та обігу кредитних історій**» (далі - Закон) визначає правові та організаційні засади формування і ведення кредитних історій, права суб'єктів кредитних історій та користувачів бюро кредитних історій, вимоги до захисту інформації, що складає кредитну історію, порядок утворення, діяльності та ліквідації бюро кредитних історій.

Терміни, що вживаються в Законі, мають таке значення:

- кредитна історія - це сукупність інформації про юридичну або фізичну особу, що її ідентифікує, відомостей про виконання нею зобов'язань за кредитними правочинами, іншої відкритої інформації відповідно до Закону;

- бюро кредитних історій (далі - Бюро) - юридична особа, виключною діяльністю якої є збір, зберігання, використання інформації, яка складає кредитну історію;

Згідно **статті 4** Закону основними принципами формування та доступу до інформації, яка складає кредитну історію, є конфіденційність інформації та її захист.

Згідно **статті 12** Закону Бюро зобов'язане забезпечити захист інформації, що складає кредитну історію, згідно із законодавством України. Бюро не мають права доручати третім особам здійснювати діяльність з ведення кредитних історій.

Бюро та Користувачі несуть відповідальність згідно із законами України за перекручення, незаконне розголошення та нецільове використання інформації, що складає кредитну історію.

Згідно **статті 15** Закону у разі, якщо Бюро передбачає здійснювати діяльність із збирання та використання інформації, яка складає кредитну історію, воно починає здійснення такої діяльності з моменту отримання відповідної ліцензії.

Основним нормативним документом в Україні щодо поводження з матеріальними носіями, які містять службову інформацію (далі - документи), є «**Інструкція про порядок обліку, зберігання й використання документів, справ, видань і інших матеріальних носіїв інформації, що містять службову інформацію**» (далі - Інструкція), затверджена постановою Кабінету Міністрів України від 27 листопада 1998 року № 1898.

Інструкція складається з таких розділів:

- загальні положення;

- приймання і облік документів;

- розмноження і розсилання (відправлення) документів;

- формування виконаних документів у справи;

- використання документів та зняття грифа «ДСК»;

- відбір документів для зберігання і знищення;

- забезпечення схоронності документів та перевірка їх наявності;

- облік, зберігання і використання печаток, штампів і бланків;

- особливості поводження з мобілізаційними документами;

- охорона документів під час прийому іноземних делегацій, груп та окремих іноземців.

**Загальні положення**

1. Переліки відомостей, які містять службову інформацію, затверджуються міністерствами, іншими центральними органами виконавчої влади, обласними державними адміністраціями.

У разі потреби на державних підприємствах, в установах і організаціях з урахуванням особливостей їхньої діяльності розробляються та за погодженням з міністерством, іншим центральним органом виконавчої влади, до сфери управління якого вони належать, вводяться в дію переліки конкретних видів документів у відповідній сфері діяльності.

2. На документах у правому верхньому кутку першої сторінки, а для видань - на обкладинці та на титулі проставляються гриф «Для службового користування» (далі - ДСК) і номер примірника.

Якщо гриф обмеження доступу неможливо нанести безпосередньо на магнітний носій інформації, він має бути зазначений у супровідному документі.

3. Необхідність проставлення грифа «ДСК» визначається на підставі переліків, зазначених у пункті 1 Інструкції: на документі - виконавцем та особою, що підписує документ; на виданні - автором (укладачем) і керівником, який підписав видання до друку.

6. Ведення обліку, зберігання, розмноження та використання службових документів, а також контроль за дотриманням вимог Інструкції покладається на управління справами, загальні відділи, канцелярії організацій (далі - канцелярії).

7. Запобігання розголошенню службової інормації та випадкам втрат службових документів покладається на режимно-секретний орган установи (далі - РСО).

8. Співробітники організацій для отримання допуску до роботи зі службовими документами зобов'язані ознайомитись під розписку з цією інструкцією, а також відповідними відомчими інструкціями. Ознайомлення здійснюють канцелярії організацій.

Співробітникам (виконавцям), які працюють зі службовими документами, забороняється повідомляти усно або письмово будь-кому відомості, що містяться у цих документах, якщо це не викликано службовою потребою.

**Розмноження і розсилання (відправлення) документів**

18. Використання ІТС для обробки службових документів може здійснюватися тільки після створення в ній КСЗІ та підтвердження її відповідності вимогам нормативних документів з питань ТЗІ в порядку, встановленому законодавством.

Дозвіл на використання ІТС для обробки службових документів надається за наказом керівника організації та наявністю атестата відповідності КСЗІ.

28. Ознайомлення представників засобів масової інформації з документами з грифом «ДСК» та передавання їм таких матеріалів допускається у кожному окремому випадку за письмовими дозволами керівників організацій, яким надано право відповідно до пункту 1 Інструкції затверджувати переліки відомостей, які містять службову інформацію.

Такі документи попередньо розглядаються експертними комісіями, які приймають письмові рішення про доцільність їх передавання або можливість зняття грифа «ДСК», якщо на момент ознайомлення або передавання відомості, що містяться у документах, втратили первісне значення.

Якщо в документах з грифом «ДСК» містяться відомості, що належать до компетенції інших організацій, передавання їх у засоби масової інформації може бути здійснене лише за письмовою згодою цих організацій.

Забороняється надсилати за кордон видання з грифом «ДСК» у порядку книгообміну або експонування на виставках, презентаціях тощо.

36. Передача службової інформації каналами зв'язку здійснюється лише з використанням засобів технічного та (або) криптографічного захисту інформації.

**Забезпечення схоронності документів та перевірка їх наявності**

55. Службові документи повинні зберігатися у службових приміщеннях у шафах (сховищах), які надійно замикаються та опечатуються. Забороняється зберігати такі документи у підсобних фондах бібліотек.

58. Забороняється виносити службові документи за межі службових приміщень організації.

У разі потреби керівник організації (структурного підрозділу) може дозволити виконавцям або співробітникам канцелярії винести зі службового приміщення організації службові документи для їх погодження, підписання тощо в організаціях, що знаходяться у межах одного населеного пункту.

59. Особам, які відряджені до інших населених пунктів, забороняється мати при собі службові матеріали. Ці матеріали повинні бути заздалегідь надіслані на адресу організації за місцем відрядження співробітника.

В окремих випадках з дозволу керівника організації дозволяється перевезення службових документів до іншого населеного пункту за умови, що такі документи перевозяться групою у складі не менше двох працівників (або одного озброєного працівника), що мають виконувати роботу з ними в іншому населеному пункті.

62. Про факти втрати службових документів або розголошення відомостей, що містяться в них, терміново доводиться до відома керівника організації, керівників РСО та канцелярії, а також письмово повідомляються органи СБУ із зазначенням обставин втрати документів чи розголошення відомостей та вжитих заходів.

Для розслідування факту втрати службових документів або встановлення факту розголошення відомостей, що містяться в них, наказом керівника організації призначається комісія, висновок якої затверджується керівником організації.

**Охорона документів під час прийому іноземних делегацій, груп та окремих іноземців**

82. Підрозділом зовнішніх відносин разом з іншими підрозділами, що беруть участь у прийомі іноземців, розробляється програма роботи з іноземцями.

83. Керівник організації або за його дорученням керівник РСО завчасно інформує у письмовій формі орган СБУ про склад закордонної делегації із зазначенням прізвищ, імен та посад її членів, а також про час перебування та мету відвідання організації.

Разом з інформацією надсилається копія програми проведення роботи з іноземцями. З урахуванням особливостей діяльності розвідувальних органів України обсяг інформації, яка подається до СБУ, визначається цими органами за погодженням із СБУ.

88. В організаціях, що систематично приймають іноземців, обладнуються виділені для цієї мети приміщення, які до початку відвідання іноземцями та після його завершення перевіряються працівниками підрозділу ТЗІ.

17 липня 2009 року постановою Кабінету Міністрів України № 733 був затверджений «**Порядок надсилання електронною поштою службових документів**» (далі - Порядок), який визначає механізм надсилання та одержання електронною поштою електронних копій службових документів, підготовлених у паперовому вигляді (далі - службові документи), для їх використання у роботі міністерств, інших центральних органів виконавчої влади та обласних держадміністрацій (далі - органи виконавчої влади):

3. Для здійснення електронного обміну службовими документами створюються електронні поштові скриньки:

- в органах виконавчої влади - *kabmin\_doc@*;

- у кожному структурному підрозділі Секретаріату Кабінету Міністрів України - *ind@kmu.gov.ua* (де *ind* - індекс структурного підрозділу).

Згідно п.4 Порядку в органах виконавчої влади визначаються особи, що відповідають за здійснення електронного обміну службовими документами (далі - відповідальні особи), -по два працівники у службах, що забезпечують діяльність керівників органів виконавчої влади, і у структурних підрозділах з питань інформаційних технологій апаратів органів виконавчої влади.

6. Відповідальні особи, які працюють у структурних підрозділах з питань інформаційних технологій апаратів органів виконавчої влади, забезпечують встановлення на відповідних комп'ютерах програми електронної пошти, антивірусних програмних засобів та пристроїв для сканування документів, підготовлених у паперовому вигляді, а також функціонування електронної пошти, поновлення її адреси.

10. Електронною поштою надсилаються службові документи, що скановані та збережені у форматі PDF. У разі необхідності допускається використання інших форматів, узгоджених відповідальними особами із структурними підрозділами з питань інформаційних технологій апаратів органів виконавчої влади.

Тексти службових документів, підготовлених у паперовому вигляді, скануються разом з підписом (або візою) посадової особи та/або штрих-кодом, який містить інформацію про відповідальний підрозділ, виконавця, реєстрацію документа тощо.

На службових документах, підготовлених у паперовому вигляді, у разі здійснення електронного обміну ними, обов'язково робиться позначка про час надсилання та адресатів.

12. Під час здійснення електронного обміну службовими документами необхідно дотримуватися вимог щодо обов'язкового:

- підтвердження факту одержання кожного службового документа;

- проведення перевірки антивірусним програмним засобом кожного службового документа, що надійшов;

- здійснення обліку службових документів в окремому журналі із зазначенням адреси електронної пошти.

13. Електронний обмін службовими документами здійснюється з використанням спеціальної інформаційно-телекомунікаційної системи органів виконавчої влади.

15. Органи виконавчої влади під час здійснення електронного обміну службовими документами дотримуються вимог нормативно-правових актів, що регулюють відносини у сфері захисту інформації.

Крім того, важливим кроками у сфері інформаційної безпеки стала ратифікація Україною двох європейських **Конвенцій** та імплементація їх положень до свого законодавства:

- у 2005 році - «**Про кіберзлочинність**», яка була підписана державами-членами Ради Європи у 2001 році;

- у 2010 році - «**Про захист осіб у зв'язку з автоматизованою обробкою персональних даних**», яка була підписана цими державами ще у 1981 році.

1. Конвенція Ради Європи № 108 «**Про захист осіб у зв'язку з автоматизованою обробкою персональних даних**» та «Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних» (ETS № 181) зобов’язує держав, які підписали ці документи, керуватися їх положеннями при розгляді питань, пов’язаних із захистом персональних даних, що підлягають чи не підлягають автоматизованій обробці, як у суспільному, так і приватному секторах.

Без цього документа інші країни відмовлялися передавати в Україну бази даних. Так, якщо європейська компанія замовляє українській розробку програмного забезпечення для обробки інформації, то вона хоче, щоб розробник ніс законну відповідальність, яка повинна бути прописана в українському законодавстві.

Згідно **статті 7** Конвенції «**Безпека даних**» для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, уживають відповідних заходів безпеки, спрямованих на запобігання випадковому чи несанкціонованому знищенню або випадковій утраті, а також на запобігання несанкціонованим доступу, зміні або поширенню.

2. Конвенція Ради Європи «**Про кіберзлочинність**» передбачає надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях, укладення домовленостей щодо дієвого міжнародного співробітництва.

Згідно Конвенції до злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відносяться незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями;

до злочинів, пов’язаних з комп’ютерами - підробка та шахрайство;

до злочинів пов’язаних зі змістом - вироблення дитячої порнографії, пропонування або надання доступу до дитячої порнографії, розповсюдження, передача, здобуття дитячої порнографії за допомогою комп'ютерних і володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації;

до злочинів щодо порушення авторських і суміжних прав - правопорушення, за які передбачено кримінальну відповідальність.

Ратифікація Конвенції є дуже суттєвим кроком України на шляху протидії злочинам у сфері використання комп’ютерних технологій. Використовуючи закладені у ній норми, вітчизняні правоохоронці зможуть отримувати необхідні їм комп’ютерні дані, що знаходяться на закордонних серверах, якщо такі дані стосуються порушених в Україні кримінальних справ.

До речі, положення **Конвенції** знайшли своє відображення в Законі України «**Про внесення змін до Кримінального та Кримінально-процесуального кодексів України**» від 23.12.2004 року, відповідно до якого в розділі 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» викладені у новій редакції такі статті Кримінального кодексу України:

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

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

- 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.

Передбачена також кримінальна відповідальність за такими статтями Кримінального кодексу України:

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

- 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;

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

Основним нормативно-прававим актом для організації боротьби з кіберзлочинністю та іншими правопорушеннями є Закон України«**Про оперативно-розшукову діяльність**» (далі - Закон). Згідно **статті 2** Закону оперативно-розшукова діяльність (ОРД) - це система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів.

Згідно **статті 5** Закону ОРД здійснюється такими оперативними підрозділами:

- Служби безпеки України;

- Служби зовнішньої розвідки;

- Державної прикордонної служби;

- Державної фіскальної служби;

- Державної пенітенціарної служби;

- Міністерства внутрішніх справ;

- управління державної охорони;

- розвідувального органу Міністерства оборони.

Згідно **статті 8** Закону оперативні підрозділи для виконання завдань ОРД за наявності передбачених статтею 6 цього Закону підстав мають право:

 9) здійснювати аудіо-, відеоконтроль особи,

 знімати інформацію з транспортних телекомунікаційних і електронних інформаційних мереж згідно з положеннями статей 260, 263-265 Кримінального процесуального кодексу України (далі - КПКУ);

10) накладати арешт на кореспонденцію, здійснювати її огляд та виїмку згідно з положеннями статей 261, 262 КПКУ;

11) спостерігати за особою, річчю або місцем та вести аудіо-, відеоконтроль місця згідно з положеннями статей 269, 270 КПКУ;

12) встановлювати місцезнаходження радіоелектронного засобу згідно з положеннями статті 268 КПКУ;

19) застосовувати засоби фізичного впливу, спеціальні засоби та вогнепальну зброю на підставах і в порядку, встановлених законами про міліцію, Службу безпеки України, Державну прикордонну службу України, державну охорону органів державної влади України та посадових осіб, Митним кодексом України.

 Згідно **статті 9** Закону під час здійснення ОРД не допускається порушення прав і свобод людини та юридичних осіб. Окремі обмеження цих прав і свобод мають винятковий і тимчасовий характер і можуть застосовуватись лише за рішенням слідчого судді з метою виявлення, попередження чи припинення тяжкого або особливо тяжкого злочину та у випадках, передбачених законодавством України, з метою захисту прав і свобод інших осіб, безпеки суспільства.

У випадках порушення прав і свобод людини або юридичних осіб в процесі здійснення ОРД, а також у разі, якщо причетність до правопорушення особи, щодо якої здійснювалась ОРД, не підтвердилась, Служба безпеки України… зобов'язані невідкладно поновити порушені права і відшкодувати заподіяні матеріальні та моральні збитки в повному обсязі.

Громадяни України та інші особи мають право у встановленому законом порядку одержати від органів, на які покладено здійснення ОРД, письмове пояснення з приводу обмеження їх прав і свобод та оскаржити ці дії.

Одержані внаслідок ОРД відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій, зберіганню не підлягають і повинні бути знищені. Відомості, одержані внаслідок ОРД, щодо підготовки до терористичних актів чи їх вчинення окремими особами та групами, зберігаються до 5 років.

Спостереження за особою, річчю або місцем, а також аудіо-, відеоконтроль місця може проводитися з метою встановлення даних про особу та про її зв'язки у разі, коли є факти, які підтверджують, що нею готується тяжкий або особливо тяжкий злочин, для отримання відомостей, які вказують на ознаки такого злочину, для забезпечення безпеки працівників суду і правоохоронних органів та осіб, які беруть участь у кримінальному судочинстві, членів їх сімей та близьких родичів цих осіб, а також з метою отримання
розвідувальної інформації в інтересах безпеки суспільства та держави.

Для одержання інформації в процесі здійснення ОРД забороняється застосовувати технічні засоби, психотропні та інші речовини, які пригнічують волю або завдають шкоди здоров'ю людей та навколишньому середовищу.

Згідно **статті 11** Закону органи державної влади, підприємства, установи, організації незалежно від форми власності зобов'язані сприяти оперативним підрозділам у вирішенні завдань ОРД.

За бажанням осіб їх співробітництво з оперативним підрозділом може бути оформлено письмовою угодою з гарантуванням конфіденційності співробітництва. Угоду про сприяння оперативним підрозділам в ОРД може бути укладено з дієздатною особою.

Особи, які залучаються до виконання завдань ОРД, зобов'язані зберігати таємницю, що стала їм відома. Розголошення цієї таємниці тягне за собою відповідальність за чинним законодавством, крім випадків розголошення інформації про незаконні дії, що порушують права людини.

Забороняється залучати до виконання завдань ОРД осіб, професійна діяльність яких пов'язана зі збереженням професійної таємниці, а саме: адвокатів, нотаріусів, медичних працівників, священнослужителів, журналістів, якщо таке співробітництво буде пов'язано з розкриттям конфіденційної інформації професійного характеру.

Окремим підзаконним нормативно-прававим актом щодо спеціальних технічних засобів негласного отримання інформації (далі - СТЗ) є «**Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації**» (далі - Положення), затвердженепостановою Кабінету Міністрів України від 27 жовтня 2001 року № 1450.

Згідно п.2 Положення замовниками розроблення, виготовлення та придбання СТЗ можуть бути центральні органи виконавчої влади, розвідувальні (далі - державні замовники), міжнародні правоохоронні організації, спеціальні служби та правоохоронні органи іноземних держав (далі - іноземні замовники).

Згідно п.3 Положення державними замовниками розроблення, виготовлення та придбання СТЗ можуть бути: СБУ, розвідувальні органи, МВС, Державна податкова адміністрація, Держкомкордон, Управління державної охорони, Державний департамент з питань виконання покарань, а також Міноборони в межах, визначених законодавством.

Згідно п.4 Положення виконавцями, а у разі потреби співвиконавцями замовлення з розроблення та виготовлення СТЗ можуть бути наукові організації та підприємства, що мають відповідні ліцензії, а також суб'єкти господарювання іноземних держав та безпосередньо державні замовники.

Згідно п.7 Положення розроблення, виготовлення та реалізація СТЗ здійснюється виключно для задоволення потреб державних та іноземних замовників.

Згідно п.8 Положення іноземні замовники отримують вироблені в Україні СТЗ відповідно до зовнішньоекономічних контрактів з урахуванням вимог законодавства про охорону державної таємниці за наявності дозволу Державної служби експортного контролю, виданого в установленому порядку.

**4. Нормативно-правові акти з охорони державної таємниці**

Охорона державної таємниці є головним аспектом інформаційної безпеки держави, тому найважливішим нормативно-правовим актом є Закон України «**Про державну таємницю**» (далі - Закон).Він регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

У Законі терміни вживаються у такому значенні:

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

- охорона державної таємниці - комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

- технічний захист секретної інформації - вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

- криптографічний захист секретної інформації - вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Згідно **статті 5** Закону спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України (далі - СБУ).

Згідно **статті 8** Закону до державної таємниці у порядку, встановленому цим Законом, відноситься визначена інформація у сферах оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

Не відноситься до державної таємниці інформація:

- про стан довкілля, про якість харчових продуктів і предметів побуту, про вплив товару (роботи, послуги) на життя та здоров’я людини;

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

- про факти порушень прав і свобод людини і громадянина;

- про незаконні дії державних органів, органів місцевого самоврядування та їх посадових і службових осіб.

Згідно **статті 12** Закону Звід відомостей, що становлять державну таємницю (далі - ЗВДТ), формує СБУ на підставі рішень державних експертів з питань таємниць(наказ СБУ від12 серпня 2005 року № 440, зареєстрований в Міністерстві юстиції України 17 серпня 2005 року за № 902/11182).

ЗВДТ складається з двох розділів: загальні положення та відомості, що становлять державну таємницю.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер статті ЗВДТ | Зміст відомостей, що становлять державну таємницю | Ступінь секрет-ності | Строк дії рішення про віднесення інформації до державної таємниці (у роках) | Суб'єкти режимно-секретної діяльності, державними експертами яких прийняті рішення про віднесення інформації до державної таємниці |
| 1. Сфера оборони |
| 2. Сфера економіки, науки і техніки |
| 3. Сфера зовнішніх відносин |
| 4. Сфера державної безпеки та охорони правопорядку |

 На підставі та в межах ЗВДТ з метою конкретизації та систематизації даних про секретну інформацію державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю (далі - РПДТ), а також можуть створювати міжгалузеві або міжвідомчі РПДТ.

Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні РПДТ. Такі переліки погоджуються із СБУ, затверджуються державними експертами з питань таємниць та реєструються в СБУ.

Згідно **статті 13** Закону строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються СБУ, та інших обставин.

Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць, затверджений Указом Президента України від 1 грудня 2009 року № 987:

**Адміністрація Президента України**

Глава Адміністрації Президента України

Перший заступник Глави Адміністрації Президента України

Заступник Глави Адміністрації Президента України (одна посадова особа)

**Кабінет Міністрів України**

Прем'єр-міністр України

Перший віце-прем'єр-міністр України

Віце-прем'єр-міністр України (дві посадові особи)

**Апарат Ради національної безпеки і оборони України**

Секретар Ради національної безпеки і оборони України

Перший заступник Секретаря Ради національної безпеки і оборони України (одна посадова особа)

Заступник Секретаря Ради національної безпеки і оборони України (одна посадова особа)

**Верховний Суд України**

Голова Верховного Суду України

Заступник Голови Верховного Суду України

**Генеральна прокуратура України**

Генеральний прокурор України

Перший заступник Генерального прокурора України (одна посадова особа)

Заступник Генерального прокурора України (три посадові особи)

**Національний банк України**

Голова Національного банку України

Перший заступник Голови Національного банку України (одна посадова особа)

**Міністерство внутрішніх справ України**

Міністр внутрішніх справ України

Перший заступник Міністра внутрішніх справ України

Заступник Міністра внутрішніх справ України

Командувач Національної гвардії України

Перший заступник командувача Національної гвардії України…

**Міністерство освіти і науки України**

Міністр освіти і науки України

Перший заступник Міністра освіти і науки України

Заступник Міністра освіти і науки України - керівник апарату тощо.

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, не може перевищувати для інформації із ступенем секретності «особливої важливості» - 30 років, для інформації «цілком таємно» - 10 років, для інформації «таємно» - 5 років.

Після закінчення передбаченого частиною першою цієї статті строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць приймає рішення про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії зазначеного рішення в межах строків, встановлених частиною першою цієї статті.

Президент України з власної ініціативи або на підставі пропозицій державних експертів з питань таємниць чи за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці, ніж строки, передбачені частиною першою цієї статті.

Згідно **статті 15** Закону засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі ЗВДТ (РПДТ), відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації. Засекречування документів здійснюється лише в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується в частині, що не засекречена.

Гриф секретності кожного матеріального носія секретної інформації не повинен бути нижче ступеня секретності інформації, яка у ньому міститься, згідно із ЗВДТ – «особливої важливості», «цілком таємно» або «таємно».

Реквізити кожного матеріального носія секретної інформації складаються із:

- грифа секретності;

- номера примірника;

- статті ЗВДТ, на підставі якої здійснюється засекречення;

- найменування посади та підпису особи, яка надала гриф секретності.

Забороняється надавати грифи секретності, передбачені цим Законом, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або конфіденційної інформації.

Згідно **статті 18** Закону з метою охорони державної таємниці впроваджуються:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

- дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями (далі - установи) діяльності, пов'язаної з державною таємницею;

- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

- режим секретності установ, що провадять діяльність, пов'язану з державною таємницею;

- спеціальний порядок допуску та доступу громадян до державної таємниці;

- технічний та криптографічний захисти секретної інформації.

Згідно **статті 20** Закону установи мають право провадити діяльність, пов'язану з державною таємницею, після надання їм СБУ спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

Надання дозволу здійснюється на підставі заявок установ та результатів спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається установам за результатом спеціальної експертизи за умови, що вони:

- відповідно до компетенції, державних завдань, програм, замовлень, договорів (контрактів) беруть участь у діяльності, пов'язаній з державною таємницею;

- мають приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів та інших матеріальних носіїв секретної інформації, що відповідають вимогам щодо забезпечення секретності зазначених робіт, виключають можливість доступу до них сторонніх осіб, гарантують збереження носіїв секретної інформації;

- додержуються передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, а також порядку здійснення технічного та криптографічного захисту секретної інформації;

- мають режимно-секретний орган, якщо інше не передбачено цим Законом.

Термін дії дозволу на провадження діяльності, пов'язаної з державною таємницею, встановлюється СБУ і не може перевищувати 5 років.

Установам, що провадять діяльність, пов'язану з державною таємницею, за результатами спеціальної експертизи надаються відповідні категорії режиму секретності (перша, друга або третя), що зазначаються СБУ у дозволах на провадження діяльності, пов'язаної з державною таємницею.

Згідно **статті 21** Закону в установах, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюється на правах окремого структурного підрозділу режимно-секретний орган (далі - РСО), який підпорядковується безпосередньо керівнику установи.

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із СБУ. У своїй роботі РСО взаємодіють з органами Служби безпеки України.

До складу РСО входять підрозділи режиму, криптографічного, технічного захисту інформації, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

В установах із значним обсягом робіт, пов'язаних з державною таємницею, вводиться посада заступника керівника з питань режиму, на якого покладаються обов'язки та права керівника РСО.

В установах з незначним обсягом робіт, пов'язаних з державною таємницею, де штатним розписом не передбачено створення РСО, облік і зберігання секретних
документів, а також заходи щодо забезпечення режиму секретності здійснюються особисто їх керівниками або спеціально призначеним наказом керівника працівником після створення необхідних умов, що забезпечують режим секретності. На них поширюються обов'язки та права працівників РСО.

Призначення осіб на посади заступників керівників з питань режиму, начальників РСО та їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності здійснюється за погодженням з органами СБУ та РСО вищестоящих установ.

Основними завданнями РСО є:

а) недопущення необгрунтованого допуску осіб до секретної інформації;

б) своєчасне розроблення та реалізація разом з іншими структурними підрозділами установ заходів, що забезпечують охорону державної таємниці;

в) запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;

г) виявлення та закриття каналів просочення секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;

д) забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин;

е) організація та ведення секретного діловодства;

є) здійснення контролю за станом режиму секретності в установах і на підпорядкованих їм об'єктах.

Згідно **статті 22** Закону залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

- перша форма - для роботи з секретною інформацією, що має ступені секретності «особливої важливості», «цілком таємно» та «таємно»;

- друга форма - для роботи з секретною інформацією, що має ступені секретності «цілком таємно» та «таємно»;

- третя форма - для роботи з секретною інформацією, що має ступінь секретності «таємно»,

а також такі терміни дії допусків:

- для першої форми - 5 років;

- для другої форми - 7 років;

- для третьої форми - 10 років.

Допуск до державної таємниці надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-технічної діяльності або навчання, органами СБУ після проведення їх перевірки.

Для розгляду питання про надання громадянам допуску до державної таємниці установами, де працюють, проходять службу або навчаються громадяни, оформляються документи, які надсилаються до органів СБУ.

Надання допуску передбачає:

- визначення необхідності роботи громадянина із секретною інформацією;

- перевірку громадянина у зв'язку з допуском до державної таємниці;

- взяття громадянином на себе письмового зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

- одержання у письмовій формі згоди громадянина на передбачені законом обмеження прав у зв'язку з його допуском до державної таємниці;

- ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

Згідно **статті 23** Закону допуск до державної таємниці не надається у разі:

1) відсутності у громадянина обгрунтованої необхідності в роботі із секретною інформацією;

2) сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом;

3) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

4) наявності у громадянина судимості за тяжкі або особливо тяжкі злочини, не погашеної чи не знятої в установленому порядку;

5) наявності у громадянина психічних розладів, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого спільним наказом Міністерства охорони здоров'я України і СБУ від 13 травня 2002 року № 174/136, зареєстрованим в Міністерстві юстиції України 28 травня 2002 року за № 458/6746:

|  |  |
| --- | --- |
| ***№*** | ***Різновид психічних захворювань (розладів)*** |
|  | *Органічні, включаючи симптоматичні психічні розлади*  |
|  | *Шизофренія, шизотипічні і маревні розлади*  |
|  | *Афективні розлади настрою*  |
|  | *Невротичні, пов'язані зі стресомі соматоформні розлади*  |
|  | *Поведінкові синдроми, пов'язані з фізіологічними порушеннями і* *фізичними чинниками*  |
|  | *Розлади зрілої особистості і поведінки в дорослих*  |
|  | *Розумова відсталість*  |
|  | *Порушення психологічного* *розвитку*  |
|  | *Поведінкові й емоційні розлади,* *що починаються звичайно в* *дитячому і підлітковому віці*  |
|  | *Розлади психіки та поведінки* *внаслідок уживання психоактивних* *речовин (алкоголю, наркоти**ків тощо)*  |

У наданні допуску до державної таємниці може бути відмовлено також у разі:

1) повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;

2) постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;

3) невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше.

Згідно **статті 24** Закону перевірка громадян у зв’язку з їх допуском до державної таємниці здійснюється органами СБУ у строк до одного місяця у порядку, встановленому цим Законом і Законом України «Про оперативно-розшукову діяльність».

Згідно **статті 26** переоформлення громадянам допуску до державної таємниці здійснюється:

- у разі закінчення терміну дії допуску до державної таємниці за необхідності подальшої роботи з секретною інформацією;

- у разі необхідності підвищення чи зниження громадянину форми допуску для роботи із секретною інформацією вищого чи нижчого ступеня секретності;

- у разі необхідності проведення додаткової перевірки, пов'язаної з можливим виникненням обставин, передбачених пунктами 2 і 4 частини першої та частиною другою статті 23 цього Закону.

Скасування раніше наданого допуску до державної таємниці здійснюється органами СБУ у разі виникнення або виявлення обставин, передбачених статтею 23 Закону, або після припинення громадянином діяльності, у зв'язку з якою йому було надано допуск, втрати ним громадянства або визнання його недієздатним на підставі інформації, здобутої органами СБУ або отриманої від установ.

На прохання громадянина його допуск до державної таємниці скасовується протягом трьох днів з часу звернення з приводу скасування допуску.

Згідно **статті 27**доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання.

Рішення про надання доступу до конкретної секретної інформації (категорії секретної інформації) та її матеріальних носіїв приймають керівники установ, у яких виконуються роботи, пов'язані з державною таємницею, або зберігаються матеріальні носії секретної інформації.

Президенту, Голові Верховної Ради, Прем'єр-міністру та іншим членам Кабінету Міністрів, Голові Верховного Суду, Голові Конституційного Суду України, Генеральному прокурору, Голові СБУ, народним депутатам України доступ до державної таємниці усіх ступенів секретності надається за посадою після взяття ними письмового зобов'язання щодо збереження державної таємниці.

Згідно **статті 28** Закону громадянин, якому надано допуск до державної таємниці, зобов'язаний:

- не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

- не брати участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;

- не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України;

- виконувати вимоги режиму секретності;

- повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні РСО про виникнення обставин, передбачених статтею 23 цього Закону, або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти у письмовій формі про свій виїзд з України;

- додержуватися інших вимог законодавства про державну таємницю.

Згідно **статті 29** Закону громадянин, якому було надано допуск та доступ до державної таємниці порядку, встановленому законодавством, і який реально був обізнаний з нею, може бути обмежений у праві виїзду на постійне місце проживання в іноземну державу до розсекречування відповідної інформації, але не більш як на п'ять років з часу припинення діяльності, пов'язаної з державною таємницею.

На громадянина також поширюються обмеження свободи інформаційної діяльності, що випливають з цього Закону.

Згідно **статті 30** Закону у разі коли за умовами своєї професійної діяльності громадянин постійно працює з відомостями, що становлять державну таємницю, йому повинна надаватися відповідна компенсація за роботу в умовах режимних обмежень, види, розміри та порядок надання якої встановлюються постановою Кабінету Міністрів України.

*Постанова Кабінету Міністрів України від 15 червня 1994 року № 414 «****Про види, розміри і порядок надання компенсації громадянам у зв’язку з роботою, яка передбачає доступ до державної таємниці****»:*

*Особам, які працюють в умовах режимних обмежень, установлюється надбавка до посадових окладів (тарифних ставок) залежно від ступеня секретності інформації:*

*- відомості та їх носії, що мають ступінь «особливої важливості», - 20 %;*

*- відомості та їх носії, що мають ступінь «цілком таємно», - 15 %;*

*- відомості та їх носії, що мають ступінь «таємно», - 10 %.*

*Особам, які працюють в умовах режимних обмежень і безпосередньо виконують науково-дослідні та дослідно-конструкторські роботи, що містять державну таємницю і передбачені державним замовленням (контрактом), встановлюється надбавка до посадових окладів (тарифних ставок) залежно від ступеня секретності та обсягу інформації:*

*- відомості та їх носії, що мають ступінь «особливої важливості», - 70-100 %;*

*- відомості та їх носії, що мають ступінь «цілком таємно», - 30-70 %;*

*- відомості та їх носії, що мають ступінь «таємно», - 10-30 %.*

*Постанова Кабінету Міністрів України від 22 грудня 1995 року № 1037 «****Про надбавки до посадових окладів працівників, зайнятих на шифрувальній роботі****»:*

*Встановити, що з 8 червня 1995 року працівникам, зайнятим безпосередньо на шифрувальній роботі, виплачується надбавка до посадового окладу за безперервний стаж на цій роботі в таких розмірах: від 1 до 3 років - 10 відсотків; від 3 до 5 років - 15 відсотків; понад 5 років - 20 відсотків. Зазначеним працівникам, які працюють в українських установах за кордоном, надбавка виплачується в іноземній валюті виходячи з інвалютного окладу.*

Згідно **статті 37** Закону СБУ має право контролювати стан охорони державної таємниці в усіх установах, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення охорони державної таємниці.

Висновки СБУ, викладені в актах офіційних перевірок за результатами контролю стану охорони державної таємниці, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їх форм власності.

Згідно **статті 39** Закону посадові особи та громадяни несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом, якщо винні у:

- розголошенні державної таємниці;

- втраті документів та інших матеріальних носіїв секретної інформації;

- недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

- засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 цього Закону;

- навмисному невіднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необгрунтованому заниженні ступеня секретності або необгрунтованому розсекречуванні секретної інформації;

- безпідставному засекречуванні інформації, у тому числі з порушенням вимог Закону України «Про доступ до публічної інформації»;

- наданні грифа секретності матеріальним носіям інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;

- порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;

- порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;

- невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

- провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в установах, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

- недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;

- невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами.

Згідно **статті 5** Закону України «**Про телебачення та радіомовлення**» не допускається використання телерадіоорганізацій для поширення відомостей, що становлять державну таємницю, або іншої інформації, яка охороняється законом.

Згідно п.14 «**Порядку надсилання електронною поштою службових документів**», затвердженого постановою Кабінету Міністрів України від 17 липня 2009 року № 733, здійснення електронного обміну службовими документами, які містять секретну інформацію, забороняється.

З метою реалізації вимог Закону 2 жовтня 2003 року Кабінет Міністрів України постановою № 1561-12 затвердив «**Порядок організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях**», який визначає конкретні вимоги щодо:

- порядку оформлення допуску осіб до державної таємниці;

- порядку отримання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею;

- облаштування приміщень та організації роботи РСО;

- правил поводження з носіями секретної інформації;

- правил автоматизованої обробки секретної інформації;

- організації режиму секретності та секретного діловодства;

- забезпечення режиму секретності під час прийому іноземців.

З метою визначення правил автоматизованої обробки секретної інформації за допомогою комп’ютерних систем ще 16 лютого 1998 року Кабінет Міністрів України постановою № 180 затвердив «**Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах** (АС)», яке визначає конкретні вимоги щодо:

- режиму обмежень під час обробки секретної інформації в АС;

- організації обробки секретної інформації в АС;

- комплексної системи захисту секретної інформації в АС;

- завдань установи щодо забезпечення режиму секретності в АС;

- документального забезпечення режиму секретності в АС;

- контролю за забезпеченням режиму під час обробки секретної інформації в АС.

Деякі вимоги щодокриптографічного захисту секретної інформаціїзустрічаються у «**Положенні про порядок здійснення криптографічного захисту інформації в Україні**», затвердженому Указом Президента України від 22 травня 1998 року № 505:

7. Для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації. Зазначені криптосистеми і засоби перебувають у державній власності.

12. До користування криптосистемами та засобами криптографічного захисту секретної інформації допускаються особи, які у встановленому законодавством України порядку одержали допуск до державної таємниці.

З метою забезпечення технічного захисту секретної інформаціївід несанкціонованого доступу при її обробці в АС класу «1» (окрема ПЕОМ) Адміністрацією Держспецзв’язку у 2007 році був розроблений спеціальний нормативний документ **НД ТЗІ 2.5-007-2007** **«Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу 1»**, який визначає вимоги щодо:

# - загальних положень щодо захисту секретної інформації в АС класу 1;

# - типових режимних умов функціонування АС класу 1;

# - визначення стандартних функціональних профілів захищеності (СФПЗ) АС класу 1;

# - забезпечення політики безпеки СФПЗ АС класу 1.

# Крім того, наказом СБУ від 28 листопада 2008 року № 841 «Про затвердження форм звіту про стан забезпечення охорони державної таємниці та інструкцій щодо порядку їх заповнення і подання», зареєстрованим в Міністерстві юстиції України 8 грудня 2008 року за № 1163/15854, були затверджені:

- форма Звіту про стан забезпечення охорони державної таємниці та Інструкція щодо його заповнення і порядку його подання;

- форма узагальнюючого Звіту про стан забезпечення охорони державної таємниці за суб'єкти режимно-секретної діяльності, підзвітні центральному органу виконавчої влади, та Інструкція щодо його заповнення.

Згідно наказу установи, що провадять діяльність, пов'язану з державною таємницею, повинні щороку подавати до органів СБУ звіт про стан забезпечення охорони державної таємниці протягом терміну дії спеціального дозволу.

Треба відмітити, що нормативно-правові акти, які зачіпають права, свободи й законні інтереси громадян або мають міжвідомчий характер підлягають державній реєстрації в Міністерстві юстиції України у відповідності до Указу Президента України від 3 жовтня 1992 року № 493 «**Про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади**» згідно вимог «**Положення про державну реєстрацію нормативно-правових актів міністерств, інших органів виконавчої влади**» (далі - Положення), затвердженого постановою Кабінету Міністрів України від 28 грудня 1992 року № 731.

Згідно п.3 Положення на державну реєстрацію подаються нормативно-правові акти, що мають міжвідомчий та неперсоніфікований характер і розраховані на неодноразове застосування незалежно від строку їх дії та характеру відомостей, що в них містяться.

Згідно п.4 Положення державній реєстрації підлягають нормативно-правові акти будь-якого виду (постанови, накази, інструкції тощо), якщо в них є одна або більше норм, що:

а) зачіпають соціально-економічні, політичні, особисті та інші права, свободи й законні інтереси громадян, проголошені й гарантовані Конституцією та законами України, міжнародними договорами України, згоду на обов'язковість яких надано Верховною Радою України, а також з урахуванням практики Європейського суду з прав людини, встановлюють новий або змінюють, доповнюють чи скасовують організаційно-правовий механізм їх реалізації;

б) мають міжвідомчий характер, тобто є обов'язковими для інших міністерств, органів виконавчої влади, а також органів місцевого самоврядування, підприємств, установ і організацій, що не входять до сфери управління органу, який видав нормативно-правовий акт.

*Офіційний сайт Міністерства юстиції: www.minjust.gov.ua.*

**5. Нормативно-правові акти щодо захисту інформації**

**в телекомунікаційних системах**

З метою обміну інформацією з обмеженим доступом з використанням телекомунікаційної мережі загального користування всі країни створюють спеціальні телекомунікаційні мережі, які забезпечують технічний та криптографічний захист інформації. Так, ще у 1930 році на території України та Росії була побудована перша телекомунікаційна лінія засекреченого зв’язку, яка з’єднала столицю УРСР Харків і столицю СРСР Москву.

У подальшому на території СРСР була побудована та функціонувала загальнодержавна мережа урядового зв’язку, що забезпечувала захист секретної інформації. У 1991 році, коли Україна стала незалежною державою, вона отримала у спадок мережу та обладнання урядового зв’язку, що знаходилось на її території.

На даний час в Україні функціонує державна система урядового зв’язку (далі - ДСУЗ) - система спеціального зв’язку, що функціонує в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану, в особливий період та забезпечує захист інформації, що містить державну таємницю, під час її передавання, приймання та обробки.

Нормативно-правовим підгрунтям функціонування ДСУЗ є закон «**Про Державну службу спеціального зв’язку та захисту інформації України**» (далі – Держспецзв’язку). Функіонування, безпеку та розвиток ДСУЗ забезпечує Держспецзв’язку на підставі спеціальних Указів Президента України та інших нормативно-правових актів, які мають, як правило, гриф секретності.

*Офіційний сайт Держспецзв’язку: www.dsszzi.gov.ua.*

Разом з тим, з метою обміну конфіденційною інформацією з використанням телекомунікаційної мережі загального користування постало питання щодо створення конфіденційної телекомунікаційної мережі. Так, у 2002 році був прийнятий Закон України «**Про Національну систему конфіденційного зв'язку**» (далі - Закон).

У цьому Законі нижченаведені терміни вживаються в такому значенні:

- спеціальна телекомунікаційна система (мережа) - телекомунікаційна система (мережа), призначена для обміну ІзОД;

- Національна система конфіденційного зв'язку (далі - НСКЗ) - сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою засобів захисту забезпечують обмін ІзОД, крім інформації, що становить державну таємницю в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану.

Згідно **статті 5** Законускладовими НСКЗ є спеціальні телекомунікаційні системи (мережі), їх фіксовані і мобільні компоненти, централізовані системи захисту інформації та оперативно-технічного управління. Структура побудови НСКЗ повинна забезпечувати відокремлення ІзОД, крім інформації, що становить державну таємницю, органів державної влади та органів місцевого самоврядування, інших юридичних та фізичних осіб з використанням криптографічних та/або технічних засобів.

Згідно **статті 6** Законууправління НСКЗ, її функціонування, розвиток, використання та захист інформації забезпечуються спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації відповідно до законодавства. Централізовані системи захисту інформації та оперативно-технічного управління перебувають у державній власності і не підлягають приватизації.

Згідно **статті 7** Законупослуги конфіденційного зв'язку надаються органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним та фізичним особам на платній основі.

Надання послуг конфіденційного зв'язку іншим юридичним та фізичним особам здійснюється відповідно до законодавства на підставі договору між споживачем та оператором.

Послуги конфіденційного зв'язку надаються операторами, які є юридичними особами та мають ліцензії на право надання послуг телефонного зв'язку, а також надання послуг у галузі криптографічного та/або технічного захисту інформації відповідно до законодавства.

З метою реалізації вимог Закону був прийнятий «**Порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям**» (далі - Порядок), затверджений постановою Кабінету Міністрів України від 11 жовтня 2002 року № 1519 (у редакції постанови Кабінету Міністрів України [від 29 квітня 2013 року № 328](http://zakon2.rada.gov.ua/laws/show/328-2013-%D0%BF/paran8#n8)):

Згідно п.5 Порядку захист інформації під час надання послуг конфіденційного зв’язку забезпечується операторами шляхом вжиття відповідно до законодавства організаційних та інженерно-технічних заходів із застосуванням криптографічних і технічних засобів захисту інформації.

Згідно п.7 Порядку послуги конфіденційного зв’язку надаються відповідно до договору, примірна форма якого затверджується Адміністрацією. До укладення договору оператор за зверненням споживача зобов’язаний безоплатно надати споживачеві для ознайомлення вичерпну інформацію про зміст, якість, вартість і порядок надання послуг конфіденційного зв’язку.

Основним нормативно-правовим актом України щодо захисту інформації в комп’ютерних системах є Закон «**Про захист інформації в інформаційно-телекомунікаційних системах**», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

У цьому Законі наведені нижче терміни вживаються в такому значенні:

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

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

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

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

- комплексна система захисту інформації (далі – КСЗІ) - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

 Згідно **статті 5** Закону власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом. Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі.

Згідно **статті 8** Закону інформація, яка є власністю держави, або інформація з обмеженим доступом (далі – ІзОД), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням КСЗІ з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення КСЗІ, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Згідно **статті 9** Закону відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляється інформація, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (*Адміністрацію Держспецзв'язку*) або підпорядкований йому регіональний орган.

Згідно **статті 10** Закону спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

- розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

- визначає вимоги та порядок створення КСЗІ, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

- організовує проведення державної експертизи КСЗІ, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

- здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом;

- здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в ІТС та дає рекомендації з питань запобігання такій загрозі.

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

Згідно п.1 «**Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України**», затвердженого Указом Президента України від 30 червня 2011 року № 717, Адміністрація є центральним органом виконавчої влади в галузі зв'язку та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

З метою реалізації положень Закону 29 березня 2006 року Кабінетом Міністрів України постановою № 373 були затверджені «**Правила забезпечення захисту інформації в ІТС**» (далі - Правила),які визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в ІТС.

У Правилах наведені нижче терміни вживаються у такому значенні:

- автентифікація - процедура встановлення належності користувачу інформації в системі (далі - користувач) пред'явленого ним ідентифікатора *(пароль)*;

- ідентифікація - процедура розпізнавання користувача в системі за допомогою імені (ідентифікатора), що сприймається системою *(логін)*.

Згідно п.4 Правил захисту в системі підлягає:

- відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених Законом України «Про доступ до публічної інформації»;

- службова інформація;

- інформація, яка становить державну або іншу передбачену законом таємницю (далі - таємна інформація);

- інформація, вимога щодо захисту якої встановлена законом.

Згідно п.5 Правил відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією в системі. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими або неавтентифікованими користувачами повинні блокуватися.

Згідно п.6 Правил під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Згідно п.7 Правил доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих або неавтентифікованих користувачів повинні призводити до їх блокування.

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

Згідно п.11 Правил у системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;

- результатів виконання користувачем операцій з обробки інформації;

- спроб несанкціонованих дій з інформацією;

- фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

- результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки).

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Реєстрація спроб несанкціонованих дій з ІзОД повинна супроводжуватися повідомленням про них адміністратора безпеки.

Згідно п.12 Правил ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

Згідно п.13 Правил передача службової і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Згідно п.15 Правил у системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

Контролюється також цілісність засобів захисту інформації. У разі порушення їх цілісності обробка інформації в системі припиняється.

Згідно п.16 Правил для забезпечення захисту інформації в системі створюється КСЗІ, яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень (далі - ПЕМВН), акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

- несанкціонованих дій, у тому числі з використанням комп'ютерних вірусів;

- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації.

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про це прийнято розпорядником інформації.

Згідно п.17 Правил відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

Згідно п.18 Правил організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації (далі - СЗІ), яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію КСЗІ, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

СЗІ утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

Згідно п.19 Правил захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого СЗІ плану захисту інформації в системі.

План захисту інформації в системі містить:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

- визначення моделі загроз для інформації в системі;

- основні вимоги щодо захисту інформації та правила доступу до неї в системі;

- перелік документів, згідно з якими здійснюється захист інформації в системі;

- перелік і строки виконання робіт службою захисту інформації.

Згідно п.20 Правил вимоги та порядок створення КСЗІ встановлюються Адміністрацією Держспецзв'язку (далі - Адміністрація).

Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або КСЗІ.

Згідно п.21 Правил у складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.

У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.

Згідно п.22 Правил порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією.

Органи виконавчої влади, які мають дозвіл на провадження діяльності з ТЗІ для власних потреб, вправі за згодою департаменту організовувати проведення державної експертизи системи захисту на підприємствах, в установах та організаціях, які належать до сфери їх управління.

Порядок проведення такої експертизи встановлюється органом виконавчої влади за погодженням з Адміністрацією.

Згідно п.23 Правил виконавцем робіт із створення системи захисту може бути суб'єкт господарської діяльності, який має ліцензію, або орган виконавчої влади, який має дозвіл на право провадження робіт у сфері ТЗІ, необхідність проведення якого визначено технічним завданням на створення системи захисту.

Для проведення інших видів робіт з ТЗІ, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.

Якщо для створення системи захисту необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

16 листопада 2002 року постановою Кабінету Міністрів України № 1772 був затверджений «**Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах**», який визначає механізм взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в ІТС.

Поняття, що використовуються у Порядку, мають таке значення:

- несанкціоновані дії - доступ або спроба такого доступу до державних інформаційних ресурсів в ІТС без відповідно оформленого власником або уповноваженою ним особою дозволу, вірусне ураження, вчинення інших дій, які можуть призвести до порушення цілісності, доступності та конфіденційності цих ресурсів;

- телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання (випромінювання) або приймання сигналів, знаків, звуків, рухомих чи нерухомих зображень або іншим способом.

Згідно п.3 Порядку органи виконавчої влади з метою захисту державних
інформаційних ресурсів в ІТС:

- визначають перелік ІТС, які містять державні інформаційні ресурси, та погоджують його з Адміністрацією Держспецзв'язку (далі - Адміністрація);

- здійснюють згідно з вимогами нормативно-правових актів з питань захисту інформації під методичним керівництвом Адміністрації заходи щодо захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, у тому числі
підключених до глобальних мереж передавання даних;

- збирають, узагальнюють та аналізують інформацію про вчинення несанкціонованих дій і здійснюють заходи щодо усунення їх наслідків;

- невідкладно (протягом доби) інформують Адміністрацію про спробу вчинення чи вчинення несанкціонованих дій;

- надають на запит Адміністрації інформацію про технічні та програмні засоби, що використовуються для надання мережних послуг, а також про зміни у способах або видах підключення до глобальних мереж передавання даних;

- оновлюють за рекомендаціями Адміністрації антивірусні програмні засоби, використовуючи при цьому лише ті з них, які пройшли державну експертизу.

Згідно п.4 Порядку Адміністрація:

- здійснює методичне керівництво та координує діяльність органів виконавчої влади, пов'язану із запобіганням, виявленням, реагуванням та усуненням наслідків несанкціонованих дій щодо державних інформаційних ресурсів в ІТС, надає в разі потреби допомогу у здійсненні заходів щодо запобігання порушенню цілісності, доступності та конфіденційності зазначених ресурсів;

- надає органам виконавчої влади відомості про антивірусні програмні засоби, які можуть застосовуватися для захисту державних інформаційних ресурсів в ІТС, та проводить перевірку їх оновлення;

- накопичує та аналізує дані про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС, а також про їх наслідки, інформує правоохоронні органи для вжиття заходів із запобігання та припинення злочинів у зазначеній сфері, оцінює стан захищеності цих ресурсів та надає відповідні рекомендації.

5. Адміністрація взаємодіє з органами виконавчої влади з питань захисту державних інформаційних ресурсів в ІТС через спеціально уповноважений підрозділ з питань безпеки ІТС Адміністрації.

6. Відновлення функціонування ІТС, виведених з ладу внаслідок вчинення несанкціонованих дій, здійснюється органами виконавчої влади за умови повного блокування таких дій та усунення їх наслідків власними силами (у разі потреби - за допомогою Адміністрації), виявлення та усунення причин, в тому числі шляхом удосконалення КСЗІ.

26 березня 2007 року наказом Адміністрації  № 45 був затверджений «**Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ**» (далі - Порядок), зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587.

Поняття, що використовуються у Порядку, мають таке значення:

- центр антивірусного захисту інформації (далі - ЦАЗІ) - організаційно-технічний комплекс, призначений для вирішення питання захисту ІТС від комп'ютерних вірусів з подальшим розвитком комплексного підходу до проблеми антивірусного захисту ІТС;

- комп'ютерний вірус - програма, що здатна створювати свої копії, модифіковані копії, які можуть цілком не відповідати оригіналу, і впроваджувати їх у різні об'єкти/ресурси ІТС безвідома користувача, й направлена на деструктивну дію;

- антивірусний програмний засіб (далі - АВПЗ) – програмне забезпечення, яке призначене для захисту об'єктів/ресурсів ІТС відушкодження комп'ютерними вірусами;

- антивірусне оновлення АВПЗ - складова частина АВПЗ, яка розробляється після створення засобу та призначена для пристосування АВПЗ до захисту об'єктів/ресурсів ІТС від ушкодженнята зараження новими вірусами.

5. Оновлення АВПЗ здійснюється шляхом організації та забезпечення процесу отримання та впровадження в АВПЗ антивірусних оновлень.

 6. Оновлення АВПЗ, який пройшов державну експертизу та має позитивний експертний висновок Адміністрації Держспецзв'язку, здійснюється з використанням антивірусних оновлень, які розміщуються на веб-сайті ЦАЗІ (*www.cazi.dsszzi.gov.ua*).

7. На веб-сайті ЦАЗІ розміщуються тільки антивірусні оновлення АВПЗ, які пройшли експрес-експертизу. Крім того, на веб-сайті можна подивитись перелік АВПЗ, що отримало позитивний експертний висновок Держспецзв'язку.

8. Експрес-експертиза антивірусного оновлення АВПЗ здійснюється ЦАЗІ шляхом перевірки АВПЗ з впровадженим антивірусним оновленням на його відповідність експертному висновку, виданому за результатами державної експертизи.

У подальшому під антивірусним оновленням АВПЗ розуміється антивірусне оновлення АВПЗ, яке пройшло експрес-експертизу.

9. Органи державної влади, органи місцевого самоврядування, утворені відповідно до законів України військові формування, підприємства, установи і організації державної форми власності:

- не менше ніж раз на день отримують антивірусні оновлення АВПЗ за допомогою веб-серверу ЦАЗІ;

- інсталюють отримані за допомогою веб-серверу ЦАЗІ антивірусні оновлення АВПЗ відповідно до технічної документації АВПЗ;

- для забезпечення авторизованого доступу до ресурсів веб-серверу ЦАЗІ щороку до 1 березня та, у разі внесення змін, протягом 3 днів надають до Адміністрації Держспецзв'язку відомості щодо кожного користувача у паперовому вигляді за визначеною формою.

10. Адміністрація Держспецзв'язку:

- організовує за допомогою спеціалізованого програмного забезпечення отримання органами державної влади, органами місцевого самоврядування, утвореними відповідно до законів України військовими формуваннями, підприємствами, установами та організаціями державної форми власності антивірусних оновлень для антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, та забезпечує функціонування веб-серверу ЦАЗІ;

- заносить надану органами державної влади, органами місцевого самоврядування, утвореними відповідно до законів України військовими формуваннями, підприємствами, установами та організаціями державної форми власності реєстраційну інформацію до бази даних користувачів ЦАЗІ. Реалізує автентифікацію та ідентифікацію користувачів відповідно до цієї бази даних;

- проводить експрес-експертизу антивірусних оновлень АВПЗ;

- розробляє рекомендації щодо тримання антивірусних оновлень антивірусного програмного засобу та їх розміщення на веб-сайті ЦАЗІ;

- використовує механізм ЕЦП для підтвердження цілісності антивірусних оновлень АВПЗ та ідентифікації підписувача після впровадження в органі державної влади, органі місцевого самоврядування, утворених відповідно до законів України військових формуваннях, підприємствах, установах та організаціях державної форми власності ЕЦП.

10 червня 2008 року наказом Адміністрації  № 94 був затверджений «**Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в ІТС**», зареєстрований в Міністерстві юстиції України 7 липня 2008 року за № 603/15294.

Терміни, що використовуються у цьому Порядку, мають таке значення:

- адміністратор безпеки ІТС - посадова особа суб'єкта координації, яка є відповідальною за дотримання політики  безпеки інформації в ІТС відповідного суб'єкта координації;

- Координатор - уповноважений структурний підрозділ Адміністрації Держспецзв'язку.

Згідно п.3 Порядку суб'єкти координації у разі виявлення спроби вчинення та/або вчинення несанкціонованих дій вживають заходів щодо:

- блокування, усунення або локалізації їх негативних  наслідків власними силами відповідно до Закону України «Про  захист інформації в ІТС» та інших нормативно-правових актів у сфері технічного захисту інформації;

- невідкладного (протягом  доби)  інформування Координатора про несанкціоновані дії, для чого адміністратор безпеки ІТС або особа, яка виконує його обов'язки,  надсилає на електронні поштові адреси Координатора відповідне електронне повідомлення, зразок якого наведено у додатку 1;

- збереження (фіксації) ознак несанкціонованих дій, у тому числі на матеріальних носіях інформації;

- захисту державних інформаційних ресурсів відповідно до рекомендацій, наданих Координатором адміністратору безпеки ІТС електронною поштою, телефоном, факсом чи іншим способом;

- надсилання до Адміністрації Держспецзв'язку письмового  повідомлення, зразок якого наведено у додатку 2, яке підтверджує надіслане раніше електронне повідомлення протягом 7 (семи) робочих днів з моменту виявлення факту несанкціонованих дій;

- забезпечення у разі необхідності фізичного доступу співробітників Координатора до ІТС для виконання заходів щодо блокування та локалізації негативних наслідків несанкціонованих дій та відновлення працездатності ІТС.

Згідно п.4 Порядку Координатор під час виконання покладених на нього завдань:

- взаємодіє з органами державної влади, провайдерами та операторами телекомунікацій, установами,   підприємствами   та організаціями усіх форм власності України;

- для організації    своєчасного    обміну    інформацією   про несанкціоновані дії використовує веб-сторінку *www.cert.gov.ua*  і електронні поштові адреси *cert@cert.gov.ua* та *cert@dsszzi.gov.ua*;

*CERT-UA (скор. – Computer Emergency Response Team of Ukraine – команда реагування на комп’ютерні надзвичайні події України) – спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем (ДЦЗ ІТС) Держспецзв’язку.*

- здійснює міжнародне співробітництво з питань,  що належать до компетенції Держспецзв'язку;

- з метою своєчасного  запобігання  та  припинення  злочинів  у сфері  використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж вживає заходів щодо своєчасного інформування правоохоронних органів України про виявлені суб'єктами координації несанкціоновані дії.

Згідно п.5 Порядку Координатор не має права:

- розголошувати відомості, що стали йому  відомі  у  процесі координації діяльності суб'єктів координації, з питань, пов'язаних із  запобіганням  вчиненню  порушень  безпеки інформації в ІТС без погодження з розпорядником інформації (інформаційного ресурсу);

- припиняти або призупиняти функціонування будь-яких ІТС та електронних інформаційних ресурсів.

Згідно п.6 Порядку аналітичні матеріали щодо несанкціонованих дій стосовно державних інформаційних ресурсів в ІТС суб'єктів координації вносяться до щорічного звіту Голови Держспецзв'язку Президенту, Верховній Раді та Кабінету Міністрів України.

Складовою частиною Національного реєстру електронних інформаційних ресурсів є Реєстр ІТС державних органів (далі - Реєстр), який ведеться згідно «**Положення про Реєстр ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління**», затвердженого постановою Кабінету Міністрів України від 3 серпня 2005 року № 688.

Ведення Реєстру забезпечує Адміністрація Держспецзв'язку згідно «**Порядку формування й користування інформаційним фондом Реєстру ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління**», затвердженого наказом Адміністрації Держспецзв'язку від 24 квітня 2007 року № 72, зареєстрованого в Міністерстві юстиції України 14.05.2007 за № 500/13767.

Цей Порядок визначає види та форми надання відомостей до інформаційного фонду Реєстру (далі - Інформаційний фонд) та правила користування ним. Відомості про ІТС подаються ще на стадії технічного проектування систем, а у разі модернізації функціонуючих ІТС - на стадії створення КСЗІ в цих системах. У разі введення в експлуатацію або припинення функціонування ІТС відповідний державний орган у 10-денний строк повідомляє про це адміністратора Реєстру.

Відомості до Інформаційного фонду подаються на оптичних носіях типу CD-R із супровідним листом за підписом керівника державного органу. Після впровадження в державному органі електронно-цифрового підпису зазначені відомості надаються з додержанням вимог чинного законодавства в електронному вигляді мережами передачі даних або надсилаються поштою на електронних носіях інформації. Носії інформації адресату не повертаються.

Державні органи двічі на рік (станом на 1 січня - до 1 лютого та станом на 1 липня - до 1 серпня) надають Адміністратору Реєстру узагальнені відомості про власні ІТС. Надалі в ті ж самі терміни державними органами надсилаються Адміністратору Реєстру відомості лише про ІТС, у яких відбулися зміни з моменту останнього надання інформації про них.

**6. Нормативно-правові акти з технічного захисту інформації**

Зростання загроз для інформації, спричинене лібералізацією суспільних та міждержавних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї, визначає необхідність розвитку технічного захисту інформації (далі - ТЗІ). ТЗІ є складовою частиною забезпечення інформаційної безпеки України.

8 жовтня 1997 року постановою Кабінету Міністрів України № 1126 була затверджена  «**Концепція ТЗІ в Україні**» (далі - Концепція), яка визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами.

Концепція має забезпечити єдність принципів формування і проведення відповідної політики в усіх сферах життєдіяльності особи, суспільства та держави і служити підставою для створення програм розвитку сфери ТЗІ.

ТЗІ - це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим
доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

Приведення інформаційних відносин у сфері ТЗІ у відповідність з міжнародними стандартами сприятиме утвердженню України у світі як демократичної правової держави.

**Загрози безпеці інформації та стан її технічного захисту**

Впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкуренто-спроможних інформаційних технологій надається перевага технічним засобам оброблення інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації. Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються.

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, радіотеплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок.

За таких умов створилися можливості витоку інформації, порушення її цілісності та блокування. Витік інформації, яка становить державну та іншу передбачену законом таємницю, службової інформації, - це одна з основних можливих загроз національній безпеці України в інформаційній сфері.

Загрози безпеці інформації в Україні зумовлені:

- не виваженістю державної політики в галузі інформаційних технологій, що може призвести до безконтрольного та неправомочного доступу до інформації та її використання;

- діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;

- недосконалістю організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) та заходів екологічного моніторингу, що може використовуватися для здобування інформації розвідувального характеру;

- діяльністю політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямованою на одержання переваги у політичній боротьбі та конкуренції;

- злочинною діяльністю, спрямованою на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

- використанням інформаційних технологій низького рівня, що призводить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ (далі - засоби забезпечення ТЗІ);

- недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу у сфері ТЗІ.

Стан ТЗІ зумовлюється:

- недосконалістю правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць (крім державної), конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави;

-недостатністю нормативно-правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення ТЗІ;

- незавершеністю створення системи сертифікації засобів забезпечення ТЗІ;

- недосконалістю системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- недостатньою узгодженістю чинних в Україні нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України.

**Система ТЗІ**

Система ТЗІ - це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами (далі - організаційні структури), нормативно-правова та матеріально-технічна база.

Принципами формування і проведення державної політики у сфері ТЗІ є:

- додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;

- єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;

- комплексність, повнота та безперервність заходів ТЗІ;

- відкритість нормативно-правових актів та нормативних документів з питань ТЗІ, які не містять відомостей, що становлять державну таємницю;

- узгодженість нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;

- обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, службової інформації, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях (далі - організації);

- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами організацій;

- покладення відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;

- ієрархічність побудови організаційних структур системи ТЗІ та керівництво їх діяльністю у межах повноважень, визначених нормативно-правовими актами;

- методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

- скоординованість дій та розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;

- фінансова забезпеченість системи ТЗІ за рахунок Державного бюджету України, місцевих бюджетів та інших джерел.

Основними функціями організаційних структур системи ТЗІ є:

- оцінка стану ТЗІ в державі, визначення пріоритетних напрямів його розвитку;

- розвиток правових засад удосконалення системи ТЗІ;

- виявлення та прогнозування загроз безпеці інформації;

- забезпечення інженерно-технічними заходами захисту інформації, що підлягає технічному захисту;

- створення умов для ТЗІ, що здійснюється суб'єктами інформаційних відносин на власний розсуд;

- формування та забезпечення реалізації державної політики щодо створення та впровадження вітчизняних засобів забезпечення ТЗІ;

- створення національної системи стандартизації та нормування у сфері ТЗІ;

- організація фундаментальних і прикладних науково-дослідних робіт та розробок у сфері ТЗІ;

- забезпечення взаємодії організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;

- організація створення та виконання програм розвитку ТЗІ;

- забезпечення ліцензування підприємницької діяльності в сфері ТЗІ;

- організація контролю за якістю засобів забезпечення ТЗІ шляхом їх сертифікації;

- організація контролю за відповідністю вимогам ТЗІ об'єктів, діяльність яких пов'язана з інформацією, що підлягає технічному захисту, шляхом їх атестації;

- організація контролю за ефективністю ТЗІ на об'єктах, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

- забезпечення підготовки фахівців для роботи у сфері ТЗІ;

- сприяння залученню інвестицій і вітчизняного товаровиробника у сферу ТЗІ;

- організація міжнародного співробітництва в сфері ТЗІ, представлення інтересів України у відповідних міжнародних організаціях;

- забезпечення (кадрове, фінансове, нормативне, матеріально-технічне, інформаційне тощо) життєдіяльності складових організаційних структур системи ТЗІ.

**Основні напрями державної політики у сфері ТЗІ**

Державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень цієї Концепції, а також програм розвитку ТЗІ та окремих проектів.

Основними напрямами державної політики у сфері ТЗІ є такі заходи:

- організаційне та нормативно-правове забезпечення;

- удосконалення чинних та розроблення нових НД ТЗІ;

- науково-технічна та виробнича діяльність.

Організаційне забезпечення складається з таких заходів:

- забезпечення створення підрозділів ТЗІ в організаціях всіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

- створення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ;

- підготовка кадрів для роботи у сфері ТЗІ;

- залучення до розв'язання проблем ТЗІ вітчизняних вчених та висококваліфікованих спеціалістів;

- розвиток міжнародного співробітництва в сфері ТЗІ.

Нормативно-правове забезпечення складається з таких заходів:

- удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу передбачену законом таємницю, службової інформації;

- розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;

- удосконалення правових механізмів організаційного забезпечення ТЗІ;

- удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері ТЗІ;

- розроблення нормативно-правових актів щодо визначення статусу головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій;

- удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій з захистом інформації та засобів забезпечення ТЗІ;

- розроблення нормативних документів з питань формування та розвитку моделі загроз для інформації;

- розроблення нормативних документів з питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту.

Удосконалення чинних та розроблення нових НД ТЗІ:

- у засобах обчислювальної техніки, в автоматизованих системах, оргтехніці, мережах зв'язку, комп'ютерних мережах та приміщеннях, де циркулює інформація, що підлягає технічному захисту;

- під час створення, експлуатації та утилізації зразків озброєнь, військової та спеціальної техніки;

- під час проектування, будівництва і реконструкції військово-промислових, екологічно небезпечних та інших особливо важливих об'єктів.

Науково-технічна та виробнича діяльність складається з таких заходів:

- моніторинг і оцінка стану ТЗІ, підготовка аналітичних матеріалів і пропозицій щодо стратегії його розвитку;

- створення інформаційно-аналітичних моделей загроз для інформації та методології їх прогнозування;

- обгрунтування критеріїв та показників рівнів ТЗІ;

- створення методології синтезу систем багаторівневого захисту інформації, адекватних масштабам загроз безпеці інформації та режиму доступу до неї;

- створення методології, призначеної для визначення зниження ефективності продукції, зумовленої витоком інформації про неї, порушенням її цілісності чи блокуванням, та методології обгрунтування заходів ТЗІ;

- системне і поетапне розроблення сучасних засобів забезпечення ТЗІ;

- пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ;

- створення умов для забезпечення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ науковим, контрольно-вимірювальним, випробувальним та виробничим обладнанням.

Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ є:

- створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

- визначення перспективних напрямів розроблення нормативних документів з питань ТЗІ на основі аналізу стану відповідної вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;

- визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку, призначених для оброблення інформації з обмеженим доступом інших засобів забезпечення ТЗІ в органах державної влади та органах місцевого самоврядування, Збройних Силах, інших військових формуваннях, органах внутрішніх справ;

- налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;

- завершення створення та розвиток системи сертифікації вітчизняних та закордонних засобів забезпечення ТЗІ;

- визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

27 вересня 1999 року Указом Президента України № 1229 було затверджено «**Положення про технічний захист інформації в Україні**» (далі - Положення), яке визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.

Ужиті в цьому Положенні терміни мають таке значення:

- конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;

- цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

- доступність - властивість інформації бути захищеною від несанкціонованого блокування;

- інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку;

- ТЗІ - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

- комплекс ТЗІ - сукупність заходів та засобів для реалізації ТЗІ в інформаційній системі або на об'єкті.

Державна політика технічного захисту інформації реалізується Державною службою спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку) у взаємодії з органами, щодо яких здійснюється ТЗІ.

Згідно п.5 Положення організація ТЗІ в установах покладається на їх керівників.

Згідно п.6 Положення нормативно-правові акти з ТЗІ є обов'язковими для виконання всіма суб'єктами системи ТЗІ.

Згідно п.8 Положення суб'єктами системи технічного захисту інформації є:

- Держспецзв'язку;

- органи, щодо яких здійснюється ТЗІ;

- науково-дослідні та науково-виробничі установи Держспецзв'язку, державні підприємства, що перебувають в управлінні Держспецзв'язку та виконують завдання з ТЗІ;

- організації всіх форм власності й громадяни-підприємці, які провадять діяльність з ТЗІ за відповідними дозволами або ліцензіями;

- навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з ТЗІ.

Згідно п.11 Положення основними завданнями організацій є:

- забезпечення ТЗІ згідно з вимогами нормативно-правових актів з питань ТЗІ;

- видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

- здійснення контролю за станом ТЗІ.

Згідно п.12 Положення організації відповідно до покладених на них завдань:

- створюють або визначають підрозділи, на які покладається забезпечення ТЗІ та контроль за його станом, узгоджують основні завдання та функції цих підрозділів;

- видають за погодженням з Адміністрацією Держспецзв'язку та впроваджують нормативно-правові акти з питань ТЗІ;

- погоджують з Адміністрацією Держспецзв'язку проведення організаціями тих науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток нормативно-правової та матеріально-технічної бази системи ТЗІ, які здійснюються за рахунок коштів державного бюджету;

- створюють або визначають за погодженням з Адміністрацією Держспецзв'язку організації, що забезпечують ТЗІ;

- забезпечують підготовку, перепідготовку та підвищення кваліфікації кадрів з ТЗІ;

- надають Адміністрації Держспецзв'язку за його запитами відомості про стан ТЗІ.

Згідно п.13 Положення основними завданнями інших суб'єктів системи ТЗІ є:

- дослідження загроз для інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні;

- створення та виробництво засобів забезпечення ТЗІ;

- розроблення, впровадження, супроводження комплексів ТЗІ;

- підвищення кваліфікації фахівців з ТЗІ.

Згідно п.15 Положення матеріально-технічна база системи ТЗІ складається з технічних засобів загального призначення та спеціальних технічних засобів.

Технічні засоби загального призначення повинні мати документ, що засвідчує їх відповідність вимогам нормативно-правових актів з ТЗІ, одержаний у порядку, що встановлюється Адміністрацією Держспецзв'язку та Державним комітетом України з питань технічного регулювання та споживчої політики.

Згідно п.16 Положення техніко-економічне обгрунтування, проектування будівництва та реконструкції об'єктів, проведення наукових досліджень та створення інформаційних систем, зразків озброєнь, військової та спеціальної техніки, критичних і небезпечних технологій виконуються за завданнями, до яких включаються вимоги з ТЗІ, якщо під час виконання передбачених завданням робіт та у процесі функціонування зазначених об'єктів, систем, зразків і технологій циркулюватиме інформація, охорона якої забезпечується державою.

Під час віднесення замовником таких робіт до особливо важливих та створення інформаційних систем державних органів завдання та результати приймання їх етапів погоджуються з Адміністрацією Держспецзв'язку. Фінансування створення цих систем здійснюється після такого погодження. Витрати на заходи з ТЗІ включаються до кошторисної вартості робіт.

Згідно п.17 Положення під час розроблення та впровадження заходів з ТЗІ використовуються засоби, дозволені Адміністрацією Держспецзв'язку для застосування та включені до відповідних переліків.

Згідно п.18 Положення контроль у сфері ТЗІ полягає в перевірці виконання вимог Положення, інших нормативно-правових актів з питань ТЗІ та в оцінюванні захищеності інформації на об'єкті, де вона циркулюватиме або циркулює.

 Оцінювання захищеності інформації здійснюється шляхом атестації або експертизи комплексів ТЗІ та інспекційних перевірок. За результатами атестації або експертизи комплексів ТЗІ визначається можливість введення в експлуатацію об'єкта, де циркулюватиме інформація, охорона якої забезпечується державою.

Згідно п.20 Положення розроблення, впровадження, атестація та експлуатація ТЗІ для власних потреб здійснюються відповідними підрозділами організацій, на які в установленому порядку покладено забезпечення ТЗІ, за наявності у них відповідного дозволу.

До виконання цих робіт можуть бути залучені суб'єкти підприємницької діяльності, що мають відповідні ліцензії.

Починаючи з 1996 року, в Україні у сфері ТЗІ були розроблені державні будівельні норми **ДБН А.2.2-2-96 «ТЗІ. Загальні вимоги до організації проектування і проектної документації для будівництва»** та державні (національні) стандарти:

- ДСТУ 3396.0-96 ТЗІ. Основні положення;

- ДСТУ 3396.1-96 ТЗІ. Порядок проведення робіт;

- ДСТУ 3396.2-97 ТЗІ. Терміни та визначення.

Національний стандарт **ДСТУ 3396.0-96 «ТЗІ. Основні положення»** установлює об’єкт, мету, основні організаційно-технічні положення забезпечення ТЗІ, неправомірний доступ до якої може завдати шкоди громадянам, організаціям та державі, а також категорії нормативних документів системи ТЗІ.

Метою ТЗІ є запобігання витоку або порушенню цілісності ІзОД. Мета ТЗІ може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ.

ТЗІ здійснюється поетапно:

- 1 етап - визначення й аналіз загроз;

- 2 етап - розроблення системи захисту інформації;

- 3 етап - реалізація плану захисту інформації;

- 4 етап - контроль функціювання та керування системою захисту інформації.

На першому етапі необхідно здійснити аналіз об’єктів ТЗІ, ситуаційного плану, умов функціювання підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.

Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

Загрози можуть здійснюватися:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкційованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Опис загроз і схематичне подання шляхів їх здійснення складають окрему модель загроз.

На другому етапі слід здійснити розроблення плану ТЗІ та визначення зон безпеки інформації.

Розроблення плану ТЗІ містить такі заходи захисту ІзОД:

- організаційні;

- первинні технічні;

- основні технічні.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу об’єкта ТЗІ.

 Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

 Основні технічні заходи передбачають захист інформації з використанням засобів ТЗІ.

Для ТЗІ слід застосовувати спосіб приховування або технічної дезінформації.

 Заходи захисту інформації повинні:

 - бути відповідними загрозам;

 - бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;

 - забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв’язання завдання захисту інформації на основі норм та вимог ТЗІ.

Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

 Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

 ТЗІ забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (далі - засоби ТЗІ) та контролю ефективності захисту, які мають cертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем (далі - засоби забезпечення ТЗІ).

Засоби ТЗІ можуть функціонувати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ.

Національний стандарт **ДСТУ 3396.1-96 «ТЗІ. Порядок проведення робіт»** установлює вимоги до порядку проведення робіт з ТЗІ.

Можливі такі варіанти захисту інформації:

- мінімальний - досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності (далі – ІД);

- оптимальний - досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД;

- максимальний - досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД.

Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням мінімального чи оптимального варіанту.

Захист інформації, яка становить державну таємницю, забезпечується, як правило, застосуванням максимального варіанту.

Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації повинні відповідати зазначеним в ДСТУ 3396.0-96 етапам і полягає в:

- проведенні обстеження підприємства, установи, організації (далі - підприємство);

- розробленні і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ;

- прийманні робіт з ТЗІ;

- атестації засобів (систем) забезпечення ІД на відповідність вимогам НД ТЗІ.

Порядок проведення робіт з ТЗІ на підприємстві установлюється наказом керівника підприємства. Роботи повинні виконуватися силами підприємства під керівництвом спеціалістів з ТЗІ.

***Організація проведення обстеження***

Метою обстеження підприємства є визначення об`єктів захисту, виявлення загроз для них, їх аналіз та побудова моделі загроз. Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника підприємства.

У ході обстеження необхідно:

- провести аналіз умов функціонування підприємства, його розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;

- дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;

- вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізацій), а також інженерних комунікацій та металоконструкцій;

- дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі - оброблення) інформації і провести необхідні вимірювання;

- визначити наявність та технічний стан засобів забезпечення ТЗІ;

- перевірити наявність на підприємстві нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;

- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;

- визначити технічні засоби і системи, застосування яких не обгрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;

- визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

За результатами обстеження слід скласти акт, який повинен бути затверджений керівником підприємства.

Матеріали обстеження необхідно використовувати під час розроблення моделі загроз, яка повинна включати:

- генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;

- схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД;

- оцінку шкоди, яка передбачається від реалізації загроз.

***Організація розроблення системи ТЗІ***

На підставі матеріалів обстеження та моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання (ТЗ) на розроблення системи захисту інформації.

ТЗ повинно включати основні розділи:

- вимоги до системи захисту інформації;

- вимоги до складу проектної та експлуатаційної документації;

- етапи виконання робіт;

- порядок внесення змін і доповнень до розділів ТЗ;

- вимоги до порядку проведення випробування системи захисту.

Основою функціонування системи захисту інформації є план ТЗІ, що повинен містити такі документи:

- перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування;

- інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;

- інструкції, що встановлюють обов`язки, права та відповідальність персоналу;

- календарний план ТЗІ.

ТЗ і план ТЗІ розробляють спеціалісти з ТЗІ, узгоджують із зацікавленими підрозділами (організаціями). Затверджує їх керівник підприємства.

***Реалізація організаційних заходів ТЗІ***

Організаційні заходи захисту інформації - комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

У процесі розроблення і реалізації організаційних заходів потрібно:

- визначити окремі задачі захисту ІзОД;

- обгрунтувати структуру і технологію функціонування системи захисту інформації;

- розробити і впровадити правила реалізації заходів ТЗІ;

- визначити і встановити права та обов`язки підрозділів та осіб, що беруть участь в обробленні ІзОД;

- придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними підприємство;

- установити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

- установити порядок контролю функціонування системи захисту інформації та її якісних характеристик;

- визначити зони безпеки інформації;

- установити порядок проведення атестації системи захисту інформації, її елементів і розробити програми атестаційного випробування;

- забезпечити керування системою захисту інформації.

Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно:

- вивчати й аналізувати технологію проходження ІзОД у процесі ІД;

- оцінювати схильність ІзОД до впливу загроз у конкретний момент часу;

- оцінювати очікувану ефективність застосування засобів ТЗІ;

- визначати (за необхідності) додаткову потребу в засобах забезпечення ТЗІ;

- здійснювати збирання, оброблення та реєстрацію даних, які відносяться до ТЗІ;

- розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

***Реалізація первинних технічних заходів захисту***

У процесі реалізації первинних технічних заходів потрібно забезпечити:

- блокування каналів витоку інформації;

- блокування НСД до інформації;

- перевірку справності засобів ТЗІ.

Блокування каналів витоку інформації може здійснюватися:

- демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано з життєзабезпеченням підприємства та обробленням ІзОД;

- видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів, з приміщень, де циркулює ІзОД;

- тимчасовим відключенням технічних засобів, які не беруть участі в обробленні ІзОД, від ліній зв'язку, сигналізації, керування та енергетичних мереж;

- застосуванням способів та схемних рішень із захисту інформації, що не порушують основних технічних характеристик засобів забезпечення ІД.

Блокування несанкційованого доступу до інформації може здійснюватися:

- створенням умов роботи в межах установленого регламенту;

- унеможливленням використання програмних, програмно-апаратних засобів, що не пройшли перевірки (випробування).

Перевірку справності та працездатності засобів ТЗІ необхідно проводити відповідно до експлуатаційних документів. Виявлені несправні блоки й елементи можуть сприяти витоку або порушенню цілісності інформації і підлягають негайній заміні (демонтуванню).

***Реалізація основних технічних заходів захисту***

У процесі реалізації основних технічних заходів захисту потрібно:

- установити засоби виявлення та індикації загроз і перевірити їхню працездатність;

- установити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність;

- застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє функційне тестування і тестування на відповідність вимогам захищеності;

- застосувати спеціальні інженерно-технічні споруди, засоби (системи).

Вибір засобів забезпечення ТЗІ зумовлюється фрагментарним або комплексним способом захисту інформації. Фрагментарний захист забезпечує протидію певній загрозі. Комплексний захист забезпечує одночасну протидію безлічі загроз.

Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) ІзОД про витік інформації чи порушення її цілісності.

Засоби ТЗІ застосовуються автономно або спільно з технічними засобами забезпечення ІД для пасивного або активного приховування ІзОД.

Для пасивного приховування ІзОД застосовують фільтри, лінійні пристрої захисту та електромагнітні екрани.

Для активного приховування ІзОД застосовують генератори лінійного та просторового зашумлення.

Програмні засоби застосовуються для забезпечення:

- ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації;

- розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем;

- цілісності інформації та конфігурації автоматизованих систем;

- реєстрації та обліку дій користувачів;

- маскування оброблюваної інформації;

- реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкційованих дій.

Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації. До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо.

Розміщення, монтування та прокладання спеціальних інженерно-технічних засобів і систем, серед них систем уземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог НД ТЗІ.

***Приймання, визначення повноти та якості робіт***

За результатами виконання реалізації заходів захисту ІзОД слід скласти у довільній формі акт приймання робіт з ТЗІ, який повинен підписати виконавець робіт, особа, відповідальна за ТЗІ, та затвердити керівник підприємства.

Для визначення повноти та якості робіт з ТЗІ слід провести атестацію. Атестація виконується організаціями, які мають ліцензії на право діяльності в галузі ТЗІ.

Об`єктами атестації є системи забезпечення ІД та їхні окремі елементи, де циркулює інформація, що підлягає технічному захисту.

У ході атестації потрібно:

- установити відповідність об`єкта, що атестується, вимогам ТЗІ;

- оцінити якість та надійність заходів захисту інформації;

- оцінити повноту та достатність технічної документації для об`єкта атестації;

- визначити необхідність внесення змін і доповнень до організаційно-розпорядчих документів тощо.

Починаючи з 1999 року, в Україні розробляються нормативні документи системи ТЗІ – НД ТЗІ, які регламентують організаційно-технічні аспекти захисту інформації та оцінки його ефективності під час всіх етапів життєвого циклу ІТС, об'єктів ІД, озброєння, військової та спеціальної техніки, небезпечних чи критичних технологій, а також містять вихідні дані для визначення потенційних загроз для інформації, розроблення комплексів (систем) її захисту тощо.

На даний час це здійснює Адміністрація Держспецзв’язку згідно «**Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації**», затвердженого наказом Адміністрації Держспецзв’язку від 22 березня 2007 року № 36, зареєстрованим в Міністерстві юстиції України 4 квітня 2007 року за № 312/13579.

Основні напрями розробки НД ТЗІ:

- ТЗІ в комп'ютерних системах;

- ТЗІ на об’єктах інформаційної діяльності;

- ТЗІ на програмно-керованих АТС.

### Нормативні документи у сфері технічного та криптографічного захисту інформації можна знайти в Інформаційному переліку Фонду таких документів на сайті Держспецзв’язку: www.dsszzi.gov.ua.

Адміністрація Держспецзв’язку веде фонд нормативних документів у сфері захисту інформації згідно «**Положення про фонд нормативних документів у сфері технічного та криптографічного захисту інформації**», затвердженого наказом Адміністрації Держспецзв’язку від 8 серпня 2008 року № 131.

На даний час Адміністрацією Держспецзв’язку надано право на розмноження та розповсюдження нормативних документів у сфері захисту інформації таким організаціям:

- Національний університет «Львівська політехніка»;

- ТОВ «НікС» (Київ);

- ТОВ «Науково-технічний центр "Євроконтакт"» (Київ).

**7. Закони України про електронний документообіг та цифровий підпис**

Криптографія є одним з найбільш потужних засобів забезпечення конфіденційності і контролю цілісності інформації. У багатьох відношеннях вона займає центральне місце серед програмно-технічних регуляторів інформаційної безпеки. Наприклад, для портативних комп'ютерів, фізично захистити які вкрай важко, тільки криптографія дозволяє гарантувати конфіденційність інформації навіть у випадку крадіжки.

Криптографічні системи (або шифри) класифікуються таким чином: симетричні та асиметричні криптосистеми. Під симетричними криптографічними розуміються такі системи, в яких для шифрування й розшифрування використовується один і той же ключ, що зберігається в секреті.

Симетричне шифрування має таку перевагу як швидкість криптографічних операцій. Воно особливо корисно для шифрування даних, що залишаються у нас. Однак, симетричне шифрування, використане саме по собі як засіб захисту цінних даних, що пересилаються, є досить витратним через складність передачі секретного ключа.

Симетричні алгоритми шифрування були єдиними загально відомими до липня 1976 року, коли новий асиметричний алгоритм запропонували американські вчені У.Діффі і М.Хеллман.

Новим класом криптографічних систем є асиметричні або двохключеві системи (на вдіміну від одноключових симетричних систем). Ці системи характеризуються тим, що для шифрування і для розшифрування використовуються різні ключі, зв'язані між собою деякою залежністю. Застосування таких шифрів стало можливим завдяки Клоду Шеннону, який запропонував будувати шифр таким способом, щоб його розкриття було еквівалентно рішенню математичної задачі, що вимагає виконання обсягів обчислень, що перевершують можливості сучасних ЕОМ.

Один з ключів (наприклад, ключ шифрування) може бути зроблений загальнодоступним, і в цьому випадку проблема отримання загального секретного ключа для зв'язку відпадає. Оскільки один ключ з пари стає загальнодоступним або публічним, такі системи отримали також назву криптосистем з відкритим ключем. Перший ключ не є секретним і може бути опублікований для використання всіма користувачами системи, які зашифровують дані. Розшифрування даних за допомогою відкритого ключа неможливо.

Для розшифрування даних одержувач зашифрованої інформації використовує другий ключ, який є секретним. Зрозуміло, ключ розшифрування не може бути визначений з ключа зашифрування.

Центральним поняттям в асиметричних криптографічних системах є поняття односторонньої функції. Під односторонньої функцією розуміється ефективно обчислювана функція, для звернення якої (тобто для пошуку хоча б одного значення аргументу по заданому значенню функції) не існує ефективних алгоритмів.

У асиметричній криптографії використовуються так звані хеш-функції. Хеш-функції - це односторонні функції, які призначені для контролю цілісності даних. При передачі інформації під час пересилання вона хешується, хеш передається одержувачу разом із повідомленням, і одержувач визначає його хеш цієї інформації повторно. Якщо обидва хеша співпали, то це означає, що інформація була передана без спотворень.

Додаткова перевага від використання криптосистем з відкритим ключем полягає в тому, що вони надають можливість створення електронних цифрових підписів (далі - ЕЦП). ЕЦП дозволяє одержувачу повідомлення переконатися в автентичності джерела інформації (іншими словами, у тім, хто є автором інформації), а також перевірити, чи була інформація змінена (перекручена), поки знаходилася в шляху.

Таким чином, ЕЦП є засобом авторизації і контролю цілісності даних. Крім того, ЕЦП забезпечує принцип незречення, що означає, що відправник не може відмовитися від факту свого авторства підписаної ним інформації. Ці можливості настільки ж важливі для криптографії, як і таємність.

ЕЦП служить тієї ж мети, що печатка або власноручний автограф на паперовому листі. Однак внаслідок своєї цифрової природи ЕЦП перевершує ручний підпис і печатку в ряді дуже важливих аспектів. ЕЦП не тільки підтверджує особистість що підписала, але також допомагає визначити, чи був зміст підписаної інформації змінений. Власноручний підпис і печатка не мають подібної якості, крім того, їх набагато легше підробити.

У той же час, ЕЦП аналогічний фізичній печатці у тому плані, що, як печатка може бути проставлена будь-якою людиною, що одержала в розпорядження печатку, так і цифровий підпис може бути згенерований ким завгодно з копією потрібного закритого ключа.

На даний час в Україні діє державний стандарт ЕЦП **ДСТУ 4145 - 2002** «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка», який установлює механізм цифрового підписування, оснований на властивостях груп точок еліптичних кривих, та правила застосування цього механізму до повідомлень, що пересилаються каналами зв’язкута/або обробляються у комп’ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства.

Крім того, використовуються радянський стандарт **ГОСТ 28147-89** «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», який у 2009 році був прийнятий в Україні як національний, і російський стандарт **ГОСТ 34.311-95** «Информационная технология. Криптографическая функция хеширования».

З метою вирішення питань криптографічного захисту інформаціїще 22 травня 1998 року Указом Президента України № 505 було затверджено «**Положення про порядок здійснення криптографічного захисту інформації в Україні**» (далі - Положення), яке визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої може завдати шкоди державі, суспільству або особі.

Згідно п.3 Положення державну політику у сфері криптографічного захисту інформації (далі - КЗІ) відповідно до закону реалізує Державна служба спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку).

Згідно п.4 Положення ліцензування діяльності, пов'язаної з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів КЗІ, а також з наданням послуг із КЗІ, здійснюється згідно із законодавством України.

Згідно п.5 Положення державні органи, підприємства, установи і організації придбавають, вивозять з України, використовують криптосистеми і засоби КЗІ за погодженням з Адміністрацією Держспецзв'язку.

Згідно п.6 Положення з метою визначення рівня захищеності від несанкціонованого доступу до інформації з обмеженим доступом проводяться сертифікаційні випробування криптосистем і засобів криптографічного захисту.

Згідно п.11 Положення діяльність, пов'язану з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів КЗІ, а також з наданням послуг із КЗІ, можуть здійснювати суб'єкти підприємницької діяльності, зареєстровані в порядку, встановленому законодавством.

Крім того, в українському законодавстві щодо КЗІ є два Закони: «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг», які були прийняті у 2003 році.

Закон України «**Про електронний цифровий підпис**» (далі - Закон) визначає правовий статус ЕЦП та регулює відносини, що виникають при використанні ЕЦП.

У цьому Законі наведені нижче терміни вживаються в такому значенні:

- 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;

- ЕЦП - вид електронного підпису, отриманого за результатом криптографічного перетворення набору даних, який додається до цього набору або логічно з ним поєднується.

ЕЦП дає змогу підтвердити цілісність даних та ідентифікувати підписувача.

ЕЦП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

- засіб ЕЦП - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки ЕЦП;

- особистий ключ - параметр криптографічного алгоритму формування ЕЦП, доступний тільки підписувачу;

- відкритий ключ - параметр криптографічного алгоритму перевірки ЕЦП, доступний суб'єктам відносин у сфері використання ЕЦП;

- засвідчення чинності відкритого ключа - процедура формування його сертифіката;

- сертифікат відкритого ключа (далі - сертифікат ключа) - документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу.

Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

- посилений сертифікат відкритого ключа (далі - посилений сертифікат ключа) - сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

- акредитація - процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

- компрометація особистого ключа - будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

- блокування сертифіката ключа - тимчасове зупинення чинності сертифіката ключа;

- підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає ЕЦП під час створення електронного документа;

- послуги ЕЦП - надання у користування засобів ЕЦП, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;

- надійний засіб ЕЦП - засіб ЕЦП, що має позитивний експертний висновок за результатами державної експертизи у сфері КЗІ. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється у порядку, визначеному законодавством.

Згідно **статті 2** Закону суб'єктами правових відносин у сфері послуг ЕЦП є:

- підписувач;

- користувач;

- центр сертифікації ключів;

- акредитований центр сертифікації ключів;

- центральний засвідчувальний орган;

- засвідчувальний центр органу виконавчої влади або іншого державного органу (далі - засвідчувальний центр);

- контролюючий орган.

Згідно **статті 3** Закону ЕЦП за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- ЕЦП підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів ЕЦП;

- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення ЕЦП;

- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

Згідно **статті 4** Закону ЕЦП призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

ЕЦП використовується фізичними та юридичними особами - суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання ЕЦП не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

**Стаття 5** Закону визначає деякі особливості застосування ЕЦП.

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Інші юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, сформованим центром сертифікації ключів, а також використовувати електронний цифровий підпис без сертифіката ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються ЕЦП без сертифіката ключа, визначається суб'єктами правових відносин у сфері послуг ЕЦП на договірних засадах.

 У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, на електронний документ накладається ще один ЕЦП юридичної особи, спеціально призначений для таких цілей.

Порядок застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності визначається Кабінетом Міністрів України.

Порядок застосування електронного підпису, у тому числі ЕЦП в банківській системі України та суб'єктами переказу коштів визначається Національним банком України.

Згідно **статті 6** Закону сертифікат ключа містить такі обов'язкові дані:

- найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);

- зазначення, що сертифікат виданий в Україні;

- унікальний реєстраційний номер сертифіката ключа;

- основні дані (реквізити) підписувача - власника особистого ключа;

- дату і час початку та закінчення строку чинності сертифіката;

- відкритий ключ;

- найменування криптографічного алгоритму, що використовується власником особистого ключа;

- інформацію про обмеження використання підпису.

Посилений сертифікат ключа, крім обов'язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника.

Згідно **статті 7** Закону підписувач має право:

- вимагати скасування, блокування або поновлення свого сертифіката ключа;

- оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку.

Підписувач зобов'язаний:

- зберігати особистий ключ у таємниці;

- надавати центру сертифікації ключів дані згідно з вимогами статті 6 цього Закону для засвідчення чинності відкритого ключа;

- своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа.

Згідно **статті 8** Закону центром сертифікації ключів може бути юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги ЕЦП та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі з дотриманням вимог статті 6 цього Закону.

Обслуговування фізичних та юридичних осіб здійснюється центром сертифікації ключів на договірних засадах.

Центр сертифікації ключів має право:

- надавати послуги ЕЦП та обслуговувати сертифікати ключів;

- отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо у юридичної або фізичної особи чи у її уповноваженого представника.

Центр сертифікації ключів зобов'язаний:

- забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;

- забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;

- встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;

- своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених цим Законом;

- своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання ЕЦП, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;

- перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;

- цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;

- вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

- забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

- забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

- надавати консультації з питань, пов'язаних з ЕЦП.

Зберігання особистих ключів підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються.

Згідно **статті 9** Закону центр сертифікації ключів, акредитований в установленому порядку, є акредитованим центром сертифікації ключів.

Акредитований центр сертифікації ключів має право:

- надавати послуги ЕЦП та обслуговувати виключно посилені сертифікати ключів;

- отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо у юридичної або фізичної особи чи її представника.

Акредитований центр сертифікації ключів має виконувати усі зобов'язання та вимоги, встановлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг ЕЦП надійні засоби ЕЦП.

Порядок акредитації та вимоги, яким повинен відповідати акредитований центр сертифікації ключів, встановлюються Кабінетом Міністрів України.

Згідно **статті 10** Закону Кабінет Міністрів України за необхідності визначає засвідчувальний центр центрального органу виконавчої влади для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги ЕЦП цьому органу і підпорядкованим йому підприємствам, установам та організаціям.

Інші державні органи за необхідності, за погодженням з Кабінетом Міністрів України, визначають свої засвідчувальні центри, призначені для виконання функцій, зазначених у частині першій цієї статті.

Засвідчувальний центр по відношенню до групи центрів сертифікації ключів, зазначених у частині першій цієї статті, має ті ж функції і повноваження, що й центральний засвідчувальний орган стосовно центрів сертифікації ключів.

Засвідчувальний центр реєструється, засвідчує свій відкритий ключ і акредитується у центральному засвідчувальному органі.

Положення про засвідчувальний центр центрального органу виконавчої влади затверджується Кабінетом Міністрів України.

Національний банк України має право створити Засвідчувальний центр для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації центрів сертифікації ключів.

Згідно **статті 11** Закону Центральний засвідчувальний орган (далі - ЦЗО):

- формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів з дотриманням вимог статті 6 цього Закону;

- блокує, скасовує та поновлює посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів у випадках, передбачених цим Законом;

- веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів;

- веде акредитацію центрів сертифікації ключів, отримує та перевіряє інформацію, необхідну для їх акредитації;

- забезпечує цілодобово доступ засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;

- зберігає посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів;

- надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов'язаних з використанням електронного цифрового підпису.

Центральний засвідчувальний орган відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Положення про центральний засвідчувальний орган затверджується Кабінетом Міністрів України.

Згідно **статті 12** Закону функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації(*Адміністрація Держспецзв'язку*).

Контролюючий орган перевіряє дотримання вимог цього Закону центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів.

Згідно **статті 13** Закону скасування, блокування та поновлення посиленого сертифіката ключа

Акредитований центр сертифікації ключів негайно скасовує сформований ним посилений сертифікат ключа у разі:

- закінчення строку чинності сертифіката ключа;

- подання заяви власника ключа або його уповноваженого представника;

- припинення діяльності юридичної особи - власника ключа;

- смерті фізичної особи - власника ключа або оголошення його померлим за рішенням суду;

- визнання власника ключа недієздатним за рішенням суду;

- надання власником ключа недостовірних даних;

- компрометації особистого ключа.

ЦЗО негайно скасовує посилений сертифікат ключа центру сертифікації ключів, засвідчувального центру у разі:

- припинення діяльності з надання послуг ЕЦП;

- компрометації особистого ключа.

ЦЗО, засвідчувальний центр, акредитований центр сертифікації ключів негайно блокують посилений сертифікат ключа:

- у разі подання заяви власника ключа або його уповноваженого представника;

- за рішенням суду, що набрало законної сили;

- у разі компрометації особистого ключа.

Скасування і блокування посиленого сертифіката ключа набирає чинності з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати та часу здійснення цієї операції.

ЦЗО, засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника.

Блокований посилений сертифікат ключа поновлюється:

- у разі подання заяви власника ключа або його уповноваженого представника;

- за рішенням суду, що набрало законної сили;

- у разі встановлення недостовірності даних про компрометацію особистого ключа.

Закон України «**Про електронні документи та електронний документообіг**» встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

Згідно **статті 5** Закону електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Згідно **статті 6** Закону електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора або підписувача електронного документа. Накладанням електронного підпису завершується створення електронного документа.

Згідно **статті 7** Закону оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з ЕЦП автора.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Згідно **статті 9** Закону 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.

Згідно **статті 11** Закону електронний документ вважається одержаним адресатом з часу надходження автору повідомлення в електронній формі від адресата про його одержання, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

Згідно **статті 12** Закону перевірка цілісності електронного документа проводиться шляхом перевірки ЕЦП.

Згідно **статті 13** Закону суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Згідно **статті 15** Закону в інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять інформацію, яка є власністю держави, або ІзОД, повинен забезпечуватися її захист відповідно до законодавства.

Застосування ЕЦП передбачено також у платіжних системах і системах розрахунків (далі - платіжні системи) згідно Закону України «**Про платіжні системи та переказ коштів в Україні**», який визначає загальні засади функціонування платіжних систем, поняття та загальний порядок проведення переказу коштів у межах України, а також визначає загальний порядок здійснення нагляду за платіжними системами.

Так, згідно **статті 18** Закону електронний документ на переказ коштів, що не засвідчений електронним підписом, забороняється приймати до виконання.

Учасник платіжної системи під час приймання електронних документів на переказ коштів має передбачити процедуру перевірки:

- електронного підпису;

- цілісності, достовірності та авторства електронного документа.

Головним органом у системі центральних органів виконавчої влади з формування та забезпечення реалізації державної політики у сфері ЕЦП є Міністерство юстиції України (далі - Мін'юст), що здійснює свою діяльність згідно вимог «**Положення про Мін'юст**» (далі - Положення), затвердженого постановою Кабінету Міністрів України від 2 липня 2014 року № 228.

Згідно вимог Положення Мін’юст відповідно до покладених на нього завдань виконує функції ЦЗО системи ЕЦП, а саме:

- проводить реєстрацію, акредитацію засвідчувальних центрів та центрів сертифікації ключів, повторну акредитацію та скасування акредитації засвідчувальних центрів та акредитованих центрів сертифікації ключів, отримує та перевіряє інформацію, необхідну для цього; видає, переоформлює, анулює відповідні свідоцтва та видає дублікати;

- забезпечує діяльність постійно діючої комісії з акредитації засвідчувальних центрів та центрів сертифікації ключів;

- генерує пари ключів (особистий та відкритий ключі) центрального засвідчувального органу;

- формує і видає посилені сертифікати відкритих ключів засвідчувальним центрам та центрам сертифікації ключів;

- формує посилені сертифікати власних відкритих ключів центрального засвідчувального органу;

- блокує, скасовує та поновлює сертифікати відкритих ключів засвідчувальних центрів та центрів сертифікації ключів у випадках, передбачених законом, про що інформує контролюючий орган;

- зберігає посилені сертифікати відкритих ключів засвідчувальних центрів, центрів сертифікації ключів, акредитованих центрів сертифікації ключів, що припинили діяльність;

- надає послугу з постачання передачі сигналів точного часу для формування та проведення перевірки позначки часу; погоджує розроблені центрами сертифікації ключів, акредитованими центрами сертифікації ключів порядки синхронізації часу із Всесвітнім координованим часом (UTC);

- веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів відкритих ключів засвідчувальних центрів, центрів сертифікації ключів, акредитованих центрів сертифікації ключів та здійснює їх розповсюдження (публікацію);

- веде Реєстр суб’єктів, які надають послуги, пов’язані з електронним цифровим підписом;

- забезпечує цілодобово доступ засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів і відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;

- надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов’язаних з використанням електронного цифрового підпису;

- розглядає заяви і скарги щодо неналежного функціонування центрів та подає відповідні пропозиції контролюючому органу;

- повідомляє контролюючому органу про обставини, які перешкоджають діяльності центрального засвідчувального органу;

- здійснює інші визначені законом повноваження, необхідні для забезпечення функціонування центрального засвідчувального органу.

28 жовтня 2004 року постановою Кабінету Міністрів України № 1451 функції ЦЗО були покладені на Міністерство юстиції України та було затверджене «**Положення про ЦЗО**».

Організаційно-методологічні, технічні та технологічні умови діяльності ЦЗО під час обслуговування посилених сертифікатів відкритих ключів центрів, проведення реєстрації, акредитації ЦСК, а також порядок взаємодії ЦСК із ЦЗО у процесі надання послуг ЕЦП визначаються «**Регламентом роботи ЦЗО**» (далі - Регламент), затвердженимнаказом Міністерства юстиції України від 29 січня 2013 року  № 183/5, зареєстрованим у Міністерстві юстиції України 30 січня 2013 року за № 191/22723.

Згідно п.3.1 Регламенту на офіційному веб-сайті ЦЗО розповсюджується (публікується) така інформація:

- перелік зареєстрованих Центрів, що надають (припинили надання) послуги ЕЦП;

- перелік акредитованих Центрів, що надають (припинили надання) послуги ЕЦП;

- сертифікати ключів ЦЗО;

- електронні реєстри чинних, блокованих та скасованих сертифікатів ключів Центрів;

- відомості про прийняття від АЦСК на зберігання документованої інформації у разі припинення діяльності АЦСК.

 *Офіційний сайт ЦЗО: http://czo.gov.ua.*

Крім того, згідно Указу Президента України від 27 червня 1996 року № 468 «**Про Єдиний державний реєстр нормативних актів**» (далі - Реєстр) на Міністерство юстиції України були покладені функції ведення Реєстру, розроблення організаційних заходів та впровадження методологічних принципів, створення фонду нормативних актів та підтримання їх у контрольному стані, надання інформації про них.

23 квітня 2001 року постановою Кабінету Міністрів України № 376 був затверджений «**Порядок ведення Єдиного державного реєстру нормативно-правових актів та користування ним**» (далі - Порядок).

Згідно п.2 Порядку Реєстр - це автоматизована система збирання, накопичення та опрацювання актів законодавства, яка складається з еталонного, страхового, робочого, інформаційного фондів та окремого розділу.

Еталонний фонд Реєстру - комп'ютерна інформаційна система, призначена для зберігання та обліку еталонних текстів нормативно-правових актів у контрольному стані. Еталонний фонд формується та зберігається в Мін'юсті.

Еталонний текст Реєстру - текст нормативно-правового акта у формі комп'ютерного файла, цілісність якого забезпечується за допомогою спеціальних ознак.

Робочий фонд Реєстру - комп'ютерна інформаційна система, яка підтримує технологію ведення Реєстру і використовується для підготовки та опрацювання текстів нормативно-правових актів при внесенні їх до еталонного фонду Реєстру.

Страховий фонд Реєстру - архівні копії еталонного фонду Реєстру, які зберігаються в Мін'юсті на електронних носіях і призначені для відновлення в автентичній формі еталонного фонду Реєстру у разі його повної або часткової втрати.

Інформаційний фонд Реєстру - спеціально створена для надання широкому колу користувачів інформації з Реєстру комп'ютерна інформаційна система у формі окремої бази даних, в якій зберігаються копії еталонних текстів нормативно-правових актів.

Копія еталонного тексту Реєстру - копія тексту нормативно-правового акта у формі комп'ютерного файла, який ідентичний відповідному еталонному тексту та зберігає всі спеціальні ознаки, що забезпечують його цілісність.

Окремий розділ Реєстру - комп'ютерна інформаційна система, що використовується для підготовки та накопичення текстів нормативно-правових актів з відповідним грифом секретності.

*Офіційний сайт Реєстру: www.reestrnpa.gov.ua.*

26 червня 2002 року наказом Міністерства юстиції України № 57/5, зареєстрованим в Міністерстві юстиції України 27 червня 2002 року за № 546/6834, була затверджена «**Інструкція про порядок та умови одержання інформації з інформаційного фонду Єдиного державного реєстру нормативно-правових актів**» (далі - Інструкція).

Згідно п.1.3 Інструкції Адміністратор технологій ведення всіх фондів Реєстру та доступу до Реєстру (Технічний адміністратор Реєстру) - **Інформаційно-аналітичний центр «ЛІГА»**, яка здійснює супроводження програмно-інформаційного забезпечення Реєстру, відповідає за його функціонування, збереження даних і захист їх від руйнування, технічну підготовку текстів нормативно-правових актів для внесення їх до відповідного фонду Реєстру із збереженням спеціальних ознак для забезпечення їх цілісності, формування та підтримання інформаційного фонду, обслуговування та технічну підтримку користувачів Реєстру.

*Офіційний сайт центру: www.liga.net.*

Згідно п.1.4 Інструкції Адміністратор обліку користувачів та контролю доступу до Реєстру (далі - Адміністратор обліку) - **державне підприємство «Інформаційний центр»** Міністерства юстиції України, яке здійснює обслуговування і веде облік користувачів Реєстру та організовує контроль доступу до нього. Для забезпечення контролю за доступом
до інформаційного фонду Реєстру кожному користувачу видається унікальний програмно-технічний ключ-ідентифікатор.

*Офіційний сайт центру: www.informjust.ua.*

Згідно п.1.5 Інструкції користувачами Реєстру можуть бути будь-які юридичні та фізичні особи, у яких виникла потреба в отриманні інформації з інформаційного фонду Реєстру та які звернулися до одного з Адміністраторів Реєстру з відповідним запитом за встановленою формою. Зазначені юридичні та фізичні особи набувають статусу користувачів Реєстру після реєстрації їх Адміністратором обліку в порядку, установленому цією Інструкцією.

31 березня 2003 року наказом Міністерства юстиції України № 25/5, зареєстрованим в Міністерстві юстиції України 31 березня 2003 року за № 243/7564, був затверджений «**Порядок та розмірів плати за надання права доступу, користування та одержання інформації з інформаційного фонду Єдиного державного реєстру нормативно-правових актів**»:

|  |  |  |  |
| --- | --- | --- | --- |
| Форма надання інформації | Одиниця виміру | Тариф для юридичнихосіб, грн. | Тариф для фізичнихосіб, грн. |
| На паперових носіях | 1 кбайт | 0,50 | 0,30 |
| У вигляді окремого комп'ютерного файла | 1 кбайт | 0,40 | 0,20 |
| Шляхом безпосереднього доступу до інформаційного фонду Реєстру | 1 кбайт | 0,20 | 0,10 |

**8. Підзаконні акти щодо електронного документообігу та цифрового підпису**

Реалізація положень Законів України визначається постановами Кабінету Міністрів України. Так, 28 жовтня 2004 року постановами Кабінету Міністрів України були затверджені такі документи:

* Типовий порядок здійснення електронного документообігу в органах виконавчої влади;

- Порядок застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності;

- Порядок обов'язкової передачі документованої інформації.

«**Типовий порядок здійснення електронного документообігу в органах виконавчої влади**», затверджений постановою Кабінету Міністрів України № 1453, визначає такі вимоги:

3. Орган виконавчої влади здійснює електронний документообіг лише за умови використання надійних засобів електронного цифрового підпису, що повинне бути підтверджено позитивним висновком за результатами державної експертизи у сфері КЗІ, одержаним на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів ключів у своїх працівників - підписувачів.

4. Орган виконавчої влади здійснює електронний документообіг через спеціальні телекомунікаційні мережі або телекомунікаційні мережі загального користування. При цьому відправлення органом виконавчої влади електронного документа через телекомунікаційні мережі загального користування здійснюється за рішенням керівника
цього органу.

5. Система електронного документообігу органу виконавчої влади повинна відповідати вимогам нормативно-правових актів у сфері захисту інформації.

6. Відповідальність за організацію здійснення електронного документообігу в органі виконавчої влади несе його керівник, якщо інше не встановлено законодавством. Здійснення електронного документообігу покладається на службу діловодства.

***Організація роботи з вхідними електронними документами***

7. Електронні документи, що надходять на адресу органу виконавчої влади, приймаються службою діловодства централізовано.

8. Електронний документ, що надійшов на адресу органу виконавчої влади, підлягає відхиленню у разі:

- відсутності у адресата надійних засобів ЕЦП;

- надходження не за адресою;

- зараження вірусом;

- негативного результату перевірки на цілісність і справжність усіх накладених на нього ЕЦП.

При цьому відправнику в дводенний строк надсилається відповідне повідомлення за формою згідно з додатком 1.

Зазначена процедура для електронного документа відповідає процедурі повернення документа на папері (далі - повернення електронного документа).

9. Кожен одержаний адресатом електронний документ перевіряється на зараження його вірусом.

10. Кожен одержаний адресатом електронний документ перевіряється на цілісність і справжність усіх накладених на нього ЕЦП, включаючи ті, що накладені (проставлені) згідно із законодавством як аналоги печатки (далі - електронні печатки).

При цьому необхідно, щоб:

- кожен ЕЦП був підтверджений з використанням посиленого сертифіката ключа за допомогою надійних засобів ЕЦП;

- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення ЕЦП;

- особистий ключ підписувача відповідав відкритому ключу, зазначеному у сертифікаті;

- на час перевірки був чинним посилений сертифікат відкритого ключа акредитованого ЦСК та/або посилений сертифікат відкритого ключа відповідного засвідчувального центру.

11. Попередній розгляд електронного документа здійснюється у його візуальній формі.

12. Визначення, чи потребує електронний документ обов'язкового розгляду керівником органу виконавчої влади або іншими посадовими особами відповідно до функціональних обов'язків, необхідності його реєстрації, а також встановлення строків
виконання цього документа структурними підрозділами чи безпосередніми виконавцями здійснюється у тому ж порядку, що й для документів на папері.

13. Вхідні, внутрішні та вихідні електронні документи реєструються в одній системі разом з відповідними документами на папері.

Реєстрація вхідних електронних документів здійснюється у тому ж порядку, що й вхідних документів на папері. Для забезпечення реєстрації, обліку, пошуку і контролю виконання вхідного електронного документа заповнюється реєстраційно-контрольна картка в електронній формі згідно з додатками 2 і 3.

Після реєстрації вхідного електронного документа адресат у дводенний строк надсилає відправнику повідомлення про його прийняття і реєстрацію за формою згідно з додатком 4.

14. Для фіксування резолюції щодо виконання вхідного електронного документа складається відповідний внутрішній електронний документ «Резолюція» за підписом відповідної посадової особи, про що зазначається в реєстраційно-контрольній картці.

15. Контроль за виконанням та оперативним використанням наявної в електронних документах інформації здійснюється в тому ж порядку, що й для документів на папері.

***Організація роботи з внутрішніми та вихідними електронними документами***

16. Оформлення і реєстрація електронних документів, що складаються в органі виконавчої влади, за винятком особливостей їх підписання або затвердження, здійснюється у тому ж порядку, що й для документів на папері.

До візуальної форми подання електронного документа за складом та розміщенням реквізитів встановлюються ті ж вимоги, що й для документа на папері.

17. Підписання або затвердження електронного документа здійснюється шляхом накладення на нього ЕЦП відповідних посадових осіб. На момент накладення останнього ЕЦП технологічно та/або організаційно забезпечується проставлення у створеному електронному документі дати і його реєстраційного номера.

У разі непідписання або незатвердження електронного документа керівником органу виконавчої влади чи іншою посадовою особою реєстрація цього документа скасовується, а його виконавець інформується про відхилення документа.

Проставлення електронної печатки на електронний документ здійснюється згідно із законодавством. При цьому зазначена процедура виконується лише після підписання або затвердження електронного документа.

18. Адресування електронних документів здійснюється з додержанням тих же вимог, що й для документів на папері.

19. На кожний внутрішній та вихідний електронний документ заповнюється реєстраційно-контрольна картка в електронній формі згідно з додатками 2 і 3.

20. Перед відправленням вихідного електронного документа проводиться перевірка його цілісності та справжності усіх накладених на нього ЕЦП з додержанням тих же вимог, що й для вхідних документів.

У разі порушення цілісності вихідного електронного документа або непідтвердження справжності накладеного на нього ЕЦП його реєстрація скасовується, а виконавець інформується про відхилення документа.

21. Вихідні електронні документи відправляються адресатам службою діловодства централізовано не пізніше наступного робочого дня після їх одержання від структурних підрозділів - виконавців.

22. Електронний документ вважається одержаним адресатом з часу надходження відправнику повідомлення про його прийняття і реєстрацію.

У разі неодержання від адресата протягом двох робочих днів повідомлення про прийняття і реєстрацію або про відхилення електронного документа відправник вживає додаткових заходів з використанням інших засобів зв'язку для одержання від адресата відповідного повідомлення.

У разі одержання від адресата повідомлення про відхилення електронного документа відправником вживаються заходи для усунення причин відхилення і забезпечення повторного відправлення цього документа.

Якщо таке повідомлення одержане від адресата, який не має надійних засобів ЕЦП, цьому адресату надсилається відповідний документ на папері.

Підтвердження факту одержання від адресата повідомлення щодо електронного документа відправником не здійснюється.

23. Реєстраційний номер, дата і час реєстрації електронного документа адресатом, зазначені у його повідомленні, фіксуються відправником у реєстраційно-контрольній картці.

***Погодження електронних документів***

24. Погодження електронного документа здійснюється шляхом накладення на нього ЕЦП посадової особи.

25. Зауваження і пропозиції до поданого електронного документа (у разі наявності) фіксуються в окремому електронному документі, на який накладається ЕЦП посадової особи.

26. Порядок внутрішнього погодження електронних документів у системі електронного документообігу органу виконавчої влади затверджується його керівником, якщо інше не встановлено законодавством.

27. У разі відсутності в органі виконавчої влади, яким погоджується електронний документ, надійних засобів ЕЦП цьому органу для погодження надається відповідний документ на папері.

***Зберігання електронних документів***

28. Оперативне зберігання електронних документів в органі виконавчої влади, підготовка і передача їх до архівної установи здійснюються з додержанням вимог нормативних актів, затверджених спеціально уповноваженим центральним органом виконавчої влади у сфері архівної справи.

29. Строк зберігання електронних документів повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

«**Порядок застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності**», затверджений постановою Кабінету Міністрів України № 1452, визначає такі вимоги:

2. Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності (далі - установи) застосовують ЕЦП лише за умови використання надійних засобів ЕЦП, що повинне бути підтверджено позитивним висновком за результатами державної експертизи у сфері КЗІ, отриманим на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів відкритих ключів у своїх працівників - підписувачів.

3. Установи застосовують ЕЦП для вчинення правочинів за участю інших юридичних та фізичних осіб лише за наявності у них посилених сертифікатів відкритих ключів.

4. Установи не застосовують ЕЦП:

- для складання електронних документів, які не можуть бути оригіналами у випадках, передбачених законодавством;

- для вчинення правочинів на суму, що перевищує 1 млн. гривень.

5. Установи отримують на договірних засадах послуги, пов'язані з ЕЦП, від акредитованого центру сертифікації ключів. При цьому установа може отримувати такі послуги лише від одного акредитованого центру сертифікації ключів. Використання підписувачами особистих ключів, відповідні відкриті ключі яких засвідчені іншими акредитованими центрами сертифікації ключів, забороняється.

6. Граничні ціни (тарифи) на послуги, пов'язані з ЕЦП, що надаються установам акредитованими центрами сертифікації ключів, установлюються Мін'юстом та погодженням з Мінекономрозвитку.

7. Установа здійснює обмін інформацією з акредитованим центром сертифікації ключів через телекомунікаційні мережі.

8. Відповідальність за організацію застосування ЕЦП в установі несе її керівник, якщо інше не встановлено законодавством.

9. Застосування ЕЦП в установі забезпечує підрозділ інформаційних технологій, а у разі відсутності такого - підрозділ, що виконує відповідні функції (далі - відповідальний підрозділ), або працівник, спеціально визначений наказом керівника цієї установи.

Зазначений підрозділ (працівник) забезпечує:

- підготовку та надання акредитованому центру сертифікації ключів інформації, необхідної для формування посилених сертифікатів відкритих ключів підписувачів;

- надання допомоги підписувачам під час генерації їх особистих та відкритих ключів;

- подання до акредитованого центру сертифікації ключів звернень про скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів;

- доступ підписувачів через телекомунікаційні мережі до акредитованих центрів сертифікації ключів у разі неможливості здійснення ними такого доступу із своїх робочих місць;

- ведення обліку засобів ЕЦП, що використовуються в установі;

- ведення обліку носіїв особистих ключів підписувачів;

- зберігання документів, на підставі яких було сформовано посилені сертифікати відкритих ключів підписувачів;

- контроль за використанням підписувачами засобів ЕЦП та зберіганням ними особистих ключів.

10. Порядок надання працівникам установи права застосування ЕЦП, ведення обліку, зберігання та знищення їх особистих ключів, а також надання акредитованому центру сертифікації ключів інформації, необхідної для формування, скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів установи, визначається наказом її керівника, якщо інше не становлено законодавством.

11. Генерація особистого та відкритого ключів здійснюється підписувачем безпосередньо в установі або в акредитованому центрі сертифікації ключів, що її обслуговує. У разі потреби під час генерації ключів підписувачеві надається допомога персоналом відповідального підрозділу (спеціально визначеним працівником) або персоналом акредитованого центру сертифікації ключів.

12. У посиленому сертифікаті відкритого ключа підписувача додатково зазначається його належність до установи та посада, яку він займає.

13. У разі коли згідно із законодавством необхідне засвідчення печаткою справжності підпису на документах та відповідності копій документів оригіналам, установа застосовує спеціально призначений для таких цілей ЕЦП (далі - електронна печатка).

Установа застосовує електронну печатку лише за наявності у неї відповідної печатки, що застосовується для документів на папері.

У посиленому сертифікаті відкритого ключа, що використовується установою для електронної печатки, додатково зазначається спеціальне призначення ЕЦП та сфера його застосування, а також відтворюється текстова інформація, розміщена на відповідній печатці.

14. Право проставлення електронної печатки на електронних документах надається лише тому працівнику установи, який проставляє відповідну печатку на документах на папері.

Отримання в акредитованому центрі сертифікації ключів посиленого сертифіката відкритого ключа для забезпечення застосування електронної печатки, а також генерація відповідних ключів здійснюється в тому ж порядку, що й для ЕЦП.

15. Підписувач може застосовувати ЕЦП лише після отримання установою від акредитованого центру сертифікації ключів посиленого сертифіката його відкритого ключа.

Після звільнення підписувача установа звертається до акредитованого центру сертифікації ключів для скасування посиленого сертифіката його відкритого ключа, а особистий ключ треба знищити методом, що не допускає можливості його відновлення.

16. Підписувач використовує у процесі виконання своїх функцій лише особистий ключ, отриманий в установі. Використання особистого ключа у випадках, не пов'язаних з діяльністю установи, забороняється.

17. Підписувач на один і той самий момент часу може мати і використовувати лише один особистий ключ, якому відповідає відкритий ключ з чинним посиленим сертифікатом, отриманим установою. Це обмеження не стосується електронної печатки.

18. Підписувач несе відповідальність за зберігання особистого ключа.

19. Копіювання особистих ключів або передача їх іншим особам забороняється.

20. Справжність ЕЦП, накладеного на електронний документ, та цілісність цього документа перевіряється з дотриманням таких вимог:

- ЕЦП повинен бути підтверджений з використанням посиленого сертифіката ключа за допомогою надійних засобів ЕЦП;

- під час перевірки повинен використовуватися посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

- особистий ключ підписувача повинен відповідати відкритому ключу, зазначеному у сертифікаті;

- на час перевірки повинен бути чинним посилений сертифікат відкритого ключа акредитованого центру сертифікації ключів та/або посилений сертифікат відкритого ключа відповідного засвідчувального центру.

21. Контроль за виконанням в установах вимог цього Порядку здійснює Адміністрація Держспецзв'язку.

13 липня 2004 року постановою Кабінету Міністрів України № 903 був прийнятий «**Порядок акредитації центру сертифікації ключів**», який визначає процедуру акредитації центру сертифікації ключів (далі - ЦСК), умови надання центром послуг ЕЦП, вимоги до його персоналу та захисту інформації:

20. Акредитований ЦСК забезпечує:

- виконання вимог щодо надання послуг ЕЦП згідно із законом;

- інформування підписувача про обмеження використання ЕЦП та порядок відшкодування збитків;

- виконання приписів контролюючого органу;

- надання допомоги підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживає заходів щодо забезпечення безпеки інформації під час генерації;

- розташування засобів програмно-технічного комплексу, за допомогою яких здійснюється надання послуг сертифікації та відкликання, в спеціальних приміщеннях та їх охорону;

- збереження програмно-технічного комплексу, іншого майна та запобігання безконтрольному проникненню в приміщення акредитованого ЦСК сторонніх осіб;

- використовання надійних засобів ЕЦП, програмно-технічний комплекс, засоби криптографічного захисту інформації відповідно до вимог Адміністрації Держспецзв'язку та Мін'юсту.

27. Акредитований ЦСК під час надання послуги сертифікації фізичним та юридичним особам зобов'язаний:

- генерувати ключі підписувача;

- формувати сертифікат згідно із законом.

13 січня 2005 року наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації (далі - ДСТСЗІ) СБУ № 3 (у редакції наказу ДСТСЗІ СБУ від 10 травня 2006 року № 50), зареєстрованим у Міністерстві юстиції України 27 січня 2005 року за № 104/10384, були затверджені «**Правила посиленої сертифікації**», які визначають організаційні, технічні і технологічні вимоги до акредитованих ЦСК під час обслуговування ними посилених сертифікатів відкритих ключів (далі - сертифікат) та забезпечення їх використання.

У Правилах організаційні, технічні і технологічні умови діяльності акредитованих центрів під час обслуговування ними сертифікатів мають назву політика сертифікації. Сертифікати, сформовані відповідно до вимог політики сертифікації, використовуються для підтримки ЕЦП, який задовольняє вимогам щодо підпису, застосованого до даних в електронній формі, у такий же спосіб, як власноручні підписи задовольняють вимогам стосовно документа на папері.

Правила складаються з таких розділів:

- обов'язки акредитованого ЦСК;

- вимоги до діяльності акредитованого ЦСК під час обслуговування сертифікатів;

- управління ключами в акредитованому центрі;

- обслуговування сертифікатів;

- забезпечення безпеки інформаційних ресурсів в акредитованому ЦСК.

Крім того, окремий додаток до Правил визначає **вимоги до спеціальних приміщень акредитованого центру**, які передбачають проведення заходів щодо пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень, а також від порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів.

26 травня 2004 року постановою Кабінету Міністрів України № 680 був затверджений «**Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу**», який визначає такі вимоги:

2. У цьому Порядку терміни вживаються у такому значенні:

- послуга фіксування часу - процедура засвідчення наявності електронного документа (електронних даних) на певний момент часу шляхом додання до нього або логічного поєднання з ним позначки часу;

- позначка часу - сукупність електронних даних, створена за допомогою технічних засобів та засвідчена ЕЦП центру сертифікації ключів, яка підтверджує наявність електронного документа (електронних даних) на певний момент часу.

3. Надання послуги фіксування часу включає:

- реєстрацію звернень, на підставі яких формується позначка часу;

- формування позначки часу за допомогою особистого ключа центру сертифікації;

- передачу користувачеві послуги фіксування часу сформованої позначки часу;

- реєстрацію та збереження позначки часу, переданої користувачеві послуги фіксування часу.

4. Час, який використовується в позначці часу, встановлюється акредитованим центром сертифікації ключів (далі – АЦСК) та центром сертифікації ключів (далі – ЦСК) за київським часом на момент її формування та синхронізований із Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

АЦСК і ЦСК отримують послугу з постачання передачі сигналів точного часу для формування та проведення перевірки позначки часу, надання якої забезпечується центральним засвідчувальним органом (далі - ЦЗО).

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) розробляється АЦСК і ЦСК та погоджується з ЦЗО.

5. У процесі фіксування часу позначка часу додається або логічно поєднується з електронними даними таким чином, щоб була виключена можливість вносити до них зміни із збереженням позначки часу після надання послуги фіксування часу.

6. Послуги фіксування часу надаються АЦСК і ЦСК на договірних засадах.

7. АЦСК надають послуги фіксування часу згідно з вимогами, які встановлюються Мін’юстом та Адміністрацією Держспецзв’язку, за допомогою особистого ключа, відповідний якому відкритий ключ засвідчено в центральному засвідчувальному органі або засвідчувальному центрі.

8. Перевірка позначки часу проводиться користувачем послуги фіксування часу за допомогою сертифіката відкритого ключа, наданого АЦСК.

9. АЦСК під час надання послуги фіксування часу зобов'язаний:

- забезпечити зберігання даних про надані послуги фіксування часу;

- забезпечити захист персональних даних користувачів відповідно до законодавства;

- подавати консультаційно-методичну допомогу користувачам послуг фіксування часу щодо порядку надання цих послуг;

- надсилати відповідно до законодавства контролюючому та центральному засвідчувальному органам інформацію про надання послуги фіксування часу.

10. АЦСК забезпечує надання послуги фіксування часу цілодобово.

11. У разі надання користувачеві послуги фіксування часу з порушенням вимог цього Порядку, зокрема недотримання вимог щодо точності часу, використання скасованого або блокованого посиленого сертифіката ключа, позначка часу вважається недійсною.

 «**Порядок обов'язкової передачі документованої інформації**», затверджений постановою Кабінету Міністрів України № 1454, визначає механізм обов'язкової передачі на зберігання центральному засвідчувальному органу (далі - ЦЗО) або засвідчувальному центру (далі - ЗЦ) посилених сертифікатів відкритих ключів (далі - сертифікати), документованої інформації акредитованим центром сертифікації ключів (далі - АЦСК) у разі припинення його діяльності.

Метою зазначеної передачі є забезпечення можливості перевірки ЕЦП, накладеного на електронний документ підписувачем, відкритий ключ якого засвідчений в АЦСК, що припиняє діяльність.

2. АЦСК, що засвідчив свій відкритий ключ у ЦЗО або ЗЦ, здійснює передачу паперових та електронних документів (далі - документована інформація) ЦЗО або ЗЦ.

Електронні документи - сформовані АЦСК сертифікати, електронний реєстр сертифікатів, електронні документи, на підставі яких були сформовані, скасовані, блоковані та поновлені сертифікати підписувачів (якщо такий спосіб передбачений регламентом роботи АЦСК).

Паперові документи - договори, на підставі яких підписувачам надавалися послуги ЕЦП, документи, на підставі яких були сформовані, скасовані, блоковані та поновлені сертифікати підписувачів, а також засвідчені в установленому порядку копії рішень (ухвал) судів щодо відшкодування збитків, завданих внаслідок неналежного виконання АЦСК своїх обов'язків.

3. Електронні документи передаються у двох примірниках.

4. Електронний реєстр сертифікатів містить такі дані:

- унікальний реєстраційний номер сертифіката;

- основні дані (реквізити) підписувача, які внесено до сертифіката;

- дата і час початку та закінчення строку чинності сертифіката;

- дата, час та причина скасування, блокування і поновлення сертифіката.

5. На електронний реєстр сертифікатів з допомогою особистого ключа АЦСК накладається ЕЦП.

6. Формат електронного реєстру сертифікатів, вимоги до носіїв інформації та порядку запису на них електронних документів визначаються ЦЗО або ЗЦ, якому передається документована інформація.

7. Документи на папері, які передаються до ЦЗО або ЗЦ, повинні бути зброшуровані. На зворотному боці останнього аркуша зазначається кількість сторінок, ставиться підпис керівника АЦСК, який скріплюється печаткою.

8. АЦСК:

- повідомляє за три місяці до припинення своєї діяльності ЦЗО або ЗЦ про рішення щодо припинення діяльності;

- узгоджує не пізніше ніж за 30 днів до припинення діяльності з ЦЗО або ЗЦ умови передачі документованої інформації.

9. АЦСК зобов'язаний подати за 15 днів до припинення своєї діяльності разом із заявою, в якій зазначаються підстави і дата її припинення, на погодження до ЦЗО або ЗЦ акт приймання-передачі документованої інформації.

Акт приймання-передачі, у якому зазначаються дата передачі, номери та назви документів, кількість аркушів у документі, типи та номери носіїв інформації, складається у трьох примірниках.

10. Документована інформація передається до ЦЗО або ЗЦ нарочним чи рекомендованим поштовим відправленням.

11. Розгляд заяви ЦЗО або ЗЦ здійснюється не пізніше ніж за п'ять днів до припинення діяльності акредитованого центру.

Установлення відповідності документованої інформації переліку в акті приймання-передачі, приймання її ЦЗО або ЗЦ, а також підписання акта його керівником здійснюються протягом доби, визначеної як дата припинення діяльності АЦСК.

Під час передачі документованої інформації на зберігання ЦЗО або ЗЦ перший примірник акта приймання-передачі залишається в ЦЗО або ЗЦ, другий видається керівнику АЦСК, третій надсилається контролюючому органу.

12. Роботи, пов'язані з передачею документованої інформації, придбанням носіїв інформації, записом електронних документів на носії інформації, упаковуванням і транспортуванням, виконуються за рахунок АЦСК, що передає документовану інформацію.

13. Приймання документованої інформації проводиться ЦЗО або ЗЦ безоплатно.

14. Відомості про прийняття від АЦСК на зберігання документованої інформації публікуються на веб-сайті ЦЗО.

ЗЦ, якому передано документовану інформацію, не пізніше ніж через три доби після підписання акта приймання-передачі подає ЦЗО для публікації на його веб-сайті відомості про прийняття на зберігання документованої інформації відповідного АЦСК.

15. У разі банкрутства АЦСК ліквідатор здійснює передачу документованої інформації ЦЗО або ЗЦ згідно з цим Порядком.

15-1. У разі скасування акредитації АЦСК передає за актом приймання-передачі ЦЗО:

- електронні документи протягом 10 робочих днів з моменту прийняття рішення про скасування акредитації;

- паперові документи протягом 20 робочих днів з моменту прийняття рішення про скасування акредитації.

Акт приймання-передачі, в якому зазначаються дата передачі, номер і назва документа, кількість аркушів у документі, тип та номер носія інформації, складається в трьох примірниках.

Перший примірник акта залишається в ЦЗО або ЗЦ, другий видається керівнику АЦСК, акредитацію якого скасовано, третій надсилається контролюючому органу.

20 серпня 2012 року спільним наказом Адміністрації Держспецзв'язку та Міністерства юстиції України № 1236/5/453 «**Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах ЕЦП**», зареєстрованим у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710, були затверджені:

- вимоги до формату посиленого сертифіката відкритого ключа;

- вимоги до структури об'єктних ідентифікаторів для криптографічних алгоритмів, що є державними стандартами

- вимоги до формату списку відкликаних сертифікатів;

- вимоги до формату підписаних даних;

- вимоги до протоколу фіксування часу;

- вимоги до протоколу визначення статусу сертифіката.

18 грудня 2012 наказом Адміністрації Держспецзв'язку № 739, зареєстрованим у Міністерстві юстиції України 14 січня 2013 року за № 108/22640, були затверджені «**Вимоги до форматів криптографічних повідомлень**».

**9. Нормативно-правові акти з ліцензування**

**діяльності у сферах інформаційної безпеки**

Основним нормативно-правовим актом України, який визначає види господарської діяльності, що підлягають ліцензуванню, порядок їх ліцензування, встановлює державний контроль у сфері ліцензування, відповідальність суб'єктів господарювання та органів ліцензування за порушення законодавства у сфері ліцензування є Закон України «**Про ліцензування видів господарської діяльності**».

Згідно **статті 1** Закону вживаються терміни, які мають таке значення:

- ліцензіат - суб’єкт господарювання, який має ліцензію на провадження встановленого законом виду господарської діяльності;

- ліцензійні умови - нормативно-правовий акт Кабінету Міністрів України, положення якого встановлюють вичерпний перелік вимог, обов’язкових для виконання ліцензіатом, та вичерпний перелік документів, що додаються до заяви про отримання ліцензії;

- ліцензія - документ, що надається органом ліцензування, на право провадження суб’єктом господарювання визначеного ним виду господарської діяльності, що підлягає ліцензуванню, в електронному вигляді (запис про наявність ліцензії у такого суб’єкта господарювання в Єдиному державному реєстрі юридичних осіб та фізичних осіб - підприємців) або на паперовому носії;

- ліцензування - засіб державного регулювання провадження видів господарської діяльності, що підлягають ліцензуванню, спрямований на реалізацію єдиної державної політики у сфері ліцензування.

Дія цього Закону не поширюється на порядок видачі, переоформлення та анулювання ліцензій на здійснення таких видів господарської діяльності:

- банківську діяльність, яка здійснюється відповідно до Закону України «Про банки і банківську діяльність»;

- діяльність в галузі телебачення і радіомовлення, яка здійснюється відповідно до Закону України «Про телебачення і радіомовлення».

Згідно **статті 5** Закону Експертно-апеляційна рада з питань ліцензування є постійно діючим колегіальним органом при спеціально уповноваженому органі з питань ліцензування та діє за регламентом, що затверджується спеціально уповноваженим органом з питань ліцензування.

Обов’язками Експертно-апеляційної ради з питань ліцензування є:

- розгляд апеляцій та інших скарг здобувачів ліцензії, ліцензіатів на дії органу ліцензування або інших заявників щодо порушення законодавства у сфері ліцензування;

- розгляд звернень органів ліцензування або спеціально уповноваженого органу з питань ліцензування щодо проведення позапланових перевірок додержання ліцензіатами вимог ліцензійних умов на підставах, передбачених пунктами 4 та 5 частини дев’ятої статті 19 цього Закону.

Згідно **статті 7** Закону ліцензуванню підлягають такі види господарської діяльності:

8) діяльність у сфері телекомунікацій з урахуванням особливостей, визначених Законом України «Про телекомунікації» (*згідно* ***статті 21*** *Закону ліцензування діяльності у сфері телекомунікацій, передбачене цим пунктом, втрачає чинність з 1 січня 2018 року*),

надання послуг у галузі КЗІ (крім послуг ЕЦП) та ТЗІ, за переліком, що визначається Кабінетом Міністрів України;

 23) діяльність, пов’язана з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших технічних засобів негласного отримання інформації (критерії належності та перелік технічних засобів негласного отримання інформації визначаються Кабінетом Міністрів України за поданням Служби безпеки України).

Згідно **статті 9** Закону ліцензіат зобов’язаний виконувати вимоги ліцензійних умов відповідного виду господарської діяльності, а здобувач ліцензії для її одержання - відповідати ліцензійним умовам.

Ліцензійні умови та зміни до них розробляються органом ліцензування, що є центральним органом виконавчої влади, підлягають погодженню спеціально уповноваженим органом з питань ліцензування та затверджуються Кабінетом Міністрів України.

Ліцензійними умовами встановлюються зміст та форма:

1) заяви про одержання ліцензії;

2) документів, що додаються до заяви про одержання ліцензії;

3) опису документів, що подаються для одержання ліцензії;

4) документів щодо кожного місця провадження господарської діяльності.

Згідно **статті 10** Закону документи, подання яких до органу ліцензування та видача яких органом ліцензування передбачені цим Законом, можуть бути подані до органу ліцензування та отримані від цього органу ліцензування за вибором здобувача ліцензії:

1) нарочно відповідно до пункту 3 частини другої статті 6 та у порядку, встановленому статтею 9 Закону України «Про адміністративні послуги»;

2) поштовим відправленням з описом вкладення (орган ліцензування надсилає поштові відправлення з повідомленням за місцезнаходженням здобувача ліцензії протягом одного робочого дня з дня оформлення відповідного документа, якщо інший строк надсилання не встановлено законом);

3) в електронному вигляді за допомогою телекомунікаційних засобів зв’язку.

Згідно **статті 11** Закону здобувач ліцензії подає до органу ліцензування заяву про отримання ліцензії за визначеною ліцензійними умовами формою.

У заяві про отримання ліцензії повинна міститися інформація про:

1) здобувача ліцензії:

2) вид господарської діяльності (повністю або частково), зазначений у статті 7 цього Закону, на провадження якого здобувач ліцензії має намір одержати ліцензію;

3) бажаний спосіб одержання документів.

Підставою для прийняття рішення про відмову у видачі ліцензії за результатом розгляду заяви про отримання ліцензії є виявлення:

1) невідповідності здобувача ліцензії ліцензійним умовам, встановленим для провадження виду господарської діяльності, зазначеного в заяві про отримання ліцензії;

2) недостовірності даних у підтвердних документах, поданих здобувачем ліцензії.

Орган ліцензування на наступний робочий день після дня прийняття ним рішення про видачу ліцензії здобувачу ліцензії передає відомості про таке рішення в електронному вигляді до Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців у порядку, визначеному розпорядником цього реєстру.

Строк прийняття рішення про видачу ліцензії становить десять робочих днів з дня одержання органом ліцензування заяви про отримання ліцензії.

Набуття здобувачем ліцензії права на провадження виду господарської діяльності, що підлягає ліцензуванню, відбувається з моменту внесення даних про рішення органу ліцензування про видачу йому ліцензії до Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців.

У повідомленні про прийняття рішення про видачу ліцензії орган ліцензування зазначає розрахункові реквізити для внесення плати за видачу ліцензії.

Ліцензія на провадження здобувачем ліцензії визначеного ним виду господарської діяльності, що підлягає ліцензуванню, оформлюється органом ліцензування в електронному вигляді (запис про рішення органу ліцензування щодо видачі ліцензії суб’єкту господарювання в Єдиному державному реєстрі юридичних осіб та фізичних осіб - підприємців).

Ліцензія видається на необмежений строк.

Форму та зміст ліцензії визначає спеціально уповноважений орган з питань ліцензування.

Ліцензія на паперовому носії має бути підписана керівником органу ліцензування, який підписав рішення про видачу ліцензії (або уповноваженою ним посадовою особою), і завірена гербовою печаткою цього органу ліцензування.

Згідно **статті 14** Закону за видачу ліцензії справляється разова плата в розмірі однієї мінімальної заробітної плати, виходячи з розміру мінімальної заробітної плати, що діє на день прийняття органом ліцензування рішення про видачу ліцензії, якщо інший розмір плати не встановлений законом (*на даний час - 1218 грн.*).

Переоформлення ліцензії є безоплатним.

Плата за видачу ліцензії вноситься ліцензіатом у строк не пізніше десяти робочих днів з дня отримання здобувачем ліцензії від органу ліцензування повідомлення про прийняте ним рішення про видачу ліцензії.

Документом, що підтверджує внесення плати за видачу ліцензії, є копія квитанції, виданої банком, копія платіжного доручення з відміткою банку, квитанція з платіжного термінала, квитанція (чек) з поштового відділення зв’язку.

Згідно **статті 19** Закону державний нагляд за додержанням органами державної влади чи державними колегіальними органами вимог законодавства у сфері ліцензування здійснює спеціально уповноважений орган з питань ліцензування шляхом проведення планових та позапланових перевірок у порядку, встановленому Кабінетом Міністрів України за поданням спеціально уповноваженого органу з питань ліцензування.

Спеціально уповноважений орган з питань ліцензування складає акт перевірки у двох примірниках в останній день перевірки.

Один примірник акта видається керівнику органу ліцензування, діяльність якого перевірялася, другий - зберігається спеціально уповноваженим органом з питань ліцензування.

У разі виявлення порушення органом ліцензування законодавства у сфері ліцензування спеціально уповноважений орган з питань ліцензування протягом п’яти робочих днів з дня складення акта перевірки видає розпорядження про усунення порушень законодавства у сфері ліцензування.

Контроль за наявністю у ліцензіатів (суб’єктів господарювання) ліцензій здійснюють державні органи, на які згідно із законом покладено функції контролю за наявністю ліцензій.

Контроль за додержанням ліцензіатами вимог ліцензійних умов здійснюють у межах своїх повноважень органи ліцензування шляхом проведення планових і позапланових перевірок відповідно до Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» з урахуванням особливостей, визначених цим Законом.

З метою забезпечення ліцензіатом присутності керівника, його заступника або іншої уповноваженої особи під час проведення органом ліцензування планової перевірки додержання ліцензіатом вимог ліцензійних умов, орган ліцензування вживає вичерпних заходів попереднього інформування (не менш як за десять робочих днів) ліцензіата про дату та місце проведення планової перевірки, зокрема за допомогою засобів поштового, телефонного, факсимільного та/або електронного поштового зв’язку.

Про проведення позапланової перевірки ліцензіат повідомляється у день перевірки.

Акт перевірки додержання ліцензіатом вимог ліцензійних умов складається в останній день проведення перевірки.

Головним органом в системі центральних органів виконавчої влади України, що забезпечує формування державної політики з питань ліцензування та дозвільної системи, є Міністерство економічного розвитку і торгівлі України (далі - Мінекономрозвитку). Воно здійснює свою діяльність згідно «**Положення про Мінекономрозвитку**» (далі - Положення), затвердженого постановою Кабінету Міністрів України від 20 серпня 2014 року № 459.

*Офіційний сайт Мінекономрозвитку: www.me.gov.ua.*

Центральним органом виконавчої влади, який реалізує державну політику з питань ліцензування та дозвільної системи у сфері господарської діяльності є Державна регуляторна служба України (далі - ДРС).

ДРС є також спеціально уповноваженим органом з питань ліцензування та дозвільної системи у сфері господарської діяльності, що здійснює свою діяльність згідно «**Положення про ДРС**» (далі - **Положення**), затвердженого постановою Кабінету Міністрів України від 24 грудня 2014 року № 724.

Згідно п.4 Положення ДРС відповідно до покладених на неї завдань:

7) погоджує проекти нормативно-правових актів з питань ліцензування, що розробляються центральними органами виконавчої влади;

21) розробляє основні напрями розвитку ліцензування, здійснює методичне керівництво та інформаційне забезпечення діяльності органів ліцензування;

22) здійснює нагляд за дотриманням органами ліцензування законодавства у сфері ліцензування та надає роз’яснення щодо його застосування;

23) розробляє форми документів у сфері ліцензування та правила їх оформлення;

24) погоджує за поданням органу ліцензування ліцензійні умови провадження певного виду господарської діяльності та порядок здійснення контролю за їх дотриманням, крім передбачених законом випадків;

25) формує експертно-апеляційну раду та здійснює її організаційне, інформаційне та матеріально-технічне забезпечення;

26) організовує підготовку, перепідготовку та підвищення кваліфікації фахівців з ліцензування органів ліцензування;

27) веде Єдиний ліцензійний реєстр;

28) організовує замовлення, постачання, ведення обліку і звітності про витрачання бланків ліцензій;

29) видає відповідно до Закону України «Про ліцензування видів господарської діяльності» розпорядження про усунення порушень законодавства у сфері ліцензування;

30) бере участь у розробленні проектів нормативно-правових актів з питань видачі документів дозвільного характеру та погоджує їх в установленому порядку;

31) здійснює в межах повноважень, передбачених законом, контроль за дотриманням вимог законодавства з питань видачі документів дозвільного характеру та методичне забезпечення діяльності дозвільних органів і державних адміністраторів;

33) є розпорядником Реєстру документів дозвільного характеру.

*Офіційний сайт ДРС: www.dkrp.gov.ua.*

Єдиний ліцензійний реєстр ведеться згідно «**Порядку формування, ведення і користування відомостями ліцензійного реєстру та подання їх до Єдиного ліцензійного реєстру**», затвердженого постановою Кабінету Міністрів України від 8 листопада 2000 року № 1658, який визначає такі вимоги:

Єдиний ліцензійний реєстр (далі - ЄЛР) - це автоматизована система збирання, накопичення та обліку даних з питань ліцензування певних видів господарської діяльності.

Розпорядником та утримувачем ЄЛР є ДРС, що веде такий реєстр, здійснює нормативно-методичне забезпечення його функціонування.

Інформація, що міститься в ЄЛР та реєстрах, є відкритою.

Відомості з реєстрів та ЄЛР можуть надаватися користувачам з використанням електронних засобів зв'язку чи електронно-магнітних носіїв інформації.

Адміністратор ЄЛР - державне підприємство «Інформаційно-ресурсний центр» (далі - ДП «ІРЦ»), що здійснює заходи з адміністрування та супроводження програмного забезпечення ЄЛР, забезпечує його функціонування в межах окремої віртуальної мережі, відповідає за збереження даних та їх захист від несанкціонованого доступу до ЄЛР, має повний прямий доступ до структури єдиної комп'ютерної бази даних і відповідає за збереження даних у ЄЛР, захист даних від руйнування.

Згідно статті 21 Закону «**Про ліцензування видів господарської діяльності**» ЄЛР ведеться до набрання чинності положення про внесення до Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців інформації про ліцензування та видання Кабінетом Міністрів України акта щодо припинення ведення ЄЛР.

ДП «ІРЦ» є технічним адміністратором Єдиного державного реєстру згідно вимог «Порядку надання відомостей з Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців», затвердженого наказом Міністерства юстиції України від 14 грудня 2012 року  № 1846/5, зареєстрованого в Міністерстві юстиції України 18 грудня 2012 року за № 2105/22417 (далі - Порядок).

ДП «ІРЦ» згідно вимог «Порядку здійснює:

- заходи зі створення та супроводження програмного забезпечення Єдиного державного реєстру;

- надання доступу до Єдиного державного реєстру;

- матеріально-технічне та технологічне забезпечення ведення Єдиного державного реєстру;

- комплекс програмних, технологічних та організаційних заходів щодо забезпечення захисту інформації, яка міститься у Єдиному державному реєстрі, від несанкціонованого доступу;

- публікацію повідомлень щодо внесення відомостей до Єдиного державного реєстру в спеціалізованому друкованому засобі масової інформації.

*Офіційний сайт ДП «ІРЦ»: http://irc.gov.ua.*

Порядок ліцензування господарської діяльності у сфері телекомунікацій визначає Закон України«**Про телекомунікації**» (далі - Закон).

Згідно **статті 42** Закону суб'єкт господарювання здійснює діяльність у сфері телекомунікацій за умови його включення до реєстру операторів телекомунікацій, а у визначених законом випадках також за наявності відповідних ліцензій та/або дозволів.

Суб'єкти господарювання, які бажають здійснювати діяльність у сфері телекомунікацій, зобов'язані не менш як за місяць до її початку подати до НКРЗІ заяву про включення до реєстру операторів телекомунікацій за формою, що затверджується НКРЗІ.

У разі якщо вид діяльності, що має намір здійснювати суб'єкт господарювання, потребує отримання ліцензії та/або дозволів, то одночасно із заявою на реєстрацію подається заява та пакет документів на отримання ліцензії та/або дозволів.

Рішення про включення суб'єкта господарювання до реєстру операторів телекомунікацій приймається НКРЗІ протягом 10 робочих днів з дня реєстрації відповідної заяви суб'єкта господарювання.

Ліцензуванню підлягають такі види діяльності у сфері телекомунікацій, як надання послуг з технічного обслуговування та експлуатації телерадіомереж (телекомунікаційних мереж, мереж ефірного теле- і радіомовлення, проводового радіомовлення та телемереж).

Згідно **статті 45** Закону суб'єкт господарювання, який має намір здійснювати діяльність у сфері телекомунікацій, що ліцензується, особисто, через уповноважений ним орган чи особу або рекомендованим листом з описом вкладення звертається до НКРЗІ із заявою про видачу ліцензії за встановленим нею зразком

Згідно **статті 46** Закону НКРЗІ приймає рішення про видачу ліцензії або про відмову в її видачі у строк, що не перевищує 30 робочих днів від дати реєстрації заяви про видачу ліцензії.

Копія рішення про видачу ліцензії або про відмову у видачі ліцензії надсилається (видається) заявникові протягом 3-х робочих днів від дати його прийняття. Одночасно з рішенням про видачу ліцензії заявникові надсилається повідомлення про розмір плати за видачу ліцензії, порядок її оплати та отримання.

Згідно **статті 48** Закону НКРЗІ повинна оформити ліцензію не пізніше ніж за 3 робочі дні від дня надходження документа, що підтверджує внесення плати за видачу ліцензії.

Строк дії ліцензії встановлює НКРЗІ у ліцензії, але не може бути меншим ніж п'ять років.

У ліцензії зазначається територія, на якій здійснюється діяльність у сфері телекомунікацій на підставі цієї ліцензії.

Ліцензія підписується керівником НКРЗІ або його заступником та засвідчується печаткою цього органу.

Згідно **статті 70** Закону номерний ресурс надається оператору телекомунікацій НКРЗІ на підставі дозволу на термін дії відповідної ліцензії, а якщо вид діяльності не ліцензується - на строк не менше 5 років, для використання без права передачі іншим особам, крім випадків, визначених цим Законом.

Номерний ресурс - сукупність цифрових знаків, що використовуються для позначення (ідентифікації) мереж, послуг, пунктів закінчення мережі в телекомунікаційних мережах загального користування.

Заява оператора телекомунікацій щодо виділення номерного ресурсу розглядається НКРЗІ протягом місяця з моменту її реєстрації. Рішення НКРЗІ щодо виділення або відмови у виділенні номерного ресурсу приймається з урахуванням ефективності використання раніше виділеного номерного ресурсу і протягом трьох робочих днів доводиться до операторів телекомунікацій.

Дозвіл на використання номерного ресурсу видається оператору телекомунікацій після надання документів, що підтверджують оплату, протягом трьох днів.

Порядок ліцензування господарської діяльності у сфері телерадіомовлення визначає Закон України«**Про телебачення і радіомовлення**».

Згідно **статті 23** Закону ліцензування мовлення здійснюється виключно НРТР відповідно до порядку та вимог, встановлених цим Законом та Законом України «Про Національну раду України з питань телебачення і радіомовлення».

2. Ліцензування мовлення іноземних телерадіоорганізацій забороняється.

3. Залежно від організаційно-технологічних особливостей розповсюдження програм НРТР видає ліцензії на такі види мовлення:

- супутникове;

- ефірне;

- кабельне;

- проводове;

- багатоканальне.

4. Залежно від території розповсюдження програм визначається територіальна категорія мовлення та територіальна категорія каналу мовлення або багатоканальної телемережі:

- загальнонаціональне мовлення - мовлення не менше ніж на дві третини населення кожної з областей України;

- регіональне мовлення - мовлення на регіон (область, декілька суміжних областей), але менше ніж на половину областей України;

- місцеве мовлення - мовлення на один чи кілька суміжних населених пунктів, яке охоплює не більше половини території області;

- закордонне мовлення - мовлення на територію поза межами державного кордону України.

5. Цифрове мовлення з використанням радіочастотного ресурсу України ліцензується як багатоканальне мовлення.

7. На конкурсних засадах здійснюється видача ліцензій на:

- ефірне мовлення;

- багатоканальне мовлення з використанням радіочастотного ресурсу.

8. Без конкурсів здійснюється видача ліцензій на:

- супутникове мовлення;

- кабельне мовлення;

- проводове мовлення;

- ефірне мовлення на каналі мовлення багатоканальної ефірної телемережі у випадку, передбаченому частиною дев'ятою статті 22 цього Закону.

9. Ліцензія на мовлення, видана НРТР, є єдиним і достатнім документом, що надає ліцензіату право відповідно до умов ліцензії здійснювати мовлення, користуватися каналами мовлення за умови наявності у володільців радіоелектронних засобів передбачених законом дозволів на їх експлуатацію.

Згідно **статті 27** Закону ліцензія на мовлення видається не пізніше ніж у 10-денний строк після прийняття НРТР рішення про видачу ліцензії за умови сплати ліцензійного збору і є єдиною законною підставою на право мовлення.

Згідно **статті 28** Закону ліцензіат не має права розповсюджувати телерадіопрограми, здатні впливати на нормальний фізичний, розумовий або моральний розвиток дітей та юнацтва, і телерадіопрограми, що містять сцени, які викликають жах, сцени вбивства, насилля та звернені до сексуальних інстинктів.

Текстовий супровід не може містити брутальних слів, висловів тощо. Умови цього пункту не поширюються на кодовані системи багатоканального мовлення.

Згідно **статті 31** Закону за видачу або продовження строку дії ліцензій на мовлення та ліцензій провайдера програмної послуги сплачується ліцензійний збір.

Методика розрахунків розмірів ліцензійного збору за видачу або продовження строку дії ліцензій на мовлення, ліцензій провайдера програмної послуги, визначення розміру плати за переоформлення ліцензії та видачу дубліката ліцензії на мовлення, ліцензії провайдера програмної послуги затверджена постановою Кабінету Міністрів України від 13 квітня 2011 року № 412.

Згідно **статті 32** Закону ліцензія на мовлення видається заявнику на підставі рішення НРТР про видачу ліцензії не пізніше ніж у 10-денний термін після внесення ним ліцензійного збору, що підтверджується відповідним документом органу, що здійснює казначейське обслуговування бюджетних коштів. У разі, якщо НРТР прийняла рішення про інший порядок сплати ліцензійного збору, ліцензія видається заявнику не пізніше ніж у 30-денний термін після прийняття рішення про видачу ліцензії на мовлення.

Згідно **статті 36** Закону ліцензія на мовлення видається на строк, визначений НРТР відповідно до заяви про видачу ліцензії, але не менш як:

- для ефірного мовлення та багатопрограмного мовлення в багатоканальних телемережах - на 7 років;

- для супутникового, проводового, кабельного мовлення - на 10 років.

Після закінчення строку дії ліцензія на мовлення втрачає чинність, за винятком випадків, коли вчасно подана ліцензіатом заява про продовження дії ліцензії на мовлення не була розглянута НРТР у визначені цим законом строки.

У цих випадках ліцензія залишається чинною до прийняття НРТР рішення про продовження дії ліцензії або про відмову у продовженні дії ліцензії відповідно до вимог цього Закону.

Згідно **статті 38** Закону суб'єкти господарювання, які отримали ліцензію на мовлення, підлягають державній реєстрації як суб'єкти інформаційної діяльності, що здійснюється НРТР.

Державна реєстрація суб'єктів господарювання, які отримали ліцензії на мовлення, здійснюється шляхом внесення відповідних даних до Державного реєстру телерадіо-організацій України у 3-денний строк з дня видачі ліцензії на мовлення, який веде НРТР.

Доступ до Державного реєстру телерадіоорганізацій України є вільним. Порядок користування зазначеним реєстром і розмір плати за надання письмової інформації щодо даних цього реєстру встановлюються НРТР.

НРТР розміщує відомості Державного реєстру телерадіоорганізацій України на веб-сайті та двічі на рік публікує їх в офіційному бюлетені Національної ради.

Згідно **статті 40** Закону для організації діяльності (мовлення) кабельного телебачення і радіомовлення суб'єкт господарювання (оператор телекомунікацій чи кабельних мереж) повинен отримати ліцензію (дозвіл) у НРТР.

Ліцензування діяльності (мовлення) кабельного телебачення і радіомовлення здійснюється за реєстраційним принципом. Ліцензія видається без конкурсу на підставі заяви на термін 10 років.

Загальна концепція (принципи, підстави) добору програм для ретрансляції (пропозиції абонентам) є обов'язковим додатком до ліцензії на діяльність (мовлення) кабельного телебачення і радіомовлення. Цей додаток підлягає щорічній перереєстрації.

Для перереєстрації ліцензіат повинен подати до НРТР інформацію про виконання концепції добору програм протягом попереднього року.

Заява про видачу ліцензії провайдера програмної послуги розглядається і рішення щодо неї приймається у місячний термін з дня її надходження до НРТР.

Згідно **статті 43** Закону організація-ліцензіат має право розпочати мовлення протягом року з дня набрання ліцензією чинності. Про початок мовлення вона зобов'язана у 10-денний термін повідомити НРТР.

Також стаття 18 Закону України«**Про Національну раду України з питань телебачення і радіомовлення**» визначає, що ліцензування телерадіомовлення здійснює НРТР, а її ліцензія на телерадіомовлення є єдиним і достатнім документом дозвільного характеру, що надає право ліцензіату вести телерадіомовлення.

Розміри плати за видачу ліцензії на провадження діяльності у сфері телекомунікацій, що справляється у межах території однієї області, визначає постанова Кабінету Міністрів України від 16 червня 2004 року № 773«**Про розміри та порядок зарахування плати за видачу, переоформлення, видачу дубліката, копії ліцензії на провадження діяльності у сфері телекомунікацій і продовження строку її дії**»:

|  |  |
| --- | --- |
| Вид діяльності | Розмір оплати, грн. |
| Надання послуг з технічного обслуговування і експлуатації телекомунікаційних мереж ефірного теле- та радіомовлення, проводового радіомовлення та телемереж: |
| ефірного телемовлення | 1 700 |
| ефірного радіомовлення | 1 700 |
| проводового радіомовлення | 340 |
| телемереж (на територію окремого населеного пункту) | 4 250 |

«**Ліцензійні умови здійснення діяльності у сфері телекомунікацій з надання послуг з технічного обслуговування і експлуатації телекомунікаційних мереж, мереж ефірного теле- та радіомовлення, проводового радіомовлення та телемереж**» (далі – Ліцензійні умови) були затверджені рішенням НКРЗІ від 11 листопада 2010 року № 513, зареєстрованим в Міністерстві юстиції України 30 листопада 2010 року за № 1200/18495.

Згідно Ліцензійних умов суб'єкти господарювання провадять діяльність у сфері телекомунікацій з надання послуг з технічного обслуговування та експлуатації мереж тільки за наявності ліцензій.

Вони можуть отримати ліцензії на надання послуг з технічного обслуговування і експлуатації:

- мереж ефірного телемовлення (у заявлених регіонах);

- мереж ефірного радіомовлення (у заявлених регіонах);

- мереж проводового радіомовлення (у заявлених регіонах);

- телекомунікаційних мереж (в окремих населених пунктах).

Порядок ліцензування користування радіочастотним ресурсом визначає Закон України «**Про радіочастотний ресурс України**».

Згідно **статті 30** Закону користування радіочастотним ресурсом здійснюється на підставі:

1) ліцензій на користування радіочастотним ресурсом та дозволів на експлуатацію - суб'єктами господарювання, які користуються радіочастотним ресурсом для надання телекомунікаційних послуг;

2) ліцензій на мовлення, виданих НРТР, та дозволів на експлуатацію - суб'єктами господарювання, які користуються радіочастотним ресурсом для розповсюдження телерадіопрограм телерадіоорганізаціями;

3) дозволів на експлуатацію - спеціальними користувачами, технологічними користувачами та радіоаматорами.

Згідно **статті 31** Закону ліцензії на користування радіочастотним ресурсом видаються НКРЗІ суб'єктам господарювання, які користуються радіочастотним ресурсом для надання телекомунікаційних послуг. Строк дії ліцензії на користування радіочастотним ресурсом встановлюється НКРЗІ, але не може бути меншим 5 років.

Користування радіочастотним ресурсом телерадіоорганізаціями та провайдерами програмної послуги для потреб телебачення та радіомовлення здійснюється на підставі ліцензії на мовлення та не потребує ліцензії на користування радіочастотним ресурсом телерадіоорганізаціями та провайдерами програмної послуги.

Згідно **статті 32** Закону суб'єкт господарювання, який має намір здійснювати діяльність у сфері телекомунікацій, що передбачає використання радіочастотного ресурсу, до НКРЗІ з заявою про видачу ліцензії на користування радіочастотним ресурсом за формою.

Згідно **статті 33** Закону НКРЗІ повинна видати ліцензію на користування радіочастотним ресурсом не пізніше ніж через 3 робочі дні від дня надходження документа, що підтверджує внесення плати за видачу ліцензії.

Інформація про видачу ліцензій на користування радіочастотним ресурсом публікується в офіційному бюлетені НКРЗІ та на її веб-сайті.

Розміри плати за видачу ліцензії на користування радіочастотним ресурсом визначає Постанова Кабінет Міністрів України від 22 лютого 2006 року № 200 «**Про розміри плати за видачу, продовження строку дії, переоформлення, видачу дублікатів ліцензій на користування радіочастотним ресурсом України**».

Зазначені розміри визначають плату за видачу ліцензій із строком дії 5 років.

|  |  |  |  |
| --- | --- | --- | --- |
| Вид радіозв'язку | Діапазон радіочастот | Розмір плати за 1 МГц смуги радіо частот у кожному регіоні, грн. | Регіон |
| 11. Радіозв'язок супутникової рухомої та фіксованої радіослужб | 30-3000 МГц3-30 ГГц | 3400 | усі регіони |
| 13. Стільниковий радіозв'язок | 800-890 МГц | 51000085000 | м.КиївЗакарпатська |
| 14. Стільниковий радіозв'язок | 890-960 МГц | 1360000170000 | м.КиївЗакарпатська |

«**Ліцензійні умови користування радіочастотним ресурсом України**» були затверджені рішенням НКРЗІ від 19 серпня 2005 року № 53, зареєстрованим в Міністерстві юстиції України 20 жовтня 2005 року за № 1237/11517.

Згідно Ліцензійних умов суб'єкти господарювання, які користуються радіочастотним ресурсом для надання телекомунікаційних послуг, мають право здійснювати свою діяльність тільки за наявності ліцензій на користування радіочастотним ресурсом та відповідних дозволів на експлуатацію радіоелектронних засобів.

Ліцензія на здійснення діяльності у сфері телекомунікацій не дає права на користування радіочастотним ресурсом та експлуатацію РЕЗ.

Суб'єкти господарювання, які мають намір відповідно до Закону України «Про телекомунікації» здійснювати діяльність на підставі ліцензії на вид діяльності, отримують вказану ліцензію одночасно з ліцензією на користування радіочастотним ресурсом України.

У залежності від регіону користування радіочастотним ресурсом ліцензії поділяються на такі види:

- національна ліцензія - ліцензія, яка надає право на користування радіочастотним ресурсом в 12-ти й більше регіонах України (області, м.Київ);

- регіональна ліцензія - ліцензія, яка надає право на користування радіочастотним ресурсом в одному або декількох (не більше 11) регіонах України;

- територіальна ліцензія - ліцензія, яка надає право на користування радіочастотним ресурсом на обмеженій території регіону.

5 серпня 2015 року постановою Кабінету Міністрів України № 609 був затверджений  «**Перелік органів ліцензування**»:

|  |  |
| --- | --- |
| **Орган ліцензування** | **Вид господарської діяльності** |
| 3. НРТР | діяльність у галузі телебачення і радіомовлення |
| 7. НКРЗІ | діяльність у сфері телекомунікацій |
| 8. АдміністраціяДержспецзв'язку | надання послуг у галузі КЗІ (крім послуг ЕЦП) та ТЗІ за переліком, що визначається Кабінетом Міністрів України |
| 20. СБУ | діяльність, пов’язана з розробленням, виготовленням, постачанням СТЗ для зняття інформації з каналів зв’язку та інших технічних засобів негласного отримання інформації (критерії належності та перелік технічних засобів негласного отримання інформації визначаються КМУ за поданням СБУ) |

4 липня 2001 року постановою Кабінету Міністрів України № 756 був затверджений «**Перелік документів, які додаються до заяви про видачу ліцензії для окремого виду господарської діяльності**»:

|  |  |  |
| --- | --- | --- |
| **№** | **Вид господарської діяльності** | **Документи, які додаються до заяви про видачу ліцензії для окремого виду господарської діяльності** |
| 9. | Розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівля спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації | відомості за підписом заявника - суб'єкта господарювання (за формою, встановленою ліцензійними умовами) про наявність: |
| матеріально-технічної бази, необхідної для провадження відповідного виду господарської діяльності та її стан; |
| спеціалістів із зазначенням їх освітнього і кваліфікаційного рівня та допуску до державної таємниці, необхідних для провадження відповідного виду господарської діяльності; |
| спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею |
| засвідчена в установленому порядку копія домовленості про співробітництво між заявником - суб'єктом господарювання та оперативним підрозділом, який провадить оперативно-розшукову діяльність |
| 10. | Надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівля криптосистемами і засобами криптографічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України) | відомості за підписом заявника - суб'єкта господарювання (за формою, встановленою ліцензійними умовами) про наявність: |
| спеціалістів із зазначенням їх освітнього і кваліфікаційного рівня та стажу роботи, необхідних для провадження відповідного виду господарської діяльності; |
| матеріально-технічної бази, необхідної для провадження відповідного виду господарської діяльності; |
| відповідних приміщень, засобів обчислювальної техніки, інформаційних та телекомунікаційних систем (комплексів), необхідних для провадження відповідного виду господарської діяльності, згідно з вимогами нормативних документів з питань криптографічного та/або технічного захисту інформації (у разі провадження виду господарської діяльності, пов'язаного з державною таємницею або конфіденційною інформацією, яка є власністю держави); |
| відповідних нормативно-правових актів, нормативних документів з питань стандартизації, а також внутрішніх положень та інструкцій, що регламентують провадження відповідного виду господарської діяльності; |
| власних або орендованих службових, виробничих приміщень, необхідних для провадження відповідного виду господарської діяльності; |
| державних замовлень, що пов'язані з криптографічним захистом інформації, до виконання яких передбачається залучити заявника - суб'єкта господарювання (у разі провадження виду господарської діяльності, пов'язаного з державною таємницею або конфіденційною інформацією, яка є власністю держави) |
| спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею |
| 12. | Надання послуг у галузі технічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України) | відомості за підписом заявника - суб'єкта господарювання (за формою, встановленою ліцензійними умовами) про наявність: |
| спеціалістів із зазначенням їх освітнього і кваліфікаційного рівня та стажу роботи, необхідних для провадження відповідного виду господарської діяльності; |
| засобів вимірювальної техніки та контролю, допоміжних засобів та обладнання, що забезпечують надання відповідних видів послуг, із зазначенням їх найменування, типу, заводського номера, дати проведення останньої повірки; |
| атестованих приміщень та/або об'єктів електронно-обчислювальної техніки із зазначенням їх найменування та категорії, а також ким і коли проведена атестація (у разі потреби); |
| нормативно-правових актів та нормативних документів з питань технічного захисту інформації, необхідних для провадження відповідного виду господарської діяльності; |
| спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею |

20 жовтня 2008 року наказом Адміністрації Держспецзв’язку № 173 був затверджений «**Стандарт надання адміністративної послуги з видачі та переоформлення ліцензії, видачі копій, дубліката ліцензії на право провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів КЗІ, надання послуг у галузі КЗІ (крім послуг ЕЦП), торгівлі криптосистемами і засобами КЗІ**».

26 грудня 2008  року наказом Адміністрації Держспецзв’язку № 221 був затверджений «**Стандарт надання адміністративної послуги з видачі, переоформлення ліцензій, видачі дублікатів та копій ліцензій на провадження господарської діяльності з розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів ТЗІ, надання послуг у галузі ТЗІ**».

18 травня 2011 року № 517постановою Кабінету Міністрів України  був затверджений «**Перелік послуг у галузі ТЗІ, господарська діяльність щодо надання яких підлягає ліцензуванню**»:

1. Оцінювання захищеності інформації.

2. Виявлення закладних пристроїв.

«**Ліцензійні умови провадження господарської діяльності з надання послуг у галузі ТЗІ (згідно з переліком, що визначається Кабінетом Міністрів України)**» були затверджені наказом Адміністрації Держспецз’язку від 14 жовтня 2014 року № 532, зареєстрованим в Міністерстві юстиції України 4 листопада 2014 року за № 1387/26164.

Провадження господарської діяльності з надання послуг, визначених цими Ліцензійними умовами, суб'єкт господарювання здійснює за умови наявності спеціалістів з повною чи базовою вищою освітою за напрямом підготовки «Інформаційна безпека» або повною чи базовою вищою інженерно-технічною освітою фахового спрямування відповідно до обраного виду послуг з додатковою підготовкою на курсах перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ за напрямами підготовки відповідно до обраного виду послуг.

Залежно від правового режиму доступу до інформації встановлюються особливі умови надання послуг з технічного захисту:

- усіх видів інформації, у тому числі що становить державну таємницю;

- інформації, що не становить державної таємниці.

Разом з тим, згідно «**Положення про дозвільний порядок проведення робіт з ТЗІ для власних потреб**», затвердженого наказом ДСТСЗІ СБУ від 23 лютого 2002 року № 9, зареєстрованим в Міністерстві юстиції України 13 березня 2002 року за № 245/6533, органи державної влади та місцевого самоврядування, які мають намір проводити роботи у галузі ТЗІ для власних потреб, можуть отримати такий дозвіл від Адміністрації Держспецз’язку у разі виконання вимог цього Положення. За відсутності у державного органу такого дозволу ці роботи повинні виконуватись тільки установою, що має ліцензію на право провадження діяльності у галузі ТЗІ.

25 травня 2011 року постановою Кабінету Міністрів України № 543був затверджений «**Перелік послуг у галузі КЗІ (крім послуг ЕЦП), господарська діяльність з надання яких підлягає ліцензуванню»**:

1. Складення конструкторської та іншої технічної документації до криптосистем і засобів криптографічного захисту інформації.

2. Монтаж (встановлення), налаштування, технічне обслуговування (супроводження) криптосистем і засобів КЗІ.

Тою же постановою був затверджений і «**Перелік криптосистем і засобів криптографічного захисту інформації, торгівля якими підлягає ліцензуванню**»:

1. Криптосистеми, комплекси, обладнання, устаткування, приладдя, апаратура, блоки, вузли, модулі, інтегральні схеми та інші засоби, спеціально призначені для КЗІ, розроблені або модифіковані із застосуванням цифрової техніки, що реалізують криптографічні алгоритми з довжиною криптографічного ключа, що перевищує 56 біт для симетричних алгоритмів або 512 біт для асиметричних алгоритмів обміну (розподілу) ключами, або 112 біт для алгоритмів по еліптичній кривій.

2. Програмне забезпечення, спеціально розроблене або модифіковане для розроблення, виробництва чи використання криптосистем і засобів КЗІ, які мають характеристики відповідно до позиції 1 цього переліку, та/або має характеристики або може виконувати чи відтворювати функції криптосистем і засобів КЗІ відповідно до позиції 1 цього переліку

Виняток складають криптосистеми та засоби КЗІ, криптографічні функції яких не можуть бути змінені самостійно користувачами, розроблених для встановлення користувачем самостійно без допомоги з боку постачальника та технічна документація (опис застосованого криптографічного алгоритму, протоколів взаємодії, інтерфейсів тощо) яких є доступною, зокрема для перевірки.

«**Ліцензійні умови провадження господарської діяльності з надання послуг у галузі КЗІ (крім послуг ЕЦП), торгівлі криптосистемами і засобами КЗІ (згідно з переліком, що визначається Кабінетом Міністрів України)**» були затверджені наказом Адміністрації Держспецз’язку від 14 жовтня 2014 року № 531, зареєстрованим в Міністерстві юстиції України 3 листопада 2014 року за № 1380/26157.

Ліцензіат здійснює облік результатів ліцензованої діяльності у галузі КЗІ за господарськими договорами (контрактами) в пронумерованому, прошнурованому та скріпленому печаткою суб’єкта господарювання журналі обліку наданих (виконаних) послуг (робіт) з ліцензованої діяльності у галузі КЗІ.

Ліцензіат до 1 лютого наступного року письмово інформує Адміністрацію Держспецзв’язку про результати ліцензованої діяльності у галузі КЗІ за формою обліку результатів ліцензованої діяльності у галузі КЗІ, який ведеться у відповідному журналі згідно з пунктом 2.13.

Залежно від правового режиму доступу до інформації встановлюються такі особливі умови провадження ліцензованої діяльності у галузі криптографічного захисту:

- інформації, що становить державну таємницю;

- службової інформації.

«**Ліцензійні умови провадження господарської діяльності з розроблення, виготовлення СТЗ для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі СТЗ для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації**» були затверджені наказом Центрального управління СБУ від 30 січня 2011 року № 35, зареєстрованим в Міністерстві юстиції України 23 лютого 2011 року за № 225/18963.

Роділ 2 Ліцензійних умов визначає господарську діяльність з розроблення, виготовлення та торгівлі СТЗ, що підлягають ліцензуванню:

- розроблення СТЗ для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації;

- виготовлення СТЗ для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації;

- торгівля СТЗ для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації.

**10. Нормативно-правові акти з державної експертизи**

**у сферах інформаційної безпеки**

Правові, організаційні і фінансові основи експертної діяльності в науково-технічній сфері визначає Закон України «**Про наукову і науково-технічну експертизу**» (далі - Закон).

Згідно **статті 1** Закону наукова і науково-технічна експертиза (далі - експертиза) - це діяльність, метою якої є дослідження, перевірка, аналіз та оцінка науково-технічного рівня об'єктів експертизи і підготовка обгрунтованих висновків для прийняття рішень щодо таких об'єктів.

 Експертиза у сфері науково-технічних розробок та дослідно-конструкторських робіт (далі - НДР), фундаментальних і прикладних досліджень, у тому числі на стадії їх практичного застосування, проводиться науково-дослідними організаціями та установами, вищими навчальними закладами, іншими організаціями та окремими юридичними і фізичними особами, які акредитовані на цей вид діяльності.

Згідно **статті 2** Закону основними завданнями експертизи є:

- об'єктивне, комплексне дослідження об'єктів експертизи;

- перевірка відповідності об'єктів експертизи вимогам і нормам чинного законодавства;

- оцінка відповідності об'єктів експертизи сучасному рівню наукових і технічних знань, тенденціям науково-технічного прогресу, принципам державної науково-технічної політики, вимогам екологічної безпеки, економічної доцільності;

- аналіз рівня використання науково-технічного потенціалу, оцінка результативності НДР;

- прогнозування науково-технічних, соціально-економічних і екологічних наслідків реалізації чи діяльності об'єкта експертизи;

- підготовка науково обгрунтованих експертних висновків.

Згідно **статті 4** Закону суб'єктами експертизи є замовники, організатори експертизи та експерти.

Замовниками експертизи можуть бути державні органи і органи місцевого самоврядування, підприємства, установи і організації, громадяни, заінтересовані у
проведенні такої експертизи.

Замовники експертизи формують завдання на проведення експертизи, забезпечують оплату витрат на її проведення та праці експертів або послуг організаторів експертизи.

Організаторами експертизи є фізичні та юридичні особи, які на підставі доручення або договору з замовниками організовують та проводять експертизу і подають експертні висновки.

Експертизу можуть проводити:

- органи виконавчої влади у межах своєї компетенції;

- підприємства, установи та організації всіх форм власності, тимчасові творчі колективи, що здійснюють наукову і науково-технічну діяльність, спеціалізовані експертні організації;

- окремі експерти, групи експертів та експертні ради.

Експертами є фізичні особи, які мають високу кваліфікацію, спеціальні знання і безпосередньо здійснюють наукову чи науково-технічну експертизу та несуть персональну відповідальність за достовірність і повноту аналізу, обгрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи.

Не дозволяється поєднання в одній особі функцій автора розробки чи іншим чином заінтересованої особи та її експерта.

Згідно **статті 5** Закону об'єктами експертизи можуть бути:

- діючі об'єкти техніки та промисловості, споруди, природні об'єкти тощо, стосовно яких виникає потреба отримати науково обгрунтовані експертні висновки;

- проекти, програми, пропозиції різного рівня, щодо яких необхідно провести науково обгрунтований аналіз і дати висновок про доцільність їх прийняття, впровадження, подальшого використання тощо.

Згідно **статті 6** Закону підставами для проведення експертизи є:

- рішення органів виконавчої влади та органів місцевого самоврядування, прийняті в межах їх повноважень;

- договори на проведення експертизи, укладені підприємствами, установами та організаціями, фізичними особами.

Згідно **статті 7** Закону фізичні особи, які на постійній або професійній основі здійснюють діяльність, пов'язану з наданням експертних послуг, крім осіб, зазначених у частині другій цієї статті, та юридичні особи, статутом яких передбачено таку діяльність, повинні пройти державну акредитацію і отримати свідоцтво, що підтверджує кваліфікацію його отримувача з питання організації та проведення експертизи.

Порядок проведення державної акредитації фізичних і юридичних осіб на право проведення експертизи, форму свідоцтва на право проведення такої експертизи та перелік документів державного зразка, що дають фізичним особам право на провадження експертної діяльності і надання експертних послуг без отримання свідоцтва, визначаються центральним органом виконавчої влади, що забезпечує формування державної політики у сфері науки.

Державну акредитацію осіб на право проведення експертизи проводить центральний орган виконавчої влади, що реалізує державну політику у сфері наукової, науково-технічної діяльностію.

Згідно **статті 10** Закону державну експертизу проводять:

- органи виконавчої влади;

- державні установи (підприємства, організації).

Згідно **статті 13** Закону об'єкти експертизи можуть передаватися на попередню, первинну, повторну, додаткову, контрольну експертизи.

Згідно **статті 14** Закону попередня експертиза проводиться з метою з'ясування відповідності формальних ознак об'єкта експертизи встановленим нормам і правилам технічної та екологічної безпеки, вимогам стандартів тощо.

Згідно **статті 15** Закону первинна експертиза передбачає здійснення всіх необхідних заходів у процесі підготовки обгрунтованого висновку щодо об'єктів експертизи, які передаються заінтересованими фізичними та юридичними особами - замовниками експертизи на аналіз та оцінку експертним організаціям або експертам.

Згідно **статті 16** Закону повторна експертиза може проводитися:

- у разі порушення встановлених вимог і правил під час проведення первинної експертизи;

- на вимогу замовника експертизи чи автора розробки за наявності обгрунтованих претензій до висновку первинної експертизи.

Згідно **статті 17** Закону додаткова експертиза проводиться стосовно об'єктів, щодо яких відкрилися нові наукові і науково-технічні обставини.

Згідно **статті 18** Закону контрольна експертиза здійснюється з ініціативи замовника для перевірки висновків первинної експертизи або з ініціативи фізичних чи юридичних осіб, заінтересованих у спростуванні окремих положень, частин або в цілому висновків раніше проведених експертиз.

Згідно **статті 22** Закону основним юридичним документом, що регламентує відносини між замовником і організатором у сфері експертизи, є договір на її проведення.

Згідно **статті 34** Закону у сфері державної експертизи фінансову підтримку діяльності експертів забезпечує держава.

В усіх інших випадках матеріальне стимулювання експертів здійснюється за рахунок коштів замовника експертизи або інших організацій і установ за дорученням замовника.

Максимальний розмір коштів, що спрямовуються на покриття витрат на експертизу, не може перевищувати:

- для експертизи наукових і науково-технічних програм та проектів - 1,5 % кошторису витрат, передбачених на їх виконання;

- для експертизи виконаних науково-дослідних або проектно-конструкторських робіт - 3 % вартості обсягу виконаних робіт.

24 квітня 1998 року наказом Міністерства України у справах науки і технологій № 131, зареєстрованим в Міністерстві юстиції України 16 липня 1998 року за № 462/2902, було затверджено «**Положення про організацію та проведення наукової та науково-технічної експертизи**» (далі - Положення), яке встановлює такі вимоги:

1.11. Під час проведення експертизи встановлюються відповідність об'єктів експертизи вимогам національної економічної, оборонної та екологічної безпеки; науково-технічна новизна об'єктів експертизи; відповідність технологій, обладнання, устаткування кращим вітчизняним та зарубіжним аналогам; відповідність вимогам чинних стандартів, вимогам технічної безпеки; реальність термінів упровадження об'єктів експертизи та актуальність об'єктів на момент її завершення; ступінь економічної ефективності, матеріаломісткості технологій і обладнання.

**2. Види експертизи**

2.1. Експертиза може бути попередня, первинна, повторна, додаткова та контрольна.

2.7. Експертиза набуває статусу державної, якщо вона провадиться державними органами або на виконання їх доручень академіями наук.

**3. Координація діяльності суб'єктів експертизи**

3.1. Замовник експертизи подає до організатора експертизи заяву про проведення експертизи разом з супровідними документами щодо об'єкта експертизи.

Замовник експертизи формує завдання на проведення експертизи, забезпечує оплату витрат на її проведення.

3.6. Основним документом, що регламентує стосунки між замовником і організатором експертизи, є договір на її проведення. До договору додаються документи, які визначають об'єкт експертизи та забезпечують її проведення. Документи подаються на паперовому та магнітному носіях.

3.8. Організатор веде реєстр поданих проектів та надає авторам проектів довідку про реєстраційний номер та консультації з процедурних питань.

**4. Вимоги до експертного висновку**

4.1. Висновок експертизи складається із вступної, констатувальної та заключної частин. Чітка і ясна оцінка проекту у висновках експертизи (за одним із вказаних варіантів) є обов'язковою. Висновок, що не має такої оцінки, не може бути підписаний чи затверджений уповноваженими посадовими особами.

4.2. Підготовлений експертний висновок підписується експертом і керівником організації (установи) - організатором експертизи.

4.6. Висновок експертизи зберігає чинність протягом терміну, визначеного договором на її проведення. Після закінчення терміну дії висновку експертизи відповідні об'єкти експертизи підлягають повторній експертизі.

**5. Права та обов'язки експертів**

5.1. Експертами є фізичні особи, які мають сертифікат на проведення експертизи або інший документ, що його заміняє, високу кваліфікацію, знання з даної галузі науки або техніки, володіють методикою науково-експертної оцінки, безпосередньо здійснюють експертизу та персонально відповідають за достовірність, повноту, об'єктивність аналізу, обгрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи та чинного законодавства.

Експерти залучаються на підставі договорів або контрактів.

5.4. Експерт письмово оформляє висновок експертизи. Не допускається повторне проведення експертизи щодо конкретного проекту одним і тим самим експертом.

**6. Порядок організації та проведення експертизи**

6.3. Термін проведення експертизи визначається замовником і, як правило, не повинен перевищувати 30 календарних днів. У разі потреби, за погодженням із замовником, термін може бути продовжений до 45 календарних днів. У виняткових випадках, залежно
від складності проблеми, - до 90 календарних днів.

Термін проведення експертизи в кожному окремому випадку визначається договорами між виконавцями і замовниками експертизи.

6.4. Термін дії висновку експертизи визначається договором, але не перевищує 2 років від дня його видачі.

6.5. Проведення експертизи здійснюється за рахунок замовника експертизи. Сума коштів, спрямованих на проведення експертизи проектів, визначається договором на проведення експертизи, але не перевищує норми, встановлені Законом України «Про наукову і науково-технічну експертизу».

6.6. Розмір оплати експертів визначається згідно з «**Нормами оплати праці експертів, які залучаються для проведення державної наукової та науково-технічної експертиз, що проводяться за рахунок коштів державного бюджету**», затвердженими наказом Міністерства соціальної політики України від 8 травня 2013 року № 262, зареєстрованим у Міністерстві юстиції України 20 травня 2013 року за № 778/23310), або окремим договором.

6.7. Право на інтелектуальну власність, що може виникнути під час проведення експертизи, належить замовнику експертизи або визначається відповідно до договору на її проведення.

Головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах наукової та науково-технічної діяльностіє **Міністерство освіти та науки України** (далі – МОНУ).

Згідно вимог «Положення про МОНУ» (далі - Положення), затвердженого постановою Кабінету Міністрів України від 16 жовтня 2014 року № 630, МОНУ відповідно до покладених на нього завдань:

29) здійснює керівництво системою наукової і науково-технічної експертизи;

37) визначає порядок та проводить державну акредитацію фізичних і юридичних осіб на право проведення наукової та науково-технічної експертизи, а також визначає форму свідоцтва на право проведення зазначеної експертизи та перелік документів державного зразка, що дають фізичним особам право на провадження експертної діяльності і надання експертних послуг без отримання свідоцтва;

74) забезпечує розвиток системи наукової і науково-технічної експертизи проектів державних, міжнародних та регіональних програм.

Проведення незалежної експертизи наукових, науково-технічних пропозицій, проектів і програм, науково-дослідних та дослідно-конструкторських робіт, інноваційних проектів, програм інформатизації та інших об'єктів на запит замовника здійснює **Державний інститут науково-технічної та інноваційної експертизи** (далі - Інститут), утворений розпорядженням Кабінету Міністрів України від 24 жовтня 2011 року № 1042-р.

#### *Офіційний сайт Інституту: www.dintie.org.*

16 травня 2007 року наказом Адміністрації Держспецзв’язку № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087, було затверджене «**Положення про державну експертизу в сфері ТЗІ**», яке визначає такі вимоги:

1.2. Державна експертиза в сфері ТЗІ (далі - експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам НД ТЗІ та можливості їх використання для забезпечення ТЗІ.

1.3. Дія цього Положення поширюється на всіх юридичних та фізичних осіб, які є суб'єктами експертизи.

Суб'єктами експертизи є:

- юридичні та фізичні особи - власники (розпорядники) АС, технічних і програмних засобів, які реалізують функції ТЗІ, - замовники експертизи (далі - Замовники);

- Адміністрація Держспецзв'язку (далі - Адміністрація);

- підрозділи Держспецзв'язку, підприємства, установи та організації, які проводять експертизу (далі - Організатори);

- державні органи, які проводять експертизу в сфері свого управління;

- фізичні особи - виконавці експертних робіт з ТЗІ (далі - Експерти).

1.4. Об'єктами експертизи є:

- КСЗІ, які є невід'ємною складовою частиною АС;

- технічні та програмні засоби, які реалізують функції ТЗІ (далі - засоби ТЗІ).

1.5. Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам нормативних документів із ТЗІ і проводиться шляхом експертних випробувань або шляхом аналізу декларації про відповідність КСЗІ вимогам НД ТЗІ (далі - декларація).

Експертиза засобів ТЗІ проводиться шляхом експертних випробувань.

1.6. Експертиза КСЗІ шляхом аналізу декларації проводиться, якщо:

- КСЗІ створено в АС класу «1», в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці, і де використовуються засоби захисту інформації, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ.

У всіх інших випадках експертиза КСЗІ в АС проводиться шляхом експертних випробувань, а саме:

- КСЗІ створено в АС класу «1», в якій передбачається обробка інформації, що становить державну та іншу передбачену законом таємницю, і де використовуються засоби захисту інформації, які не мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ;

- КСЗІ створено в АС класу «2» або «3»;

- КСЗІ створено в АС з використанням засобів захисту інформації, які не мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ.

1.7. Експертиза може бути первинною, додатковою та контрольною.

Первинна експертиза є основним видом експертизи і передбачає виконання Організатором усіх потрібних заходів, визначених у розділі 3 цього Положення, для підготовки та прийняття рішення щодо об'єкта експертизи.

Додаткова експертиза проводиться стосовно об'єктів експертизи, щодо яких відкрилися нові наукові та науково-технічні обставини або в зв'язку з закінченням терміну дії документів, що засвідчують результати експертизи.

Контрольна експертиза проводиться іншим Організатором з ініціативи Замовника за наявністю у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи Адміністрації для перевірки висновку первинної чи додаткової експертизи.

**3. Порядок організації та проведення експертизи**

3.1. Для проведення експертизи шляхом експертних випробувань Замовник надсилає заяву на ім'я Голови Держспецзв'язку (крім випадків, передбачених у розділі 5 цього Положення) про проведення експертизи КСЗІ в ІТС або засобу ТЗІ, а шляхом аналізу декларації - декларацію про відповідність КСЗІ вимогам НД ТЗІ (додаток 3), формуляр ІТС і акт про завершення робіт зі створення КСЗІ згідно з керівним документом із стандартизації РД 50-34.698-90 «**Автоматизированные системы. Требования к содержанию документов**».

3.2. З метою розгляду декларацій і заяв, координації заходів і прийняття рішень щодо проведення експертиз в Адміністрації створюється Експертна рада з питань державної експертизи у сфері ТЗІ (далі - Експертна рада).

3.3. За результатами аналізу декларації і поданих разом із нею документів Експертна рада в місячний строк приймає рішення про реєстрацію декларації. Зареєстровану декларацію та інші подані документи Адміністрація повертає Замовнику.

3.4. У разі ненадання документів, зазначених у пункті 3.1 цього розділу, неповноти наданих у них відомостей або невідповідності порядку створення КСЗІ вимогам НД ТЗІ Адміністрація в місячний строк повертає Замовнику декларацію для доопрацювання.

3.5. Адміністрація має право в установленому порядку зупинити дію декларації або скасувати її реєстрацію.

3.6. Строк дії зареєстрованої декларації є необмеженим. У разі внесення змін, не передбачених у технічному завданні на створення КСЗІ, Замовник зобов'язаний надіслати на ім'я Голови Держспецзв'язку декларацію в порядку, передбаченому в пункті 3.1 цього розділу.

3.7. За результатами розгляду заяви Експертна рада у місячний термін приймає рішення про доцільність проведення експертизи та визначає її Організатора.

3.8. У разі наявності у Замовника обґрунтованих претензій щодо порядку проведення або результатів експертизи він може звернутися до Адміністрації з пропозицією щодо здійснення контролю за проведенням Організатором експертних випробувань або із заявою на ім'я Голови Держспецзв'язку про проведення контрольної експертизи.

3.10. Основним документом, що регламентує відносини між Замовником і Організатором, є укладений між ними договір на проведення експертизи.

3.12. Результати, матеріали, висновки експертизи та створене або придбане за кошти Замовника матеріально-технічне забезпечення є його власністю, якщо інше не передбачено договором між Замовником і Організатором.

3.13. Термін проведення експертизи визначається договором і не повинен перевищувати 6 місяців. У випадку значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації та Замовника.

3.14. Список Експертів, які залучаються до виконання експертних робіт, визначається Організатором.

3.16. Організатор, за результатами аналізу наданих документів і з урахуванням загальних методик оцінювання задекларованих характеристик засобів ТЗІ і КСЗІ, формує програму і окремі методики проведення експертизи об'єкта та розробляє, у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань і відповідне програмно-технічне забезпечення.

3.17. Програма проведення експертизи узгоджується із Замовником та Департаментом з питань захисту інформації в ІТС (далі – ДЗІ ІТС) Адміністрації, а окремі методики - з зазначеним департаментом.

3.18. Терміни розробки окремої методики та необхідних програмно-апаратних засобів залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи.

3.19. Під час проведення експертизи кожний Експерт виконує експертні роботи тільки за дорученням Організатора та у відповідності з визначеною окремою методикою.

3.20. Результати роботи оформлюються у вигляді протоколу виконання робіт (додаток 6) за підписом Експертів, які її виконували. Протокол затверджується Організатором.

3.23. У протоколі можуть бути зафіксовані особливі думки Експертів відносно результатів виконаних робіт.

3.24. У разі виявлення невідповідності об'єкта експертизи вимогам НД ТЗІ Організатор може запропонувати Замовнику виконати доробку об'єкта.

3.26. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.

3.27. Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку.

3.28. Висновки щодо кожного пункту окремої методики, а також особливі думки Експертів, зафіксовані в протоколах, включаються до Експертного висновку як складові частини без унесення до них будь-яких змін.

3.29. За результатами проведених робіт Організатор складає Експертний висновок відповідного змісту щодо відповідності об'єкта експертизи вимогам НД ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації.

**4. Порядок надання Експертного висновку та Атестата**

4.1. Експертний висновок на засіб ТЗІ розглядається Експертною радою і, у разі затвердження результатів експертизи, реєструється та видається Замовнику.

4.2. На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності за підписом Голови Держспецзв'язку.

4.3. Адміністрація має право в установленому порядку зупинити дію або скасувати Експертний висновок або Атестат.

**5. Особливості проведення експертиз КСЗІ державними органами**

5.1. Адміністрація надає державному органу повноваження з організації та проведення первинних або додаткових експертиз КСЗІ в ІТС шляхом експертних випробувань за умови погодження з Адміністрацією порядку їх здійснення.

5.2. Державні органи, які мають дозвіл Адміністрації на проведення робіт з ТЗІ для власних потреб та отримали від Адміністрації зазначені повноваження:

- здійснюють організацію та проведення експертиз КСЗІ в ІТС у сфері свого управління шляхом експертних випробувань;

- видають Атестат відповідності, який реєструється Адміністрацією.

19 березня 2009 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «**Стандарт надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ**», метою якого є підвищення якості надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ.

До заяви про проведення первинної або додаткової експертизи додаються:

- технічне завдання на створення КСЗІ в ІТС;

- формуляр ІТС.

Прийняте Адміністрацією Держспецзв’язку рішення про можливість проведення експертизи КСЗІ в ІТС за заявою, поданою одержувачем, та про визначення організатора експертизи повідомляється одержувачу у термін, що не повинен перевищувати 15 робочих днів.

Атестат відповідності КСЗІ в ІТС вимогам нормативних документів з ТЗІ оформляється протягом 5 робочих днів на підставі позитивного рішення Адміністрації Держспецзв’язку щодо результатів експертизи. Зареєстрований атестат надсилається організатору експертизи для видачі одержувачу разом з експертним висновком.

Адміністративна послуга з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ надається безоплатно.

Інформація щодо порядку проведення експертизи КСЗІ в ІТС та форми заяв про проведення експертизи КСЗІ в ІТС розміщені на офіційному сайті Держспецзв’язку в мережі Інтернет (електронна адреса: www.dsszzi.gov.ua, розділ «Діяльність» - «Експертиза» - «Технічний захист інформації»).

1 жовтня 2010 року наказом Адміністрації Держспецзв’язку № 291 було затверджене «**Положення про Експертну раду з питань державної експертизи в сфері ТЗІ**», яка є постійно діючим колегіальним органом Адміністрації Держспецзв'язку з питань організації та проведення державної експертизи у сфері ТЗІ.

Метою діяльності Експертної ради є координація заходів з дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативно-правових актів і НД ТЗІ та оцінювання результатів експертизи.

Формою роботи Експертної ради є засідання, які проводяться за потреби, але не рідше одного разу на місяць.

На підставі рішень Експертної ради про затвердження результатів державних експертиз оформляються, реєструються та надаються замовникам Експертні висновки на засоби ТЗІ, оформляються та видаються Атестати відповідності КСЗІ.

16 квітня 2008 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «**Порядок формування Реєстру організаторів державної експертизи у сфері ТЗІ та Реєстру експертів з питань ТЗІ**»

До реєстру Організаторів вносяться всі підрозділи Держспецзв'язку, підприємства, установи та організації, визначені Експертною радою як Організатори, за результатами розгляду заяв замовників про проведення державної експертизи у сфері ТЗІ.

До реєстру Експертів вносяться всі фахівці з питань ТЗІ, які залучаються Організаторами до виконання експертних робіт під час проведення державних експертиз у сфері ТЗІ.

Картки реєстрації Організатора та Експертів зберігаються в окремій справі ДЗІ ІТС відповідно до встановлених у Держспецзв'язку вимог щодо ведення діловодства.

25 березня 2011 року наказом Адміністрації Держспецзв'язку № 65 був затверджений НД ТЗІ 2.6-001-11 «**Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІТС**», який складається з таких основних розділів:

- вступні положення щодо порядку проведення експертизи засобів ТЗІ від несанкціонованого доступу та КСЗІ;

- опис порядку проведення робіт з експертизи засобів ТЗІ від несанкціонованого доступу;

- опис порядку проведення робіт з експертизи КСЗІ.

Він має такі додатки:

- рекомендації щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи КСЗІ;

- вимоги щодо змісту програми проведення експертизи КСЗІ в ІТС;

- вимоги щодо змісту методики проведення експертизи КСЗІ в ІТС;

- рекомендації щодо викладення змістовної частини протоколу експертизи засобу ТЗІ від несанкціонованого доступу;

- рекомендації щодо викладення змістовної частини протоколу експертизи КСЗІ;

- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи засобу ТЗІ від несанкціонованого доступу

- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи КСЗІ.

23 червня 2008 року наказом Адміністрації Держспецзв’язку № 100, зареєстрованим в Міністерстві юстиції України 16 липня 2008 року за № 65115342, було затверджене «**Положення про державну експертизу у сфері КЗІ**»:

Використані в цьому Положенні терміни вживаються в такому значенні:

- державна експертиза у сфері КЗІ (далі - експертиза) - діяльність, метою якої є підготовка обґрунтованих висновків і надання рекомендацій для прийняття рішення про використання об'єктів експертизи та яка передбачає перевірку відповідності об'єктів експертизи вимогам нормативних документів та оцінку рівня захисту інформації об'єктами експертизи;

- експертний висновок - документально оформлений результат експертизи, який надається Адміністрацією Держспецзв'язку за результатами експертних досліджень;

- експертні дослідження - дослідження та аналіз конкретних властивостей об'єкта експертизи з метою перевірки його відповідності вимогам нормативних документів та оцінки рівня захисту інформації цим об'єктом.

Суб'єктами експертизи є:

- замовники експертизи;

- Адміністрація Держспецзв'язку;

- експертні заклади.

Експертними закладами можуть бути підприємства, установи та організації, які мають ліцензію на право провадження діяльності в галузі КЗІ щодо експертизи засобів КЗІ.

Організація експертизи здійснюється безкоштовно Адміністрацією Держспецзв'язку.

Експертні дослідження проводять експертні заклади або Адміністрація Держспецзв'язку за договорами на проведення експертних досліджень.

Для координації та здійснення експертизи в Адміністрації Держспецзв'язку створюється Експертна комісія з питань проведення державної експертизи в сфері КЗІ Держспецзв'язку (далі - Експертна комісія).

***Порядок організації та проведення експертизи***

Експертний заклад призначається Адміністрацією Держспецзв'язку з урахуванням пропозицій замовника. Рішення Адміністрації Держспецзв'язку надсилається замовнику та експертному закладу.

Договір на проведення експертних досліджень між замовником та експертним закладом укладається після отримання ними рішення Адміністрації Держспецзв'язку.

Процедури відбору та ідентифікації зразків засобів КЗІ проводяться після ухвалення рішення Адміністрації Держспецзв'язку. Ідентифікація зразків оформлюється актом ідентифікації зразків для проведення державної експертизи у сфері КЗІ.

Відбір зразків оформлюється актом відбору зразків для проведення державної експертизи у сфері КЗІ. Відібрані зразки разом з комплектом документів та матеріалів передаються Адміністрацією Держспецзв'язку до експертного закладу для проведення експертних досліджень.

***Порядок підготовки експертного висновку***

Для проведення експертних досліджень експертними закладами у місячний термін з моменту укладання договору на проведення досліджень та отримання об'єкта експертизи і необхідного комплекту документів розробляються програми та методики проведення експертних досліджень.

За результатами експертних досліджень експертні заклади готують, затверджують та подають до Адміністрації Держспецзв'язку протоколи експертних досліджень. Зміст протоколів експертних досліджень повинен відповідати вимогам програми та методики проведення експертних досліджень.

Експертна комісія протягом місяця з дня отримання протоколів експертних досліджень розглядає їх на предмет відповідності програмі та методиці проведення експертних досліджень, повноти, об'єктивності, достатності та інших характеристик, а також готує рішення.

У разі відповідності протоколів експертних досліджень програмі та методиці проведення експертних досліджень на підставі рішення Експертної комісії Адміністрацією Держспецзв'язку готується та надсилається замовнику експертний висновок. Термін підготовки та надсилання замовнику експертного висновку не повинен перевищувати 20 робочих днів з дати ухвалення рішення Експертною комісією.

Термін дії експертного висновку визначається з урахуванням криптографічних якостей засобу КЗІ, терміну дії нормативних документів, умов та граничного терміну експлуатації засобу КЗІ, але не більше термінів, зазначених у додатку до цього Положення.

Експертний висновок може бути виданий на один зразок засобу КЗІ, партію засобів, а також засіб, що виробляється серійно, за наявності технічних умов на нього.

Експертні висновки, термін дії яких закінчився, утрачають чинність.

Підставами для анулювання експертного висновку є:

- закінчення терміну дії експертного висновку;

- несанкціоноване внесення змін в об'єкт експертизи або документацію на нього;

- зміна (порушення) технології виробництва засобів КЗІ.

**Варіанти схем проведення експертизи засобів КЗІ**

|  |  |  |  |
| --- | --- | --- | --- |
| **Засоби, що проходять** | **Контроль за виробництвом** | **Експертні дослідження** | **Документ, що видається, термін його дії** |
| Одиночні засоби | Не проводиться | Здійснюються для кожного засобу | Експертний висновок на кожний засіб терміном дії до 3 років |
| Партія засобів | Не проводиться | Здійснюються для засобів, відібраних у порядку та кількості, визначених Адміністрацією | Експертний висновок на партію засобів терміном дії до 3 років |
| Засоби, що виготовляються серійно | Здійснюється | Здійснюються для засобів, відібраних у порядку та кількості, визначених Адміністрацією | Експертний висновок на засоби, що виготовлені серійно, терміном дії до 5 років |

29 листопада 2008 року наказом Адміністрації Держспецзв’язку № 200 був затверджений «**Стандарт надання адміністративної послуги з організації державної експертизи у сфері КЗІ**», метою якого є підвищення якості надання адміністративної послуги з видачі експертних висновків на засоби КЗІ.

Експертні дослідження технічних засобів (виробів) на предмет їх віднесення до СТЗ проводяться відповідно до базового нормативно-технічного документу – «**Загальна методика віднесення об’єктів до СТЗ негласного отримання інформації**» (для службового користування), зареєстрованого в Міністерстві юстиції України 2 березня 2011 року за № 17.0.01.

Експертні дослідження та судові експертизи проводяться державною спеціалізованою установою - **Українським науково-дослідним інститутом спеціальної техніки та судових експертиз СБУ**.

Методика визначає загальні принципи проведення експертних досліджень, встановлює й регламентує порядок застосування методів та процедур проведення експертного дослідження. Це дозволяє визначити й обґрунтувати необхідну й достатню сукупність технічних ознак, на підставі яких формулюється висновок експерта щодо віднесення технічного засобу до СТЗ. При проведенні судової експертизи (дослідження) основними критеріями віднесення засобу до СТЗ є технічна придатність та функціональна призначеність цього засобу, які встановлюються на підставі спеціальних знань судового експерта відповідно до вимог та у порядку, визначеному Методикою.

При цьому, до СТЗ відносяться технічні засоби, що можуть бути скритно застосовані для негласного отримання інформації у властивих для вирішення завдань оперативно-розшукової діяльності формах та методах.

Поняття «скритність» і «негласне отримання інформації» мають таке значення:

- негласне отримання інформації – процес скритного отримання інформації, що здійснюється без відома та згоди суб’єкта інформації;

- скритність - можливість конспіративного застосування технічного засобу, яка зумовлена ступенем захисту від виявлення фактів його встановлення та застосування.

Висновок державного експерта є результатом визначення технічних характеристик, функціональних можливостей та конструктивних особливостей наданого на дослідження технічного засобу, оцінки його якісних характеристик (скритність, негласність доступу до об’єкта інформаційної діяльності, прихованість керування, безвідмовність функціонування у певних умовах застосування), що притаманні певному типу СТЗ, найближчому аналогу до досліджуваного засобу.

Прикладами суттєвих конструктивних ознак, що визначають якісні характеристики певного виду СТЗ, є:

- виконання відео-, аудіозаписуючого пристрою у вигляді звичайного побутового предмета;

- значна мінімізація розмірів відео-, аудіозаписуючого пристрою;

- конструктивна побудова технічного засобу, яка дозволяє здійснювати швидке та скритне розміщення на об’єкті;

- відсутність індикації про режими роботи технічного засобу;

- можливість отримання інформації за межами контрольованої зони об'єкта;

- мінімізація кількості та багатофункціональність елементів керування;

- розмір вхідного отвору для об’єктиву мікротелекамери, який забезпечує можливість його маскування;

- маскування місцезнаходження акустичного отвору мікрофону тощо.

**Рекомендована література**

**1. Конституція України**

**2. Закони України**

Про основи національної безпеки України

Про інформацію

Про Національну програму інформатизації

Про Концепцію Національної програми інформатизації

Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки

Про доступ до публічної інформації

Про захист персональних даних

Про електронний документообіг

Про електронний цифровий підпис

Про захист інформації в інформаційно-телекомунікаційних системах

Про захист суспільної моралі

Про організацію формування та обігу кредитних історій

Про державну таємницю

Про телекомунікації

Про радіочастотний ресурс

Про Національну систему конфіденційного зв'язку

Про телебачення і радіомовлення

Про суспільне телебачення і радіомовлення України

Про кінематографію

Про видавничу справу

Про бібліотеки і бібліотечну справу

Про друковані засоби масової інформації

Про авторське право і суміжні права

Про культуру

Про рекламу

Про адміністративні послуги

Про ліцензування певних видів господарської діяльності

Про основні засади державного нагляду (контролю) у сфері господарської діяльності

Про підтвердження відповідності

Про акредитацію органів з оцінки відповідності

Про стандартизацію

Про стандарти, технічні регламенти та процедури оцінки відповідності

Про наукову і науково-технічну експертизу

Про метрологію та метрологічну діяльність

Про оперативно-розшукову діяльність

Про Уповноваженого Верховної Ради України з прав людини

Про Державну службу спеціального зв’язку та захисту інформації України

Про Службу безпеки України

Про Національну Раду з питань телебачення і радіомовлення

Про Національний архівний фонд та архівні установи

**3. Кодекси України**

Цивільний кодекс України

Кодекс України про адміністративні правопорушення

Кримінальний кодекс України

**4. Укази Президента України**

Стратегія національної безпеки України«Україна у світі, що змінюється». Указ від 12.02.2007 № 105/2007 (в редакції Указу від 08.06.2012 № 389/2012)

Положення про технічний захист інформації в Україні. Указ від 27.09.1999 № 1229/99

Положення про порядок здійснення криптографічного захисту інформації в Україні. Указ від 22.05.1998 № 505/98

Про заходи щодо захисту інформаційних ресурсів держави. Указ від 10.04.2000 № 734/2000

Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі. Указ від 31.07.2000 № 928/2000

Про рішення Ради національної безпеки і оборони України «Про заходи щодо захисту національних інтересів у галузі зв'язку та телекомунікацій». Указ від 23.08.2001 № 731/2001

Про додержання прав людини під час проведення оперативно-технічних заходів. Указ від 07.11.2005 № 1556/2005

Про впорядкування виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв'язку. Указ від 13.04.2001 № 256/2001

Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації. УПУ від 14.12.2004 № 1483/2004

Про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади. Указ від 03.10.1992 № 493/92

Про Єдиний державний реєстр нормативних актів. Указ від 27.06.1996 № 468/96

Про рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Указ від 01.05.2014 № 449/2014

Положення про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки та оборони України. УПУ від 22 січня 2002 № 63/2002

Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України. Указ від 30.06.2011 № 717/2011

Положення проНаціональну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації. Указ від 23.11.2011 № 1067/2011

Положення про Державний комітет телебачення і радіомовлення України. УПУ від 7 травня 2011 № 559/2011

Положення про Міністерство економічного розвитку і торгівлі України. Указ від 31.05.2011 № 634/2011

**Положення про** Державну службу України з питань регуляторної політики та розвитку підприємництва. Указ від 30.03.2012 № 237/2012

**5. Декрети, постанови та розпорядження Кабінету Міністрів України**

Стратегія розвитку інформаційного суспільства в Україні. Розпорядження від 15.05.2013 № 386-р

Про стандартизацію і сертифікацію. Декрет від 10.05.1993 № 46-93

Положення про державну реєстрацію нормативно-правових актів міністерств, інших органів виконавчої влади. Постанова від 28.12.1992 № 731

Порядок ведення Єдиного державного реєстру нормативно-правових актів та користування ним. Постанова від 23.04.2001 № 376

Концепція формування системи національних електронних інформаційних ресурсів. Розпорядження від 05.05.2003 № 259-р

Положення про Національний реєстр електронних інформаційних ресурсів. Постанова від 17.03.2004 № 326

Порядок ведення Єдиного державного порталу адміністративних послуг. Постанова від 03.01.2013 № 13 (у редакції постанови від 11.07.2013 № 556)

Положення про національний фонд нормативних документів. Постанова від 18.09.2002 № 1395

Інструкція про порядок обліку, зберігання й використання документів, справ, видань і інших матеріальних носіїв інформації, що містять службову інформацію. Постанова від 27.11.1998 № 1898

Концепція технічного захисту інформації в Україні. Постанова від 08.10.1997 № 1126.

Перелік обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних. Постанова від 04.02.1998 № 121

Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова від 13.03.2002 № 281/2002

Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Постанова від 16.11.2002 № 1772

Порядок підключення до глобальних мереж передачі даних. Постанова від 12.04.2002 № 522

Порядок оприлюднення в мережі Інтернет інформації про діяльність органів виконавчої влади. Постанова від 04.01.2002 № 3

Про заходи щодо створення електронної інформаційної системи «Електронний Уряд». Постанова від 24.02.2003 № 208

Концепція розвитку електронного урядування в Україні. Розпорядження від 13.12.2010 № 2250-р

Концепція створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів. Розпорядження від 05.09.2012 № 634-р

Положення про систему електронної взаємодії органів виконавчої влади. Постанова від 18.07.2012 № 670

Порядок надання послуг конфіденційного зв’язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям. Постанова від 11.10.2002 № 1519

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інфор-маційно-телекомунікаційних системах. Постанова від 29.03.2006 № 373

Порядок обов'язкової передачі документованої інформації. Постанова від 28.10.2004 № 1454

Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу. Постанова від 26.05.2004 № 680

Порядок надсилання електронною поштою службових документів. Постанова від 17.07.2009 № 733

Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності. Постанова від 28.10.2004 № 1452

Типовий порядок здійснення електронного документообігу в органах виконавчої влади. Постанова від 28.10.2004 № 1453

Порядок здійснення процедури призначення органів з оцінки відповідності продукції, процесів і послуг вимогам технічних регламентів. Постанова від 24.01.2007 № 59

Перелік центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів. Постанова від 13.03.2002 № 288

Порядок акредитації центру сертифікації ключів. Постанова від 13.07.2004 № 903

Положення про центральний засвідчувальний орган. Постанова від 28.10.2004 № 1451

Перелік платних адміністративних послуг, що надаються Адміністрацією Держспецзв'язку. Постанова від 09.06.2011 № 626

Перелік платних адміністративних послуг, що надаються Службою безпеки. Розпорядження від 09.06.2011 № 526-р

Перелік послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню. Постанова від 18.05.2011 № 517

Перелік послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), господарська діяльність з надання яких підлягає ліцензуванню. Перелік криптосистем і засобів криптографічного захисту інформації, торгівля якими підлягає ліцензуванню. Постанова від 25.05.2011 № 543

Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації. Постанова від 27.10.2001 № 1450

Перелік органів ліцензування. Постанова від 05.08.2015 № 609

Про запровадження ліцензії єдиного зразка для певних видів господарської діяльності. Постанова від 20.11.2000 № 1719

Перелік документів, які додаються до заяви про видачу ліцензій для окремого виду господарської діяльності. Постанова від 04.07.2001 № 756

Про строк дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу. Постанова від 29.11.2000 № 1755

Про розміри та порядок зарахування плати за видачу, переоформлення, видачу дубліката, копії ліцензії на провадження діяльності у сфері телекомунікацій і продовження строку її дії. Постанова від 16.06.2004 № 773

 Про розміри плати за видачу, продовження строку дії, переоформлення, видачу дублікатів ліцензій на користування радіочастотним ресурсом України. Постанова від 22.02.2006 № 200

Порядок формування, ведення і користування відомостями ліцензійного реєстру та подання їх до Єдиного ліцензійного реєстру. Постанова від 08.11.2000 № 1658

Критерії, за якими оцінюється ступінь ризику від провадження господарської діяльності у галузях криптографічного та технічного захисту інформації та визначається періодичність здійснення планових заходів державного нагляду (контролю). Постанова від 22.08.2012 № 791

Критерій, за яким оцінюється ступінь ризику від провадження господарської діяльності у сфері послуг електронного цифрового підпису і визначається періодичність проведення планових заходів, пов'язаних з державним наглядом (контролем) Адміністрацією Держспецзв'язку. Постанова від 13.08.2014 № 329.

Критерій, за яким оцінюється ступінь ризику від провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі ними і визначається періодичність проведення планових заходів державного нагляду (контролю). Постанова від 15.12.2010 № 1137

Положення про Національну експертну комісію з питань захисту суспільної моралі. Постанова від 17.11.2004 № 1550

**6. Наказ Уповноваженого Верховної Ради України з прав людини** **від 08.01.2014 № 1/02-14**

Типовий порядок обробки персональних даних

Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації

[Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних](http://zakon3.rada.gov.ua/laws/show/v1_02715-14#n92)

**7. Накази Служби безпеки України**

Звід відомостей, що становлять державну таємницю. Наказ від12.08.2005  № 440, зареєстрований в Мін’юсті 17.08.2005 за № 902/11182

Ліцензійні умови провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації. Наказ від 31.01.2011 № 35, зареєстрований в Мін’юсті 23.02.2011 за № 225/18963

Ліцензійні умови провадження господарської діяльності з впровадження, ввезення, вивезення голографічних захисних елементів. Наказ від 12.10.2010 № 524, зареєстрованим в Мін’юсті 09.11.2010 за № 1065/18360

Порядок контролю за додержанням Ліцензійних умов провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації. Наказ від 31.01.2011 № 35, зареєстрований в Мін’юсті 23.02.2011 за № 225/18963

Порядок контролю за додержанням Ліцензійних умов провадження господарської діяльності з впровадження, ввезення, вивезення голографічних захисних елементів. Наказ від 12.10.2010 № 524, зареєстрованим в Мін’юсті 09.11.2010 за № 1065/18360

Інструкція про порядок оформлення матеріалів про адміністративні правопорушення у сфері охорони державної таємниці та конфіденційної інформації, що є власністю держави.Наказ від 17.08.2006 № 549, зареєстрований в Мін’юсті 11.09.2006 за № 1047/12921

**8. Накази Адміністрації Держспецзв’язку**

Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації. Наказ від 22.03.2007 № 36, зареєстрований в Мін’юсті 04.04.2007 за № 312/13579

Положення про фонд нормативних документів у сфері технічного та криптографічного захисту інформації. Наказ від 08.08.2008 № 131

Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ від 10.04.2008 № 94, зареєстрований в Мін’юсті 07.07.2008 за № 603/15294

Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ від Наказ від 02.12.2014 № 660, зареєстрований в Мін’юсті 28.01.2015 за № № 90/26535

Перелік адміністративних послуг, які безоплатно надаються Адміністрацією Держспецзв'язку. Наказ від 29.11.2011 № 350, зареєстрований в Мін’юсті 15.12.2011 за № 1455/20193

Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Наказ від 23.02.2002 № 9, зареєстрований в Мін’юсті 13.03.2002 за № 245/6533

Положення про державну експертизу у сфері криптографічного захисту інформації. Наказ від 23.06.2008 № 100

Порядок формування Реєстру організаторів державної експертизи у сфері технічного захисту інформації та Реєстру експертів з питань технічного захисту інформації. Наказ від 16.04.2008 № 64.

Положення про Експертну раду з питань державної експертизи в сфері технічного захисту інформації. Наказ від 01.10.2010 № 291

Положення про державний контроль за станом технічного захисту інформації. Наказ від 16.05.2007 № 87, зареєстрований в Мін’юсті 10.07.2007 за № 785/14052

Положення про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп. Наказ від 16.05.2007 № 86, зареєстрований в Мін’юсті 04.06.2007 за № 577/13844

Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису. Наказ від 24.07.2007 № 143, зареєстрованим в Мін’юсті 08.08.2007 за № 914/14181

Положення про державну експертизу в сфері технічного захисту інформації. Наказ від 16.05.2007 № 93, зареєстрований в Мін’юсті 16.07.2007 за № 820/14087

Стандарт надання адміністративної послуги з видачі атестатів відповідності комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах вимогам нормативних документів з технічного захисту інформації. Наказ від 19.03.2009 № 64

Стандарт надання адміністративної послуги з організації державної експертизи у сфері криптографічного захисту інформації. Наказ від 29.11.2008 № 200

Стандарт надання адміністративної послуги з видачі, переоформлення ліцензій, видачі дублікатів та копій ліцензій на провадження господарської діяльності з розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг у галузі технічного захисту інформації. Наказ від 26.12.2008  № 221

Ліцензійні умови провадження господарської діяльності з надання послуг у галузі технічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України). Наказ від 14.10.2014 № 532, зареєстрований в Мін’юсті 04.11.2014 за № 1387/26164

Порядок контролю за додержанням Ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України). Наказ від 14.10.2014 № 532, зареєстрований в Мін’юсті 04.11.2014 за № 1388/26165

Ліцензійні умови провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України). Наказ від 14.10.2014 № 531, зареєстрований в Мін’юсті 03.11.2014 за № 1380/26157

Порядок контролю за додержанням Ліцензійних умов провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України). Наказ від 14.10.2014 № 531, зареєстрований в Мін’юсті 03.11.2014 за № 1381/26158

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Наказ від 20.07.2007 № 141 (у редакції наказу від 14.12.2015 № 767)

Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації. Наказ від 12.06.2007 № 114

Правила посиленої сертифікації. Наказ від 13.01.2005 № 3, зареєстрований в Мін’юсті 27.01.2005 за № 104/10384

Інструкція про порядок оформлення та складання Державною службою спеціального зв’язку та захисту інформації України матеріалів про адміністративні правопорушення. Наказ від 29.05.2007 № 100, зареєстрований в Мін’юсті 12.06.2007 за № 618/13885

**9. Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації**

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
|

|  |
| --- |
|  |

 |

 |

 |

Про затвердження зразка заяви про видачу ліцензії на здійснення діяльності у сфері телекомунікацій. Рішення від 05.11.2013 № 716, зареєстроване в Мін’юсті 22.11.2013 за № 1994/24526

Ліцензійні умови здійснення діяльності у сфері телекомунікацій з надання послуг з технічного обслуговування і експлуатації телекомунікаційних мереж, мереж ефірного теле- та радіомовлення, проводового радіомовлення та телемереж. Рішенням від 11.11.2010 № 513, зареєстроване в Міністерстві юстиції України 30.11.2010 за № 1200/18495

Ліцензійні умови користування радіочастотним ресурсом України. Рішенням від 19.08.2005 № 53, зареєстроване в Мін’юсті 20.10.2005 за № 1237/11517

Порядок здійснення державного нагляду за ринком телекомунікацій. Рішення від 13.12.2012 № 649, зареєстроване в Мін’юсті 10.01.2013 за № 92/22624

Порядок здійснення державного нагляду за користуванням радіочастотним ресурсом України в смугах радіочастот загального користування. Рішення від 27.12.2012 № 684, зареєстроване в Мін’юсті 22.01.2013 за № 175/22707

**10. Спільні накази**

Перелік психічних захворювань (розладів), які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянинові не надається. Наказ Міністерства охорони здоров'я та Служби безпеки України від 13.05.2002 № 174/136, зареєстрований в Мін’юсті 28.05.2002 за № 458/6746

Порядок інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади. Порядок функціонування веб-сайтів органів виконавчої влади. Наказ Державного комітету інформаційної політики, телебачення і радіомовлення України та Державного комітету зв'язку та інформатизації України від 25.11.2002 № 327/225, зареєстрованим в Мін’юсті 29.12.2002 за № 1021/7309

Правила проведення робіт із сертифікації засобів захисту інформації. Наказ Адміністрації Держспецзв’язку та Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.2007 № 75/91, зареєстрований в Мін’юсті 14.05.2007 за № 98/13765

**11. Державні стандарти України, нормативні документи ТЗІ**

ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення.

ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

ДСТУ 1.5:2003 Національна стандартизація. Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.

НД ТЗІ 1.6-002-03 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.