**Заняття 2.**

**23.09.2020р.**

**Нормативно-правовий захист інформації в ІТС.**

**Вступ.**

**Питання 1.** Етапи та види захисту від загроз для електронних інформаційних ресурсів автоматизованих (комп’ютерних) систем.

**Питання 2.** Нормативно-правові акти України, які визначають необхідність створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

**Питання 3.** Нормативні документи ТЗІ, які визначають порядок створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

**Питання 1.**

Загальний аналіз проблем організовування захисту від будь-яких загроз дає можливість визначити 4 головні принципи та етапи заходів:

1) організація зовнішніх рубежів безпеки з метою своєчасного виявлення загроз;

2) організація протидії загрозам та їх блокування, тобто зупинення та локалізації загроз під час їх реалізації;

3) забезпечення нейтралізації та ліквідації загроз, а також подолання наслідків загроз, які не вдалося блокувати;

4) попередження загроз, тобто аналіз відомих загроз та впровадження відповідних запобіжних заходів.

Стосовно автоматизованих (комп’ютерних) систем (далі - АС) ці принципи та етапи дають можливість також визначити 4 етапи та види захисту від загроз для електронних інформаційних ресурсів АС, які циклічно повторюються з метою постійного оновлення та підвищення ефективності заходів і засобів захисту.

**Виявлення ► Зупинення ► Нейтралізація ► Попередження**

**1. Етап виявлення**

*На організаційному рівні* – це забезпечення пропускного режиму, цілодобової охорони та контролю периметра безпеки, а також контррозвідувальних заходів служби безпеки установи.

*На інженерно-технічному рівні*– це використання інженерних споруд і технічних засобів пропускного режиму, охоронної сигналізації та відеоспостереження.

**2. Етап зупинення**

Ці заходи забезпечують апаратно-програмне блокування спроб несанкціонованого доступу (далі - НСД) порушника (хакера) до інформації в АС або ураження системи вірусами за допомогою спеціальних апаратних комплексів та програмних засобів захисту інформації. Для цього в АС встановлюються міжмережові екрани, файерволи (брандмауери), антивірусні програмні засоби та спеціальні комплекси засобів захисту інформації від НСД.

Зазначимо, що ці заходи можуть бути спрямовані на документування методів НСД до АС для наступного дослідження їх; збереження слідів правопорушення; взаємодію (у разі необхідності) з державними правоохоронними органами щодо виявлення та розкриття правопорушення (в тому числі за готування до злочину і за замах на злочин); сприяння притягненню винних до відповідної відповідальності (кримінальної, адміністративної, цивільно-правової, дисциплінарної).

**3. Етап нейтралізації**

*На організаційно-правовому рівні* – це дисциплінарне або адміністративне (кримінальне) розслідування правопорушення (злочину) та притягнення винних до відповідальності.

*На апаратно-програмному**рівні*– це подолання наслідків реалізації загроз у разі порушень:

- технологічих процесів - їх відновлення за допомогою плану аварійного відновлення та проведення ремонтних заходів;

- операційної системи та програмних засобів - їх відновлення за допомогою інсталяційних файлів (дисків);

- інформаійних ресурсів - їх відновлення за допомогою резервних і архівних копій, які зберігаються на зовнішніх носіях.

**4. Етап попередження**

*На організаційному рівні* – це проведення аналізу відомих загроз, прогнозування нових загроз і пошук відповідних запобіжних заходів, дезінформаційне легендування об’єктів захисту, розширення периметру безпеки, періодичне оновлення політики безпеки та плану захисту, постійне навчання та тренування персоналу.

*На інженерно-технічному рівні*– це застосування пасивних засобів захисту: закриття вікон та встановлення на них грат і штор (жалюзі), закриття та опечатування дверей, пломбування системних блоків, роз’ємів технічних засобів АС тощо, використання систем екранування, заземлення та зашумлення, а також модернізація наявної системи захисту та впровадження нових засобів ТЗІ.

**Питання 2.**

Історія захисту інформації в Україні розпочалася з Закону України **«Про захист інформації в автоматизованих системах»**, прийнятого постановою Верховної Ради України № 81/94-ВР від 5 липня 1994 року.

У тому же році постановою Кабінету Міністрів України (далі - ПКМУ) від 9 вересня 1994 року № 632 було затверджене **«Положення про технічний захист інформації в Україні»** (далі - ТЗІ), згідно якого була створена Державна служба України з питань ТЗІ.

Через 3 роки постановою КМУ від 8 жовтня 1997 року № 1126 була затверджена **«Концепція ТЗІ в Україні»**. Вонавизначає поняття ТЗІ таким чином: 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.

А вже через 2 роки з’явилося нове **«Положення про ТЗІ в Україні»**, затверджене Указом Президента України від 27 вересня 1999 року № 1229. Пов’язане це було з тим, що питання ТЗІ були покладені на Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (скорочено - ДСТСЗІ СБУ), до складу якого і увійшла Державна служба з питань ТЗІ. Старе положення втратило чинність згідно постанови КМУ від 13 березня 2002 року № 281.

**«Положення про ТЗІ в Україні»** визначає поняття ТЗІ таким чином: це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності важливої для держави, суспільства і особи інформації.

Воно визначає також такі терміни:

- **конфіденційність** - властивість інформації бути захищеною від несанкціонованого ознайомлення;

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

- **доступність** - властивість інформації бути захищеною від несанкціонованого блокування;

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

Тепер з'ясуємо, яку інформацію треба захищати:

**Закон України «Про інформацію» (1992)**

**Стаття 20. Доступ до інформації**

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

**Стаття 21. Інформація з обмеженим доступом**

1. Інформацією з обмеженим доступом (далі - ІзОД) є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

**Закон України «Про доступ до публічної інформації» (2011)**

**Стаття 7. Конфіденційна інформація**

1. Конфіденційна інформація - інформація, 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.

2. 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.

**Стаття 8. Таємна інформація**

1. Таємна інформація - інформація, 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.

**Стаття 9. Службова інформація**

1. 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.

2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування».

**Закон України «Про захист персональних даних****» (2010)**

**Стаття 5. Об'єкти захисту**

1. Об'єктами захисту є персональні дані.

2. Персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом.

**Закон України «Про електронні документи та електронний документообіг****» (2003)**

**Стаття 15. Обіг електронних документів, що містять інформацію з обмеженим доступом**

В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять інформацію, яка є власністю держави, або ІзОД, повинен забезпечуватися захист цієї інформації відповідно до законодавства.

*Таким чином, потрібно захищати ІзОД та інформацію, що є власністю держави та циркулює в інформаційно-телекомунікаційних системах.*

**Види захисту інформації**

**1. Організаційний** - попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (охорона, пропускний режим, регламентація доступу тощо).

**2. Інженерний** - попередження доступу на об'єкт інформаційної діяльності сторонніх осіб та руйнування об’єкту захисту внаслідок навмисних дій або природного впливу інженерно-технічними засобами (обмежуючі конструкції доступу, відеоспостереження, охоронно-пожежна сигналізація тощо).

**3. Технічний** (ТЗІ) - забезпечення обмеження доступу до інформації апаратно-технічними засобами (зашумлення, маршрутизатори, антивіруси, фаєрволи, смарт-карти тощо):

- захист від витоку технічними каналами;

- захист від НСД.

**4. Криптографічний** (КЗІ) - попередження доступу до інформації за допомогою математичних перетворень:

- попередження несанкціонованої модифікації;

- попередження несанкціонованого розголошення.

Закон України «**Про захист інформації в автоматизованих системах**» визначив термін захист інформації: це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. *Разом з тим, у законі ще не застосовувалось таке поняття як комплексна система захисту інформації.*

Також він визначив термін автоматизована система (далі - АС): це система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки та зв'язку), а також методи і процедури, програмне забезпечення.

**Згідно ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення»:**

АС - організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність.

Згідно НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»:

- АС - організаційно-технічна система, що реалізує інформаційну технологію та поєднує у собі: обчислювальну систему, фізичне середовище, персонал та інформацію, яка обробляється.

- захист інформації в АС - діяльність, спрямована на забезпечення безпеки оброблюваної в АС інформації та системи у цілому, що дає змогу запобігти реалізації загроз або унеможливити її, та зменшити ймовірність завдання збитків від реалізації загроз.

- комплексна система захисту інформації (далі - КСЗІ) - це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Наступним етапним документом став

**Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»**, який був прийнятийу2005 році на заміну Закону «Про захист інформації в АС».Він визначив багато нових термінів, зокрема, такі:

- КСЗІ - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

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

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

- телекомунікаційна система - організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;

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

- інформаційний ресурс - будь-які дані в електронному вигляді, які обробляються або зберігаються в інформаційно-телекомунікаційній системі.

**Закон України «Про захист інформації в ІТС»**

**Стаття 2. Об'єкти захисту в системі**

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

**Стаття 8. Умови обробки інформації в системі**

Інформація, яка є власністю держави, або 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 сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

**Стаття 9. Забезпечення захисту інформації в системі**

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, 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 або підпорядкований йому регіональний орган.

**Стаття 10. Повноваження державних органів у сфері захисту інформації в системах**

Вимоги до забезпечення захисту інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

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.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом.

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

**Закон України «Про Державну службу спеціального зв'язку**

**та захисту інформації України» (2006)**

*Згідно цього закону ДСТСЗІ СБУ вийшов зі складу СБУ та був реорганізований у Державну службу спеціального зв'язку та захисту інформації України (скорочено –* ***Держспецзв'язку****), яка є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.*

**Стаття 16.** На Держспецзв'язку згідно визначених завдань покладаються такі обов'язки:

3) розроблення порядку та вимог щодо захисту державних інформаційних ресурсів\* в ІТС, криптографічного та технічного захисту інформації, яка є власністю держави, або   
інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

***\**** *-* ***державні інформаційні ресурси*** *- систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб’єктами владних повноважень.*

*У «Положенні про Реєстр ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління», затвердженому постановою Кабінету Міністрів України від 03.08.2005 № 688:*

***державні електронні інформаційні ресурси*** *- відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством.*

11) накопичення та аналіз даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС, а також про їх наслідки, інформування правоохоронних органів для вжиття заходів із запобігання та припинення кримінальних правопорушень у зазначеній сфері; оцінка стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, надання відповідних рекомендацій;

13) погодження проектів створення ІТС, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої  
встановлена законом, проведення їх експертної оцінки і визначення можливості введення в експлуатацію;

16) встановлення порядку і вимог щодо використання ІТС, у тому числі загального користування, органами державної влади, органами місцевого самоврядування, підприємствами, установами і організаціями незалежно від форм власності, які збирають, обробляють, зберігають та передають інформацію, яка є власністю держави, або інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом;

32) видача атестата відповідності комплексних систем захисту інформації ІТС, із застосуванням яких обробляється інформація, яка є власністю держави, або інформація з   
обмеженим доступом, вимога щодо захисту якої встановлена законом, вимогам нормативних документів з питань технічного захисту інформації.

**Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, які містять службову інформацію**(затверджена ПКМУ від 19.10.2016 № 736)

11. Забороняється використовувати для передачі службової інформації відкриті канали зв’язку.

14. Використання інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем чи засобів копіювально-розмножувальної техніки, що застосовуються під час обробки службової інформації, здійснюється на підставі розпорядчого документа керівника установи з дотриманням вимог законодавства у сфері захисту інформації.

15. Особливості ведення обліку, зберігання, передачі, пересилання, транспортування і знищення документів з відміткою «Літер “К”», засобів криптографічного захисту службової інформації, ключових документів, нормативної, технічної (експлуатаційної) документації визначаються нормативно-правовими актами Адміністрації Держспецзв’язку.

54. Передача службової інформації телекомунікаційними, інформаційно-телекомунікаційними мережами здійснюється лише з використанням засобів криптографічного захисту інформації, що в установленому порядку допущені до експлуатації, з дотриманням вимог технічного захисту інформації.

Основний керівний нормативно-правовий акт: «**ПРАВИЛА   
забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (далі – Правила 373)**

(затверджені ПКМУ від 29.03.2006 № 373 з останніми змінами згідно № 938 від 07.09.2011)

3. У Правилах наведені нижче терміни вживаються у такому значенні:

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

- ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою *(логін)*.

4. 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.

5. 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. 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 користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

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

7. Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

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

11. 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 інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

12. 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.

13. 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.

14. Порядок підключення систем, в яких обробляється службова і таємна інформація, до глобальних мереж передачі даних визначається законодавством.

15. 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 програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

**Організаційні засади забезпечення захисту інформації**

16. Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі - 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 з інформацією, 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 необхідність такого захисту прийнято розпорядником інформації.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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 технічного захисту інформації 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.

23. Виконавцем робіт із створення системи захисту може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації, необхідність проведення якого визначено технічним завданням на створення системи захисту.

Для проведення інших видів робіт з технічного захисту інформації, 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.

**Питання 3.**

**Основні нормативно-правові акти України**

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 з останніми змінами згідно ПКМУ № 938 від 07.09.2011.

**Державні стандарти України та Росії**

ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення.

ДСТУ 2851-94. Програмні засоби ЕОМ. Документування результатів випробувань.

ДСТУ 2853-94. Програмні засоби ЕОМ. Підготовлення і проведення випробувань.

ДСТУ 3396.0-96. Технічний захист інформації. Основні положення.

ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт.

ДСТУ 3396.2-97. Технічний захист інформації. Терміни та визначення.

ГОСТ 34.201-89 Виды, комплектность и обозначение документов при создании автоматизированых систем

РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов

**Нормативні документи системи технічного захисту інформації**

**Створення КСЗІ в автоматизованій системі**

НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБ України від 08.11.2005 № 125 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

НД ТЗІ 1.6-005-2013. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, затверджений наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215

НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

**Захист інформації в комп'ютерних системах від несанкціонованого доступу**

НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.

НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.

НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.

НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 № 22.

НД ТЗІ 2.5-008-2002. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБ України від 13.12.2002 № 84 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

НД ТЗІ 2.5-010-2003. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

**Створення комплексів ТЗІ на об'єктах інформаційної діяльності**

ТР ЕОТ - 95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок, затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.95 № 25.

НД ТЗІ 1.1-005-2007. Створення комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

НД ТЗІ 2.1-002-2007. Випробування комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

НД ТЗІ 3.1-001-2007. Створення комплексу технічного захисту інформації. Передпроектні роботи, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

НД ТЗІ 3.3-001-2007. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

**Державна експертиза КСЗІ**

Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93 та зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Порядок формування реєстру організаторів державної експертизи у сфері ТЗІ та реєстру експертів з питань ТЗІ, затверджений наказом Адміністрації Держспецзв’язку від 16.04.2008 № 64

НД ТЗІ 2.6-001-2011. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Держспецзв'язку від 25.03.2011 № 65 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

НД ТЗІ 2.7-009-2009. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

НД ТЗІ 2.7-010-2009. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172.

**Основний керівний документ – це НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»**

Він визначає порядок прийняття рішень щодо складу КСЗІ в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Побудований у вигляді керівництва, яке містить перелік робіт і посилання на діючі нормативні документи, у відповідності до яких ці роботи необхідно виконувати. Якщо якийсь з етапів чи видів робіт не нормовано, наводиться короткий зміст робіт та якими результатами вони повинні закінчуватись.

Дія цього НД ТЗІ поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом. Відповідно, для таких ІТС чинні всі нормативно-правові акти та нормативні документи щодо створення ІТС та щодо захисту інформації в АС. НД ТЗІ не встановлює нових норм, а систематизує в одному документі вимоги, норми і правила, які безпосередньо або непрямим чином витікають з положень діючих нормативних документів.

НД ТЗІ призначений для суб’єктів інформаційних відносин (власників або розпорядників ІТС, користувачів), діяльність яких пов’язана з обробкою інформації, що підлягає захисту, розробників КСЗІ в ІТС, для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.

Встановлений цим НД ТЗІ порядок є обов’язковим для всіх суб’єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб’єкти системи ТЗІ можуть використовувати як рекомендації.

Порядок створенняКСЗІ в ІТС є єдиним незалежно від того, створюється КСЗІ в ІТС, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту інформації або модернізації вже створеної КСЗІ.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

Порядок створення КСЗІ в ІТС розглядається цим НД як сукупність впорядкованих у часі, взаємопов’язаних, об’єднаних в окремі етапи робіт, виконання яких необхідне й достатньє для КСЗІ, що створюється.

Створення КСЗІ повинно виконуватись у комплексі із заходами, щодо забезпечення режиму секретності, протидії технічним розвідкам, а також з режимними заходами щодо охорони інформації з обмеженим доступом, яка не є державною таємницею.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів тощо;

- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС.

Створення **комплексів технічного захисту інформації від витоку технічними каналами** здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

Створення **комплексу засобів захисту від несанкціонованого доступу** (далі – КЗЗ) здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.

Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.

Для організації робіт зі створення КСЗІ в ІТС створюється Служба захисту інформації в ІТС. Вона створюється після прийняття рішення про необхідність створення КСЗІ.

**Цей НД ТЗІ визначає такі етапи створення КСЗІ та її документів:**

1. Формування вимог до КСЗІ в ІТС

1.1. Обґрунтування необхідності створення КСЗІ і призначення СЗІ:

**-** наказ про порядок проведення робіт зі створення КСЗІ

- наказ про створення СЗІ

- положення про СЗІ

- перелік інформації, що підлягає обробленню в ІТС та потребує захисту

1.2. Категоріювання ІТС:

- наказ про призначення комісії з категоріювання

- акт категоріювання

1.3. Обстеження середовищ функціонування ІТС:

- наказ про призначення комісії з обстеження

- акт обстеження

- формуляр ІТС

1.4. Опис моделі порушника політики безпеки інформації: модель порушника

1.5. Опис моделі загроз для інформації: модель загроз

1.6. Формування завдання на створення КСЗІ: звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ

2. Розробка політики безпеки інформації в ІТС

2.1. Вибір варіанту КСЗІ

2.2. Складання політики безпеки

2.3. Складання плану захисту

2.4. Складання календарного плану робіт із захисту інформації

3. Розробка Технічного завдання на створення КСЗІ:

- складання технічного завдання та погодження його з органами Держспецзв’язку

4. Проектування КСЗІ:

- складання документів ескізного проекту КСЗІ

- складання документів технічного проекту КСЗІ

- складання документів робочого проекту КСЗІ

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

5.1. Підготовка КСЗІ до введення в дію:

- інструкція про порядок введення в експлуатацію КСЗІ

5.2. Навчання користувачів:

- інструкція адміністратора безпеки в ІТС

- інструкція системного адміністратора ІТС

- інструкція користувача ІТС

- правила управління паролями в ІТС

- правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу в ІТС

5.3. Комплектування КСЗІ

5.4. Будівельно-монтажні роботи:

- наказ про призначення комісії з приймання робіт

- акт приймання робіт

5.5. Пуско-налагоджувальні роботи:

- акт інсталяції та налагоджування АВПЗ і КЗЗ від НСД

- акт оцінки відповідності проведених робіт вимогам експлуатаційних документів

5.6. Попередні випробування КСЗІ:

- наказ про створення комісії з проведення випробувань

- програма та методика попередніх випробувань

- протокол про проведення попередніх випробувань

- акт про приймання КСЗІ у дослідну експлуатацію

5.7. Дослідна експлуатація КСЗІ:

- наказ про введення ІТС в дослідну експлуатацію

- акт про завершення дослідної експлуатації

- акт про завершення робіт зі створення КСЗІ

5.8. Державна експертиза КСЗІ:

- заявка на проведення державної експертиза КСЗІ

- експертний висновок щодо відповідності КСЗІ вимогам НД ТЗІ

- атестат відповідності КСЗІ вимогам НД ТЗІ

- наказ про дозвіл на обробку в ІТС інформації, яка підлягає захисту

**6. Супровід КСЗІ:**

- наказ про порядок забезпечення захисту інформації в ІТС

- інструкція щодо забезпечення правил обробки ІзОД в ІТС

- інструкція з антивірусного захисту інформації в ІТС

- інструкція про порядок використання засобів КЗІ в ІТС

- інструкція про порядок обліку та використання машинних носіїв інформації

- інструкція з правил управління паролями в ІТС

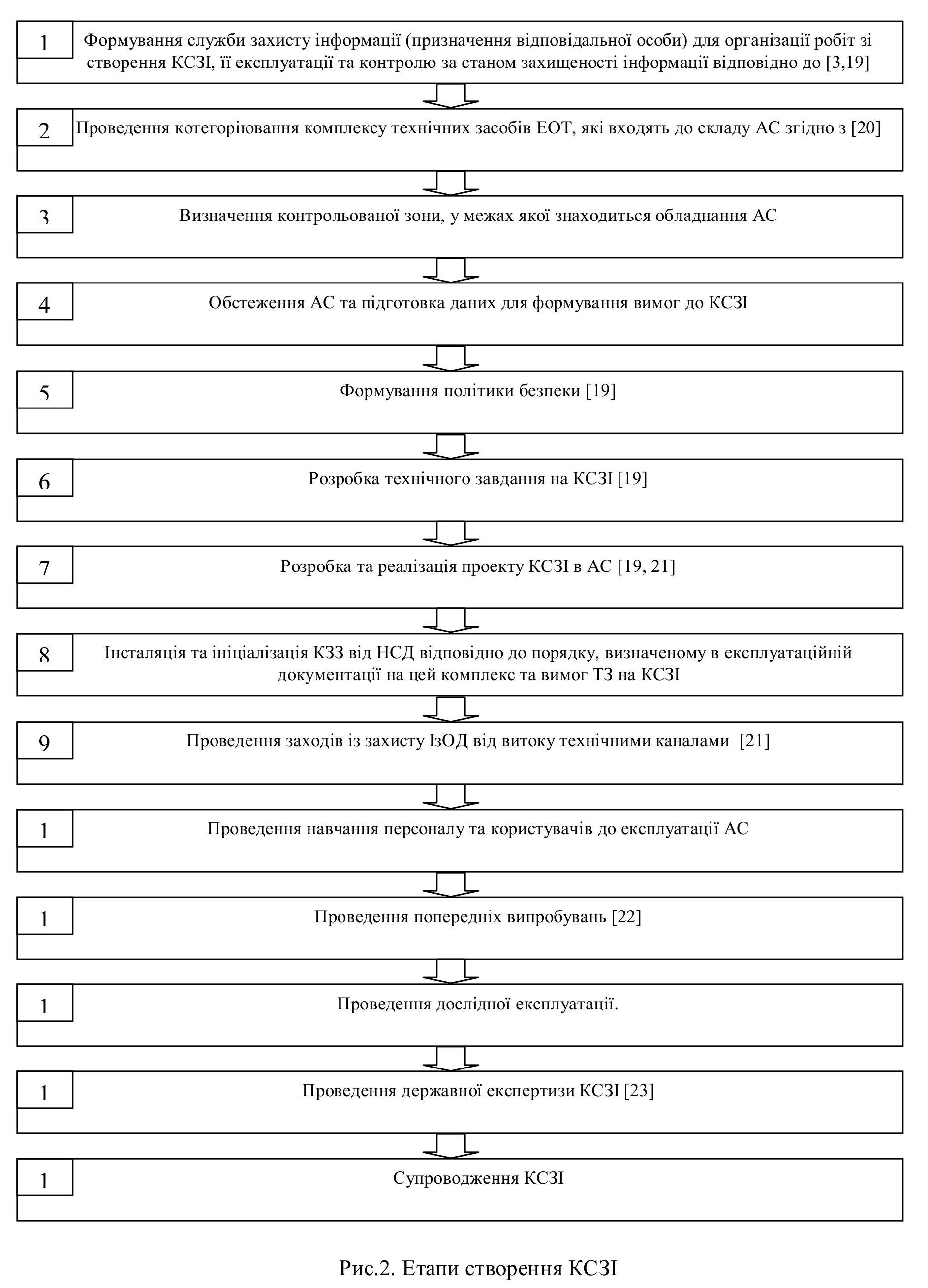
- інструкція про порядок створення і зберігання резервних копій інформаційних ресурсів ІТС

- інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС

- інструкція про порядок супроводу та модернізації КСЗІ в ІТС

- інструкція про **порядок відновлювальних та ремонтних робіт** ІТС

- інші інструкції.

**Варіант схематичного вигляду етапів створення КСЗІ.**

**Контрольні питання**

Які є головні принципи та етапи захисту від загроз?

Як вирішується перший етап захисту від загроз?

Як вирішується другий етап захисту від загроз?

Як вирішується третій етап захисту від загроз?

Як вирішується четвертий етап захисту від загроз?

Що таке ТЗІ згідно Положення?

Який закон України розподіляє інформацію за порядком доступу?

Як поділяється інформація за порядком доступу?

Яка інформація є інформацією з обмеженим доступом?

Який закон України визначає службову інформацію?

Якою інформацією за режимом доступу є персональні дані?

Яка інформація підлягає захисту?

Які властивості щодо ТЗІ має інформація?

Що таке конфіденційність інформації?

Що таке доступність інформації?

Що таке цілісність інформації?

Хто затвердив діючу «Концепцію ТЗІ в Україні»?

Хто затвердив діюче «Положення про ТЗІ в Україні»?

Які є види захисту інформації?

Яку назву мав перший закон України з питань захисту інформації?

Яку назву має діючий закон України з питань захисту інформації?

Що таке КСЗІ згідно Закону?

Що таке захист інформації в системі згідно Закону?

Що таке інформаційний ресурс згідно Закону?

Яку назву має закон України, що передбачає створення КСЗІ?

Яку назву має постанова Кабінету Міністрів, що передбачає створення КСЗІ?

Що є об'єктами захисту в системі згідно Закону?

На кого покладається відповідальність за забезпечення захисту інформації в системі?

Із застосуванням чого повинна оброблятися ІзОД в системі згідно Закону?

За результатами чого здійснюється підтвердження відповідності КСЗІ?

Що повинні мати засоби захисту інформації, які використовуються для створення КСЗІ?

Який підрозділ утворює власник системи, в якій обробляється ІзОД?

На кого покладається забезпечення захисту інформації в системі та контролю за ним?

Хто є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації?

Хто встановлює особливості захисту інформації в банківських системах?

Яка відкрита інформація підлягає захисту?

Що повинна зберігати відкрита інформація під час обробки в системі?

Для захисту від яких загроз інформації в системі створюється КСЗІ?

Які системи треба захищати від витоку інформації технічними каналами?

Які системи треба захищати від несанкціонованих дій з інформацією?

Коли треба захищати інформацію від спеціального впливу на засоби обробки інформації?

Згідно якого розробленого СЗІ документа здійснюється захист інформації на всіх етапах створення та експлуатації системи?

Яким документом встановлюються вимоги до захисту інформації кожної окремої системи?

Яку назву має НД ТЗІ, що визначає етапи створення КСЗІ?

Коли в ІТС здійснюється створення комплексів ТЗІ від витоку технічними каналами?

Хто приймає рішення щодо захисту ІТС від спеціальних впливів на інформацію?

Після чого створюється служба захисту інформації в ІТС?

Скільки є етапів створення КСЗІ згідно НД ТЗІ?

Яку назву має перший етап створення КСЗІ?

Яку назву має другий етап створення КСЗІ?

Яку назву має третій етап створення КСЗІ?

Яку назву має четвертий етап створення КСЗІ?

Яку назву має п’ятий етап створення КСЗІ?

Яку назву має шостий етап створення КСЗІ?