МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ТЕОРІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОБМЕЖЕНОГО ДОСТУПУ

Конспект лекцій

Для студентів з галузі знань F «Інформаційні технології»
за спеціальністю F5 «Кібербезпека та захист інформації»

Київ 2026

Конспект лекцій для студентів другого (магістерського) рівня вищої освіти з дисципліни «Теорія захисту інформаційних ресурсів обмеженого доступу»/ Укладач: А.М. Котенко к.т.н. доцент, – К.:ДУІКТ, 2026. – 105 с.

Укладач:
А.М. Котенко, канд. техн. наук, доцент

Рецензент: Щавінський Ю.В. - канд. техн. наук, доцент

Конспект лекцій затверджено на засіданні кафедри технічних систем кіберзахисту протокол № 12 від 09 червня 2026 р.

Схвалено Вченою радою Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій, (протокол № 12 від 09.06.2026 р).

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. **Лекції** з дисципліні «Теорія захисту інформаційних ресурсів обмеженого доступу» для студентів спеціальності F5 «Кібербезпека та захист інформації» охоплюють розділи курсу, що пов’язані з розглядом причин втрати інформації з обмеженим доступом в ІКС на ОІД та технологію побудови системи захисту інформації з обмеженим доступом.

2. Метою лекційних занять є підготовка висококваліфікованих фахівців з кібербезпеки та захисту інформації за освітньо-професійною програмою технічні системи інформаційного та кібернетичного захисту які здатні здійснювати професійну діяльність у системі державних та комерційних підприємств, пов’язану з наданням послуг щодо захисту інформації на ОІД, які володіють компетентностями необхідними для ефективного захисту інформації на ОІД та здатні вирішувати практичні та науково-дослідні завдання.

2. ЛЕКЦІЙНИЙ МАТЕРІАЛ

Лекція №1

Тема: Нормативно-правове забезпечення захисту інформаційних ресурсів обмеженого доступу

ПЛАН ЛЕКЦІЇ

1. Поняття інформації, її види
2. Вимоги до захисту інформації
3. Термінологія технічного захисту інформації
4. Термінологія технічного захисту інформації

1. Поняття інформації, її види

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (*Закон України Про інформацію № 2657-XII від 2 жовтня 1992 року).*

За змістом інформація поділяється на такі види:
інформація про фізичну особу;
інформація довідково-енциклопедичного характеру;
інформація про стан довкілля (екологічна інформація);
інформація про товар (роботу, послугу);
науково-технічна інформація;
податкова інформація;
правова інформація;
статистична інформація;
соціологічна інформація;
інші види інформації.

Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

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.

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.

Інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище. Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Інформація про стан довкілля (екологічна інформація) - відомості та/або дані про:

- стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;

- фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми).

Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги). Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Правовий режим науково-технічної інформації визначається Законом України "Про науково-технічну інформацію", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та

юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Для практичного використання більш важливою є класифікація інформації за режимом правового доступу до неї (рис. 1.1).

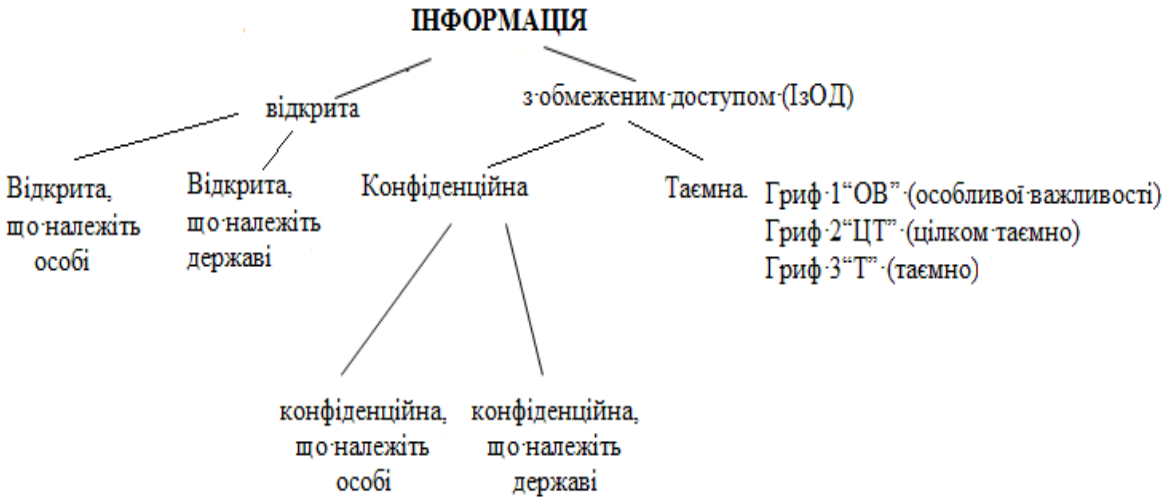

Рис. 1.1 Класифікації інформації за режимом правового доступу

Відкрита інформація – вся інформація окрім віднесеної законом до інформації з обмеженим доступом (п. 2 ст. 20 Закону Про інформацію).

Інформація з обмеженим доступом це інформація яка за своїм правовим режимом поділяється на *конфіденційну* і *таємну*.

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ - надано статус конфіденційної.

Таємна інформація (секретна інформація) - вид 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 Законом, державною таємницею і підлягають охороні державою.

Перелік посад, які дають право посадовим особам, що їх займають, надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником органу державної влади, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження визначеного державним експертом з питань таємниць ступеня секретності такої інформації або скасування рішення про віднесення її до державної таємниці керівники органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі матеріальні носії секретної інформації.

Об’єкт інформаційної діяльності – інженерно-технічна споруда, де здійснюється діяльність пов’язана з інформацією, яка підлягає захисту. (Закон України Про Державну службу спеціального зв’язку та захисту інформації України (ст.1) м. Київ, 23 лютого 2006 року №3475-IV).

2. Система правового регулювання соціальних інформаційних відносин

Відповідно до основних положень, поданих вище, розглянемо систему правового регулювання суспільних інформаційних відносин. Ця система умовно поділяється (за суб'єктами регулювання і виникнення норм права) на дві частини:

1) приватно-правове регулювання (на рівні правочинів, звичаїв, угод, традицій, норм суспільної моралі, корпоративної (ділової) етики);

2) публічно-правове (державне) регулювання. Публічно-правове регулювання знаходить місце у законодавстві: законах, нормативно-правових актах, прирівняних до законів, та підзаконних нормативно-правових актах.

Під категорією "інформаційне законодавство України" ми розуміємо множину нормативно-правових актів, прийнятих Верховною Радою України у формі законів та постанов нормативного змісту, які регулюють суспільні відносини щодо інформації.

За правовою доктриною нашої країни основні положення інформаційного

права базуються на юридичних нормах, визначених у Конституції України, тобто основоположним законодавчим актом у сфері регулювання інформаційних відносин у нашій країні є Конституція України. У публічному праві України вже створено велику кількість нормативних актів, які прямо або опосередковано регулюють інформаційні відносини у різних галузях суспільного буття. Зазначені у Конституції України положення набувають розвитку в 260 Законах України та у 290 Постановах Верховної Ради. Окремі положення правового регулювання суспільних інформаційних відносин відображено в Указах та розпорядженнях Президента України; постановах та розпорядженнях Кабінету Міністрів України; нормативних актах міністерств і відомств.

Системоутворюючим інформаційного законодавства є Закон України "Про інформацію" (від 2 жовтня 1992 р.). Цей Закон закріплює конституційні засади щодо права громадян України на інформацію, закладає правові основи інформаційної діяльності. На підставі Декларації про державний суверенітет України та Акта проголошення незалежності України Закон визначає правові форми міжнародного співробітництва в галузі інформації. Мету і завдання Закону викладено у ст. 2: "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". Ст. З Закону визначає сферу його дії. Вона поширюється на інформаційні відносини, які виникають в усіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Законодавство України про інформацію утворюють: Конституція України; Закон України "Про інформацію"; законодавчі акти про окремі галузі, види, форми і засоби інформації; міжнародні договори та угоди, ратифіковані Україною; принципи і норми міжнародного права. Закон України "Про Національну програму інформатизації" (від 4 лютого 1998 р.) вводить у сферу державного регулювання на законодавчому рівні загальні засади формування, виконання та коригування Національної програми інформатизації, якою визначається стратегія розв'язав- ня проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення. Цим Законом визначаються організаційноправові засади державного регулювання процесів інформатизації в Україні.

За Законом, 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. Національна програма інформатизації формується, виходячи з довгострокових пріоритетів соціально-економічного, науково-технічного, національно-культурного розвитку країни з урахуванням світових напрямів розвитку та досягнень у сфері інформатизації, і спрямована на розв'язання найважливіших загальносуспільних проблем (забезпечення розвитку освіти, науки, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави, демократизації суспільства) та створення умов для інтеграції України у світовий інформаційний простір відповідно до сучасних тенденцій інформаційної геополітики. Національна програма інформатизації становить комплекс взаємопов'язаних окремих завдань (проектів) інформатизації, спрямованих на реалізацію державної політики та пріоритетних напрямів створення сучасної інформаційної інфраструктури України за рахунок концентрації та раціонального використання фінансових, матеріально- технічних та інших ресурсів, виробничого і науково-технічного потенціалу держави, а також координації діяльності органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій усіх форм власності та громадян у сфері інформатизації (ст. 2 Закону).

Завдання законодавства про Національну програму інформатизації визначаються у ст. З названого Закону. Це створення таких засад регулювання процесу формування і виконання цієї Програми та окремих її завдань (проектів):

- правових;
- організаційних;
- науково-технічних;
- економічних;
- фінансових;
- методичних;
- гуманітарних.

Законодавство про Національну програму інформатизації складається з цього Закону та інших нормативно-правових актів. Сферу дії Закону визначено у ст. 4: відносини, що виникають у процесі формування та виконання Національної програми інформатизації. Закон України "Про Концепцію Національної програми інформатизації" (від 4 лютого 1998 р.) розвиває попередній закон, відкриваючи в Україні новий етап взаємодії інформатики та права в соціальних відносинах, — вводить до законодавчої практики державного регулювання такий соціальний феномен, як інформатизація.

Цим законом Верховна Рада України схвалила названу Концепцію. У Цьому нормативному акті подається визначення кількох суттєвих понять інформаційних відносин. Прийняттю цих законодавчих актів передувала відповідна законотворча робота, спрямована на створення правових основ регулювання соціальних інформаційних відносин в Україні. Особливу інституцію в інформаційному законодавстві започатковує Закон України "Про захист

інформації в автоматизованих системах" (від 5 липня 1994 р.). Метою цього Закону є встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації.

Дія Закону поширюється на будь-яку інформацію, що обробляється в автоматизованих системах. Виходячи з інформаційного суверенітету України та загальновизнаних принципів міжнародного порядку у сфері інформації, Закон України "Про державну таємницю" (від 21 січня 1994 р.) регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречуванням та охороною з метою захисту життєво важливих інтересів України у сфері оборони, економіки, зовнішніх відносин, державної безпеки та охорони правопорядку. Згідно із Законом (ст. 1) державна таємниця — це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоду життєво важливим інтересам України і які визнані у порядку, встановленому цим Законом, державною таємницею та підлягають охороні з боку держави.

Ступінь секретності — категорія, яка характеризує важливість такої інформації, можливу шкоду внаслідок її розголошення, ступінь обмеження доступу до неї та рівень її охорони державою. Ст. 2 Закону визначає, що законодавство України про державну таємницю базується на Законі України "Про інформацію" і складається з цього Закону та інших актів законодавства України, прийнятих відповідно до нього. Дія законодавства України про державну таємницю не поширюється на відносини, пов'язані з охороною комерційної чи банківської таємниці, іншої конфіденційної та таємної інформації, якщо остання одночасно не є державною таємницею. Закон України "Про зв'язок" (від 16 травня 1995 р.) встановлює правові, економічні й організаційні основи діяльності в галузі зв'язку в Україні та визначає відносини підприємств, об'єднань, установ і організацій зв'язку з органами державної виконавчої влади, місцевого самоврядування і споживачами послуг зв'язку, а також особливості галузі, пов'язані з особливими суспільними інтересами. Закон захищає інтереси держави, громадян, підприємств, об'єднань, установ і організацій, що користуються послугами зв'язку, а також працівників галузі зв'язку. Відносини у галузі зв'язку (ст. 3) регулюються Конституцією України, цим Законом, іншими актами законодавства України та нормативними актами міністерств і відомств України.

Правовий статус, повноваження та обов'язки операторів зв'язку, а також використання радіочастотного ресурсу визначаються окремими законодавчими актами України. Відповідно до ст. 4 Закону його дія поширюється на відносини у галузі зв'язку, в яких беруть участь органи державної влади, місцевого

самоврядування, підприємства, установи й організації зв'язку та споживачі послуг зв'язку і радіочастот. Дія цього Закону не поширюється (крім питань використання радіочастотного ресурсу) на державну систему урядового зв'язку, а також на мережі технологічного зв'язку, відомчі мережі зв'язку та відносини, що забезпечують функціонування їх, за винятком питань їхньої взаємодії з мережами зв'язку загального користування. Закон України "Про власність" (від 7 лютого 1991 р.) визначає, що Українська держава є суверенною в регулюванні всіх відносин власності на своїй території, у тому числі власності на інформацію, що визначено Законом "Про інформацію". Закон "Про власність" спрямований на реалізацію Декларації про державний суверенітет України.

Мета цього Закону полягає в забезпеченні вільного економічного самовизначення громадян, використанні природного, економічного, науково-технічного та культурного потенціалу республіки для підвищення рівня життя її народу Закон України "Про авторське право і суміжні права" (від 23 грудня 1993 р.) у ст. 1 визначає, що охороняються особисті (немайнові) і майнові права авторів та їхніх правонаступників, пов'язані зі створенням та використанням творів науки, літератури і мистецтва (авторське право), та права виконавців, виробників фонограм і організацій мовлення (суміжні права). Ст. 2 визначає, що законодавство України про авторське право і суміжні права складається з цього Закону та інших законодавчих актів України, що охороняють особисті (немайнові) та майнові права осіб, яким належать авторське право і суміжні права. Закон України "Про охорону прав на винаходи і корисні моделі" (від 15 грудня 1993 р.) регулює відносини, що виникають у зв'язку з набуттям і здійсненням права власності на винаходи і корисні моделі в Україні.

Системоутворюючим інститутом галузі інформаційного права можна вважати Закон України "Про друковані засоби масової інформації (пресу) в Україні" (від 16 листопада 1992 р.). Цей Закон створює правові основи діяльності друкованих засобів масової інформації (преси) в Україні, встановлює державні гарантії свободи їх відповідно до Конституції України, Закону України "Про інформацію" та інших актів чинного законодавства і визнаних Україною міжнародно-правових документів. У ст. 1 "Друковані засоби масової інформації (преса) в Україні" подається визначення, що друкованими засобами масової інформації (пресою) в Україні є періодичні і такі, що продовжуються, видання, які виходять під постійною назвою, з періодичністю один і більше номерів (випусків) протягом року на підставі свідоцтва про державну реєстрацію. Додатки до друкованих засобів масової інформації у вигляді видань газетного та журнального типу є окремими періодичними і такими, що продовжуються, друкованими виданнями і підлягають реєстрації на загальних підставах.

Зазначені в частинах першій та другій цієї статті Закону друковані видання можуть включати до свого складу інші носії інформації (платівки, дискети, магнітофонні та відеокасети тощо), розповсюдження яких не заборонено чинним

законодавством України. Друкований засіб масової інформації вважається виданим, якщо він підписаний до виходу в світ і видрукуваний будь-яким тиражем. Сфера розповсюдження друкованого засобу масової інформації не обмежується. Закон України "Про телебачення і радіомовлення" (від 21 грудня 1993 р.) відповідно до Закону України "Про інформацію" регулює діяльність телерадіоорганізацій на території України, визначає правові, економічні, соціальні, організаційні умови функціонування їх, спрямовані на реалізацію свободи слова, прав громадян на отримання повної, достовірної та оперативної інформації, на відкрите і вільне обговорення суспільних питань. Дія цього Закону поширюється на відносини між суб'єктами в галузі телебачення і радіомовлення незалежно від форм власності, мети створення і виду статутної діяльності цих телерадіоорганізацій, а також від способу розповсюдження телерадіоінформації, якщо їхні передачі розраховані на масове приймання споживачами.

Дія Закону не поширюється на відносини, що регулюють створення та діяльність спеціальних телевізійних і радіомовних систем закритого типу (виробничих, технологічних, навчальних, службових тощо), радіоаматорський зв'язок, радіоспорт або інші види зв'язку, що діють на основі індивідуального виклику чи використовуються для поширення інформації спеціального призначення і не розраховані на масове приймання їхніх передач; на діяльність з неефірного прокату відео- та аудіопродукції в різних установах (ст. З Закону).

3. Взаємозв'язок інформатики та права в інформаційному суспільстві

Взаємозв'язок інформатики та права в інформаційному суспільстві виявляється у кількох аспектах.

По-перше — як наук. Інформатика відпрацьовує методи дослідження, які після відповідної адаптації дають можливість вирішувати проблеми правової науки. Серед таких методів — методи формування гіперсистем, агрегації, комп'ютерного моделювання, алгоритмізації тощо.

По-друге — як галузей суспільної діяльності. Право визначає межі дозволеної поведінки, правопорушення і відповідальності у сфері інформаційних відносин.

Право може забороняти, стримувати або стимулювати інформаційні відносини, розвиток їх, тенденції тощо. На межі інформатики та права виникло таке соціальне явище, як інформаційне право. Категорія "інформаційне право" може розглядатися в кількох аспектах: • як галузь суспільних відносин; • як інституція в юридичній науці; • як навчальна дисципліна. Як галузь суспільних відносин інформаційне право може розглядатися у двох змістах: об'єктивному і суб'єктивному. В об'єктивному змісті інформаційне право — це врегульований нормативними актами комплекс суспільних відносин, об'єктом яких є інформація. У суб'єктивному змісті інформаційне право — це комплекс прав і обов'язків

суб'єктів суспільних відносин щодо інформації.

Як інституція в юридичній науці інформаційне право — це відносно автономна інституція правової науки щодо дослідження проблем суспільних відносин, об'єктом яких є інформація. Як навчальна дисципліна інформаційне право — це комплекс знань, що подаються для вивчення теорії і практики регулювання суспільних відносин, об'єктом яких є інформація.

4. Термінологія технічного захисту інформації

Згідно з Положенням про технічний захист інформації в Україні Затвердженим Указом Президента України від 27 вересня 1999 р. № 1229:

Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їх керівників.

Нормативно-правові акти з технічного захисту інформації є обов'язковими для виконання всіма суб'єктами системи технічного захисту інформації.

Критерії інформаційної безпеки**:**

Цілісність — властивість інформації бути захищеною від несанкціонованого знищення, модифікації.

Конфіденційність — властивість інформації бути захищеною від несанкціонованого ознайомлення.

Доступність — властивість інформації бути захищеною від несанкціонованого блокування.

Об'єкти технічного захисту в інформаційно-комунікаційній системі (ІКС) - інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Суб'єкти системи технічного захисту інформації:

- Держспецзв'язку України; *(Абзац другий пункту 8 із змінами, внесеними згідно з Указом Президента N 333/2008 від 11.04.2008)*

- органи, щодо яких здійснюється ТЗІ;

- науково-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації;

- військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

- навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

- забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

- видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

- здійснення контролю за станом технічного захисту інформації.

Політика безпеки інформації — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Загроза — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Безпека інформації — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Комплекс засобів захисту (КЗЗ) від несанкціонованих дій з інформаціїю — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Захищена комп'ютерна система — комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз.

Користувач — фізична особа, яка може взаємодіяти з (комп'ютерною системою) КС через наданий їй інтерфейс.

Об'єкт-користувач — подання фізичного користувача в КС, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

Ідентифікатор об'єкта КС — унікальний атрибут об'єкта КС, що дозволяє однозначно виділити даний об'єкт серед подібних.

Санкціонований доступ до інформації — доступ до інформації, що не порушує ПРД (правила розмежування доступу).

Захист від несанкціонованого доступу;— запобігання або істотне утруднення несанкціонованого доступу до інформації.

Право доступу — дозвіл або заборона здійснення певного типу доступу.

Повноваження — права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об'єктів.

Авторизація — надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (створившим його користувачем або процесом).

Авторизований користувач — користувач, що володіє певними повноваженнями.

Роль користувача — сукупність функцій щодо керування КС, КЗЗ і обробки інформації, доступних користувачеві.

Адміністратор безпеки — адміністратор, відповідальний за дотримання політики безпеки.

Порушник — користувач, який здійснює несанкціонований доступ до інформації.

Критична інформація — інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація,

ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.

Спостереженість — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Атака — спроба реалізації загрози.

Ризик — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Ідентифікація — процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; впізнання.

Автентифікація — процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

Цифровий підпис — дані, одержані в результаті криптографічного перетворення блоку даних і/або його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника і т. ін.), що дозволяють приймальнику даних впевнитись в цілісності блоку і справжності джерела даних і забезпечити захист від підробки і підлогу.

Види захисту інформації в ІКС.

Організаційний захист інформації — комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення технічного захисту інформації. Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів.

Інженерний захист інформації — попередження руйнування носія інформації внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація). Закон України "Про захист інформації в інформаційно-

телекомунікаційних системах" №80/94-ВР від 05.07.1994 визначає інженерний ЗІ як складову технічного захисту інформації.

Технічний захист інформації - діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами.

Витік інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї

Несанкціонований доступ до інформації в ІКС – це доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Несанкціонований доступ може здійснюватись як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу комп'ютерної системи (КС) розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

Контрольована зона – простір (територія, будівля, частина будівлі), в якому виключено неконтрольоване знаходження співробітників та відвідуівчів організації, а також транспортних засобів. Межою контрольованої зони може бути периметр території организації, а також обмежуючі конструкції охороаняємої будівлі або охороаняємої частини будівлі, якщо воно разміщено на території яка не охороняється.

Комплекс технічного захисту інформації - сукупність заходів і засобів, призначених для реалізації технічного захисту інформації на ОІД. Для оцінки ефективності комплексу ТЗІ проводиться його атестація на відповідність вимогам нормативних документів.

З метою обґрунтування заходів з технічного захисту ІзОД, що циркулює на об'єктах, проводиться, так зване, категорирование. Категорування підлягають об'єкти, в яких обговорюється, циркулює, пересилається, приймається, перетворюється, накопичується, обробляється, відображається і зберігається інформація з обмеженим доступом (ІзОД).

Контрольні запитання

1. Назвати розподіл інформації по видам за змістом.
2. Визначення конфіденційної інформації про фізичну особу
3. Визначення інформації з обмеженим доступом.
4. Визначення таємної інформації.
5. Назвати критерії безпеки інформації.
6. Визначення доступності інформації.
9. Визначення цілісності інформації.
7. Сутність організаційного захисту інформації.

8. Визначення об’єкту інформаційної діяльності.
9. Сутність інженерного захисту інформації.
10. Визначення несанкціонованого доступу до інформації.
11. Призначення технічного захисту інформації.
12. Визначення контрольованої зони.
13. Визначення ідентифікації та автентифікації.
14. Що є об'єктом технічного захисту в ІКС.
15. Визначення політики безпеки інформації.

Лекція №2

Тема: Загрози витоку інформації та несанкціонованих дій з інформацією в інформаційно-комунікаційних системах

ПЛАН ЛЕКЦІЇ

1. Класифікація загроз інформації в інформаційно-комунікаційних системах
2. Шляхи витоку інформації при експлуатації інформаційно-комунікаційних систем
3. Принципи протидії втрати інформації від витоку через побічні електромагнітні випромінювання
4. Типи систем захисту інформації в інформаційно-комунікаційних системах

1. Класифікація загроз інформації в інформаційно-комунікаційних системах

Модель загроз інформації - це опис методів і засобів здійснення загроз для інформації в конкретних умовах функціонування автоматизованої інформаційної системи і можливого збитку від реалізації погрози.

Формування моделі загроз інформації є одним з головних чинників забезпечення її безпеки, оскільки безпосередньо пов'язане з вибором необхідного переліку послуг безпеки, заходів і засобів захисту, що реалізуються в автоматизованій системі (АС). Довершеність і повнота аналізу загроз дає необхідну впевненість, що враховані всі суттєві загрози безпеки інформації.

Конструктивним шляхом створення моделі загроз є формування окремих моделей загроз для кожної компоненти системи зокрема, для АС - центральний вузол АС (наприклад, центральний сервер при клієнт-серверній архітектурі тощо; окремі досить незалежні підсистеми АС; канали зв'язку і комутаційний центр окремих підсистем; вузол зв'язку з Internet і ін.) і типових об'єктів захисту (робочих станцій, серверів, мережевого обладнання ЛВС тощо). Формування окремих моделей загроз повинно здійснюватися на підставі загальної класифікації загроз інформації.

Протягом життєвого циклу кожної АС модель загроз необхідно переглядати в зв'язку з модернізацією і розвитком АС, а також періодично, в зв'язку з удосконаленням технічних і програмних засобів подолання механізмів захисту.

Згідно з нормативними документами ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) за результатами впливу на інформацію і систему її обробки загрози поділяються на чотири класи:

− порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);

− порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав'язування неправдивої інформації);

− порушення доступності інформації (втрата часткова або повна працездатності системи, блокування доступу до інформації);

− втрата спостереженості або керованості системи обробки (порушення процедур ідентифікації та аутентифікації користувачів і процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

Для забезпечення конфіденційності, цілісності та доступності інформації, а також керованості системою (спостереженість) необхідно захищати інформацію не тільки від витоку технічними каналами та несанкціонованого доступу, а й виключати можливість негативного впливу на інформацію, втручання в процес її обробки, порушення працездатності системи. Таким чином, захищати необхідно всі компоненти АС: апаратуру та обладнання, програми, дані, персонал.

Процес прояви можливих загроз інформації (далі - загроз) і впливу їх на інформацію грунтується на системній класифікації (рис. 2.1):

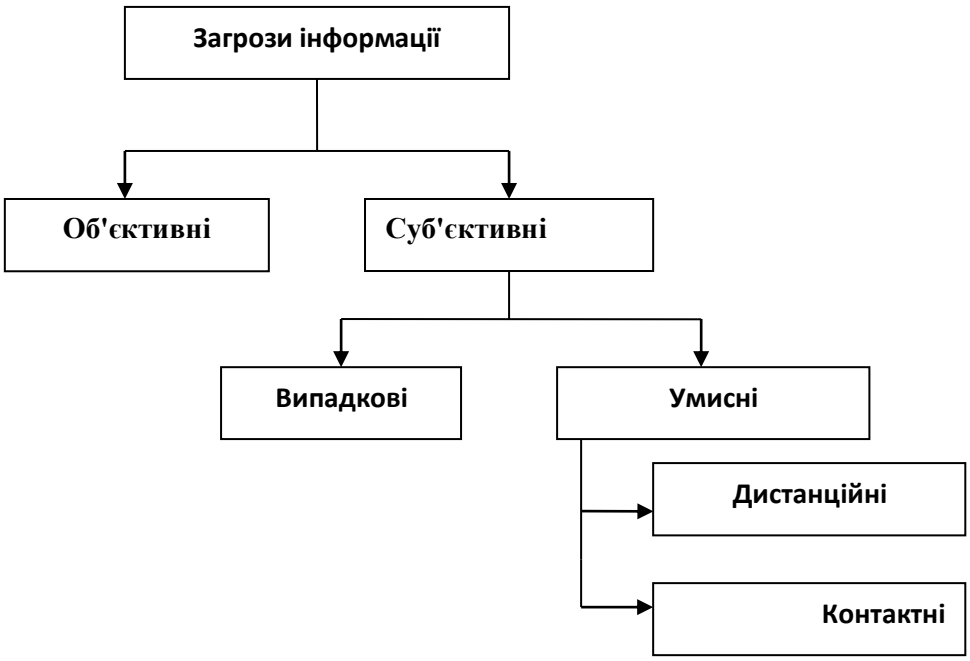

Рис. 2.1.Загальна класифікація загроз інформації в АС

Об'єктивні загрози викликаються стихійними природними явищами та об'єктивними фізичними процесами.

Суб'єктивні загрози є наслідком діяльності людини, технічних засобів і систем;

− за мотивами походження суб’єктивні загрози поділяються на випадкові і навмисні. Випадкові загрози викликаються помилками проектування автоматизованої системи та системи захисту інформації, помилками в програмному забезпеченні, збоями та відмовами апаратури і систем забезпечення, помилками персоналу тощо. Навмисні загрози обумовлені цілеспрямованими діями людей (порушників);

− за місцем розміщення джерела загроз щодо автоматизованої системи навмисні загрози поділяються дистанційні та контактні. До дистанційним відносяться загрози, джерело яких знаходиться за межами контрольованої території. Контактні загрози здійснюються в межах контрольованої зони, як правило, при проникненні в приміщення, де розташовані засоби обробки і зберігання інформації.

Перелік можливих загроз інформації, яка обробляється в автоматизованій системі та циркулює в зв'язку з цим у відповідних приміщеннях, наводиться в таблиці 1. У графі "Наслідки" наведені основні властивості інформації і відповідної автоматизованої системи, порушення яких можливо при реалізації загроз.

2. Шляхи витоку інформації при експлуатації інформаційно-комунікаційних систем

З точки зору захисту інформації ці технічні пристрої є прекрасним прикладом для вивчення практично всіх каналів витоку інформації - починаючи від радіоканалу і закінчуючи матеріально-речовим. Розглянемо детальніше принципи утворення каналів витоку інформації при експлуатації автоматизованої системи (АС).

Як відомо, сучасні АС можуть працювати як незалежно один від одного, так і взаємодіючи з іншими ЕОМ по комп'ютерних мережах, причому останні можуть бути не тільки локальними, а й глобальними.

З урахуванням цього фактора, повний перелік тих ділянок, в яких можуть знаходитися підлягають захисту дані, може мати наступний вигляд:

− безпосередньо в оперативній або постійної пам'яті АС;

− на знімних магнітних, магнітооптичних, лазерних та інших носіях;

− на зовнішніх пристроях зберігання інформації колективного доступу RAID масиви, файлові сервери і т.п.);

− на екранах пристроїв відображення (дисплеї, монітори, консолі);

− в пам'яті пристроїв введення / виведення (принтери, графічні, сканери);

− в пам'яті керуючих пристроїв і лініях зв'язку, що утворюють канали сполучення комп'ютерних мереж.

Природні канали витоку інформації утворюються як при роботі ЕОМ, так і в режимі очікування.

Джерелами таких каналів є:

електромагнітні поля (*радіоканал витоку інформації*) – ПЕМВ (побічні ел. магнітні випромінення АС);

наведення струмів і напруг у проводних системах (живлення, заземлення та з'єднувальних) *(електричний канал витоку*).

Крім того, класифікацію можливих каналів витоку інформації у першому наближенні можна провести на підставі принципів, відповідно до яких обробляється інформація, що отримується з можливого каналу витоку. Передбачаються три типи обробки: людиною, апаратурою, програмою. Відповідно до кожного типу обробки всілякі канали витоку також розбиваються на три групи. Стосовно до ПЕОМ групу каналів, в яких основним видом обробки є **обробка людиною**, складають наступні можливі канали витоку:

− розкрадання матеріальних носіїв інформації (магнітних дисків, стрічок, карт);

− читання інформації з екрану сторонньою особою;

− читання інформації з залишених без нагляду паперових роздруківок.

− У групі каналів, в яких основним видом обробки є обробка апаратурою, можна виділити наступні можливі канали витоку:

− підключення до АС спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

− використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань технічних засобів АС.

У групі каналів, в яких основним видом обробки є програмна обробка, можна виділити наступні можливі канали витоку:

− несанкціонований доступ програми до інформації;

− розшифровка програмою зашифрованої інформації;

− копіювання програмою інформації з носіїв;

− блокування або відключення програмних засобів захисту.

Технічному контролю повинні піддаватися наступні потенційні канали витоку інформації:

− побічні електромагнітні випромінювання в діапазоні частот від 1 МГц до 1000 МГц;

− наведення сигналів в ланцюгах електроживлення, заземлення і в лініях зв'язку;

− щляхи витоку інформації, що утворюються в результаті впливу високочастотних електромагнітних полів на різні дроти, які знаходяться в приміщенні і можуть, таким чином, стати прийомною антеною.

В цьому випадку перевірка проводиться в діапазоні частот від 1 МГц до 1000 МГц

Найбільш небезпечним каналом витоку є дисплей, так як з точки зору захисту інформації він є найслабшою ланкою в системі. Це обумовлено принципами роботи відеоадаптера, що складається зі спеціалізованих схем для генерування електричних сигналів управління обладнанням, яке забезпечує генерацію зображення.

Розглянемо докладніше можливості витоку інформації, що обробляється на ПЕОМ, через побічні електромагнітні випромінювання (ПЕМВ).

При проведенні аналізу можливості витоку інформації необхідно враховувати такі особливості радіоканалу витоку з вузлів цифрової електронної техніки.

Не всі ПЕМВ є небезпечними з точки зору реальної витоку інформації. Як правило, найбільший рівень відповідає неінформативним випромінюванням (в АС найбільший рівень мають випромінювання, породжувані системою синхронізації).

Наявність великої кількості паралельно працюючих електричних ланцюгів призводить до того, що інформативні та неінформативні випромінювання можуть перекриватися за діапазоном (взаємна перешкода).

3. Принципи протидії втрати інформації від витоку через побічні електромагнітні випромінювання

Основними напрямками захисту інформації від витоку технічними каналами є:

- запобігання витоку оброблюваної інформації за рахунок побічних електромагнітних випромінювань і наведень, створюваних функціонуючими технічними засобами, а також за рахунок електроакустичних перетворень;
- виявлення впроваджених на об'єкти і в технічні засоби електронних пристроїв перехоплення інформації (закладних пристроїв).

Захист інформації, що обробляється технічними засобами, здійснюється із застосуванням пасивних і активних методів і засобів.

Пасивні методи захисту інформації спрямовані на:

− ослаблення побічних електромагнітних випромінювань (інформаційних сигналів) основних технічних засобів і систем (ОТЗС) на межі контрольованої зони до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів;

− ослаблення наведень побічних електромагнітних випромінювань (інформаційних сигналів) ОТЗС в сторонніх провідниках і сполучних лініях допоміжних технічних засобів і систем (ДТЗС), що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів;

− виключення (ослаблення) просочування інформаційних сигналів ОТЗС у кола електроживлення, що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів.

Активні методи захисту інформації спрямовані на:

− - створення маскувальних просторових електромагнітних завад з метою зменшення відносини сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗС;

− створення маскувальних електромагнітних перешкод в проводах і сполучних лініях ДТЗС з метою зменшення відносини сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗС.

Існують наступні способи і методів захисту інформації, що обробляється засобами цифрової електронної техніки, від витоку через ПЕМВ.

Електромагнітне екранування приміщень в широкому діапазоні частот є складним технічним завданням, вимагає значних капітальних витрат, постійного контролю і не завжди можливо по естетичним і ергономічним міркуванням. Доопрацювання засобів електронної техніки з метою зменшення рівня ПЕМВ здійснюється організаціями, що мають відповідні ліцензії. Використовуючи різні радіопоглинаючі матеріали і схемо технічні рішення, за рахунок доопрацювання вдається істотно знизити рівень випромінювань. Вартість такого доопрацювання залежить від радіуса необхідної зони безпеки і становить від 20% до 70% від вартості ПЕОМ.

Шифрування здійснюється або програмно, або апаратно за допомогою вбудованих засобів. Такий спосіб захисту виправдовується при передачі інформації на великі відстані по лініях зв'язку.

Активне радіотехнічне маскування передбачає формування і випромінювання маскуючого сигналу у безпосередній близькості від об’єкту, що захищається. Розрізняють декілька методів активного радіотехнічного маскування: енергетичні методи; метод "синфазної перешкоди"; статистичний метод.

При *енергетичному маскуванні методом "білого шуму"* випромінюється широкосмуговий шумовий сигнал з постійним енергетичним спектром, рівень якого істотно перевищує максимальний рівень випромінювання електронної техніки. На даний час дуже поширений. До його недоліків слід віднести створення неприпустимих перешкод радіотехнічним і електронним засобам, що знаходяться поблизу від захищаємої апаратури.

Спектрально-енергетичний метод полягає в генеруванні перешкоди, що має енергетичний спектр, який визначається модулем спектральної щільності інформативних випромінювань техніки. Даний метод дозволяє визначити

оптимальну перешкоду з обмеженою потужністю для досягнення необхідного співвідношення сигнал/перешкода на кордоні контрольованої зони.

Перераховані методи можуть бути використані для захисту інформації як в аналоговій, так і в цифровій апаратурі. Як показник захищеності в цих методах використовується співвідношення сигнал/перешкода. Наступні два методи призначені для захисту інформації у техніці, що працює з цифровими сигналами.

У методі "синфазної перешкоди" в якості маскуючого сигналу використовуються імпульси випадкової амплітуди, що збігаються за формою і часу існування з корисним сигналом. В цьому випадку перешкода майже повністю маскує сигнал, прийом сигналу втрачає сенс, тому що апостеріорні ймовірності наявності і відсутності сигналу залишаються рівними їх апріорним значенням. Показником захищеності в даному методі є гранична повна ймовірність помилки (ГПВП) на кордоні мінімально допустимої зони безпеки. Однак через відсутність апаратури для безпосереднього вимірювання цієї величини пропонується перерахувати ГПВП в необхідне співвідношення сигнал / перешкода.

Статистичний метод захисту інформації полягає в зміні ймовірнісної структури сигналу, що приймається розвідприймачем шляхом випромінювання спеціальним чином сформованого маскуючого сигналу.

До переваг даного методу варто віднести те, що рівень маскуючого сигналу не перевищує рівня інформативних ПЕМВ техніки.

Механізм виникнення ПЕМВ засобів цифрового електронного техніки.

Побічні електромагнітні випромінювання, які генеруються електромагнітними пристроями, обумовлені протіканням диференціальних і синфазних струмів.

У напівпровідникових пристроях електромагнітне поле утворюється при синхронному протікання диференційних струмів в контурах двох типів. Один тип контуру формується провідниками плати або шинами, по яких напівпровідникові прилади підключені до джерела живлення. Інший тип контура утворюється при передачі логічних сигналів від одного пристрою до іншого з використанням у якості зворотнього проводу шини живлення. Провідники передачі даних спільно з шинами живлення формують динамічно працюючі контури, що з'єднують передавальні та прийомні пристрої.

Випромінювання, викликане синфазними струмами, обумовлено виникненням падінь напруги в пристрої, що створює синфазну напругу відносно землі. Як правило, в цифровому електронному обладнанні здійснюється синхронна робота логічних пристроїв. В результаті при перемиканні кожного логічного пристрою відбувається концентрація енергії в імпульсні складові, що збігаються за часом. При їх накладенні між собою, сумарні рівні випромінювання можуть виявитися вище, ніж може створити будь-який з окремих пристроїв.

У багатьох випадках основними джерелами випромінювань виявляються кабелі, по яких передається інформація в цифровому вигляді. Такі кабелі можуть розміщуватися всередині пристрою або з'єднувати їх між собою.

Застосування у якості заземлення обплетення кабелю або проводу, які характеризуються великими індуктивністю і активним опором для ВЧ перешкод, призводить до того, що кабель починає діяти як передавальна антена.

Технічна реалізація пристроїв активного радіотехнічного маскування

Для здійснення активного радіотехнічного маскування ПЕМВ використовуються пристрої, що створюють шумове електромагнітне поле у діапазоні частот від декількох кГц до 1000 МГц із спектральним рівнем, що істотно перевищує рівні природних шумів та інформаційних випромінювань ОТЗС. Для цих цілей використовуються малогабаритні надширокосмугові передавачі шумових маскуютчих коливань.

Сформований генератором шумовий сигнал за допомогою антени випромінюється в простір.

Спектральна щільність випромінюваного електромагнітного поля рівномірно розподілена по частотному діапазону і забезпечує необхідну перевищення маскуючого сигналу над інформативним в задану кількість разів (як вимагають нормативні документи) на кордонах контрольованої зони об'єктів.

4. Типи систем захисту інформації в інформаційно-комунікаційних системах

Комплексна система захисту інформації — взаємопов'язана сукупність організаційних, інженерних та технічних заходів, криптографічних засобів і методів захисту інформації для забезпечення безпеки інформації.

Комплексна система захисту інформації призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, 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.

Організаційний захист інформації — комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення

ТЗІ. Організаційні заходи включають в себе створення *концепції інформаційної безпеки*, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- - навчання правилам інформаційної безпеки користувачів.

Інженерний захист інформації — попередження руйнування носія інформації внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація). Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" №80/94-ВР від 05.07.1994 визначає інженерний ЗІ як складову технічного захисту інформації.

Технічний захист інформації - діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами.

Виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї

Порушення цілісності інформації в системі - - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.

Під НСД розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Несанкціонований доступ може здійснюватись як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу КС розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

До основних способів НСД відносяться:

- безпосереднє звертання до об'єктів з метою одержання певного виду доступу;
- створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє здійснити НСД;
- впровадження в КС програмних або апаратних механізмів, що порушують структуру і функції КС і дозволяють здійснити НСД.

Засіб технічного захисту інформації від НСД – це програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну програмну та/або конструкторську документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз НСД для інформації в КС, або використовується для контролю ефективності захисту інформації від НСД в таких системах.

Захист від НСД може здійснюватися в різних *складових* інформаційної системи:

- прикладне та системне ПЗ.
- апаратна частина серверів та робочих станцій.
- комунікаційне обладнання та канали зв'язку.
- периметр інформаційної системи.

Для захисту периметра ОІД створюються:

- системи охоронної й пожежної сигналізації;
- системи цифрового відеоспостереження;
- системи контролю й управління доступом (СКУД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується такими засобами та заходами:

- використанням екранованого кабелю та прокладка проводів та кабелів в екранованих конструкціях;
- встановленням на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень («капсул»);
- використанням екранованого обладнання;
- встановленням активних систем зашумлення;
- створенням контрольованої зони.

Другий тип системи захисту інформаціх - комплекс технічного захисту інформації від витоку технічними каналами.

Комплекс технічного захисту інформації від витоку технічними каналами – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об’єктах інформаційної діяльності.

Створення комплексу ТЗІ містить у собі проведення організаційних, інженерних і технічних заходів на ОІД, де передбачається:

– озвучення ІзОД (при проведенні нарад, показів зі звуковим супроводженням кіно- і відеофільмів тощо);

– здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання ІзОД тощо);

– обіг іншої ІзОД при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо.

У створенні комплексу ТЗІ беруть участь:

– установа, яка є замовником створення комплексу ТЗІ (далі – замовник або установа-замовник);

– виконавець робіт зі створення комплексу ТЗІ (далі – виконавець робіт з ТЗІ);

– виконавець проведення випробувань щодо створення комплексу ТЗІ (далі – виконавець випробувань);

– виконавець проведення атестації комплексу ТЗІ (далі – виконавець атестації).

Контрольні запитання

1. Як поділяються, за результатами впливу на інформацію і систему її обробки, загрози інформації?
2. Охарактеризувати об’єктивні та суб’єктивні загрози інформації
3. Що являє собою радіоканал витоку інформації?
4. Що являє собою електричний канал витоку інформації?
5. На що спрямовані пасивні методи захисту інформації в АС?
6. На що спрямовані активні методи захисту інформації в АС?
7. Охарактеризувати метод захисту інформаціх - активне радіотехнічне маскування
8. Визначення комплексної системи захисту інформації
9. Розсказати призначення комплексної системи захисту інформації
10. Сутність інженерного захисту інформаціх
11. Сутність організаційного захисту інформації
12. Що застосовується для захисту периметра ОІД?
13. Визначення комплексу технічного захисту інформації від витоку технічними каналами
14. У яких випадках створюється комплекс технічного захисту інформації від витоку технічними каналами?

Лекція № 3

Тема: **Класи автоматизованих систем. Профіль захищеності інформації від несанкціонованого доступу**

ПЛ АНЛЕКЦІЇ

1. Класифікація АС.
2. Функціональні профілі захищеності АС від НСД з інформацією

1. Класифікація АС.

Автоматизована система являє собою організаційно-технічну систему, що об'єднує ОС (сукупність програмних-апаратних засобів, призначених для обробки інформації.), фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми.

За сукупністю характеристик АС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас «1» — одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотні особливості:

в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється;

технічні засоби (носії інформації і засоби У/В) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і/або У/В всієї інформації.

Приклад — автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності.

Приклад — ЛОМ.

Клас «З» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Приклад — глобальна мережа.

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю. В зв'язку з цим, в кожному класі АС виділяються такі підкласи:

– автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності оброблюваної інформації (підкласи «х. К»);

– автоматизована система, в якій підвищені вимоги до — забезпечення цілісності оброблюваної інформації (підкласи «х.Ц»);

– автоматизована система, в якій підвищені вимоги до — забезпечення доступності оброблюваної інформації (підкласи «х.Д»);

– автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності і цілісності оброблюваної інформації (підкласи» х.КЦ»);

– автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності і доступності оброблюваної інформації (підкласи «х.КД»);

– автоматизована система, в якій підвищені вимоги до — забезпечення цілісності і доступності оброблюваної інформації (підкласи «х.ЦД»).

– автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (підкласи «х.КЦД»).

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ ОС, проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

2. Функціональні профілі захищеності АС від несанкціонованих дій з інформацією

Визначення і призначення

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Семантика профілю

Опис профілю складається з трьох частин: буквено-числового ідентифікатора, знака рівності і переліку рівнів послуг, взятого в фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу АС (1, 2 або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов'язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.

Наприклад, 2.К.4 — функціональний профіль номер чотири, що визначає вимоги до АС класу 2, призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення конфіденційності.

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостей реєстрації приведе до появи нової версії. Тим не менше, при внесенні деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого класу чи підкласу АС.

Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені в НД ТЗІ "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

Стандартні профілі

В розд. 7 НД ТЗІ 2.5-005 наведені стандартні профілі захищеності для різних класів АС, що описують вимоги до КЗЗ ОС, які входять до складу цих АС. Оскільки класифікація АС достатньо умовна, той факт, що деякий профіль не потрапив до наведеного нижче переліку, не означає, що він некоректний або гірший за перелічені. Наведені профілі відповідають тим видам КС, потреба в яких найактуальніша.

Розд. 7 являє собою довідник щодо функціональних профілів захищеності для різних класів АС. Багато профілів наведені лише для повноти класифікації, а

не для практичного використання. Особливо це стосується профілів, що містять послуги, які забезпечують захист тільки від одного типу загроз.

До всіх профілів включені послуги спостереженості, оскільки, з одного боку, реалізація багатьох з них є необхідною умовою для реалізації інших послуг, а з іншого, — спостереженість та керованість важливі для будь-якої системи, що реалізує будь-які функції захисту інформації.

Вибір профілю захищеності залежно від призначення автоматизованих систем

1 Стандартні функціональні профілі захищеності в КС, що входять до складу автоматизованих систем, призначених для автоматизації діяльності органів державної влади

В автоматизованих системах, призначених для автоматизації діяльності органів державної влади, часто обробляється інформація з обмеженим доступом. Основними загрозами для інформації в таких системах є загрози, що призводять до несанкціонованого ознайомлення з інформацією, тобто загрози (порушення) конфіденційності. У зв'язку з цим до КЗЗ ОС, що входять до складу АС, , у першу чергу пред'являються вимоги щодо забезпечення конфіденційності оброблюваної інформації, персональної відповідальності користувачів за дотримання режиму секретності.

Політика безпеки, що реалізується, повинна відбивати встановлені в Україні правила роботи з секретними документами. Зокрема, механізми, що реалізують послугу адміністративної конфіденційності, повинні здійснювати розмежування доступу на підставі грифів документів (пасивних об'єктів) і рівнів допуску користувачів.

У зазначених АС рекомендується використовувати ОС, КЗЗ яких реалізують профілі х.К.х. Якщо, крім вимоги забезпечення конфіденційності, існують додаткові вимоги щодо забезпечення цілісності і/або доступності інформації, то рекомендується використовувати профілі х.КЦ.х., КД. х., х. КЦД.х.

2 Стандартні функціональні профілі захищеності КС, що входять до складу автоматизованих систем, які призначені для автоматизації банківської діяльності

Основні загрози для банківської інформації — це в першу чергу загрози шахрайства (підробка, відмова від авторства, відмова від одержання) і порушення технології роботи, а в другу — порушення доступності і конфіденційності. У зв'язку з цим до КЗЗ ОС, що входять до складу банківських АС, пред'являються вимоги щодо забезпечення захисту від зазначених загроз. Крім того, вимоги істотно залежать від того, чи здійснюється обробка в реальному часі або відкладена обробка. Необхідно врахувати, що банківські АС, як правило, відносяться до класу 3, тобто є розподіленими.

В зазначених АС рекомендується використовувати ОС, КЗЗ яких реалізують профілі 3. КЦД.х.

3 Стандартні функціональні профілі захищеності в КС, що входять до складу автоматизованих систем, які призначені для керування технологічними процесами

Основними загрозами для інформації оброблюваної в АС керування технологічними процесами є загрози порушення доступності АС і технології обробки інформації. В зв'язку з цим до КЗЗ ОС, що входять до складу таких АС, в першу чергу пред'являються вимоги до забезпечення доступності і адміністративного керування доступом щодо інформації з боку об'єктів-процесів.

В зазначених АС рекомендується використовувати ОС, КЗЗ яких реалізують профілі 1.ЦД. х., 2.ЦД.х.

4 Стандартні функціональні профілі захищеності в КС, що входять до складу довідково-пошукових систем

Основними загрозами для довідково-пошукових систем масового обслуговування є порушення їх доступності. В зв'язку з цим до КЗЗ ОС, що входять до складу таких систем, в першу чергу пред'являються вимоги щодо забезпечення доступності.

В зазначених АС рекомендується використовувати ОС, КЗЗ яких реалізують профілі х.Д.х., х.ЦД.х.

Побудова і структура критеріїв захищеності інформації

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

- вимоги до функцій захисту (послуг безпеки);
- вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення *n*, де *n* — унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі "Критерії конфіденційності". В цьому розділі описані такі послуги (в дужках наведені умовні позначення для кожної послуги):

довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі "Критерії цілісності". В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі "Критерії доступності". В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі "Критерії спостереженості". В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Гаряча заміна

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти захисту. Основна мета реалізації даної послуги полягає в тому, що встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки, що реалізується нею, стане скомпрометованою.

Необхідною умовою для реалізації всіх рівнів даної послуги, є реалізація рівня НО-1 послуги розподіл обов'язків (і, як наслідок, — рівня НИ-1 послуги ідентифікація і автентифікація), а для рівнів ДЗ-2 і ДЗ-3 — рівня ДС-1 послуги стійкість до відмов, оскільки для того, щоб забезпечити можливість гарячої заміни компонента, система повинна забезпечувати свою працездатність у разі відмови даного компонента.

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають

вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Для того, щоб КС одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

Всі описані послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги *аналіз прихованих каналів* залежність між функціональними послугами і гарантіями відсутня. Рівень послуги *цілісність комплексу засобів захисту* НЦ-1 є необхідною умовою абсолютно для всіх рівнів всіх інших послуг.

Порядок оцінки комп'ютерної системи на предмет відповідності цим Критеріям визначається відповідними нормативними документами. Експертна комісія, яка проводить оцінку комп'ютерної системи, визначає, які послуги і на якому рівні реалізовані в даній комп'ютерній системі, і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

Довірча конфіденційність

Послуги довірча конфіденційність і адміністративна конфіденційність, довірча цілісність і адміністративна цілісність, а також деякою мірою — використання ресурсів, є класичними послугами, що безпосередньо реалізують ту частину політики безпеки, яка складає ПРД.

Основні особливості і відмінність довірчого і адміністративного керування доступом розглянуті в НД ТЗІ 1.1-004-99 “Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу". Система, яка реалізує адміністративне керування доступом, повинна гарантувати, що потоки інформації всередині системи встановлюються адміністратором і не можуть бути змінені звичайним користувачем. З іншого боку, система, яка реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати, в т. ч. створювати нові потоки інформації всередині системи.

Послуга довірча конфіденційність дозволяє користувачеві керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Як правило, під об'єктами, що належать домену користувача, маються на увазі об'єкти, власником яких є користувач (створені користувачем).

Для відображення функціональності КС у простір, в якому не розглядаються права власності, використовується концепція матриці доступу. Матриця доступу являє собою таблицю, уздовж кожного виміру якої відкладені ідентифікатори об'єктів КС, а як елементи матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двовимірною (наприклад, користувачі/пасивні об'єкти) або тривимірною (користувачі/процеси/пасивні об'єкти). Матриця доступу може бути повною, тобто містити вздовж кожної з осей ідентифікатори всіх існуючих в даний час об’єктів КС даного типу, або частковою. Повна тривимірна матриця доступу дозволяє точно описати хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чого (ідентифікатор пасивного об'єкта) та який вид доступу може отримати.

Рівні послуги довірча конфіденційність ранжируются на підставі повноти захисту і вибірковості керування.

Мінімальна довірча конфіденційність (КД-1). Найбільш слабкою мірою гарантії захисту від несанкціонованого ознайомлення є накладення обмеження на одержання інформації процесами. На цьому рівні дозволені потоки інформації від об'єкта тільки до певних процесів. Хоч і не існує обмеження на те, хто може активізувати процес, тобто, хто може одержувати інформацію, КЗЗ обмежує потоки інформації фіксованому списку процесів, грунтуючись на атрибутах доступу об'єктів і процесів. Користувач, домену якого належить об’єкт, може змінювати список процесів, які можуть одержувати інформацію від об'єкта. Для такої системи можна побудувати часткову або повну матрицю доступу процесів до захищених об'єктів.

Базова довірча конфіденційність (КД-2). В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів. Прикладом реалізації даного рівня послуги є реалізоване в UNIX керування доступом на підставі тріад власник / група / всі інші.

Повна довірча конфіденційність (КД-3). Основна відміна від попереднього рівня це те, що КЗЗ повинен забезпечувати більш високу вибірковість керування тим, які користувачі можуть одержати інформацію від об'єкта або ініціювати процес. Користувач, домену якого належить об'єкт, може вказати права доступу для кожного конкретного користувача і групи користувачів. Є можливим включати або вилучати користувачів із списку доступу. Для такої системи можна побудувати повну матрицю доступу користувачів до захищених об'єктів і процесів. Така вибірковість керування може бути одержана, наприклад, за рахунок використання списків доступу.

Абсолютна довірча конфіденційність (КД-4). Даний рівень забезпечує повне керування потоками інформації в КС. Атрибути доступу користувача, процесу і об'єкта повинні містити інформацію, що використовується КЗЗ для визначення користувачів, процесів і пар процес/користувач, які можуть отримати інформацію від об'єкта. Таким чином гарантується, що інформація надсилається об'єктом потрібному користувачеві через авторизований процес. Вимоги до вибірковості керування залишаються такими ж самими, як і для попереднього рівня. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар користувач/процес до захищених об'єктів і процесів.

Для всіх рівнів даної послуги необхідною умовою є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, що цілком очевидно. Для рівнів КД-3 і КД-4 необхідною умовою є реалізація рівня КО-1 послуги повторне використання об'єктів, оскільки, якщо при виділенні об'єкта користувачеві в цьому об'єкті міститься інформація, що залишилась від попереднього користувача, то це може призвести до витоку інформації, і всі зусилля щодо реалізації даних рівнів послуги будуть марні.

Адміністративна конфіденційність

Послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів.

Згідно з політикою адміністративної конфіденційності об'єкту присвоюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі або процеси, які намагаються одержати інформацію. Найбільше розповсюдження отримав механізм, коли у вигляді атрибутів доступу використовуються мітки, що визначають рівень конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином КЗЗ на підставі порівняння міток об'єкта і користувача може визначити, чи є користувач, що здійснює запит на доступ до інформації, авторизованим користувачем.

Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування повністю аналогічне рівням послуги довірча конфіденційність з тією відмінністю, що тільки адміністратор або авторизований

адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

Як і для послуги довірча конфіденційність, для всіх рівнів даної послуги необхідною умовою є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, а для рівнів КА-3 і КА-4 — рівня КО-1 послуги повторне використання об'єктів. Додатковою необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків, оскільки в системі повинні бути визначені ролі звичайного користувача і адміністратора.

Повторне використання об'єктів

КС забезпечує послугу повторне використання об'єктів, якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і скасовуються попередні права доступу до об’єкта. Реалізація даної послуги дозволяє забезпечити захист від атак типу "збирання сміття ".

Критерії не встановлюють, коли саме має виконуватися очищення об'єкта. Залежно від реалізованих механізмів можна виконувати очищення об'єкта під час його звільнення користувачем або безпосередньо перед його наданням наступному користувачу. Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

Контрольні запитання

1. Вихначення автоматизованої системи
2. Охарактризувати АС класу 1
3. Охарактризувати АС класу 2
4. Охарактризувати АС класу 3
5. Охарактеризувати функціональний профіль захищеності АС від несанкціонованих дій з інформацією
6. Семантика функціонального профілю захищеності АС від несанкціонованих дій з інформацією
7. Які основні вимоги до стандартних функціональних профілів захищеності в КС призначених для автоматизації діяльності органів державної влади?
8. Які основні вимоги до стандартних функціональних профілів захищеності в КС призначених для керування технологічними процесами?
9. Розказати про Критерії гарантій профілю захищеності АС від несанкціонованих дій з інформацією
10. Охарактеризувати послугу провіля Абсолютна довірча конфіденційність.

Лекція № 4

Тема: **Створення системи захисту інформації в ІКС**

ПЛАНЛЕКЦІЇ

1. Порядок створення системи захисту інформації в ІКС
2. Категоріювання об’єктів захисту
3. Обстеження середовищ функціонування автоматизованої системи

1. Категоріювання об’єктів захисту

Категорування об’єктів захисту є одним з початкових етапів створення КСЗІ (рис. 4.1).

Категоріюванню підлягають об'єкти, в яких обговорюється, мається, пересилається, приймається, перетворюється, накопичується, обробляється, відображається й зберігається (дали - циркулює) інформація з обмеженим доступом (ізОД).

До об'єктив, що підлягають категоріюванню, відносяться:

- автоматизовані системи (АС) й засоби обчислювальною техніки (ЗОТ), що діють й проектуються;
- технічні засоби, яки призначені для роботи з ізОД й не відносяться до АС, за винятком тих, що засновані на криптографічних методах захисту;
- приміщення, призначені для проведення нарад, конференцій, обговорень тощо з використанням ізОД;
- приміщення, в яких розміщені АС, ЗОТ, інші технічні засоби, призначені для роботи з ізОД, у тому числи й основані на криптографічних методах захисту.

Категоріювання проводиться з метою вживання обгрунтованих заходів щодо технічного захисту ізОД, яка циркулює на об`єктах, вид витоку каналами побічних електромагнітних випромінювань й наводок, а також акустичних (віброакустичних) полив.

Установлюються чотири категорії об'єктів залежно від правового режиму доступу до інформації, що циркулює в них:

- до першої категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, яки становлять державну таємницю, для якою встановлено гриф секретності "особливої важливості";

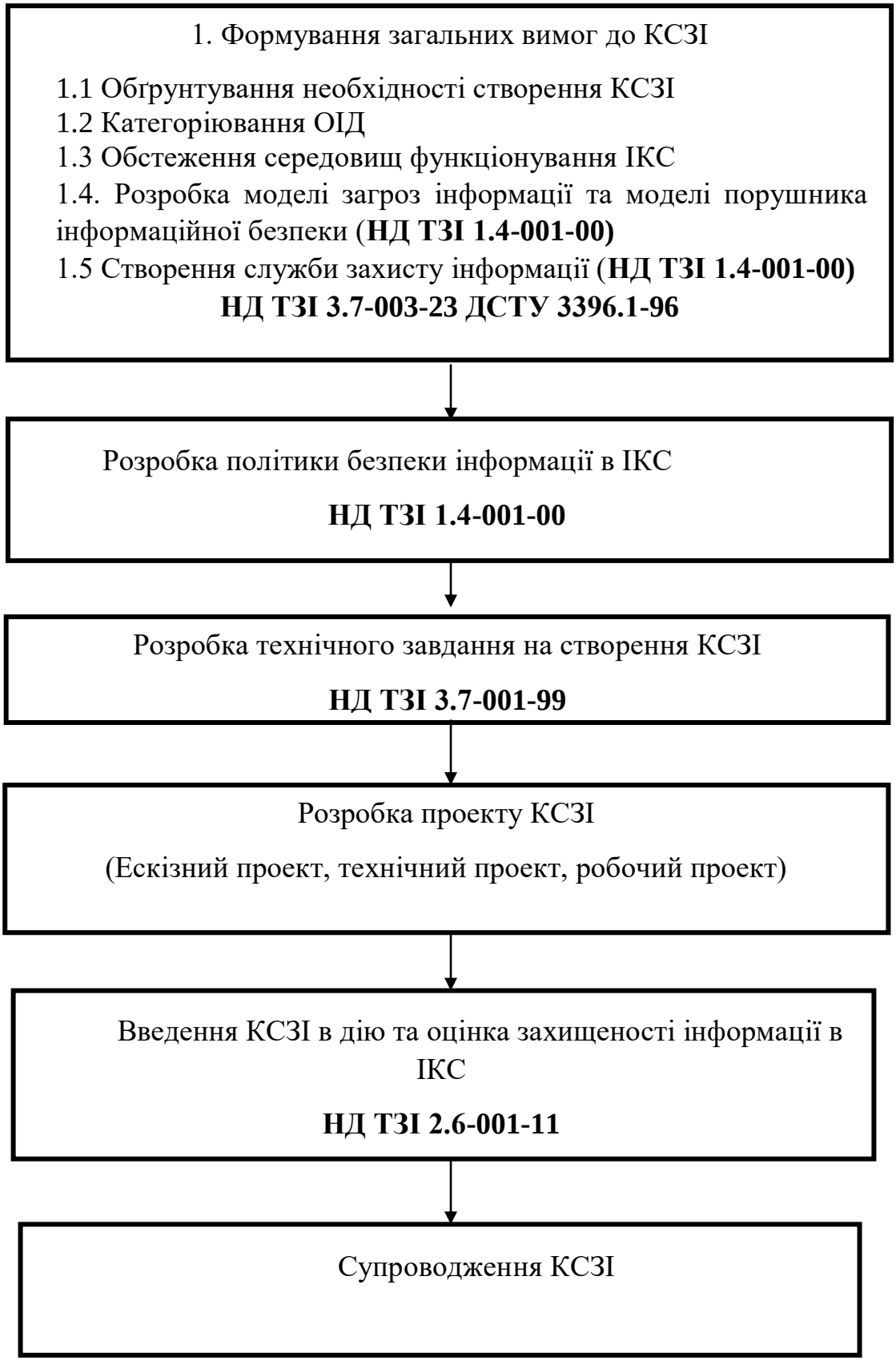

Рис. 4.1 Технологія побудови системи захисту інформації в ІКС

- до другою категорії відносяться об’єкти, в яких циркулює інформація, що містить відомості, яки становлять державну таємницю, для якою встановлено гриф секретності "цілком таємно";

- до третьою категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, яки становлять державну таємницю, для якою встановлено гриф секретності "таємно", а також інформація, що містить відомості, яки становлять іншу передбачену законом таємницю, розголошення якою завдає шкоди особи, суспільству й держави;

- до четвертою категорії відносяться об'єкти, в яких циркулює конфіденційна інформація.

Відповідальність за проведення робіт з категоріювання об'єктів несуть керівники центральних й місцевих органів державною виконавчою влади, органів виконавчою влади Автономною Республіки Крим, місцевих Рад народних депутатів та їх органів, військових частин всіх військових формувань, підприємств, установ й організацій всіх форм власності, представництв України за кордоном (дали - організації) й громадяни, у виданні яких знаходяться відповідні об`єкти.

Для проведення робіт з категоріювання об`єктів наказом керівника організації призначається комісія. У наказі відбивається мета створення комісії, її склад, об'єкти, що підлягають категоріюванню, строки подання результатів.

Комісія з категоріювання визначає:

- вищий гриф секретності інформації, що циркулює на об'єкти;

- підставу для категоріювання (*первинне, планове, у зв`язку зі змінами*).

За результатами роботи комісію складаються акти довільною форми, в яких наводяться зазначені відомості, раніше встановлена категорія та прийняте рішення про категоріювання. Акти затверджуються керівником організації. Під час проведення робіт з категоріювання об`єктів, на яких циркулює інформація, що містить державну таємницю, враховуються додаткові вимоги, викладені у додатку. У цьому випадку комісією складаються акти за формою, наведеною у додатку.

Акти категоріювання об`єктів з підставою для планування й проведення заходив щодо технічного захисту ІзОД відповідно до вимог Положення про технічний захист інформації в Україні та інших чинних нормативно-методичних документів.

Повторне категоріювання об'єкта проводиться у такому ж порядку у випадку змини вищого грифа секретності інформації, що циркулює на об'єкті, і (або) умов розміщення технічних засобів, але не рідше одного разу в 5 років.

Повторне категоріювання об'єкта, на якому циркулює інформація, що містить державну таємницю, проводиться також у випадку змини додаткових чинників, викладених у додатку.

За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об’єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об’єктам може встановлюватися ІІІ категорія.

Об’єкти, яким встановлено відповідну категорію, вносяться до Перелікукатегорійованих об’єктів, який ведеться власником (розпорядником, користувачем) об’єктів інформаційної діяльності.

2. Обстеження середовищ функціонування інформаційно-комунікаційної системи

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 та ін;

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

У НД ТЗІ 3.7-003-23 подано терміни та визначення згідно із ДСТУ 3396.2, ДСТУ 2226, НД ТЗІ 1.1-003.

Інші терміни вживаються у такому значенні:

інформаційна система – організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

комунікаційна 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;

інтегрована система - сукупність двох або кількох взаємопов’язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Під інформаційно-комунікаційною системою в цьому НД ТЗІ розуміється будь-яка система, яка відповідає одному з трьох наведених вище видів автоматизованих систем.

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

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

Створення КЗЗ здійснюється в усіх ІКС, де обробляється інформація, що є власністю держави, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІКС, 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) ІКС з дотриманням вимог нормативно-правових актів щодо провадження господарської діяльності у сфері захисту інформації.

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІКС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

Обстеження середовищ функціонування ІКС

Під час виконання цих робіт ІКС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище

користувачів, оброблювану інформацію і технологію її обробки (далі - середовища функціонування ІКС).

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІКС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

Примітка:

Слід враховувати, що середовища функціонування є множинами, що перетинаються, окремі їхні елементи можуть входити одночасно до різних середовищ і мати в них різні якості. Наприклад, програмне забезпечення може розглядатись обчислювальною системою як об’єкт-процес, а в інформаційному середовищі – як пасивний об’єкт КС.

Обстеження виконується, коли розроблена концепція ІКС (основні принципи і підходи побудови), визначені основні завдання і характеристики ІКС, функціональних комплексів ІКС та існує варіант(и) їх реалізації.

При обстеженні обчислювальної системи ІКС повинні бути проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

- види і характеристики каналів зв'язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

- можливі обмеження щодо використання засобів та ін.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІКС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІКС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об’єктів КС) її представлення в ІКС.

Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІКС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

При обстеженні фізичного середовища здійснюється аналіз взаємного розміщення засобів обробки інформації ІКС на об’єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1.

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІКС (генеральний план, ситуаційний план);

- наявність охорони території та перепускний режим;

- наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІКС;

- режим доступу до компонентів фізичного середовища ІКС;

- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

- наявність елементів комунікацій, систем життєзабезпечення і зв’язку, що мають вихід за межі контрольованої зони;

- наявність та технічні характеристики систем заземлення;

- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов’язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІКС, доступу до ІКС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІКС.

- наявності СЗІ в ІКС.

Результати обстеження середовищ функціонування ІКС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІКС (далі - План захисту), який розробляється згідно з НД ТЗІ 1.4-001.

За результатами обстеження середовищ функціонування ІКС затверджується перелік об'єктів, а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003. Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.

Розробка політики безпеки інформації в ІКС.

Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт

На цьому етапі розробник КСЗІ проводить детальне вивчення об'єкта, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконує у разі необхідності додаткові науково-дослідні роботи, пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з НДР, що виконувалися.

Вибір варіанту КСЗІ.

У загальному випадку за результатами робіт попереднього етапу готуються альтернативні варіанти концепції створення КСЗІ і планів їх реалізації, здійснюється оцінка переваг і недоліків кожного варіанту, вибір найбільш оптимального варіанту. Концепція оформлюється у вигляді звіту.

Оформлення політики безпеки.

На цьому етапі здійснюється:

- вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІКС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

- документальне оформлення політики безпеки інформації.

Політика безпеки може розроблятись для ІКС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001. Політику безпеки рекомендується оформляти у вигляді окремого документу Плану захисту.

Примітка:

1. Положення політики безпеки, які пов'язані з рішеннями, що приймаються на наступних етапах робіт (стосовно проектних рішень, організації робіт, встановлення відповідальності, порядку впровадження і експлуатації КСЗІ та ін.), вносяться до документу після прийняття цих рішень на відповідних етапах.

2. Як виняток виконання робіт, передбачених пп. 6.2, 6.1.3, 6.1.2.9, може включатися до вимог технічного завдання на створення КСЗІ, а самі роботи виконуватись відповідно до етапів, визначених в ТЗ.

Контрольні запитання

1. Для чого проводиться категорування?
2. Ким здійснюється здійснює категорування?
3. Що являється об'єктами категорування?
4. На якому етапі створення системи захисту інформації проводиться категорування?
5. Які існують вили категорування?
6. Що є підставою для проведення позачергового категорування?
7. Які існують категорії об'єктів захисту?
8. Що відноситься до об'єктів четвертої категорії?
9. Яким документом засвідчується категорування?
10. Шо здійснюється при обстеженні фізичного середовища функціонування ІКС?
11. Шо здійснюється при обстеженні обчислювального середовища функціонування ІКС?
12. Шо здійснюється при обстеженні середовища користувачів ІКС?
13. Шо здійснюється при обстеженні інформаційного середовища функціонування ІКС?

Лекція № 5

Тема: Аналіз загроз інформації в автоматизованій системі

План лекції

1. **Політика інформаційної безпеки в АС**
2. **Модель порушника інформаційної безпеки**
3. **Модель загроз інформації в АС**

1. Політика інформаційної безпеки в АС

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги що реалізується системою (набору функцій), і т. Ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама АС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в АС кожного з цих видів.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

*Політика безпеки розробляється на підготовчому етапі створення КС*ЗІ. Методологія розроблення політики безпеки включає в себе наступні роботи:

- розробка концепції безпеки інформації в АС;
- аналіз ризиків;
- визначення вимог до заходів, методів та засобів захисту;
- вибір основних рішень з забезпечення безпеки інформації;
- організація виконання відновлювальних робіт і забезпечення неперервного функціонування АС;
- документальне оформлення політики безпеки.

Концепція безпеки інформації в АС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної АС і виконується на підставі аналізу наступних чинників:

- правових і (або) договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями АС;
- загроз, впливу яких зазнають ресурси АС, що підлягають захисту.
- За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в АС:
- мета і пріоритети, яких необхідно дотримуватись в АС під час забезпечення безпеки інформації;
- загальні напрями діяльності, необхідні для досягнення цієї мети;
- аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;

- відповідальність посадових осіб та інших суб’єктів взаємовідносин в АС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

Аналіз ризиків

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС. **Під час проведення аналізу ризиків** необхідним є виконання наступних робіт:

1. Визначення компонентів і ресурсів АС, які необхідно враховувати при аналізі;

2. Ідентифікація загроз з об’єктами захисту

3. Оцінка ризиків

4. Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз

5. Вибір варіанту побудови КСЗІ:

В залежності від конфіденційності інформації, яка обробляється в АС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника АС, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ. Можливі наступні варіанти:

- досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в АС;

- досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в АС;

- досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в АС.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

6. Оцінювання витрат на КСЗІ

Визначення вимог до заходів, *методів та* ***засобів захисту***

Вихідними даними є:

- завдання і функції АС;

- результати аналізу середовищ функціонування АС;

- модель загроз, модель порушників;

- результати аналізу ризиків.

На підставі цих даних визначаються компоненти АС (наприклад, окрема ЛВС, спеціалізований АРМ, Internet-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в АС.

Вибір основних рішень з забезпечення *безпеки інформації*

Комплекс заходів з забезпечення безпеки інформації розглядається на трьох рівнях:

- правовому;

- організаційному;

- технічному.

Організація проведення відновлювальних робіт і забезпечення неперервного функціонування АС.

- Повинні бути вироблені підходи щодо планування і порядку виконання відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування АС в захищеному режимі. **Під час планування цих робіт рекомендується врахо**вувати наступні питання:

- виявлення критичних з точки зору безпеки процесів у роботі АС;

- визначення можливого негативного впливу **надзвичайних ситуацій** на роботу АС;

- визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;

- підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

- План п**роведення відновлювальних робіт і забезпечення неперервного функціонування АС** повинен описувати дії щодо улагодження інцидента, дії щодо резервування, дії щодо відновлення. Він включає в себе:

- опис типових надзвичайних ситуацій, які потенційно найбільш можливі в АС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;

- опис процедур реагування на надзвичайні ситуації, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;

- опис процедур тимчасового переводу АС або окремих її компонентів на аварійний режим роботи;

- опис процедур поновлення нормальної виробничої діяльності АС або окремих її компонентів;

- порядок тестування плану, тобто проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

*План **п**роведення відновлювальних робіт і забезпечення неперервного функціонування АС підлягає перегляду у разі* виникнення істотних змін в АС. Такими змінами можуть бути:

- встановлення нового обладнання або модернізація існуючого, включення до складу АС нових компонентів;

- встановлення нових систем життєзабезпечення АС (сигналізації, вентиляції, пожежогасіння, кондиціонування та ін.);

- проведення будівельно-ремонтних робіт;

- організаційні зміни у структурі АС, виробничих процесах, процедурах обслуговування АС;

- зміни у технології обробки інформації;

- зміни у програмному забезпеченні;

- будь-які зміни у складі і функціях КСЗІ.

Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів АС, складають правила розмежування доступу (ПРД). ПРД - це певний абстрактний механізм, який виступає посередником при будь-яких взаємодіях об'єктів АС і є найбільш суттєвим елементом політики безпеки.

Результати робіт з розроблення політики безпеки оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в АС. Структурно до політики безпеки (документів, що її складають) повинні входити наступні розділи:

- *загальний*, у якому визначається відношення керівництва АС (організації) до проблеми безпеки інформації;

- *організаційний*, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки та ін.);

- *класифікаційний*, де визначаються матеріальні та інформаційні ресурси, які є у наявності в АС, та необхідний рівень їхнього захисту;

- *розділ, у якому визначаються ПРД до інформації*;

- розділ, у якому визначається підхід щодо керування робочими станціями, серверами тощо;

- розділ, у якому висвітлюються питання фізичного захисту;

- розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;

- розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;

- **розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування АС;**

- юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

Для розробки політики безпеки інформації необхідно визначити модель порушника та модель загроз інформаційної безпеки.

2. Модель порушника інформаційної безпеки

Основою для формування вимог до системи захисту інформації є розробка **моделі загроз** для інформації та **моделі порушника**.

Для побудови ефективної системи захисту інформації в автоматизованих системах управління мало виявити канали витоку інформації, проаналізувати

можливі загрози інформації, наслідки їх реалізації та оцінити втрати. Потрібно ще добре уявляти вигляд порушника.

Порушник це особа, зробив спробу виконання заборонених операцій помилково, незнання або свідомо використовує для цього різні можливості, методи і засоби.

Будь-порушник для реалізації своїх задумів керується певною мотивацією і намірами, володіє сукупністю знань, умінь і навичок здійснення протиправних дій із застосуванням технічних засобів, що мають відповідним потенціалом. Тільки сукупність знань про всі елементи вигляду порушника дозволить адекватно зреагувати на можливі загрози і, відповідно, вибрати відповідні засоби захисту.

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до автоматизованої системи (АС) порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Припускається, що в своєму рівні порушник — це фахівець вищої кваліфікації, який має повну інформацію про комп'ютерну систему (КС) і комплекс засобів захмсту (КЗЗ).

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС — можливість запуску фіксованого набору завдань (програм), що реалізують

заздалегідь передбачені функції обробки інформації;

- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань про АС усіх порушників можна класифікувати як таких, що:

- володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

- володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;

- володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

- використовують виключно агентурні методи одержання відомостей;

- використовують пасивні технічні засоби перехоплення інформаційних сигналів;

- використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

- використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

- без одержання доступу на контрольовану територію організації (АС);

- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

- з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

- з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

- з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

Рекомендується така структура моделі порушника:

Категорії порушників:

- внутрішні порушники;
- користувачі;
- інженерний склад;
- співробітники відділів що супроводжують ПЗ;
- технічний персонал який обслуговує будинок;
- співробітники служби безпеки;
- керівники;

Зовнішні порушники.

Мета порушника:

- отримання необхідної інформації;
- отримання можливості вносити зміни в інформаційні потоки відповідно до своїх намірів;
- завдання збитків шляхом знищення матеріальних та інформаційних цінностей.

Технічна оснащеність порушника:

- апаратні засоби;
- програмні засоби;
- спеціальні засоби.

Повноваження порушника в АС:

- запуск фіксованого набору програм (задач);
- створення і запуск власних програмних засобів;
- керування функціонуванням і внесення змін у конфігурацію системи;
- підключення чи змінення конфігурації апаратних засобів.

Кваліфікація порушника:

- під час проведення аналізу загроз вважають що порушник має високу кваліфікацію.

3. Модель загроз для інформації в АС

Інформація в КС існує у вигляді даних, тобто представляється в формалізованому вигляді, придатному для обробки.

Інформація для свого існування завжди вимагає наявності носія. Як носій інформації може виступати поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

При аналізі проблеми захисту інформації, яка може циркулювати в КС, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції

інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів обчислювального середовища, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою.

Загроза інформації є основним поняттям інформаційної безпеки. Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.

Модель загроз для інформації - формалізований опис методів та засобів здійснення загроз для інформації та їх наслідків. Для побудови такої моделі слід здійснити аналіз моделі порушника і визначити несанкціоновані дії (навмисні чи випадкові) які можне здійснити кожен з таких порушників відносно ресурсів АС.

Для створення **моделі загроз** необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкціонованим доступом 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 та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

- збої і відмови у роботі обладнання та технічних засобів АС;

- наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) АС під час експлуатації;

- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

Джерелом ненавмисних загроз інформаційних систем можуть бути вихід з ладу апаратних чи програмних засобів, неправильні дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні і т.д. Такі загрози можуть нанести значний збиток. Однак більш значними з точки зору ефективності функціонування ІКСМ є навмисні загрози, які, на відміну від випадкових, мають на меті завдання збитків інформаційній системі або користувачам. *Навмисні загрози* можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами, тощо. Наслідки наступні: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- неумисне зараження ПЗ комп'ютерними вірусами;

- невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

- наслідки некомпетентного застосування засобів захисту;

- інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);
- порушення режимів функціонування АС (обладнання і ПЗ);
- впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;
- використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");
- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;
- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
- інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

- на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості АС);
- джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);
- можливі способи здійснення загроз.

Модель загроз є також основою для аналізу можливих збитків внаслідок відсутності засобів чи заходів захисту, а відтак і для визначення можливих контрзаходів. Зрозуміло що визначення найбільш суттєвих загроз є основою для

визначення потрібних засобів захисту відповідних функціональних властивостей захищеності інформаційних ресурсів ,а отже визначення складу потрібних контрзаходів для забезпечення припустимої захищеності, необхідних для захисту засобів, механізмів та функцій захист.

Процедура побудови моделі загроз інформаційній безпеці складається з наступних кроків:

1. Виявлення джерел загроз.
2. Виявлення критичних обєктів інформаційної системи.
3. Виявлення переліку загроз для кожного критичного обєкту.
4. Виявлення способів реалізації загроз.
5. Оцінення матеріальної шкоди та інших наслідків від можливої реалізації загрози.

Моделі загроз складаються на основі постійно змінюющихся даних і тому повинні регулярно пересмотрюватися та обновлятися.

Методика розроблення такої моделі полягає в тому, що в один зі стовпчиків таблиці заноситься по можливості повний перелік видів загроз. Надалі для кожної з можливих загроз шляхом їхнього аналізу (можливо й методом експертних оцінок) необхідно визначити:

— ймовірність виникнення таких загроз. Як перший крок визначення такої ймовірності можна використати її якісні оцінки. У таблиці можуть бути наведені якісні оцінки їхньої ймовірності — неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька;

— на порушення яких функціональних властивостей захищеності інформації вона спрямована (порушення конфіденційності — к, цілісності — ц, доступності — д);

— можливий (такий, що очікується) рівень шкоди. Приклад цієї оцінки наведено також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока). Наявність таких оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної із властивостей захищеності інформації;

— механізми реалізації (можливі шляхи здійснення загроз). Наявність такої інформації дозволяє побудувати загальну модель системи захисту; оцінити значення залишкового ризику, як функцію захищеності по кожній із функціональних властивостей захищеності; визначити структуру системи захисту та її основні компоненти.

Контрольні запитання

1. Визначення безпечної або захищеної системи
2. Які існують класи загроз для інформації.
3. Які існують дестабілізуючі фактори

4. Визначення моделі загроз інформації
5. Процедура побудови моделі загроз
6. Визначення моделі порушника ІБ

Лекція № 6

Тема: Технічне завдання на створення комплексної системи захисту інформації

ПЛАН ЛЕКЦІЇ

1. Загальні вимоги до розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
2. Вимоги до змісту розділів технічного завдання

1. Загальні вимоги до розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

Загальні положення

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі.

Технічне завдання на КСЗІ розробляється у разі необхідності розробки або модернізації КСЗІ існуючої (що функціонує) АС. В разі розробки КСЗІ в процесі проектування АС допускається оформлення вимог з захисту інформації в АС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на АС або розділу загального ТЗ на АС.

Технічне завдання на КСЗІ повинно розроблятись з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу АС.

В технічному завданні на КСЗІ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброблення в обчислювальній системі АС. Додатково треба викласти вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою АС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Перелік вимог з захисту інформації, які включаються в ТЗ на КСЗІ, може бути для кожної конкретної АС як розширений, так і скорочений відносно рекомендованого в даному документі переліку в рамках діючих законодавчих і нормативних документів.

Вимоги повинні передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

Технічне завдання на КСЗІ є одним із обов'язкових засадничих документів під час проведення експертизи АС на відповідність вимогам захищеності інформації.

Порядок розроблення технічного завдання

Вихідними даними для розроблення ТЗ на КСЗІ є функціональний профіль захищеності КС від НСД і вимоги до захищеності інформації від витоку технічними каналами.

Функціональний профіль захищеності інформації в конкретній АС може бути визначений в результаті проведення аналізу загроз та оцінки ризиків або обраний на підставі класу АС відповідно до НД ТЗІ 2.5-005-99.

Вимоги до захищеності інформації від витоку технічними каналами визначаються на підставі НД ТЗІ 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" і ТР ПЕМВН-95 "Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок ".

В технічному завданні повинно бути наведено обгрунтування вибору функціонального профілю захищеності і вимог до показників захищеності інформації від витоку технічними каналами.

Перелік основних робіт етапу формування ТЗ такий:

- - класифікація та опис ресурсів АС (ОС, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, місця зберігання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень і т. ін.);
- - розробка інформаційної моделі для існуючої АС, тобто опис (формальний або неформальний) інформаційних потоків АС, інтерфейсів між користувачем і АС і т. ін.;
- - визначення переліку загроз і можливих каналів витоку інформації;
- - експертна оцінка очікуваних втрат у разі здійснення загроз;
- - визначення послуг безпеки, які треба реалізувати;
- - обгрунтування необхідності проведення спецперевірок і спецдосліджень ЗОТ та інших технічних засобів, а також спеціального обладнання приміщень;
- - визначення вимог до організаційних, фізичних та інших заходів захисту, що реалізуються у доповнення до комплексу програмно-технічних засобів захисту;
- - визначення вимог до метрологічного забезпечення робіт;
- - визначення переліку макетів, що розробляються, і технологічних стендів;
- - оцінка вартості і ефективності обраних засобів;

– - прийняття остаточного рішення про склад КСЗІ.

Вимоги з захисту інформації визначаються замовником, погоджуються з розробником АС і виконавцем робіт по створенню КСЗІ в АС. Виконавець повинен мати відповідну ліцензію Державної служби спеціального зв'язку та та захисту інформації України (Департамент). У випадках, передбачених Положенням про технічний захист інформації в Україні, ТЗ на КСЗІ погоджується з Департаментом.

Зміст технічного завдання

Технічне завдання на КСЗІ оформлюється відповідно до того ж самого ДСТУ, що і основне ТЗ на АС, і в загальному випадку повинно містити такі основні підрозділи:

- загальні відомості;
- мета і призначення комплексної системи захисту інформації;
- загальна характеристика автоматизованої системи та умов її функціонування;
- вимоги до комплексної системи захисту інформації;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;
- порядок внесення змін і доповнень до ТЗ;
- порядок проведення випробувань комплексної системи захисту інформації.

2. Вимоги до змісту розділів технічного завдання

1 Загальні відомості

В підрозділі зазначають:

повне найменування КСЗІ та її умовне позначення;

шифр теми і реквізити договору;

найменування підприємств-розробників і замовника (користувача) КСЗІ та їх реквізити;

перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи;

планові терміни початку і закінчення роботи із створення КСЗІ;

відомості про джерела і порядок фінансування робіт;

порядок оформлення і подання замовнику результатів робіт із створення КСЗІ, з виготовлення і налагодження окремих засобів (технічних, програмних, інформаційних) і програмно-технічних (програмно-методичних) комплексів системи.

2 Мета і призначення комплексної системи захисту інформації

Вказується мета розробки КСЗІ в АС, функціональне призначення і особливості застосування. Необхідно зазначати, на підставі яких нормативно-

правових актів, інших нормативних документів регламентується порядок захисту інформації в АС.

3 Загальна характеристика автоматизованої системи і умов її функціонування

В підрозділі рекомендується зазначити такі моменти, які впливають на безпеку інформації під час її оброблення в АС та на загальні вимоги до реалізації СЗІ:

загальну структурну схему і склад ОС АС (перелік і склад устаткування, технічних і програмних засобів, їх зв'язки, особливості конфігурації і архітектури, особливості підключення до локальних або глобальних мереж тощо);

технічні характеристики каналів зв'язку (пропускна спроможність, типи кабельних ліній, види зв'язку з віддаленими сегментами АС і користувачами і т. ін.);

характеристики інформації, що обробляється (категорії інформації, вищий гриф секретності і т. ін.);

характеристики персоналу (кількість користувачів і категорій користувачів, форми допуску тощо);

характеристики фізичного середовища (наявність категорованих приміщень, територіальне розміщення компонентів АС, їх фізичні параметри, вплив на них чинників навколишнього середовища, захищеність від засобів технічної розвідки і т.п.);

загальну технічну характеристику АС (обсяги основних інформаційних масивів і потоків, швидкість обміну інформацією і продуктивність системи під час розв'язання функціональних завдань, тривалість процедури підготовки АС до роботи після подачі живлення на її компоненти, тривалість процедури відновлення працездатності після збоїв, наявність засобів підвищення надійності і живучості і т. ін.);

особливості функціонування АС (надання машинного часу або устаткування в оренду стороннім організаціям, цілодобовий режим роботи без відключення живлення тощо);

особливості реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту (режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежна охорона і т. ін.);

інші чинники, що впливають на безпеку оброблюваної інформації;

потенційні загрози інформації (способи здійснення НСД, можливі технічні канали витоку інформації і умови їх формування, стихійні лиха і т. ін.), а також можливі наслідки їх реалізації;

клас АС згідно з НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Крім того, треба описати функціонуючі в складі АС (для існуючої АС) засоби захисту, а також засоби захисту, реалізовані в компонентах, які планується використовувати для побудови АС. При цьому треба враховувати, що функції захисту, які реалізуються засобами імпортного виробництва, не мають зв'язаного з ними рівня гарантій. Використання таких засобів у складі КСЗІ можливе тільки за наявності експертного висновку, зареєстрованого Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

В підрозділі не вказуються ті характеристики і умови функціонування АС, опис яких є в ТЗ на АС або в інших документах. Даються тільки посилання на розділи цих документів.

4 Вимоги до комплексної системи захисту інформації

4.1 Вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу

Вимоги до комплексної системи захисту інформації в АС в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу " (далі - Критерії). Згідно з цим документом в процесі оцінки захищеності КС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

Має бути вказаний функціональний профіль захищеності, який передбачається реалізувати. Профіль може бути або вибраний із профілів, описаних в НД ТЗІ 2.5-005-99. Повинен бути вказаний рівень гарантій, що передбачається досягти.

Опису послуг має передувати опис політики безпеки інформації, яку повинен реалізувати комплекс засобів захисту ОС АС. Опис політики безпеки має включати в себе опис:

об'єктів (елементів ресурсів) ОС;

принципів керування доступом користувачів до інформації (довірче і/або адміністративне керування доступом);

правил розмежування інформаційних потоків;

правил маркірування носіїв інформації;

основних атрибутів доступу користувачів, процесів і пасивних об'єктів;

правил розмежування доступу користувачів і процесів до пасивних об'єктів;

правил адміністрування КЗЗ і реєстрації дій користувачів;

інші загальні моменти політики безпеки, які вважає за потрібне описати розробник ТЗ.

Вимоги до послуг безпеки мають бути викладені і згруповані в тому порядку і стилі, в якому вони подані в Критеріях. В розділі мають бути викладені вимоги до реалізації послуг забезпечення:

– конфіденційності;
– цілісності;
– доступності;
– спостереженості.

Для кожної включеної до розділу послуги відповідно до Критеріїв має бути визначений рівень послуги, який передбачається реалізувати. Має бути описана політика даної послуги: визначення об'єктів, до яких застосовується дана послуга, і правил (в тому числі, що застосовуються за умовчуванням), відповідно до яких повинні функціонувати механізми, що реалізують послугу. Відповідно до особливостей розроблюваної АС мають бути конкретизовані всі вимоги, що викладені в Критеріях для відповідного рівня кожної послуги.

У разі, якщо передбачається реалізувати послуги безпеки, які не зазначені в Критеріях, їх також необхідно описати, дотримуючись, по можливості, стилю, прийнятого для опису інших послуг.

Вимоги до гарантій також мають бути викладені і згруповані в тому порядку і стилі, як вони подані в Критеріях. Це передбачає включення вимог:

до архітектури КЗЗ (додатково до загальних вимог до архітектури на даному етапі бажано визначити основні модулі (підсистеми), з яких повинен складатися КЗЗ);

до середовища розробки (організації процесу розробки і системи керування конфігурацією);

до гарантій проектування (етапності розробки і проектної документації);

до середовища функціонування;

до експлуатаційної документації;

до випробувань комплексу засобів захисту.

Всі вимоги повинні відповідати належному рівню гарантій.

Оскільки деякі з вимог гарантій стосуються розроблюваної системи в цілому, а не тільки КЗЗ, то в даному розділі допускається дати посилання на інші підрозділи ТЗ. Зокрема, вимоги до етапності розробки і складу документації мають бути визначені в розділах "Вимоги до складу проектної та експлуатаційної документації" та "Етапи виконання робіт". Крім того, допускаються посилання на інші документи, що розробляються на більш пізніх етапах.

4.2 Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами

Мають бути сформульовані загальні вимоги до об'єктів (компонентів АС), що захищаються, визначені засоби захисту і засоби їх використання (наприклад, реалізація вимог до захищеності повинна досягатись без застосування екранування приміщень, активні засоби мають застосовуватись тільки для захисту інформації головного сервера АС і т. ін.).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами.

Мають бути вказані вимоги до розмірів зони безпеки інформації.

Мають бути вказані необхідні величини показників захищеності, що враховують реальну завадову обстановку на об'єкті електронної обчислювальної техніки. Основними показниками є:

відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завад на об'єкті ЕОТ;

відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завад на об'єкті ЕОТ;

величина нерівномірності струму, який споживається по мережі електроживлення;

коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх ЕМВ.

Гранично допустимі значення основних показників є нормованими величинами і визначаються за відповідними методиками.

Відношення розрахованих (виміряних) значень основних показників до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації.

Мають бути вказані вимоги щодо застосування способів, методів і засобів досягнення необхідних показників захищеності. Рекомендується застосування таких способів, методів і засобів:

а) системо- і схемотехнічних методів:

обмеження використання інтерфейсів з передачею сигналів у вигляді послідовного коду і в режимі багатократних повторень;

використання мультиплексних режимів обробки інформації, а також ЗОТ і системного забезпечення, що базуються на багаторозрядних платформах, інтерфейсів з передачею сигналів у вигляді багаторозрядного паралельного коду;

використання раціональних способів монтажу, за яких забезпечується мінімальна довжина електричних зв'язків і комунікацій;

використання ЗОТ і технічних засобів, до складу яких входять стійкі до самозбудження схеми, розв'язувальні і фільтрувальні елементи, комплектуючі з низькими рівнями ЕМВ;

використання мережевих фільтрів для блокування витоку ІзОД мережами електроживлення, а також лінійних (високочастотних) фільтрів для блокування витоку ІзОД лініями зв'язку;

використання ЗОТ і технічних засобів у захисному виконанні;

б) засобів просторового і лінійного "зашумлення";

в) засобів локального або загального екранування;

г) засобів оптимального розміщення ЗОТ і технічних засобів з метою мінімізації зони, в межах якої граничне відношення сигнал/шум не перевищує встановлених норм.

Мають бути вказані вимоги до проведення спецдосліджень ЗОТ і технічних засобів, мета яких — пряме вимірювання показників ЕМВ.

Мають бути вказані вимоги до проведення спецперевірки ЗОТ, мета якої — виявлення та вилучення (блокування) спеціальних електронних (закладних) пристроїв.

5 Вимоги до складу проектної та експлуатаційної документації

В цьому розділі слід навести перелік проектної та експлуатаційної документації, що розробляється в процесі створення КСЗІ в АС.

Склад обов'язкової проектної і експлуатаційної документації визначається вимогами нормативних документів, відповідно до яких проводиться розробка (зокрема, вимогами Критеріїв для відповідного рівня гарантій). Повний перелік необхідної документації визначається розробником КСЗІ і погоджується із замовником.

6 Етапи виконання робіт

Процес створення КСЗІ доцільно поділяти на три основні етапи: попередній, проектування і розробки КСЗІ, проведення випробувань і передачі в експлуатацію КСЗІ. Кожний з етапів допускається поділяти на окремі підетапи.

Приблизний перелік основних робіт, що проводяться на попередньому етапі, наведено в підрозділі 5.

До переліку робіт етапу проектування і розробки КСЗІ включаються роботи з вибору і модернізації штатних засобів захисту ПЗ і апаратури, що використовуються, архітектури ЗОТ, стандартних інтерфейсів і протоколів обміну, а також з розробки додаткового ПЗ і апаратної частини засобів захисту.

Етап випробувань і передачі в експлуатацію КСЗІ містить роботи, пов'язані з забезпеченням організації та проведення випробувань, включаючи, в разі необхідності, розробку спеціальної апаратури, ПЗ і відповідної документації.

Всі основні роботи кожного етапу відображаються в календарному плані, де зазначаються терміни проведення робіт за окремими етапами, види звітності і форми подання результатів замовнику.

7 Порядок внесення змін і доповнень до технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

Зміни затвердженого ТЗ на створення КСЗІ в АС, необхідність внесення яких виявлена в процесі виконання робіт, оформляються окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до ТЗ на створення КСЗІ в АС складається з вступної частини і змінюваних підрозділів. У вступній частині зазначається причина випуску

доповнення. В змінюваних підрозділах наводяться номери та зміст змінюваних, нових або пунктів, що скасовуються.

8 Порядок проведення випробувань комплексної системи захисту інформації

Для кожного виду випробувань (попередніх, державних, сертифікаційних та ін.) комплексної системи (підсистеми, компонента) захисту виконавець розробляє "Програму і методику випробувань комплексної системи (підсистеми, компонента) захисту інформації в АС", яка затверджується в установленому порядку. Терміни подання проекту Програми, його розгляду і затвердження погоджуються з замовником.

Для проведення випробувань замовником призначається комісія, склад якої погоджується з розробником КСЗІ.

Випробування проводяться з використанням умовної інформації (що не є ІзОД).

Наводиться необхідне для проведення випробувань забезпечення (необхідна нормативна, методична та інша документація, програмні та технічні засоби, метрологічне, спеціальне та інше обладнання, створення інших умов для проведення випробувань), сторона, що його надає, порядок усунення зауважень і т.ін.

Наводиться перелік документів, якими завершуються випробування (етапи випробувань): акт приймання, сертифікат (атестат, експертний висновок) відповідності встановленим критеріям, наказ про введення в експлуатацію тощо.

Контрольні запитання

1. Розказати основні роботи етапу формування ТЗ
2. Зміст технічного завдання
3. Зміст розділу ТЗ загальні відомості
4. Зміст розділу ТЗ мета і призначення комплексної системи захисту інформації
5. Зміст розділу загальна характеристика автоматизованої системи і умов її функціонування
6. Структура розділу ТЗ вимоги до комплексної системи захисту інформації
7. Що відзначається у розділі ТЗ вимоги до складу проектної та експлуатаційної документації
8. Які вимоги до складу проектної та експлуатаційної документації
9. З яких основних етапів складається процес створення КСЗІ
10. Який порядок внесення змін і доповнень до технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
11. Який, у відповідності до ТЗ, порядок проведення випробувань комплексної системи захисту інформації

Лекція № 7

Тема: Проект комплексної системи захисту інформації в ІКС

ПЛАН ЛЕКЦІЇ

1. Ескізний проект КСЗІ.
2. Технічний проект.
3. Робочий проект.
4. Техноробочий проект.

Після узгодження «Технічного завдання на створення КСЗІ» з Контролюючим органом Виконавець розробляє пакет документів Проект КСЗІ. Це комплект документів, до якого входить частина документів розроблених на попередніх етапах і ряд нових документів , в яких описано , як саме створюватиметься, експлуатуватися і, в разі необхідності, модернізуватися КСЗІ.

Під час розробки проекту обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. Проект виконується на таких стадіях створення ІКС: ескізна, технічна та робоча. Для всіх стадій розробки проекту склад документації визначається ТЗ, види та зміст – ГОСТ 34.201 — 89 «Виды, комплектность и обозначение документов при создании автоматизированных систем». Документація на програмні засоби складається згідно комплексу стандартів Єдиної системи проектної документації (далі – ЄСПД), а на технічні засоби – згідно з комплексом стандартів Єдиної системи конструкторської документації (далі - ЄСКД)

Дозволяється вилучати етап “Ескізний проект КСЗІ”, а також поєднувати етапи “Технічний проект КСЗІ” і “Робочий проект КСЗІ” в один етап “Техноробочий проект КСЗІ”.

1. Ескізний проект КСЗІ.

На цьому етапі здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Пропонуються попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ.

На цій стадії визначаються:

– функції КСЗІ в цілому та функції її окремих складових частин;

– склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту;

– склад КЗЗ від НСД;

– склад комплексів ТЗІ від витоку технічними каналами та спеціальних впливів;

- готується та оформляється документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розроблення відповідних засобів.

- пропонуються попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ. Дозволяється вилучати стадію ескізного проекту, у такому випадку документація ескізного проекту не розробляється.

Виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня технічного проекту.

Дозволяється вилучати стадію ескізного проекту, у такому випадку документація ескізного проекту не розробляється.

2. Технічний проект КСЗІ (Розробка проектних рішень КСЗІ)

Технічний проект

На цій стадії виконується розробка:

– загальних проектних рішень, необхідних для реалізації вимог ТЗ;

– рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів);

– рішень щодо архітектури КЗЗ від НСД (у тому числі щодо АнтиВірПЗ, засобів виявлення та попередження про мережеві вторгнення тощо);

– рішень щодо механізмів реалізації послуг безпеки, визначених ФункцПрофЗах;

– рішень щодо алгоритмів, порядку та умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ для реалізації певних функцій захисту.

Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до заданих рівнем гарантій реалізації послуг безпеки згідно вимог НД ТЗІ.

Виконується розробка, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ. Зміст та стиль проектної документації повинні бути достатніми для забезпечення реалізації вимог ТЗ.

Готується та оформляється документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розробку відповідних засобів.

Здійснюється розроблення, оформлення і затвердження завдань на проектування з суміжних питань, які пов'язані зі створенням КСЗІ або впливають на умови її функціонування (будівельні, електротехнічні, санітарно-технічні та інші підготовчі роботи).

3. Робочий проект КСЗІ

На цьому етапі здійснюється розроблення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та, у разі необхідності, її окремих складових частин.

У документації робочого проекту КСЗІ мають бути наведені детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ та взаємодії її компонентів, а також відомості, необхідні для проведення пусконалагоджувальних робіт і тестування підсистем та засобів КСЗІ.

Проводиться розробка засобів захисту інформації, або адаптація готової продукції до умов функціонування КСЗІ. Розробка засобів захисту інформації від НСД здійснюється згідно з НД ТЗІ 3.6-001 (*Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.*).

До складу робочої документації на комплекси технічного захисту інформації від витоку технічними каналами повинні входити схеми розміщення ОТЗ ІКС, кабельного обладнання, мереж живлення та систем заземлення, які виконуються у відповідності до вимог нормативних документів ТР ЕОТ – 95, ТР ТЗІ-ПЕМВН-95, СТР-2, СТР-3, СВТР-78. При цьому враховуються умови їх розміщення і мінімально допустимі відстані між цими засобами та ДТЗ (засоби зв'язку, системи та засоби кондиціювання, сигналізації, електроосвітлення, радіомовлення, тощо), що знаходяться у приміщенні, де розташоване обладнання ІКС, та у суміжних приміщеннях. Зазначені умови розміщення та мінімально допустимі відстані беруться з експлуатаційної документації, яка супроводжує сертифіковані ОТЗ.

Зазначені умови розміщення та мінімально допустимі відстані беруться з експлуатаційної документації, яка супроводжує сертифіковані засоби ІКС.

До складу робочої документації на КЗЗ повинні входити описи таких процедур:

– інсталяції та ініціалізації комплексу,

– налагодження всіх механізмів розмежування доступу користувачів до ресурсів ІКС,

– формування та актуалізації баз даних захисту,

– контролю за діями користувачів,

– контролю цілісності ПЗ та баз даних захисту.

Експлуатаційна документація включає настанови (інструкції) користувачам та опис порядку функціонування та супроводження КСЗІ впродовж життєвого циклу ІКС.

Документація кожної стадії проектування має бути затверджена розробником КСЗІ (за його наявності) та керівником установи-власника (розпорядника) ІКС.

4. Техно-робочий проект

Згідно вимог вище зазначених стандартів техно-робочий проект повинен містити такі документи:

1) відомість проекту;
2) відомість виробів, що закуповуються;
3) пояснювальна записка до проекту;
4) опис завдань і функцій;
5) опис інформаційного забезпечення;
6) опис комплексу технічних засобів;
7) опис програмного забезпечення;
8) опис комплексу засобів захисту від НСД;
9) опис алгоритмів реалізації послуг безпеки;
10) опис організаційної структури;
11) відомість устаткування та матеріалів;
12) кошторисний розрахунок створення КСЗІ;
13) проектна оцінка надійності КСЗІ.

1. Документ «Відомість проекту» містить перелік всіх документів, розроблених на передпректних стадіях створення КСЗІ.

2. Документ «Відомість виробів, що закуповуються» містить перелік виробів, які планується придбати для створення КСЗІ.

3. Документ «Пояснювальна записка до проекту» містить такі розділи:

– загальні положення;

– інформаційна діяльність;

– основні технічні рішення;

– підготовка КСЗІ до введення в дію.

3.1. У розділі «Загальні положення» наводять:

– найменування ІКС і найменування документів, їх номери та дати затвердження, на підставі яких ведеться проектування КСЗІ;

– перелік організацій, що беруть участь в розробці КСЗІ, терміни виконання стадій проектування;

– мета, призначення та сфери використання КСЗІ;

– підтвердження відповідності проектних рішень діючим нормативно-правовим актам;

– перелік використаних при проектуванні нормативно-технічних документів;

– перелік етапів створення КСЗІ і обсяг кожного етапу.

3.2. У розділі «Інформаційна діяльність» відображають склад процедур (операцій) інформаційної діяльності з урахуванням взаємодії всіх заходів захисту інформації, формують вимоги до організації робіт в реальних умовах функціонування ІКС.

3.3. У розділі «Основні технічні рішення» наводять рішення щодо:

– структури КСЗІ, засобів і способів інформаційного обміну між її компонентами;

– взаємодії всіх заходів захисту інформації в ІКС;

– режимів функціонування та діагностування роботи КСЗІ;

– чисельності, кваліфікації та функцій персоналу ІКС, режиму його роботи та порядку взаємодії;

– складу функцій і завдань, що реалізовуються КСЗІ;

– комплексу технічних засобів КСЗІ, його розміщення на об'єкті;

– складу інформації, обсягу, способів її організації, видів машинних носіїв, послідовності обробки інформації та інших компонентів;

– програмних засобів, алгоритмів процедур і методів їх реалізації.

3.4. У розділі «Підготовка КСЗІ до введення в дію» приводять заходи щодо:

– навчання персоналу ІКС та перевірки його кваліфікації;

– створення необхідних підрозділів і робочих місць;

– проведення змін в ІКС для впровадження КСЗІ тощо.

4. Документ «Опис завдань і функцій» містить два розділи:

– опис завдань КСЗІ;

– опис функцій КСЗІ.

4.1. У розділі «Опис завдань» наводять:

– призначення завдань захисту інформації;

– перелік об'єктів і підрозділів установи, при керуванні якими вирішуються завдання КСЗІ;

– умови, при яких припиняється вирішення завдань КСЗІ (за необхідністю);

– взіємодія даного комплексу завдань з іншими комплексами (завданнями) ІКС;

– посади осіб і (або) найменування підрозділів, що визначають умови та характеристики вирішення конкретного завдання КСЗІ;

– розподіл дій між персоналом і технічними засобами при різних ситуаціях вирішення комплексу завдань КСЗІ.

4.2. У розділі «Опис функцій» наводять:

– перелік початкових матеріалів і документів, використаних при розробці проекту КСЗІ;

– опис функцій, спрямованих на виконання завдань КСЗІ;

– перелік підсистем КСЗІ з визначенням функцій та завдань, що реалізовуються в кожній підсистемі;

– необхідні пояснення до розподілу функцій на дії (операції), що виконуються технічними засобами та персоналом;

– перелік типових рішень з визначенням функцій та завдань захисту, для виконання яких вони застосовуються.

5. Документ «Опис інформаційного забезпечення» містить такі розділи:

– склад інформаційного забезпечення;

– організація інформаційного забезпечення;

– організація поводження з інформацією;

– організація інформаційної бази КСЗІ;

– організація інформаційних баз ІКС.

5.1. У розділі «Склад інформаційного забезпечення» вказують найменування та призначення всіх баз даних ІКС і КСЗІ.

5.2. У розділі «Організація інформаційного забезпечення» наводять:

– принципи організації інформаційного забезпечення ІКС і КСЗІ;

– обгрунтування вибору носіїв даних і принципи розподілу інформації по типах носіїв;

– опис прийнятих видів і методів контролю технологій обробки даних при створенні та функціонуванні інформаційних баз з визначенням вимог контролю.

5.3. У розділі «Організація поводження з інформацією» наводять:

– перелік джерел і носіїв інформації з оцінюванням інтенсивності та обсягу потоків інформації;

– опис загальних вимог до організації поводження з інформацією, її контролю та коригування.

5.4. У розділі «Організація інформаційної бази КСЗІ» наводять:

– опис принципів побудови інформаційної бази КСЗІ, характеристики її складу та обсягу;

– опис структури інформаційної бази КСЗІ на рівні баз її даних з визначенням функцій КСЗІ, при реалізації яких використовують кожну базу даних, характеристики даних, що містяться в кожній базі даних.

5.5. У розділі «Організація інформаційних баз ІКС» наводять характеристики складу і обсягу інформаційних баз ІКС та принципи їх побудови.

6. Документ «Опис комплексу технічних засобів» містить такі розділи:

– загальні положення;

– структура комплексу технічних засобів;

– засоби обчислювальної техніки;

– апаратура обміну даними.

6.1. У розділі «Загальні положення» наводять початкові дані, використані при проектуванні технічного забезпечення КСЗІ.

6.2. У розділі «Структура комплексу технічних засобів» наводять:

– обгрунтування вибору структури комплексу технічних засобів (КТЗ), зокрема технічні рішення щодо використання КЗЗ від НСД, мережного та зв’язкового обладнання, комплексу ТЗІ та посилання на документи, що підтверджують їх постачання або придбання;

– опис функціонування КТЗ, зокрема в пускових і аварійних режимах;

– опис розміщення КТЗ на об'єкті з урахуванням виконання вимог техніки протипожежної та електробезпеки, а також дотримання технічних умов експлуатації технічних засобів;

– обгрунтування методів захисту технічних засобів від несанкціонованого доступу до них;

– план розташування КТЗ, систем електроживлення та заземлення на схемі об’єкта, де встановлена ІКС.

6.3. У розділі «Засоби обчислювальної техніки» наводять:

– обгрунтування та опис основних рішень з вибору ПЕОМ;

– обгрунтування та опис основних рішень з вибору типів периферійних засобів, зокрема засобів отримання, контролю, підготовки, збору, реєстрації, зберігання і відображення інформації;

– опис структурної схеми технічних засобів, розміщених у серверному приміщенні (за необхідністю) та на робочих місцях персоналу;

– результати розрахунку або розрахунок кількості засобів і потреби в машинних носіях даних;

– обгрунтування чисельності персоналу, що забезпечує функціонування засобів в різних режимах;

– технічні рішення з оснащення робочих місць персоналу, включаючи опис робочих місць і розрахунок їх площ;

– опис особливостей функціонування засобів в пусковому, нормальному і аварійному режимах.

6.4. У розділі «Апаратура обміну даними» наводять:

– обгрунтування та опис рішень з вибору засобів телекомунікацій та обміну даними, зокрема рішення з вибору каналів зв'язку (цифрових потоків) та результати розрахунку або розрахунок їх кількості;

– рішення з вибору технічних засобів, що забезпечують сполучення ПЕОМ в мережі (комутатор), зокрема результати розрахунку (або розрахунок) їх потреби;

– рішення з вибору технічних засобів, що забезпечують сполучення з каналами зв'язку (модем), зокрема результати розрахунку (або розрахунок) їх потреби;

– вимоги до орендованих каналів зв'язку (цифрових потоків);

– відомості про розміщення пунктів віддалених абонентів і характеристики передаваних даних;

– основні показники надійності, достовірності та інших технічних характеристик засобів

телекомунікацій та обміну даними.

7. Документ «Опис програмного забезпечення» містить такі розділи:

– структура ПЗ;

– функції ПЗ;

– операційна система;

– антивірусне ПЗ;

– прикладне та спеціальне ПЗ.

7.1. У розділі «Структура ПЗ» наводять перелік ПЗ з визначенням їх взаємодії та обгрунтуванням застосування кожного з них.

7.2. У розділі «Функції ПЗ» наводять призначення та опис основних функцій для кожного програмного засобу.

7.3. У розділі «Операційна система» наводять:

– найменування, позначення і стислу характеристику обраної ОС та її версії з обгрунтуванням вибору та указанням її виробника;

– найменування керівництва, згідно якого повинна здійснюватися експлуатація обраного варіанту ОС;

– експертний висновок щодо відповідності ОС вимогам НД ТЗІ, його номер та термін дії;

– опис функціонального профілю захищеності та рівня гарантій.

7.4. У розділі «Антивірусне ПЗ» (далі – АВПЗ) наводять:

– найменування, позначення і стислу характеристику обраного АВПЗ та його версії з обгрунтуванням вибору та указанням його виробника;

– найменування керівництва, згідно якого повинна здійснюватися експлуатація обраного варіанту АВПЗ;

– експертний висновок щодо відповідності АВПЗ вимогам НД ТЗІ, його номер та термін дії;

– опис функціонального профілю захищеності та рівня гарантій.

8. Документ «Опис КЗЗ від НСД» містить, крім загальних положень, такі описи:

– призначення та функцій;

– структури;

– ФПЗ;

– послуг безпеки.

8.1. У розділі «Загальні положення» наводять:

– найменування, позначення і стислу характеристику обраного КЗЗ та його версії з обгрунтуванням вибору та указанням його виробника;

– найменування керівництва, згідно якого повинна здійснюватися експлуатація обраного варіанту КЗЗ;

– експертний висновок щодо відповідності КЗЗ вимогам НД ТЗІ, його номер та термін дії.

8.2. У розділі «Опис призначення та функцій» наводять призначення та сферу застосування, перелік основних характеристик та функцій КЗЗ.

8.3. У розділі «Опис функціонального профілю захищеності» наводять функціональний профіль захищеності та рівень гарантій реалізації послуг безпеки, який забезпечує КЗЗ.

8.4. У розділі «Опис послуг безпеки» наводять перелік і опис послуг:

– конфіденційності;

– доступності;

– цілісності;

– спостереженості.

9. Документ «Опис алгоритмів реалізації послуг безпеки» містить опис алгоритмів реалізації КЗЗ таких послуг безпеки:

– ідентифікація та автентифікація користувачів;

– розмежування обов'язків користувачів;

– розмежування доступу користувачів до каталогів і файлів;

– керування потоками інформації;

– контроль за виведенням інформації на друк;

– контроль за експортом/імпортом інформації з використанням з’ємних носіїв;

– гарантоване видалення інформації;

– розмежування доступу прикладних програм до каталогів і файлів;

– контроль цілісності прикладного ПЗ;

– контроль за використанням дискового простору;

– блокування пристроїв інтерфейсу користувача;

– контроль цілісності та самотестування КЗЗ;

– відновлення функціонування КЗЗ після збоїв;

– реєстрація подій;

– ведення архіву зареєстрованих даних аудиту.

10. Документ «Опис організаційної структури» містить такі розділи:

– зміни в організаційній структурі керування ІКС;

– організація Служби захисту інформаці в ІКС;

– реорганізація існуючих підрозділів управління.

10.1. У розділі «Зміни в організаційній структурі управління ІКС» наводять:

– проектні рішення щодо зміни організаційної структури управління ІКС і їх обгрунтування;

– опис змін у взаємодії між підрозділами.

10.2. У розділі «Організація Служби захисту інформаці в ІКС» наводять:

– опис організаційної структури та функцій підрозділу, що створюється з метою захисту інформаці в ІКС;

– опис регламенту робіт Служби захисту інформаці в ІКС;

– перелік категорій працівників і кількість штатних одиниць.

10.3. У розділі «Реорганізація існуючих підрозділів управління» наводять опис змін, обумовлених створенням КСЗІ, які необхідно здійснити в кожному з діючих підрозділів управління ІКС в: організаційній структурі, функціях підрозділів, регламенті роботи, складі персоналу підрозділів.

11. Документ «Відомість устаткування та матеріалів» містить відомості, необхідні для складання кошторисів на придбання і монтаж засобів технічного забезпечення КСЗІ.

12. Документ «Кошторисний розрахунок створення КСЗІ» містить відомості про кошторисну вартість придбання та монтаж засобів технічного забезпечення КСЗІ, а також проведення робіт, що виконуються при створенні КСЗІ.

13. Документ «Проектна оцінка надійності КСЗІ» містить такі розділи:

– вихідні дані;

– методика розрахунку;

– розрахунок показників надійності;

– аналіз результатів розрахунку.

13.1. У розділі «Початкові дані» наводять:

– дані про надійність (паспортні і довідкові) елементів КСЗІ, що враховуються при розрахунку надійності;

– дані про режими та умови функціонування КСЗІ;

– відомості про організаційні форми, режими та параметри експлуатації ІКС.

13.2. У розділі «Методика розрахунку» указують обгрунтування вибору методики розрахунку та нормативно-технічний документ, згідно якого проводять розрахунок, або короткий опис методики розрахунку та посилання на джерела, де вона опублікована.

13.3. У розділі «Розрахунок показників надійності» наводять:

– структури компонентів КСЗІ (комплексу технічних засобів, програмного забезпечення та персоналу) по всіх оцінюваних функціях надійності;

– необхідні обчислення;

– результати розрахунку.

13.4. У розділі «Аналіз результатів розрахунку» наводять:

– підсумкові розрахункові дані по кожній оцінюваній функції (функціональній підсистемі) КСЗІ та кожному нормованому показнику надійності;

– висновки про достатність або недостатність отриманого рівня надійності КСЗІ по кожній оцінюваній функції (функціональній підсистемі) КСЗІ та, за необхідністю, рекомендації з підвищення надійності.

Якщо в обґрунтованих випадках при оцінці надійності КСЗІ не можна врахувати рівень надійності ПЗ і дій персоналу ІКС, то в документі «Проектна оцінка надійності системи» указують відомості за оцінкою надійності КСЗІ тільки з урахуванням надійності комплексу технічних засобів.

Контрольні запитання

1. Сутність ескізного проекту КСЗІ
2. Сутність технічного проекту КСЗІ
3. Сутність робочого проекту КСЗІ
4. Сутність технороботочого проекту КСЗІ

Лекція № 8

Тема: Оцінка відповідності системи захисту інформаційних ресурсів обмеженого доступу в інформаційно-комунікаційній системі вимогам керівних документів

ПЛАН ЛЕКЦІЇ

1. Державнв експертиза КСЗІ
2. Порядок організації та проведення експертизи
3. Порядок надання Експертного висновку та Атестата
4. Особливості проведення експертиз КСЗІ державними органами
5. Етапи роботи експерта
6. Супровід КСЗІ

1. Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІКС.

Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІКС в експлуатацію **(НД ТЗІ 2.6-001-11).**

Державна експертиза КСЗІ в ІКС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації.

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. 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.

Вимоги до експертного висновку.

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.

Підготовлений експертний висновок підписується експертом і керівником організації (установи) – організатором експертизи.

Висновок експертизи зберігає чинність протягом терміну, визначеного договором на її проведення. Після закінчення терміну дії висновку експертизи відповідні об'єкти експертизи підлягають повторній експертизі.

Права та обов'язки експертів

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, обґрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи та чинного законодавства.

Експерти залучаються на підставі договорів або контрактів.

Експерт письмово оформляє висновок експертизи. Не допускається повторне проведення експертизи щодо конкретного проекту одним і тим самим експертом.

Порядок організації та проведення експертизи

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.

Термін дії висновку експертизи визначається договором, але не перевищує 2 років від дня його видачі.

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».

Право на інтелектуальну власність, що може виникнути під час проведення експертизи, належить замовнику експертизи або визначається відповідно до договору на її проведення. 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. 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.

2. 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) ІКС, 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).

3. Об'єктами експертизи є:

– КСЗІ, які є невід'ємною складовою частиною ІКС;

– технічні та програмні засоби, які реалізують функції ТЗІ (далі – засоби ТЗІ).

4 Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам НД 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.

5. Експертиза КСЗІ *шляхом аналізу декларації проводиться у випадках, якщо:*

– КСЗІ створено в ІКС, яка згідно з НД ТЗІ 2.5-005-99 «**Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу**» класифікована як АС класу 1 і 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;

– закінчився строк дії атестата відповідності КСЗІ в ІКС вимогам НД ТЗІ (далі – Атестат), яка згідно з нормативними документами із ТЗІ класифікується як АС класу 1 і в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці. У всіх інших випадках експертиза КСЗІ в ІКС проводиться шляхом експертних випробувань.

6. 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.

2. Порядок організації та проведення експертизи

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 ІКС або засобу ТЗІ, а шляхом аналізу декларації - декларацію про відповідність КСЗІ вимогам нормативних документів із ТЗІ, формуляр ІКС і акт про завершення робіт зі створення КСЗІ.

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 технічного захисту інформації (далі – Експертна рада).

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.

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.

5. Адміністрація має право в установленому порядку зупинити дію декларації або скасувати її реєстрацію

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.

7. За результатами розгляду заяви Експертна рада у місячний термін приймає рішення про доцільність проведення експертизи та визначає її Організатора.

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.

9. Основним документом, що регламентує відносини між Замовником і Організатором, є укладений між ними договір на проведення експертизи.

10. 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.

11. Термін проведення експертизи визначається договором і не повинен перевищувати, як правило, 6 місяців. У випадку значного обсягу експертних робіт

термін проведення експертизи може бути продовжений за згодою Адміністрації та Замовника.

12. Список Експертів, які залучаються до виконання експертних робіт, визначається Організатором.

13. 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.

14. Програма проведення експертизи узгоджується із Замовником та Департаментом з питань захисту інформації в ІКС (далі – ДЗІ ІКС) Адміністрації, а окремі методики – з зазначеним департаментом.

15. Терміни розробки окремої методики та необхідних програмно-апаратних засобів залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи.

16. Під час проведення експертизи кожний Експерт виконує експертні роботи тільки за дорученням Організатора та у відповідності з визначеною окремою методикою.

17. Результати роботи оформлюються у вигляді протоколу виконання робіт за підписом Експертів, які її виконували. Протокол затверджується Організатором.

18. У протоколі можуть бути зафіксовані особливі думки Експертів відносно результатів виконаних робіт.

19. У разі виявлення невідповідності об'єкта експертизи вимогам НД ТЗІ Організатор може запропонувати Замовнику виконати доробку об'єкта.

20. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.

21. Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку.

22. 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.

23. 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.

3. Порядок надання Експертного висновку та Атестата

1. Експертний висновок на засіб ТЗІ розглядається Експертною радою і, у разі затвердження результатів експертизи, реєструється та видається Замовнику.

2. На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності за підписом Голови Держспецзв'язку.

3. Адміністрація має право в установленому порядку зупинити дію або скасувати Експертний висновок або Атестат.

4. Особливості проведення експертиз КСЗІ державними органами

1. Адміністрація надає державному органу повноваження з організації та проведення первинних або додаткових експертиз КСЗІ в ІКС шляхом експертних випробувань за умови погодження з Адміністрацією порядку їх здійснення.

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 ІКС у сфері свого управління шляхом експертних випробувань;

– видають Атестат відповідності, який реєструється Адміністрацією.

5. Етапи роботи експерта

Робота експерта КСЗІ складається з 3-х етапів аналізу:

– розроблених документів;

– проведених робіт;

– розпорядчих документів.

5.1. Аналіз розроблених документів:

– аналіз Технічного завдання на створення КСЗІ та проектної документації;

– перевірка відповідності комплекту документації на КСЗІ вимогам НД ТЗІ;

– перевірка повноти та змісту документів.

У Додатку до НД ТЗІ 2.6-001-2011 «Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІКС» вказаний перелік документів, які повинні бути розроблені в процесі створення КСЗІ та надані Організатору експертизи для використання Експертом в процесі проведення експертизи.

При цьому в таблиці використовуються такі позначення:

– ІДТ – інформація, що становить державну таємницю; СІ – службова інформація; КІ – конфіденційна інформація, що не є власністю держави; ВІВД – відкрита інформація, що є власністю держави; ВІ – відкрита інформація, що не є власністю держави;

– «+» – вимога щодо наявності документа висувається на підставі положень чинної нормативно-правової бази в сфері ТЗІ; «+/—» – вимога щодо наявності документа висувається за рішенням власника (розпорядника) інформації, що обробляється в ІКС;

“—“ – вимога щодо наявності документа не висувається.

№ з/п	Тип документа	Характеристика інформації згідно режиму доступу					Клас / підклас ІТС
		ІДТ	СІ	КІ	ВІВД	ВІ	
1	Перелік інформації, що підлягає обробленню в ІТС та потребує захисту	+	+	+	+	+	1-3.ххх
2	Акт категоріювання ІТС	+	+	+/–	–	–	1-3.Кхх
3	Положення про службу захисту інформації	+	+	+	+	+	1-3.ххх
4	Результати обстеження середовищ ІТС	+	+	+	+	+	1-3.ххх
5	Опис політики безпеки інформації в ІТС	+	+	+	+	+	1-3.ххх
6	Опис моделі порушника безпеки в ІТС	+	+	+	+	+	1-3.ххх
7	Опис моделі загроз для інформації в ІТС	+	+	+	+	+	1-3.ххх
8	Звіт за результатами аналізу ризиків та формування завдань на створення КСЗІ	+	+	+	+	+	1-3.ххх
9	План захисту інформації в ІТС	+	+	+	+	+	1-3.ххх
10	Технічне завдання на створення КСЗІ в ІТС	+	+	+	+	+	1-3.ххх
11	Інструкції щодо забезпечення правил оброблення ІзОД в ІТС	+	+	–	–	–	1-3.Кхх
12	Інструкції співробітників СЗІ, персоналу та користувачів ІТС	+	+	+	+	+	1-3.ххх
13	Технологічні інструкції щодо адміністрування та обслуговування КСЗІ	+	+	+	+	+	1-3.ххх
14	Інструкції про порядок використання засобів КЗІ	+	+	+	+	+	1-3.Кхх 1-3.хЦх
15	Журнали обліку сховищ і матеріальних носіїв ІзОД	+	+	–	–	–	1-3.Кхх

5.2. Аналіз проведених робіт:

– перевірка реальних умов експлуатації;

– перевірка відповідності реально встановлених засобів ІКС та інших технічних засобів та систем вказаним в Акті обстеження;

– перевірка впроваджених заходів захисту інформації;

– перевірка виконання вимог щодо функціонування системи антивірусного захисту.

На цьому етапі Експерт вимагає від Замовника та перевіряє:

– специфікації апаратних та апаратно-програмних засобів ІКС;

– опис програмного забезпечення з номерами ліцензій та підтвердженням, що ПЗ придбане без порушення авторських прав, (підтвердити рахунками-фактурами, ліцензіями (пас портами), серійними номерами). На встановлене антивірусне програмне забезпечення робочих станцій, серверів Замовник повинен надати експертні висновки Адміністрації Держспецзв’язку та підтвердити, що оновлення баз даних проводиться у відповідності до вимог НД ТЗІ;

– відповідність КЗЗ від НСД з визначеним рівнем гарантії вимогам НД ТЗІ у обсязі функцій, сукупність яких визначається ФПЗ та наявність експертного висновку Адміністрації Держспецзв'язку.

5.3. Аналіз розпорядчих документів:

– перевірка наявності відповідних наказів керівника Замовника на різних етапах створення та впровадження КСЗІ;

– перевірка наявності інструкцій, які регламентують функціонування КСЗІ в АС.

На цьому етапі Експерт перевіряє:

– наказ про проведення робіт зі створення КСЗІ на ОІД з висновками щодо обмеження грифу обмеження доступу до інформації, що обробляється в АС та призначення відповідальних осіб;

– наказ щодо створення служби захисту інформації;

– наказ про створення комісії з проведення випробувань КСЗІ в АС;

– наказ про забезпечення захисту інформації в АС;

– наказ про введення АС в дослідну експлуатацію тощо;

– інструкцію про порядок введення в експлуатацію КСЗІ в АС;

– інструкцію про порядок модернізації КСЗІ в АС;

– інструкцію системному адміністратору;

– інструкцію адміністратору безпеки при роботі в АС;

– інструкцію користувачу.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, Організатор може запропонувати Замовнику виконати доробку об'єкта. Термін доробки об'єкта експертизи визначається спільним протоколом або додатковою угодою до договору між Замовником та Організатором. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.

Після завершення передбачених актом робіт проводиться повторна експертиза. Для інтегрованих ІКС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо. Державна експертиза КСЗІ інтегрованої ІКС полягає у перевірці взаємодії (адміністрування, обміну даними бази даних захисту тощо) вже оцінених модулів. Документи, що містять результати робіт кожного з етапів (протоколи, акти, атестати відповідності)

для КСЗІ ІКС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ. Результати робіт, визначених методикою, узагальнюються Організатором в Експертному висновку. Висновки щодо кожного пункту методики, а також особлива думка Експерта, зафіксовані в протоколах, ключаються до Експертного висновку як складові частини без унесення до них будь-яких змін.

За результатами проведених робіт Організатор складає Експертний висновок щодо відповідності об’єкта експертизи вимогам нормативних документів з ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації. На підставі позитивного рішення щодо експертизи КСЗІ Замовнику безоплатно видається зареєстрований Атестат відповідності за підписом Голови Держспецзв’язку згідно вимог «Переліку адміністративних послуг, які безоплатно надаються Адміністрацією Держспецзв'язку», затвердженого наказом Адміністрації Держспецзв'язку від 29.11.2011 №350,

зареєстрованого в Міністерстві юстиції України 15.12.2011 за №1455/20193.

Згідно вимог п.1.6 **Стандарту** термін дії Атестату відповідності становить 5 років. Отримання Атестату фіксується відповідним записом у формулярі ІКС. Атестат відповідності є підставою для Замовника видати наказ про введення КСЗІ в ІКС в постійну експлуатацію, після чого в ІКС можна обробляти ІзОД.

6. Супровід КСЗІ (НД ТЗІ 1.4-001-00).

Весь період функціонування КСЗІ забезпечується її супроводом, під час якого персоналом ІКС виконуються такі роботи щодо КСЗІ:

– керування КСЗІ згідно Плану захисту та експлуатаційної документації;

– вдосконалення та модернізації КСЗІ.

Крім того, під час супроводу КСЗІ здійснюються такі заходи:

– організаційне забезпечення працездатності ІКС;

– гарантійне та післягарантійне технічне обслуговування засобів КСЗІ;

– періодичне поновлення документів КСЗІ.

Всі заходи супроводу та модернізації КСЗІ вносяться до Календарного плану робіт із захисту інформації в ІКС, який щорічно поновлюється.

Він складається з 4-х розділів:

– організаційні заходи;

– контрольно-профілактичні заходи;

– інженерно-технічні заходи;

– кадрові заходи.

Організаційні заходи

Організаційні заходи – це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування КСЗІ.

Заходи	Виконавець	Регламент робіт	Терміни / період
Коригування політики безпеки	СЗІ, Адміністратори	Коригування положень ПБ Розробка додаткових інструкцій	у разі змін умов функціонування ІТС
Коригування Плану захисту	СЗІ, Адміністратори	Розробка нових підходів до планування заходів захисту	щорічно
Планування модернізації КСЗІ	СЗІ, Адміністратори	Розробка ТЗ на модернізацію КСЗІ згідно НД ТЗІ 3.7-001-99	згідно плану розвитку КСЗІ
Чергове категоріювання	Комісія установи	Згідно НД ТЗІ 1.6-005-2013	через 5 років
Чергова державна експертиза	Адміністрація ДССЗЗІ	Згідно вимог «Положення про державну експертизу»	через 5 років

Контрольно-профілактичні заходи

Контрольні заходи – це комплекс заходів контролю за виконанням персоналом ІКС вимог нормативно-правових актів України у сфері захисту інформації, розроблених в установі інструкцій і положень, а також заходів, розроблених за результатами попередніх перевірок.

Профілактичні заходи – це комплекс заходів, спрямованих на формування у користувачів мотивів поведінки, які спонукають їх на безумовне виконання у повному обсязі вимог правил проведення робіт із захисту інформації тощо, а також формування відповідного моральноетичного стану в колективі.

Заходи	Виконавець	Регламент робіт	Терміни / період
Проведення занять з персоналом ІТС щодо виконання вимог політики безпеки в установі	Служба захисту	Згідно «Плану навчання в установі»	щоквартально
Формування в трудовій угоді розділу відповідальності за виконання вимог політики безпеки	Служба захисту	Згідно вимог трудового законодавства	за рішенням керівника установи
Контроль працездатності та виконання вимог політики безпеки	Системний адміністратор	Перевірка справності ОС і ПЗ ІТС	щодня
	Адміністратор безпеки	Перевірка виконання вимог політики безпеки користувачами	щомісячно
	Служба захисту	Перевірка виконання політики безпеки адміністраторами	щоквартально
Перевірка стану захисту інформації	Комісія установи	Згідно «Положення про захист інформації в ІТС»	щорічно
Перевірка наявності МНІ	Комісія установи	Згідно «Інструкції про організацію діловодства»	щорічно

Інженерно-технічні заходи

Інженерно-технічні заходи – це комплекс заходів, спрямованих на налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування апаратних і програмних засобів захисту інформації в ІКС, інженерне обладнання споруд і приміщень, в яких розміщуються засоби ІКС.

Заходи	Виконавець	Регламент робіт	Терміни / період
Супровід КСЗІ	Розробник КСЗІ	Гарантійне обслуговування	Гарантійний термін
Технічне обслуговування ІТС	Адміністратори	Згідно «Регламенту техобслуговування»	згідно термінів регламенту
Резервування баз даних і фондів	Адміністратор безпеки	Згідно «Інструкції з резервування баз даних»	щомісячно
Поновлення антивірусних баз	Адміністратор безпеки	Згідно «Інструкції з антивірусного захисту»	щодня
Перевірка МНІ і ІТС на наявність вірусів	Користувач (МНІ)	Згідно «Інструкції з антивірусного захисту»	щодня
	Адміністратори (ІТС)		щотижня
Модернізація КСЗІ	Розробник КСЗІ	Заміна (додавання) окремих компонентів КСЗІ	згідно плану розвитку КСЗІ

Кадрові заходи

Кадрові заходи – це комплекс навчально-педагогічних заходів, спрямованих на розширення світогляду та підвищення професійної майстерності персоналу ІКС, що визначається її особливостями та технологіями захисту інформації, які використовуються в ній.

Заходи	Виконавець	Регламент робіт	Терміни / період
Вступне ознайомлення з положеннями політики безпеки інформації (під розпис)	Служба захисту	Оформлення допуску до роботи	після прийому на роботу
	Адміністратор безпеки	Згідно «Інструкції користувачу»	під час їх реєстрації в ІТС
Інструктаж користувачів щодо дій у випадку позаштатної ситуації	Адміністратор безпеки	Згідно «Плану робіт у випадку позаштатної ситуації»	щорічно
Проведення занять з професійної підготовки персоналу ІТС	СЗІ, Адміністратори	Згідно «Плану професійної підготовки в установі»	щотижня
Направлення на курси підвищення кваліфікації	Служба захисту	Згідно «Плану підвищення кваліфікації в установі»	згідно термінів плану

Виконання Календарного плану забезпечується ***Службою захисту інформації*** *в ІКС (далі – СЗІ), яка у процесі супроводу КСЗІ повинна виконувати такі функції:*

– організація процесу керування КСЗІ;

– розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;

– вжиття заходів у разі виявлення спроб НСД до ресурсів ІКС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

– забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

– організація керування доступом до ресурсів ІКС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів тощо);

– супроводження та актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мі`тки об’єктів, ідентифікатори користувачів тощо);

– спостереження (реєстрація та аудит подій в ІКС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

– підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в ІКС, впровадження нових технологій захисту і модернізації КСЗІ;

– організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІКС або КСЗІ;

– участь в роботах з модернізації ІКС – узгодженні пропозицій з введення до складу ІКС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

– забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;

– проведення аналітичної оцінки поточного стану безпеки інформації в ІКС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз тощо);

– інформування власників інформації про технічні можливості захисту інформації в ІКС і типові правила, встановлені для персоналу і користувачів ІКС;

– негайне втручання в процес роботи ІКС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

– регулярне подання звітів керівництву організації про виконання користувачами ІКС вимог щодо захисту інформації;

– аналіз відомостей щодо засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для організації;

– розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу ІКС;

– участь в організації і проведенні навчання користувачів і персоналу ІКС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;

– участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою тощо;

– контроль за виконанням персоналом і користувачами ІКС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації;

– контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

– інше.

Супровід КСЗІ забезпечується виконанням вимог інструкцій та веденням журналів, які були розроблені при введенні КСЗІ в експлуатацію.

До складу супровідної документації КСЗІ згідно вимог НД ТЗІ входять:

– інструкції щодо забезпечення правил оброблення ІзОД в ІКС;

– інструкції співробітників СЗІ, персоналу та користувачів ІКС;

– технологічні інструкції щодо адміністрування та обслуговування КСЗІ;

– інструкція про порядок використання криптографічних засобів;

– інструкція про порядок супроводження та модернізації КСЗІ;

– інструкція про порядок резервування інформаційних ресурсів ІКС;

– порядок обліку і супроводження архівів та ротації носіїв інформації;

– інструкція про порядок оперативного відновлення функціонування ІКС;

– інструкція про організацію контролю за функціонуванням КСЗІ;

– інструкція про порядок проведення ремонтних робіт.

– порядок розробки, впровадження та модернізації ПЗ ІКС;

– правила видачі, вилучення та обліку персональних ідентифікаторів;

– правила управління паролями в ІКС;

– правила класифікації та класифікатор інформації і користувачів ІКС;

– формуляр (паспорт) ІКС;

– журнали, які використовуються для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.

Складовою супроводу КСЗІ є контроль за забезпеченням режиму під час обробки ІзОД в ІКС, який полягає у перевірці виконання персоналом ІКС вимог нормативно-правових актів з питань збереження ІзОД і нормативних документів з технічного та криптографічного захисту інформації.

Контроль режиму обробки ІзОД в ІКС здійснюється за такими формами:

– планові перевірки;

– позапланові перевірки;

– повсякденний контроль.

Планові перевірки здійснюються комісіями, до складу яких входять начальники РСО і підрозділу ТЗІ, співробітники СЗІ та представники інших підрозділів установи. Головою комісії призначається керівник СЗІ. Підстави проведення перевірки, строки роботи і склад комісії, а також перелік об'єктів ІКС, які підлягають перевірці, зазначаються в наказі керівника установи.

Позапланові перевірки здійснюються у разі наявності відомостей щодо порушень виконання вимог «Інструкції щодо забезпечення правил оброблення ІзОД в ІКС», НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації. Вони організовуються СЗІ та здійснюються комісіями, до складу яких входять начальники РСО і підрозділу ТЗІ, співробітники СЗІ та представники інших підрозділів установи. Планова або позапланова перевірка проводиться у присутності начальника підрозділу установи, в якому проводиться перевірка, або особи, яка його заміщає, представника СЗІ та співробітника, відповідального за користування об'єкта ІКС.

Під час планових та позапланових перевірок перевіряються такі питання:

– дотримання користувачами ІКС встановлених вимог щодо забезпечення режиму

обробки та захисту ІзОД;

– комплектація ІКС згідно з Формуляром;

– наявність та дотримання вимог приписів на експлуатацію об'єктів ІКС;

– виконання заходів щодо забезпечення захисту ІзОД від НСД на відповідність вимогам технічної та експлуатаційної документації, згідно з якими здійснюється експлуатація ІКС;

– відповідність ступеня обмеження доступу інформації, яка обробляється з використанням ІКС, наданій категорії об'єкта ІКС;

– відповідність ступеня обмеження доступу інформації, яка зберігається на машинних носіях даних, грифу обмеження доступу машинних носіїв даних;

– наявність атестата відповідності КСЗІ вимогам НД ТЗІ, організаційно-технічних документів та експлуатаційної документації.

За результатами перевірки складається акт, в якому зазначаються результати оцінки відповідності забезпечення режиму обробки та захисту ІзОД в ІКС вимогам НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації, виявлені недоліки та рекомендації щодо їх усунення. Акт затверджується керівником установи, після чого з ним ознайомлюється началь-

ник підрозділу, в якому проводилася перевірка. Акт направляється в установленому порядку вищестоящому органу згідно з підпорядкованістю установи та регіональному органу Держспецзв'язку на його вимогу.

Повсякденний контроль за забезпеченням режиму під час обробки інформації в ІКС здійснюється СЗІ. Порядок його проведення та усунення виявлених недоліків або порушень вимог НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації визначається окремою інструкцією, яка розробляється СЗІ, узгоджується з РСО і підрозділом ТЗІ та затверджується керівником установи. Начальники підрозділів установи організовують усунення виявлених у ході перевірок недоліків та порушень. Контроль за виконанням зазначених заходів покладається на СЗІ.

Контрольні запитання

1. Для чого проводиться Державна експертиза КСЗІ Чим засвідчується?
2. Доповісти загальний порядок організації та проведення експертизи
3. Що є об’єктами та суб’єктами Державної експертизи КСЗІ?
4. У якому випадку Державна експертиза КСЗІ проводиться шляхом аналізу декларації?
5. З яких етапів складається робота Експерта Державної експертизи КСЗІ?
6. Що виконується на етапі Державної експертизи КСЗІ *Аналіз розпорядчих документів*?
7. Що розуміється під супроводом КСЗІ?
8. З яких розділів складається Календарний план робіт із захисту інформації в ІКС?
9. Перерахувати склад супровідної документації на КСЗІ згідно вимог НД ТЗІ
10. Які існують форми Контролю режиму обробки ІзОД в ІКС?
11. Що перевіряється під час *планових та позапланових перевірок під час* Контролю режиму обробки ІзОД в ІКС?

Лекція № 9

Тема: Захист акустичної інформації обмеженого доступу

ПЛАН ЛЕКЦІЇ

1. Критерій захищеності акустичної інформації
2. Пасивні методи захисту акустичної інформації.
3. Активні методи захисту акустичної інформації.

1. Критерії захищеності акустичної інформації

Захист мовної інформації є важливим завданням в загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта чи установи. Для її перехоплення передбачуваний порушник інформаційної безпеки може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, дозволяють перехоплювати мовну інформацію по прямому акустичному, віброакустичному, оптико-електронному каналам. Як розглянуто у попередньому пункті основними засобами неголосного отримання акустичної інформації є [1, 2, 3]:

- портативна апаратура звукозапису (малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки);
- спрямовані мікрофони;
- акустичні стетоскопи;
- різноманітні закладні пристрої;
- оптико-електронні (лазерні) стетоскопи.

Використання тих чи інших методів і засобів визначається характеристиками об'єкта захисту і апаратурою розвідки, умовами її ведення, а також вимогами, що пред'являються до ефективності захисту акустичної (мовної) інформації. У якості показника оцінки захищеності мовної інформації використовується словесна розбірливість мови (W) на виході каналу витоку інформації [3]. Критерії ефективності захисту акустичної (мовної) інформації багато в чому залежать від цілей, переслідуваних при організації захисту, наприклад:

- приховати смисловий зміст ведення розмови;
- приховати тематику ведення розмови і т.д.

Процес сприйняття мови в шумі супроводжується втратами складових елементів мовного повідомлення. Зрозумілість мовного повідомлення характеризується кількістю правильно прийнятих слів, що відбивають якісну

область зрозумілості, яка виражена в категоріях подробиці довідки про перехоплений розмові, яку зводять «агентом». З практичних міркувань може бути встановлена шкала оцінок якості перехопленого мовного повідомлення:

1. Перехоплене мовне повідомлення містить кількість правильно зрозумілих слів, достатнє для складання докладної довідки про практичний зміст перехопленого розмови.

2. Перехоплене мовне повідомлення містить кількість правильно зрозумілих слів, достатнє лише для складання короткої довідки-анотації, що відбиває предмет, проблему, мету і загальний сенс перехопленого розмови.

3. Перехоплене мовне повідомлення містить окремі правильно зрозумілі слова, що дозволяють встановити предмет розмови.

4. При прослуховуванні перехопленого мовного повідомлення можливо встановити факт наявності мови, але не можна встановити предмет розмови.

Відповідно до проведених досліджень [10] встановлено, що розуміння переданої по каналах зв'язку мови з великим напруженням уваги, перепитав і повтореннями спостерігається при складової розбірливості 20-40%, а при складової розбірливості менше 20% має місце нерозбірливість зв'язного тексту (зрив зв'язку) протягом тривалих інтервалів часу:

Повний захист (конфіденційність забезпечено):

Словесна розбірливість: W < 20%.

Розбірливість фраз: (0%).

Результат: Складові звуки чути, але зрозуміти зміст розмови чи виділити окремі слова неможливо.

Слабкий (недостатній) захист:

Словесна розбірливість: (20% < W <40%).

Результат: Окремі слова стають зрозумілими, можна перехопити загальну тему бесіди.

Перехоплення інформації (захист відсутній):

Словесна розбірливість: (W > 40%).

Розбірливість фраз: понад (60% - 70%).

Результат: Зміст розмови вільно фіксується та документується сторонніми особами.

Таким чином зрив зв'язку буде спостерігатися при словесної чіткості менш ніж 70%. Захист мовної інформації досягається проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням електронних пристроїв перехоплення інформації. Використання тих чи інших методів і засобів визначається характеристиками об'єкта захисту і апаратури розвідки, умовами її ведення, а також вимог, що пред'являються до ефективності

захисту акустичної (мовної) інформації, у якості показника оцінки якої використовується словесна розбірливість мови *W*.

2. Пасивні методи захисту інформації

Визначено, що для зниження розбірливості мови необхідно прагнути до зменшення відношення «рівень мовного сигналу / рівень шуму» (сигнал / шум) в місцях можливого розміщення датчиків апаратури акустичної розвідки. Зменшення відношення сигнал/шум можливо наступними способами (рис. 9.1):

- Пасивні методи захисту (зменшення (ослаблення) рівня мовного сигналу);

- Активні методи захисту (збільшення рівня шуму (створення акустичних і вібраційних перешкод)).

Рис. 9.1 Методи захисту акустичної інформації

Ослаблення акустичних сигналів здійснюється шляхом звукоізоляції приміщень, яка спрямована на локалізацію джерел акустичних сигналів усередині них. Звукоізоляція оцінюється величиною ослаблення акустичного сигналу і забезпечується за допомогою архітектурних та інженерних рішень, а також застосуванням спеціальних будівельних та оздоблювальних матеріалів.

У разі якщо звукоізоляція приміщення не забезпечує необхідної ефективності захисту інформації, то для її підвищення використовують спеціальні звукопоглинальні матеріали.

Підвищення звукоізоляції стін і перегородок приміщення також досягається установкою на відстані в 6 ... 10 см від них одношарових і багатошарових (частіше подвійних) огороджень. У багатошарових огорожах доцільно підбирати матеріали шарів з різко відрізняються акустичними властивостями (наприклад, бетон — поролон). Для зниження величини

вібраційного сигналу використовуються м'які віброізольовані опори, якими розв'язуються один від одного різні огороджувальні конструкції. В якості таких опор застосовують тверду гуму, пробку, свинець. Одним з найбільш слабких звукоізолюючих елементів огороджувальних конструкцій виділених приміщень є двері і вікна. Звукопоглинальна здатність вікон залежить, головним чином, від поверхневої густини скла і ступеня притиснення притворів. Збільшення звукоізолюючої здатності дверей досягається застосуванням ущільнюючих прокладок, оббивкою або облицюванням полотен дверей спеціальними матеріалами. Для захисту інформації в особливо важливих приміщеннях використовуються двері зі звукоізольованим дверним прорізом, виконаному у вигляді тамбура з глибиною не менше 0,5 м При цьому внутрішній простір тамбура має бути оброблено звукопоглинальним матеріалом, полотна дверей обладнані ущільнювачами, а двері оббиті звукопоглиначем із оббивних матеріалів. В особливо важливих приміщеннях використовують спеціальні звукоізолюючі двері. Пасивні методи захисту інформації, як правило, реалізуються при будівництві або реконструкції будівель на етапі розробки проектних рішень, що дозволяє заздалегідь врахувати типи будівельних конструкцій, способи прокладки комунікацій, оптимальні місця розміщення виділених приміщень. У разі технічної неможливості використання пасивних засобів захисту приміщень або якщо вони не забезпечують необхідних норм по звукоізоляції, використовуються активні заходи захисту.

3. Активні методи захисту інформації

Якщо необхідно розробляти захист приміщення по акустичному каналу, слід впливати на середу поширення. Для цієї мети використовуються акустичні генератори шуму. Крім того, генератори шуму широко використовуються для оцінки акустичних властивостей приміщень. Під акустичним шумом розуміють шум, який характеризується нормальним розподілом амплітудного спектра і постійністю спектральної щільності потужності на всіх частотах. Для зашумлення приміщень широко застосовуються перешкоди, що представляють собою суміш випадкових і нерівномірних періодичних процесів. Найпростіші методи отримання білого шуму зводяться до використання шумливих електронних елементів (лампи, транзистори, різні діоди) з посиленням напруги шуму. Більш досконалими є цифрові генератори шуму, які генерують коливання, що представляють собою тимчасової випадковий процес, близький за своїми властивостями до процесу фізичних шумів. Цифрова послідовність двійкових символів в цифрових генераторах шуму являє собою послідовність прямокутних імпульсів з псевдовипадковими інтервалами між ними. Період повторень всієї

послідовності значно перевищує найбільший інтервал між імпульсами. Найбільш часто для отримання сигналу зворотного зв'язку застосовуються послідовності максимальної довжини, які формуються за допомогою регістрів зсуву і підсумовуються по модулю За принципом дії всі технічні засоби просторового зашумлення можна розділити на три великі групи [2, 3]:

- генератори шуму в акустичному діапазоні;
- пристрої віброакустичного захисту;
- технічні засоби ультразвукового захисту приміщень.

Генератори шуму в мовному діапазоні отримали досить широке поширення в практиці ЗІ. Вони використовуються для захисту від несанкціонованого отримання акустичної інформації шляхом маскування безпосередньо корисного звукового сигналу. Маскування проводиться білим шумом з коригувати спектральної характеристикою. Білий шум - стаціонарний шум (шум характеризується постійністю середніх параметрів: інтенсивності (потужності), розподілу інтенсивності по спектру (спектральна щільність), автокореляційної функції), спектральні складові якого рівномірно розподілені по всьому діапазону задіяних частот. Найбільш ефективним засобом захисту приміщень, призначених для проведення конфіденційних заходів, від знімання інформації через шибки, стіни, системи вентиляції, труби опалення, двері і т.д. є пристрої віброакустичного захисту. Дана апаратура дозволяє запобігти прослуховування за допомогою дротових мікрофонів, звукозаписної апаратури, радіомікрофонів і електронних стетоскопів, систем лазерного знімання акустичної інформації з вікон і т.д. Протидія прослуховуванню забезпечується внесенням віброакустичних шумових коливань в елементи конструкції будівлі.

Генератор формує білий шум в діапазоні звукових частот. Передача акустичних коливань на огороджувальні конструкції проводиться за допомогою п'єзоелектричних і електромагнітних вібраторів з елементами кріплення. Конструкція і частотний діапазон випромінювачів повинні забезпечувати ефективну передачу вібрації. Віброперетворювачі збуджують шумові віброколивання в огороджувальних приміщеннях, забезпечуючи при цьому мінімальний рівень завадового акустичного сигналу в приміщенні, який практично не впливає на комфортність проведення переговорів. Передбачена в більшості виробів можливість підключення акустичних випромінювачів дозволяє зашумлять вентиляційні канали та дверні тамбури.

Як правило, є можливість плавного регулювання рівня шумового акустичного сигналу. Відмінною особливістю цих засобів є вплив на мікрофонний пристрій і його підсилювач достатньо могутнім ультразвуковим сигналом, що викликає блокування підсилювача або виникнення значних нелінійних спотворень, що призводять, в кінцевому рахунку, до порушення працездатності

мікрофонного пристрою. Оскільки вплив здійснюється по каналу сприйняття акустичного сигналу, то абсолютно не важливі його подальші трансформації і способи передачі. Акустичний сигнал пригнічується саме на етапі сприйняття чутливим елементом. Все це робить комплекс достатньо універсальним в порівнянні з іншими засобами активного захисту.

Захист від вбудованих і спрямованих мікрофонів.

Мікрофони, як відомо, перетворюють енергію звукового сигналу в електричні сигнали. У сукупності зі спеціальними підсилювачами і фільтрами вони використовуються в якості пристроїв аудіоконтролю приміщень. Для цього створюється прихована провідна лінія зв'язку (або використовуються деякі з наявних в приміщенні провідних ланцюгів), виявити яку можна лише фізичним пошуком або за допомогою контрольних вимірів сигналів у всіх проводах, наявних в приміщенні. Природно, що методи радіоконтролю, ефективні для пошуку радіозакладок, в даному випадку не мають сенсу. Для захисту від вбудованих і вузько спрямованих мікрофонів рекомендуються такі заходи:

- при проведенні нарад слід обов'язково закривати вікна і двері (найкраще, щоб кімната для наради представляла собою ізольоване приміщення);
- для проведення переговорів потрібно вибирати приміщення, стіни яких не є зовнішніми стінами будівлі;
- необхідно забезпечити контроль приміщень, що знаходяться на одному поверсі з кімнатою для нарад, а також приміщень, що знаходяться на суміжних поверхах.

Із застосовуваних зараз технічних засобів захисту акустичної інформації можна виділити наступні основні групи:

- генератори акустичного шуму;
- нелінійні локатори;
- скремблери (системи захисту телефонних переговорів);
- детектори мережі 230 В 50 Гц;
- детектори підключень до телефонної лінії;
- комплекси, що забезпечують виконання декількох функцій по “очищенню приміщень”.

Завдання технічної контррозвідки ускладнюється тим, що, як правило, невідомо, яке конкретно технічний пристрій контролю інформації застосовано. Тому робота з пошуку і знешкодження технічних засобів спостереження дає обнадійливий результат тільки в тому випадку, якщо вона проводиться комплексно, коли обстежать одночасно всі можливі шляхи витоку інформації. Класифікація пристроїв пошуку технічних засобів підслуховування може бути наступною:

1. Пристрої пошуку активного типу:

- нелінійні локатори (досліджують відгук на вплив електромагнітним полем);

- ретгенметри (просвічують за допомогою рентгенівської апаратури);

2. Пристрої пошуку пасивного типу:

- металошукачі;

- тепловізори;

3) пристрої та системи пошуку по електромагнітному випромінюванню (скануючий приймач, детектор електромагнітного поля);

4). пристрою пошуку по зміні параметрів телефонної лінії (напруги, індуктивності, ємності, добротності);

5). пристрою пошуку по зміні магнітного поля (детектори записуючої апаратури).

Спеціальні приймачі для пошуку працюють передавачів в широкому діапазоні частот називають сканерами. З активних засобів пошуку апаратури прослуховування в основному використовують нелінійні локатори. Принцип їх дії заснований на тому, що при опроміненні радіоелектронних пристроїв, що містять нелінійні елементи, такі, як діоди, транзистори і т.п., відбувається відображення сигналу на вищих гармоніках. Відбиті сигнали реєструються локатором незалежно від режиму роботи радіоелектронного пристрою, тобто незалежно від того, включено воно або вимкнено. Для захисту приміщень широко використовуються пристрої постановки перешкод. Сигнали перешкоди радіодіапазоні прийнято ділити на загороджувальні і прицільні. Загороджувальна перешкода ставиться на весь широкий діапазон частот, в якому передбачається робота радіопередавача, а прицільна - точно на частоті цього пристрою радіосигналу. Принцип роботи постановника прицільної перешкоди полягає в наступному. Постановник перешкоди працює в автоматичному режимі. Приймач-сканер сканує весь радіодіапазон, а частотомір вимірює частоти виявлених радіопередавачів. Потім пристрій аналізує дані, що надходять і порівнює їх із записаними в пам'ять. При появі сигналів, про які в пам'яті відсутня інформація, видається команда радіопередавачу на постановку прицільної перешкоди. Недоліком таких комплексів є їх висока вартість.

Постановники перешкод інфрачервоного і надвисокочастотного діапазону є складними і дорогими системами. Це пов'язано з тим, що передавачі та приймачі цих діапазонів мають гостру діаграму спрямованості, і, щоб придушити сигнал передавача цих діапазонів, постановник перешкоди повинен точно встановити розташування приймального пристрою, інакше перешкода буде малоефективна. Отже, чим більше спрямованими антенами забезпечені радіомікрофони та їх приймальні пристрої, тим важче поставити проти них перешкоду. Крім того, при

тому ж рівні сигналу такі радіолінії мають більшу дальність, що, в свою чергу, ускладнює постановку перешкод.

Найбільш поширеними є постановники перешкод акустичного діапазону з використанням функції створення віброзавад. Це відносно прості й недорогі пристрої, які створюють просторове зашумлення в основному спектрі звукових частот, що забезпечує маскування розмов і знижує ефективність систем прослуховування, і створюють вібраційні завади на будівельних конструкціях та інженерних комунікаціях ОІД (підлога, стелі, стіни, вентиляційні отвори, батареї опалення та ін.

Наприклад прикладом такого приладу є сучасний генератор акустичного та віброакустичного шуму вітчизняної розробки “РІАС-2ГС” рис. 9.2 [11].

Він призначений для захисту об'єктів від витоку конфіденційної інформації акустичними та віброакустичними каналами шляхом створення шумового сигналу в діапазоні частот від 180 Гц до 5,6 кГц.

Комплекс віброакустичного захисту “РІАС-2ГС” має чотири канали формування перешкод, до кожного з яких можуть підключатися віброперетворювачі п'єзоелектричного або електромагнітного типу, а також акустичні системи, що забезпечують перетворення електричного сигналу, який формується приладом, в механічні коливання в огороджувальних конструкціях приміщення, вікон, а також в акустичні коливання повітря.

Максимальна вихідна потужність акустичного та електромеханічного каналу - не менше 10 Вт.

Рис. 9.2 Сучасний генератор акустичного та віброакустичного шуму

Вихідна середньоквадратична напруга акустичного та електромагнітного каналів при мінімальному опорі навантаження 4 Ом - не менше 5 В. Максимальна вихідна потужність п'єзоелектричного каналу - не менше 10 Вт. Вихідна середньоквадратична напруга п'єзоелектричного каналу при максимальній ємності навантаження 0,5 мкФ - не менше 20 В. Прилад забезпечує глибину

регулювання окремо низько та високочастотної складових шумового сигналу в робочому діапазоні частот не менше 20 дБ.

Контрольні запитання

1. Назвати основні засоби перехоплення мовної інформації.
2. Що використовується в якості критерію ефективності захисту акустичної інформації?
3. За рахунок чого добиваються зниження розбірливості мови?
4. Чим забезпечується реалізація пасивного методу захисту акустичної інформації?
5. Розказати про активний метод захисту інформації по акустичні каналу.
6. Розказати про пасивні методу захисту інформації по акустичні каналу.
7. Розказати про віброакустичний захист приміщень по акустичному каналу.

3. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України. Про захист інформації в автоматизованих системах (Відомості Верховної Ради (ВВР), 1994, № 31, ст.286) (Вводиться в дію Постановою ВР № 81/94-ВР від 05.07.94, ВВР, 1994, № 31, ст.287.
2. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".
3. Закон України "Про захист інформації в інформаційно-телекому-нікаційних системах" (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286) {Вводиться в дію Постановою ВР N 81/94-ВР від 05.07.94, ВВР, 1994, N 31, ст.287}
4. Закон України. Про державну таємницю. №1079-XIV 21 вересня 1999 року.
5. Указ Президента України "Про Положення про технічний захист інформації в Україні" від 27 вересня 1999 р. № 1229
6. Постанова КМУ. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних інформаційно-телекомунікаційних системах від29 березня 2006 р № 373
7. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации Под ред. В.А. Хорошко. – К.: 2010. – Том I - II. Несанкционированное получение информации.
8. Тихонов Ю.О., Савченко В.А., Котенко А.М., Зідан А.М. Лабораторний практикум з теорії кіл і сигналів в інформаційному та кіберпросторах. Практикум. - К.: ДУТ, 2019.- 221с.
9. Котенко А.М. Курс лекцій для студентів зі спеціальності 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на об'єкти інформаційної діяльності». –К, ДУІКТ, 2024. – 79 с.
10. Закон України. Про інформацію № 2657-XII від 2 жовтня 1992 року.