УДК 004.43(031):681.3.01(02) **Луценко В.М.**

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДОВІЛЬНОЇ СКЛАДНОСТІ

Розглядаються властивості методів та засобів створення проектів систем захисту інформації. Наголос робиться на створенні автоматизованих систем проектування. Запропоновано підхід до вдосконалення методики проектування комплексних систем захисту інформації.

Ключові слова: об'єкт інформаційної діяльності, режимно-секретний орган, інформація з обмеженим доступом.

Вступ. Об'єкт інформаційної діяльності (ОІД) у вигляді окремої кімнати, у котрій циркулює інформація з обмеженим доступом (ІзОД), або локальної території, як, наприклад, територія для наукових чи технологічних робіт, територія військового призначення, виділене приміщення (ВП) для нарад у складі режимно-секретного органу (РСО) держустанови, тощо, є специфічним об'єктом захисту інформації (ОЗІ), для котрого визначеними є правила захисту від несанкціонованого доступу (НСД) (unauthorized access to information) до неї [1]. З іншого боку, інформаційно-комунікаційні системи (ІКС) при наявності ІзОД, також є об'єктом захисту та мають специфічні властивості [2,3] у сенсі забезпечення інформаційної безпеки телекомунікаційних мереж від НСД, а саме - «…здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації».

Постановка проблеми. Якщо розглядати захист інформації (ЗІ) в Україні як сукупність організаційних, технічних та правових заходів, направлених на запобігання нанесенню збитків власникам інформації, тоді логічним є діюче наразі визначення комплексних систем захисту інформації (КСЗІ), котрі діють в рамках правових норм, як «взаємопов'язану сукупність організаційних та інженерно-технічних заходів і методів захисту інформації» [3]. При цьому, визначення КСЗІ не розділяє об'єкти захисту на ОІД - окремо, та ІКС – окремо. Якщо ж розглядати ОІД у вигляді ВП, а згідно визначення ВП таке приміщення взагалі може не мати у своєму складі ніяких технічних засобів , не те що ІКС, тоді виходить, що КСЗІ для них взагалі не може існувати, адже КСЗІ регламентується згідно [4,5] виключно для ІКС,.

Метою статті є викладення підходу до вирішення зазначеного протиріччя за рахунок перегляду загальної структури ОІД.

Виклад основного матеріалу. Визначимося з варіантами структур різних типів існуючих наразі об'єктів.

Структура ОІД та ІКС. Перш за все, можливо, має сенс поєднати ОІД та ІКС у вигляді об'єкту захисту загальної структури (ОЗЗС), для котрого визначеними є наступні структурні варіанти типів об'єктів захисту:

- ІКС спеціального або загального призначення;
- ОІД, котрий не вміщує у своєму складі ІКС;
- ОІД, у склад котрого входить ІКС, або декілька ІКС, у тому числі, мережа загального користування (як мережа INTERNET, або телефонна мережа);
- ІКС, у склад котрої входить ОІД, або декілька ОІД однакового або різного функціонального призначення (офісні приміщення, склади товарів, технологічні та виробничі приміщення, тощо);
- ОЗЗС, котрі визначені як головний ІКС у склад котрого входять також і ОІД з своїм, визначеним для цього ІКС призначенням, що не несе функціональні обов'язки, характерні для головної ІКС. Назвемо такі ОЗЗС гібридними ОЗЗС першого типу;

- ОЗЗС, котрі визначені як головний ОІД у склад котрого входять також і ІКС з своїм, визначеним для цього ОІД призначенням, що не несе функціональні обов'язки, характерні для головного ОІД – гібридні ОЗЗС другого типу.

Таким чином визначається функціональна структура будь-якого ОЗЗС, але в рамках декотрого інфраструктурного рівня, такого, наприклад, як ОЗЗС всередині структури підприємства, установи, тощо, що дислокується у межах району, або більш розгалужені в межах міста, області, або загальнодержавного масштабу що не пов'язані з локальним розташуванням. Фактично, така структура і є характерною, але наразі створення СЗІ та КСЗІ об'єктів захисту здійснюється без урахування їх приналежності до загальної структури цих об'єктів. Тобто, наприклад, характерним є випадок, коли розроблюється КСЗІ ОІД у вигляді регіонального офісного приміщення. Це офісне приміщення є фрагментом більш загальної структури, наприклад системи зв'язку та ІКС для системи мобільного зв'язку (гібридний ОЗЗС першого типу). При цьому для цієї ІКС КСЗІ вже є розробленою та діючою системою. Але розробка КСЗІ даного нового офісу може здійснюватися незалежно від КСЗІ його ІКС, у тому числі і різними виконавцями. Тут знову формуються умови життєдіяльності ОІД, вимоги до СЗІ, модель загроз, і.т.д., хоча ця робота вже є проведеною для усього ОЗЗС і немає ніяких гарантій того, що проект захисту даного офісу буде вміщувати складові що не мають протиріччя з КСЗІ ІКС. Загалом, КСЗІ офісу має повторювати пункти КСЗІ його ІКС, або має створюватися як копія фрагменту КСЗІ його ІКС. Таким чином, КСЗІ складних об'єктів має виглядати як ієрархічна структура жорстко пов'язаних між собою КСЗІ об'єктів нижнього рівня, узагальнення пунктів КСЗІ котрих складає КСЗІ об'єктів наступного, вищого рівня, і так далі до КСЗІ загального ОЗЗС. В інших випадках, навпаки, КСЗІ загального ОЗЗС має розділятися на свої фрагменти у вигляді КСЗІ його ОІД та КСЗІ його ІКС і знову ж таки створювати ієрархічну структуру у котрій об'єкт захисту нижнього рівня є точним фрагментом КСЗІ ОЗЗС. У будь якому випадку КСЗІ нижнього рівня не може вміщувати будь-яких вимог, котрих немає у КСЗІ вищого рівня.

Правила формування КСЗІ складних об'єктів. З огляду на викладене вище можна визначитися з положеннями щодо підходу до проектування КСЗІ у випадках, коли ОЗЗС є розгалужена однорівнева або ієрархічна багаторівнева структура.

Загалом, система захисту за структурою має відповідати структурі об'єкту захисту, тобто структурі ієрархічної розподіленої автоматизованої системи класу 3, аналогічної системі «Рубіж» [6] для АС. Тоді загальна структура системи ЗІ є сукупністю КЗЗ певних рівнів, як є наведеним на Рис.1.

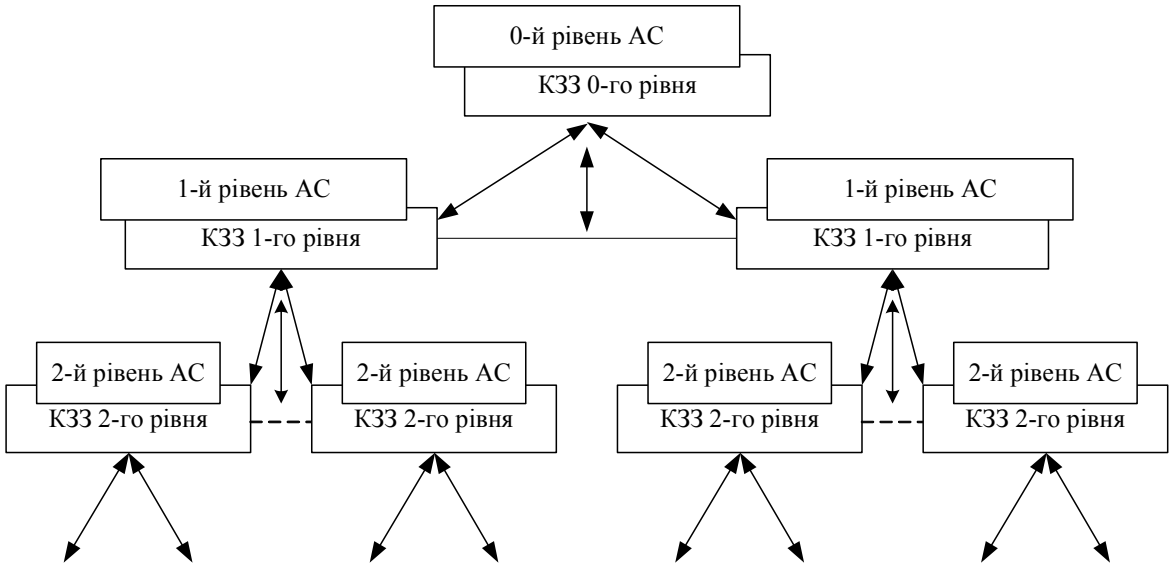

Рис.1 Багаторівнева КЗЗ.

Якщо поєднати наведені вище вимоги та такий структурний підхід, тоді правила формування КСЗІ для ОЗЗС можуть формулюватися для наступних випадків:

Для ієрархічного розподіленого ОЗЗС:

а) Випадок, коли ОЗЗС будується, починаючи з нульового рівня структури, передбачаючи ієрархічність структури, що створюється, або обслідується.

1. Технічне завдання (ТЗ) на КСЗІ має формулюватися, починаючи з вищого, нульового рівня КЗЗ ієрархічної структури;
2. До складу ТЗ на КСЗІ вищого рівня мають входити усі загальні вимоги до ТЗ КЗЗ нижчих рівнів;
3. До складу ТЗ на КСЗІ нижчих рівнів не можуть включатися будь-які вимоги, котрі є відсутніми у складі ТЗ на КСЗІ нульового рівня;
4. Проект КСЗІ для вищого рівня ОЗЗС має вміщувати у своєму складі проекти КСЗІ всіх об'єктів захисту нижнього рівня у якості своїх складових.

б). Випадок, коли ОЗЗС будується, починаючи з нижчого рівня структури, а майбутня ієрархічність загальної структури ОЗЗС є невизначеною.

1. КСЗІ для окремих ОЗЗС визначеного рівня створюються незалежно один від одного та без урахування майбутньої ієрархічності структури ОЗЗС;
2. При появі фрагменту ОЗЗС наступного, вищого рівня, ТЗ на його КСЗІ та проект захисту створюється як сукупність пунктів ТЗ та проектів КСЗІ об'єктів нижчого рівня;
3. ТЗ та проекти КСЗІ об'єктів вищого рівня можуть включати пункти, специфічні для ОЗЗС даного рівня при умові, якщо вони не мають протиріч з ТЗ та КСЗІ, визначених для будь-яких ОЗЗС нижчих рівнів;
4. ТЗ та проект КСЗІ для ОЗЗС кожного наступного рівня має вміщувати усі пункти ТЗ та проектів КСЗІ, котрі були визначеними для усіх ОЗЗС попередніх, більш нижчих рівнів, у тому числі, специфічні за п.3 даного переліку, для попереднього рівня.

Для однорівневого розподіленого ОЗЗС:

1. ТЗ та проект КСЗІ створюються для кожного ОЗЗС незалежно один від одного;
2. Пункти ТЗ та проектів КСЗІ будь-якого ОЗЗС не повинні мати протиріч з будь-якими пунктами ТЗ та проектів КСЗІ інших ОЗЗС;
3. ТЗ та пункти проектів КСЗІ, що є специфічними для окремого ОЗЗС структури додаються до його ТЗ та проекту КСЗІ у вигляді окремого пункту, тобто не можуть включатися як підпункт до вже існуючого переліку пунктів, визначених для інших ОЗЗС даної структури.

При виконанні таких правил виникає можливість створення КСЗІ будь-яких видів ОІД, котрі складатимуть єдину технологічно-інформаційну структуру державного рівня. В таку структуру включаються усі ОІД незалежно від їх призначення, масштабу та складності. Крім того, вперше з'являється реальна можливість створення методології побудови КСЗІ будь-якої складності у тому числі і за рахунок використання автоматизованої системи проектування. Тобто процес проектування отримує принципову можливість автоматизації за єдиною універсальною методологією.

Висновки

За такого підходу та при умові розробки відповідних ДСТУ і нормативно - методичної документації з'являється можливість створення єдиної методики проектування ОЗЗС що відрізняється досконалістю за рахунок прийняття рішень при реалізації проекту, незалежних від суб'єктивних властивостей проектанта. Нагальність створення такої методики є безумовною, оскільки при створенні методики проектування СЗІ (та КСЗІ для АС та інформаційно-комунікаційних систем (ІКС)) базою є комплект ДСТУ, нормативні та методичні документи що у своїй сукупності відрізняються взаємною неузгодженістю [7]. Таким чином, наразі, проекти СЗІ створюються в умовах об'єктивної неможливості

виконання усіх вимог діючої нормативно-методичної документації, а запропонований підхід передбачає можливість вирішення зазначених протиріч.

ЛІТЕРАТУРА

1. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

2. Закон України «Про телекомунікації» (Відомості Верховної Ради України ВВР, 2004, №12, ст..155).

3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах" (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286).

4. ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».

5. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

6. М.Будько, В.Василенко, М.Короленко, О.Буточнов. Система захисту інформації від НСД „РУБІЖ". Практичні аспекти реалізації концепції централізованого управління безпекою корпоративної системи. „Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". Науково-технічний збірник. Київ, НТУУ „КПІ", вип. 4, 2002 р., с. 154-161.

7. В.М. Луценко. Відповідність етапів побудови систем захисту інформації стадіям створення автоматизованих систем. «Захист інформації». Наук. тех. журнал., НАУ, Київ, №3 (52), 2011, с. (в ред).

Надійшла: 30.04.2012

Рецензент: д.т.н., проф. Щербак Л.М.