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

ВІДПОВІДНІСТЬ ЕТАПІВ ПОБУДОВИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ СТАДІЯМ СТВОРЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

Розглядаються властивості методів та засобів створення проектів систем захисту інформації. Визначено основні властивості таких проектів. Головна увага приділяється створенню систем захисту інформації на визначених етапах створення автоматизованих систем. Запропоновано підхід до вдосконалення методики проектування системи захисту інформації на об'єктах інформаційної діяльності та комплексних систем захисту інформації..

Вступ. Побудова систем захисту інформації (СЗІ) на об'єктах інформаційної діяльності (ОІД) та створення комплексних систем захисту інформації (КСЗІ) на визначених стадіях створення автоматизованих систем (АС) загалом є напрямком, котрий має тенденцію до розвитку [1,2]. Проекти захисту інформації (ЗІ) за якісними показниками мають об'єктивно відтворювати умови життєдіяльності об'єктів, але наразі відстають від життєвих вимог. При створенні методики проектування СЗІ (та КСЗІ для АС та інформаційно-комунікаційних систем (ІКС)) базою є напрацювання комплекту ДСТУ, нормативних та методичних документів, за допомогою яких кваліфікований виконавець може здійснювати проектування. Логічно будувати СЗІ за етапами [3] на стадіях створення ОІД або АС [4] з відповідною [5] документацією. При необхідності одночасного створення КСЗІ, така система має створюватися за етапами згідно [6] на визначеному етапі створення СЗІ. Якщо відтворити загальний перелік хоча б основних загальних документів, на котрі при цьому необхідно спиратися при створенні КСЗІ, їх список буде мати вигляд [7], а додатково, перелік спеціальних документів (наприклад при створенні КСЗІ в АС тільки першого класу (АС-1). Для зменшення обсягу матеріалу список НД ТЗІ та ДСТУ є викладеним за номерами, але без повної назви), складає перелік, котрий є наведеним у [8]. Що стосується переліку засобів захисту, вони визначаються окремо для спеціальних засобів захисту та засобів загального призначення. Якщо відокремити тільки засоби загального призначення, тоді для АС необхідно розрізняти КСЗІ в АС-1, окремо, та в АС-2, окремо (згідно з НД ТЗІ 2.5-005-99). Для прикладу, тільки для АС-1 маємо перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації та у відповідності до вимог нормативно-правових документів [9].

Шість етапів виконання робіт при створенні КСЗІ для класу АС-1 можна навести за пунктами:

1. Обстеження АС-1, аналіз документації, організація процесу експлуатації АС-1, категоріювання об'єкта ЕОТ, розробка та узгодження ТЗ на КСЗІ в АС-1. Результатом етапу є: Акт категоріювання, Акт обстеження та ТЗ на КСЗІ в АС-1.

2. Розробка проектів організаційно-технічної документації та забезпечення захисту інформації в АС-1. Результатом етапу є: Формуляр на АС-1, Положення про службу захисту інформації в АС, План захисту інформації в АС-1, Модель загроз, Інструкція щодо забезпечення режиму доступу в АС-1, Інструкція адміністратора безпеки в АС-1, Інструкція системного адміністратора АС-1, Інструкція користувача АС-1, Інструкція з антивірусного захисту інформації в АС-1.

3. Розробка програми та методики попередніх випробувань КСЗІ в АС-1. Результатом етапу є «Програма та методика приймальних випробувань КСЗІ в АС- 1».

4. Проведення попередніх випробувань КСЗІ в АС-1 та передача КСЗІ в АС-1 у дослідну експлуатацію. Результатом етапу є «Протокол про проведення попередніх випробувань КСЗІ в АС-1».

5. Проведення дослідної експлуатації КСЗІ в АС-1. Результатом етапу є «Акт завершення дослідної експлуатації КСЗІ в АС-1», «Акт завершення робіт по створенню КСЗІ в АС-1».

6. Подання КСЗІ в АС-1 на державну експертизу. Результатом етапу є «Експертний висновок» та «Атестат відповідності».

Наведений матеріал є найпростішим прикладом КСЗІ для об'єкту захисту у складі АС і вимагає використання мінімум 25 документів (наведених у [8,9]) та наочно ілюструє той факт, що процес розвитку технології проектування КСЗІ поступово набуває властивості набуття «критичної маси», при котрому подальший розвиток цього напрямку вимагає нових підходів з вищим рівнем технологічності. Практично, такі підходи існують, але обслуговують технологічні напрямки не пов'язані з напрямком захисту інформації (ЗІ).

Однак факт наявності таких високотехнологічних підходів дозволяє оптимістично споглядати в майбутнє напрямку ТЗІ і не створює ситуації глухого кута. Розвиток напрямку проектування КСЗІ можна характеризувати як такий, котрий вимагає розвитку і вдосконалення за рахунок залучення відомих технологій і не вимагає радикального перегляду у підході до загальної методології КСЗІ. Але наразі, при відсутності діючої загальної концепції ЗІ, відмінної або частково узгодженої з попередньою «Протидією іноземним технічним розвідкам», залучення більш технологічних підходів передбачає ревізію методики створення КСЗІ в рамках діючих документів. Така необхідність визначається неузгодженістю основних документів, котрі регламентують етапи (термін «стадії», що є використаним за [4]) створення АС, етапи створення (термін «побудови» є використаним за [3]) СЗІ та етапи створення КСЗІ [6] для АС.

До шляхів виправлення недоліків цих документів відноситься дана стаття.

Послідовність етапів створення АС, СЗІ та КСЗІ. Послідовність дій при створенні СЗІ та КСЗІ має бути узгодженою у часі з послідовністю стадій створення АС, як це є наведеним на рис.1 в якості ілюстрації. Стрілки вказують, на якому підґрунті (початок стрілки) виконуються ті чи інші дії (кінець стрілки) у послідовності визначених етапів. Таким чином, створюється можливість визначити послідовності дій на етапах створення КСЗІ, котрі мають виконуватися в рамках чи бути узгодженими з етапами побудови СЗІ, у відповідності зі стадіями створення АС. На самому початку відзначимо, що створення АС є можливим за двома варіантами сценарію. Один є таким, при котрому необхідність у захищеності системи визначається на декотрому етапі створення АС, наприклад при розробці концепції АС. Другий є таким, при котрому АС створюється в захищеному виконанні апріорно, або при формуванні вимог до АС. Якщо саме таким чином розділяти ці варіанти сценарію, тоді для першого варіанту логічною є перестановка між собою пунктів 1 «Формування вимог до АС» та 2 «Розробка концепції АС» стадій створення АС. У будь-якому разі послідовність дій при створенні КСЗІ формується одночасно і у відповідності з стадіями створення АС і у відповідності з етапами побудови СЗІ. Логіка зв'язків має бути однозначною, а якщо можливими є порушення цієї логіки, тоді такі випадки мають передбачатися самими зазначеними документами.

Аналіз етапів, визначених за рис.1, вказує на недоліки у формуванні послідовності дій при створенні КСЗІ. Наприклад, п.2 етапів створення КСЗІ, а саме, «Обґрунтування необхідності створення КСЗІ» є можливим тільки після стадії 2 створення АС «Розробка концепції АС» (стрілка штрихова). Але якщо при «Формуванні вимог до АС» за п.1 стадій створення АС апріорно визначається необхідність використання захищених каналів зв'язку або виділених приміщень, тощо (наприклад, з огляду на те, що АС створюється для військового призначення або подібних причин), тоді «Обґрунтування необхідності створення КСЗІ» втрачає сенс на етапі 2 «етапів створення КСЗІ» і за стадією 2 створення АС слідує етап 1 «етапів створення КСЗІ». При цьому з етапу 2 вилучається пункт у частині «Обґрунтування необхідності створення КСЗІ». Якщо саме таким чином проаналізувати надану етапність за усіма пунктами, можна виявити невідповідність послідовності виконання деяких пунктів.

Так, повернемося до стадії 2 створення АС «Розробки концепції АС». Загалом, на основі рішень за цією стадією мають бути прийняті рішення на етапах 3, 4 та 5 «Етапів створення КСЗІ» і після виконання етапу 4, котрий включає: «Вивчення об'єкта», «Вибір

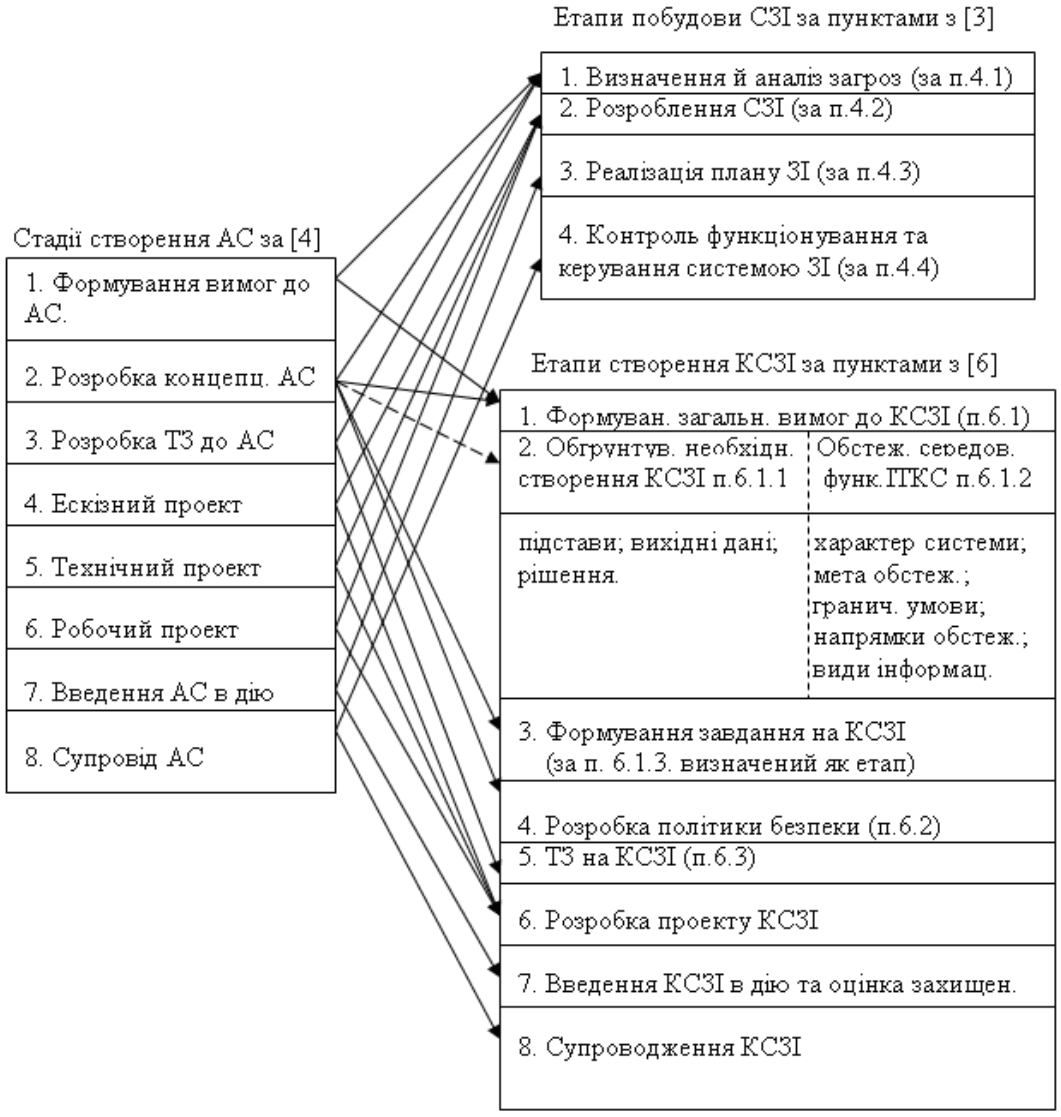
варіанту КСЗІ» та «Оформлення політики безпеки», стає відомо про те, які фрагменти АС підлягають захисту. Однак, ще на етапі 2 створення КСЗІ у частині «Обстеження середовища функціонування ІТКС» мають виконуватися підпункти цього пункту, такі як: «Визначення переліку об'єктів захисту»; «Перелік загроз»; «Модель загроз»; «Модель порушника», де вже повинні бути визначеними дані щодо фрагментів АС, що підлягають захисту. Тобто підґрунтя для виконання етапу 2 отримується пізніше, на етапі 4, і, таким чином, етап 2 не може бути виконаним.

Аналогічно, визначення загроз за етапом 1 побудови СЗІ (п.4.1) не можна отримати раніше формування ТЗ для АС на стадії 3 для АС, оскільки ще не є відомою конфігурація АС, склад АС, перелік апаратури, можливо – місце розміщення та комунікації АС. Але водночас, на цій третій стадії для АС має вже бути виконуватися розробка ТЗ для КСЗІ (етап 5 «Етапів створення КСЗІ»). Тобто ТЗ на КСЗІ має створюється до того, як будуть визначені і проаналізовані загрози на 1-му етапі створення СЗІ. Очевидно, що це не є можливим.

Такий детальний розгляд приводить до висновку про те, що «Стадії створення АС» та «Етапи побудови СЗІ» при їх виконанні є сумісною у часі між собою парою. Аналогічним чином пару «Стадії створення АС» та «Етапи КСЗІ» також можна сумістити в більшості випадків. Але всі три послідовності дій не є сумісними у часі.

Крім того, згідно етапу 2 створення КСЗІ при обстеженні середовища функціонування ІТКС п.6.1.2 (див. рис.1) при визначенні моделі загроз наголос на нормативне забезпечення здійснюється згідно НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003. Але відсутні посилання на вимоги документа [2]. Таким чином, модель складається щодо загроз для КСЗІ ІКС, а для ОІД у складі котрих ІКС відсутні (наприклад, виділені приміщення (ВП)) нормативно-методичне забезпечення є невизначеним.

Також, при виконанні цього ж пункту 6.1.2 визначаються граничні умови для КСЗІ при наявності концепції АС. Тобто визначається для ІТКС концепція, завдання та характеристики ІТКС, комплекси ІТС та їх варіанти реалізації. Такі дані можливо отримати не раніш як на етапі 4 (ескізний проект) створення АС, що за визначеною послідовністю дій згідно рис.1 не є можливим. Такий висновок випливає хоча б з того, що на це вказує вимога п.6.3 етапу 5 створення КСЗІ, де за підпунктом 6.3.2 момент створення ТЗ на КСЗІ визначений як такий, що здійснюється на деякому етапі створення ІТС. Тобто ТЗ на КСЗІ має створюватися паралельно ІТС на основі комплексного підходу, при котрому визначаються у подробицях всі заходи захисту від різних загроз на різних етапах життєвого циклу ІТС. Тобто ТЗ на КСЗІ може створюватись не раніше стадії 4 створення АС.



ІТКС у п. 6.1.2 – інформаційно - телекомунікаційна система.

Рис.1. Послідовність дій при створенні СЗІ та КСЗІ для АС

Щодо можливості вирішення питання сумісності етапів створення системи захисту. Розв'язання зазначених неузгодженостей за рахунок створення нового документу має небезпеку ще більше заплутати ситуацію. Очевидно, що бажаним шляхом розв'язання питання є корекція вже діючого документу. Одним з таких шляхів може бути зміна послідовності фрагментів етапів створення КСЗІ без зміни їх змісту. Так, якщо на етапі 2 створення КСЗІ при формуванні загальних вимог до КСЗІ в ІТС пункт 6.1 залишити без змін у частині обґрунтування необхідності створення КСЗІ (п.6.1.1), а п.6.1.2 перенести до етапу 4 «Розробка політики безпеки» та додати до складу підпункту 6.2.1 «Вивчення об'єкта у вигляді НДР» пункту 6.2, тоді зазначені у розділі 1 даної статті моменти часової несумісності дій на стадіях створення АС та етапах КСЗІ враховуються. При цьому етапи побудови СЗІ залишаються незмінними у своїй послідовності.

Висновки. Для подальшого розвитку напрямку безпеки інформації у частині моделювання КСЗІ як для ІТС, так і для ОІД до складу котрих ІТС не входить, має бути проведеною ревізія нормативно – методичної документації, котрі відноситься до створення КСЗІ, на предмет її узгодженості з іншими нормативними документами з суміжних напрямків. При цьому необхідно брати до уваги необхідність зменшення обсягу документації, або хоча б недопущення його збільшення.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC TR 13335:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1: Концепції та моделі безпеки інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій.

2. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт».

3. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення».

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

5. ГОСТ 34.201-89 «Види, комплектність і позначення документів при створенні АС».

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

7. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах, затверджене постановою Кабінету Міністрів України від 16.02.98 р. № 180.

8. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”

9. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373.

Надійшла: 20.09.2011

Рецензент: д.т.н., проф. Жуков І.А.