Література: 1. Концепція (основи державної політики) національної безпеки України. Постанова ВР України від 16 січня 1997 року, № 3/97-ВР. 2. Окинавская хартия глобального информационного общества. 3. Доктрина информационной безопасности Российской Федерации. Независимая газета – № 146, 2002. 4. Гончаренко О. М., Лисицин Е. М. Стратегія національної безпеки України та військова реформа // Наука і оборона. – № 1, 2000. – с. 35–38. 5. Гончаренко А., Джангужин Р., Лисицин Э. Гражданский контроль и система национальной безопасности Украины // Зеркало недели. – № 34, 2002. 6. Богданович В. Ю. Роль та місце воєнно-політичної моделі держави у розробленні та здійсненні політики забезпечення її воєнної безпеки // Наука і оборона. – № 1, 1999, – с. 34–37. 7. Кучма Л. Д. Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002–2010 роки. – Київ, 2002. 8. Програма дяльності кабінету Міністрів України на 2002–2004 роки. 9. OECD Guidelines for Security of Information Systems and Networks. – OECD, 2002. 10. OECD Guidelines for Cryptography Policy. – OECD, 1997. 11. Емельянов Г. В.,Сстрельцов А. А. О Доктрине информационной безопасности Российской Федерации // Информационное общество, вып 3, 2000. – С. 22–24. 12. Емельянов Г. В. Основы государственной политики Российской Федерации в обеспечении информационной безопасности и безопасности компьютеризованных систем // Информационное общество, вып. 6, 2000. – С. 16–19. 13. Каландин А. П. Роль Гостехкомиссии России в обеспечении информационной безопасности и защиты информации в Российской Федерации // Труды II Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества». – Москва, 2001. 14. Закон Украины «О Национальной программе информатизации» № 74/98-ВР – Ведомости Верховного совета – 1998 – № 27–28.

УДК 681.3:34

КОНЦЕПЦІЯ РОЗВИТКУ НОРМАТИВНОЇ БАЗИ ЩОДО СТВОРЕННЯ КОМПЛЕКСІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Марк Семенко

Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

Анотація: **Наведено аналіз стану та можливі шляхи розвитку нормативної бази системи технічного захисту інформації щодо створення комплексів захисту інформації від витоку технічними каналами.**

Summary: **The concept contains analyses of condition and possible development ways of standard base system of technical protection of information about creation of complex protect system against technical channel information leakage.**

Ключові слова: **Інформація, технічний захист інформації, нормативна база, витік інформації технічними каналами, комплекс технічного захисту інформації.**

Відповідно до Концепції технічного захисту інформації в Україні систему технічного захисту інформації в державі складають три головні компоненти: нормативна база, організаційні структури та матеріальна база. Безперечним є те, що головною складовою системи, яка впливає на дві інші, є нормативна база.

Нормативна база – це нормативно-правові акти організаційно-розпорядчого характеру та нормативні документи технічного характеру. Не применшуючи значення нормативно-правових актів, слід зазначити, що нормативні документи технічного характеру великою мірою визначають стан технічного захисту інформації в Україні.

Становлення технічного захисту інформації в Україні в значній мірі здійснювалося, виходячи з концепцій і підходів, що застосовувалися в системі протидії технічним розвідкам колишнього СРСР. І на цей час основу бази нормативних документів технічного характеру, за напрямом найбільш традиційним – напрямом визначення вимог і рекомендацій щодо забезпечення технічного захисту інформації від витоку технічними каналами, складають нормативно-методичні документи вищезгаданої системи СРСР.

Досвід розвитку технічного захисту інформації в Україні показує, що заміна директивних організаційних методів в сфері ТЗІ на підходи, засновані на використанні принципів системності і стандартизації, а також комплексності є нагальною потребою. До цього спонукає також велике урізноманітнення сучасних технічних засобів оброблення інформації, використання їх у різних сполученнях та умовах, що у загальному випадку виключає можливість надання конкретних однозначних рекомендацій, схем та засобів для забезпечення захисту інформації від витоку, подібних тим, які наводяться в нормативно-методичних документах системи

протидії іноземним технічним розвідкам (різні “Специальные указания”, “Специальные временные технические рекомендации” тощо).

Перехід до вибору і обґрунтування заходів (засобів) забезпечення захисту інформації як до процедури проектування, що застосовується в сфері техніки і будівництва, дозволяє пропонувати підходити до процесу забезпечення захисту інформації від витоку технічними каналами на конкретному об’єкті як до дослідно-конструкторського розроблення певного технічного комплексу (на засадах, встановлених для продукції одиничного виробництва), який впроваджується на місці експлуатації.

Такий підхід дозволяє упорядкувати процеси розроблення, впровадження, приймання та експлуатації сукупності заходів (засобів) технічного захисту інформації від витоку технічними каналами на певному об’єкті, поширивши на них загальні підходи, передбачені відповідними стандартами ЄСКД (в тому числі в галузі автоматизованих систем) та державними будівельними нормами (ДБН).

Згадана вище можливість існування сукупності різних за принципами дії засобів обробленої інформації, яка підлягає захисту, різних умов її оброблення (при наявності різних технічних засобів, не призначених для оброблення такої інформації, але таких, що сприяють її витоку) та різноманітність зовнішніх загроз для неї визначають необхідність раціонального системного комплексного підходу під час вибору заходів і технічних рішень, які забезпечують захист інформації на адекватному важливості інформації та загрозам їй рівні. Такий підхід передбачає застосування принципу мінімальної достатності заходів, який забезпечує необхідну ефективність ТЗІ за умови мінімуму витрат.

Обговорюючи застосування засад системності і стандартизації щодо практичного забезпечення ТЗІ на конкретних об’єктах, неможливо оминути питання побудови системи нормативних документів (НД) у цій галузі та суміжних сферах. За результатами аналізу особливостей діяльності в галузі технічного захисту інформації можна запропонувати такі напрями системи НД, які визначили б основні загальні засади і правила створення передумов і безпосереднього забезпечення на об’єктах технічного захисту інформації від витоку технічними каналами:

- загрози для інформації від витоку технічними каналами, їх класифікація, норми і методи контролю захисту інформації відповідно до загроз;
- рекомендації та методи і способи захисту інформації відповідно до загроз;
- засоби забезпечення технічного захисту інформації від витоку технічними каналами (засоби із захистом інформації, засоби ТЗІ, засоби контролю за ТЗІ);
- створення комплексів технічного захисту інформації від витоку технічними каналами.

НД за останнім напрямом мають бути взаємопов’язаними з документами щодо:

- створення систем захисту інформації в автоматизованих системах;
- проектування та здійснення будівельних робіт з врахуванням ТЗІ;
- організація забезпечення ТЗІ на об’єктах.

Переліченим можливим напрямам НД очевидно мають бути присвячені відповідні “пакети” НД. Предметом даного викладу є “пакет” документів щодо створення комплексів ТЗІ, “пакети” інших НД є суміжними, але обов’язково пов’язаними з ним.

Перший “пакет” – загрози для інформації від витоку технічними каналами, нормування та методи контролю за її захистом – може складатися із документів:

- класифікація та модель загроз для інформації під час її оброблення технічними засобами та під час озвучення мовної інформації;

- норми захисту інформації відповідно до загроз – вагомий вкладений “пакет”, основою якого на даний час є відповідні документи ПДІТР;

- методи контролю за ефективністю захисту (відповідно до загроз і норм – теж вкладений “пакет”, подібний попередньому); нові створювані методи контролю мають бути метрологічно атестованими відповідно до Закону України “Про метрологію і метрологічну діяльність”;

- методичні вказівки із створення окремої моделі загроз; типові моделі загроз для характерних об’єктів – диппредставництва, органів управління тощо.

Другий “пакет” – рекомендації та методи і способи захисту відповідно до загроз. В частині захисту від загроз витоку інформації технічними каналами сучасних документів майже не існує. Належить в тій мірі, як це стосується рекомендацій та методів захисту від витоку технічними каналами, користуватися нормативно-методичними документами системи ПДІТР, виходячи із сучасного стану науки і техніки. Зокрема, щодо захисту інформації, оброблюваної комп’ютеризованими засобами, від витоку каналами ПЕМВН такими документами є різні СТР, щодо захисту мовної інформації – СПУ, щодо захисту інформації під час виготовлення та копіювання документів – СПУ СИРД тощо.

Третій “пакет” – засоби забезпечення ТЗІ – може складатися з таких НД:

- класифікація; загальні вимоги щодо захисту інформації; контроль виконання вимог; основні положення;

- класифікатор засобів із захисту інформації; загальні вимоги до захищеності інформації (це може бути вкладений “пакет” за класами відповідно до основного призначення);

- методики контролю захищеності інформації в засобах із захистом інформації (аналогічний попередньому вкладений “пакет”);

- класифікатор засобів ТЗІ; загальні вимоги за основним призначенням (це може бути вкладений “пакет” за класами);

- методики контролю засобів ТЗІ на відповідність вимогам за основним призначенням (це може бути подібний до попереднього вкладений “пакет”, окремий або об’єднаний з попереднім);

- класифікатор засобів контролю за ефективністю ТЗІ; загальні вимоги за основним призначенням; методи контролю цих вимог (йдеться про спеціально призначені метрологічні засоби для галузі ТЗІ; методи контролю мають бути метрологічно атестованими відповідно до законодавства в сфері метрології);

- загальні (загальнотехнічні) вимоги до засобів ТЗІ та засобів контролю за ефективністю ТЗІ, методи контролю цих вимог (вкладений “пакет” за класами, необхідність таких документів визначається тим, що такі загальнотехнічні вимоги відсутні саме для засобів контролю та засобів ТЗІ, адже ж для засобів із захистом інформації такі вимоги встановлюються головним замовником засобу під час формування вимог за основним призначенням);

- розроблення та поставлення засобів забезпечення ТЗІ на виробництво; основні положення (НД має адаптувати для сфери ТЗІ ГОСТ 15.001-88, ДСТУ 3974-2000 за видами засобів);

- сертифікація засобів забезпечення ТЗІ.

Четвертий “пакет” має відповідати напряму – створення комплексів ТЗІ. Більш детальному розгляду саме цього “пакета” присвячено подальший виклад.

Аналізуючи засади і правила створення продукції одиничного виробництва, передбачені стандартами системи розроблення і поставлення продукції на виробництво (стандарти СРПП), а також порядок створення проектної документації, передбачений державними будівельними нормами (ДБН), можна встановити спільність стадій та етапів розроблення і впровадження як продукції технічного призначення та об’єктів будівництва з одного боку з порядком вибору та впровадження заходів ТЗІ. Засади створення технічної продукції і об’єктів будівництва подібні засадам створення автоматизованих систем, оскільки така подібність була прийнята базовою під час створення “пакету” нормативних документів щодо автоматизованих систем.

Виходячи з того, що заходи ТЗІ в загальному випадку пов’язані з будівельними роботами, відповідно і порядок розроблення і впровадження заходів має бути узгодженим з порядком створення будівельних об’єктів, передбачений ДБН. Згідно з ДБН порядок розроблення проектної документації на нове будівництво однаковий для випадку розширення, реконструкції та переоснащення об’єктів. Це є суттєвим, оскільки в сучасних умовах більш поширеним є саме реконструкція або пристосування приміщень для діяльності, пов’язаної з використанням інформації, що підлягає захисту. Таким чином, як у разі нового будівництва, так і в разі пристосування старого приміщення для вищезазначеної діяльності всі заходи, пов’язані із будівельними особливостями об’єкта, мають відповідати ДБН.

Не викликає сумніву необхідність взаємоузгодження фахівців ТЗІ і будівельників у разі створення в пристосовуваному приміщенні екранованої камери. Але навіть якщо існуюче приміщення задовольняє певним вимогам ТЗІ на час його пристосування (наприклад, щодо забезпечення захисту від витоку акустичним каналом), фахівцям ТЗІ не оминути узгодження існуючої проектно-кошторисної документації з метою виключення можливості внесення змін у приміщення будівельниками на власний розсуд без відома фахівців ТЗІ. Це витікає з того, що відповідно до ДБН А.2.2-3-97 вимоги ТЗІ, які формуються відповідними фахівцями, мають враховуватися на всіх етапах створення проектно-кошторисної документації для нового будівництва.

Таким чином, документація на приміщення, яке із самого початку було призначене для робіт з інформацією, що підлягає захисту, має бути узгоджена із фахівцями ТЗІ, і ніякі зміни до неї без фахівців ТЗІ не можуть бути внесені. Відповідно і у разі пристосування приміщення узгодження існуючої проектно-кошторисної документації виключає внесення змін у характеристики приміщення без відома фахівців ТЗІ. Звичайно йдеться про існування певного правового поля.

Не вимагає обґрунтування положення, за яким порядок розроблення і впровадження заходів технічного захисту інформації від витоку технічними каналами в автоматизованих системах має бути узгодженим з порядком створення як самих автоматизованих систем, так і безпосередньо систем захисту інформації, яка застосовується під час їх використання.

Стандартами СРПП, нормативними документами із стандартизації щодо АС (далі – НД з АС), а також державними будівельними нормами передбачені певні передпроектні роботи, безпосереднє проектування для обґрунтування та узгодження запропонованих рішень, створення робочої та експлуатаційної документації для впровадження проекту і експлуатації певного об'єкту, безпосередньо роботи із створення об'єкту та його приймання за визначеним порядком. Передпроектними роботами є:

- згідно з СРПП – дослідження і обґрунтування розроблення із створенням технічного завдання ТЗ або аванпроект;

- згідно з НД з АС – формування вимог до АС та розроблення концепції АС, які містять обстеження та дослідження об'єкта з обґрунтуванням створення АС та формування ТЗ;

- згідно з ДБН – техніко-економічне обґрунтування, яке є підставою для розроблення проектної документації.

Інші стадії створення технічної продукції, зокрема АС або будівельного об'єкта, є в такій мірі загальними, що не вимагають такого детального розгляду. Виходячи з цього виглядає доцільним встановити для комплексу ТЗІ такі стадії створення: обстеження, створення моделі загроз для інформації від витоку технічними каналами, визначення необхідних рівнів захисту інформації від витоку технічними каналами (категоріювання вимог), розроблення ТЗ на створення комплексу ТЗІ. Ці стадії складають передпроектні дослідження, які мають проводитися для створення комплексу.

Після передпроектного дослідження має проводитися проектування (ескізне, технічне чи ескізно-технічне). На цій стадії і має здійснюватися вибір і всебічне технічне та економічне обґрунтування заходів ТЗІ з розглядом компетентними фахівцями ТЗІ, узгодженням із суміжними спеціалістами (будівельниками, зв'язківцями, енергетиками, фахівцями охорони тощо) та затвердженням заходів замовником. Затверджений проект є підставою для подальшого розроблення та закупівлі основного устаткування (не поодинокими сьогодні є випадки закупівлі засобів та обладнання без необхідного обґрунтування та узгодження доцільності їх застосування).

Затверджений проект є підставою для створення робочої та експлуатаційної документації. Тут слід наголосити, що робочої документації, в якій відбиваються технічні рішення з ТЗІ, як правило (подібно до структури документів на АС) не існує. Ці технічні рішення відбиваються в будівельній робочій проектно-кошторисній документації за відповідними напрямами: у будівельних кресленнях, планах приміщень, схемах енергетики, зв'язку, вентиляції, контрольно-охоронній тощо. Експлуатаційна ж документація може бути створена окремо за напрямом ТЗІ і використовуватися під час монтажу, налагоджування, приймання та експлуатації комплексу.

Після проведення будівельних, монтажно-налагоджувальних робіт за затвердженою програмою здійснюється приймання комплексу комісією, яку створює замовник. Прийнятий комісією комплекс ТЗІ підлягає атестації. Атестація може бути суміщена з прийманням. За позитивних результатів атестації комплекс готовий до експлуатації.

Вимоги експлуатаційних документів на комплекс є обґрунтуванням для організаційних документів забезпечення ТЗІ щодо якісного (за напрямом і рівнем кваліфікації) та кількісного складу обслуговуючих комплекс фахівців. У разі, якщо комплекс ТЗІ є складовою частиною комплексної системи захисту інформації в АС (КСЗІ), експлуатаційні документи на комплекс ТЗІ включаються до складу експлуатаційних документів на КСЗІ і враховуються під час створення останніх.

Відповідно до запропонованих стадій загальні вимоги та правила щодо створення комплексів ТЗІ можуть бути викладені в "пакеті" НД у складі:

1 Створення комплексів захисту інформації. Основні положення;
2 Створення комплексів захисту інформації. Передпроектні дослідження. Основні положення;
3 Створення комплексів захисту інформації. Види, комплектність та зміст документів;
4 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

Нормативні документи "пакету" мають відповідати Правилам побудови, викладення, оформлення та позначення НД системи ТЗІ, затвердженим Наказом Державної служби України з питань ТЗІ від 26. 07. 96 р. № 51 і створюватися згідно з Положенням про порядок опрацювання, прийняття, перегляду та скасування НД системи ТЗІ, затвердженим наказом вищезазначеної Служби від 01. 07. 96 р. № 44 і зареєстрованим в Міністерстві юстиції України 18. 07. 96 р. № 366/1391.

Основною змістовною частиною першого НД, крім опису вищенаведених стадій створення комплексу ТЗІ, мають бути вкладені загальні технічні вимоги та порядок випробувань комплексу. Що стосується передпроектних досліджень, документів, які розроблюються під час створення комплесу та атестації, то розгорнуті вимоги до цих стадій в цьому НД не розглядаються, а містяться лише посилання на відповідні НД "пакету".

Загальні технічні вимоги мають передбачати застосування:

- типових технічних рішень, принцип робототехніки, перевагу використанню технічних засобів з захистом оброблюваної інформації перед "незахищеними" засобами, пасивних перед активними, вітчизняних перед імпортними;
- сертифікованих засобів забезпечення ТЗІ або засобів, що мають позитивний атестат за результатами відповідної експертизи;
- засобів забезпечення ТЗІ як загального користування, так і спеціально створюваних для даного об'єкта (екрановане приміщення, граничний хвилевод тощо);
- засобів просторового електромагнітного зашумлення за узгодженням з Укрчастотнаглядом;
- організаційно-технічних рішень в обґрунтованих випадках – згідно з якими у забезпеченні ТЗІ на необхідний період бере участь обслуговуючий персонал (відключення сигнальних, електроживлюючих комунікацій, збільшення контрольованої зони тощо).

Крім того, в цьому розділі НД мають бути викладені загальні вимоги до складу комплексу та створювальної документації, до безпечного використання комплексу, до необхідності узгодження технічних рішень за напрямами, яких своїми технічними рішеннями торкається комплекс (енергетика, зв'язок, пожежна і загальна охорона тощо), до надійності та гарантійних зобов'язань виконавця.

Розділ цього НД щодо приймальних випробувань має містити перелік видів випробувань (попередні, приймальні, атестаційні, під час експертизи в складі КСЗІ в АС, під час перевірок стану ТЗІ уповноваженим державним органом), загальний порядок організації випробувань, вимоги щодо проведення випробувань за відповідними програмами і методиками та щодо матеріально-технічного забезпечення. В розділі має бути наведений порядок проведення попередніх, приймальних випробувань та обов'язки комісії з випробувань та її Голови, а також вимоги до програми і методики випробувань.

Другий НД "пакету" має містити розгорнуті загальні вимоги до проведення обстеження об'єкта, створення окремої моделі загроз до інформації, що підлягає захисту від витоку технічними каналами, визначення необхідних рівнів такої інформації та до змісту технічного завдання на розроблення комплесу. У додатках мають бути наведені рекомендовані зразки акту обстеження, окремої моделі загроз від витоку технічними каналами, акту визначення необхідних рівнів захисту інформації та технічного завдання.

Третій НД "пакету" має містити загальні вимоги до видів, комплектності та позначення створюваних документів; надані найменування документів та їх відношення до проектно-кошторисної (будівельної) або експлуатаційного документації. Суттєвими розділами НД мають бути розділи з вимогами до змісту документів, створюваних під час проектування та розроблення комплексу, та розділ з викладенням вимог до експлуатаційних документів (ЕД). В останньому розділі мають бути викладені загальні вимоги до ЕД та передбачено можливість створення єдиного документу – паспорту на комплекс. Розділ повинен містити рекомендовану структуру паспорту та вимоги до змісту його складових частин з наданням рекомендованих форм, які заповнюються під час монтажу, приймання комплексу та його експлуатації, включаючи проведення атестації та контролю уповноваженими державними органами.

Література: 1. Концепція технічного захисту інфомації в Україні. 2. Закон України "Про метрологію і метрологічну діяльність". 3. Государственный стандарт Союза ССР. Система разработки и постановки продукции на производство. Продукция производственно-технического назначения. ГОСТ 15.001.-88. 4. Державний стандарт України. Державна система стандартизації України. Порядок розроблення, побудови, викладу, оформлення, ... та реєстрації технічних умов., ДСТУ 1.3.-93. 4. Державний стандарт України. Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення. ДСТУ 3974-2000. 5. Державні будівельні норми і правила проектування. Склад, порядок розроблення, узгодження та затвердження проектної документації для будівництва. ДБН А.2.2-3-97. 6. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания ГОСТ 34.601-90. 7. Положення про порядок опрацювання, прийняття, перегляду та скасування НД системи ТЗІ (затверджене наказом Державної служби України з питань технічного захисту інформації від 01.07.96 р. № 44 і зареєстроване в Міністерстві юстиції України 18.07.96 р. № 366/1391).

УДК 002.5.004:551.438.5