УДК 004.056(045)

Домарєв Д. В., аспірант

КЛАСИФІКАЦІЯ НОРМАТИВНО-ПРАВОВИХ ДОКУМЕНТІВ В СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Національний авіаційний університет

В результаті аналізу нормативно-правових документів у сфері забезпечення інформаційної безпеки запропоновано їх класифікацію. Відмічено найбільш важливий розділ для створення Українського сегменту мережі зовнішнього зв'язку та передачі даних космічного ракетного комплексу «Циклон». Зроблено висновок про потребу узгодження законодавчої бази.

Актуальність

Для створення ефективної системи захисту інформації потрібна законодавча база, добре впорядкована за етапами побудови системи захисту інформації (СЗІ). На момент проведення дослідження, забезпечення безпеки інформаційних технологій регулюється більш ніж ста двадцятьма законодавчими, нормативно-правовими та методичними документами, що не скоординовані за термінологією, критеріями оцінки, послідовністю і напрямками створення систем захисту інформації.

Сформульовано завдання: провести аналіз нормативно-правових документів у сфері технологій інформаційної безпеки. Класифікувати існуючі документи з метою узгодити положення Українського законодавства.

Проведення аналізу

Складові СЗІ можуть бути розділені на три групи, як показано на рис. 1:

1. Основи (з чого складається СЗІ);
2. Напрямки (для чого призначена);
3. Етапи (як працює).

Рис. 1. Групи складових СЗІ

Існують чотири **основи** (рис. 2):

1. Законодавча, нормативно-правова та наукова база;
2. Структура і завдання органів (підрозділів), що забезпечують безпеку ІТ;
3. Організаційно-технічні і режимні заходи та методи (політика інформаційної безпеки);
4. Програмно-технічні засоби і способи.

Напрямки формуються виходячи з конкретних особливостей об'єкту захисту. Враховуючи типову структуру інформаційної системи (ІС) і види робіт, що історично склалися, по захисту інформації, запропоновано розглянути наступні **напрямки** (рис. 3):

1. Захист об'єктів інформаційних систем;
2. Захист процесів, процедур і програм обробки інформації;
3. Захист каналів зв'язку;
4. Придушення побічних електромагнітних випромінювань;
5. Управління і контроль системи захисту.

Існують наступні **етапи** створення та функціонування СЗІ (рис. 4):

1. Визначення інформаційних і технічних ресурсів, а також об'єктів ІС, що підлягають захисту;
2. Виявлення множини потенційних загроз і каналів витоку інформації;
3. Оцінка вразливості і ризиків інформації (ресурсів ІС) при наявній множині загроз і каналів витоку;
4. Формування вимог до системи захисту інформації;

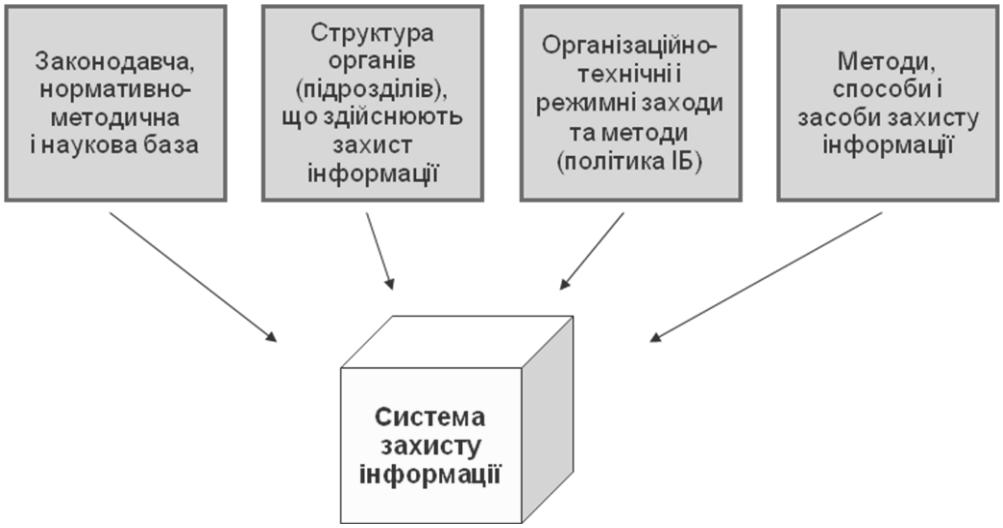

Рис. 2. Основи створення та функціонування СЗІ

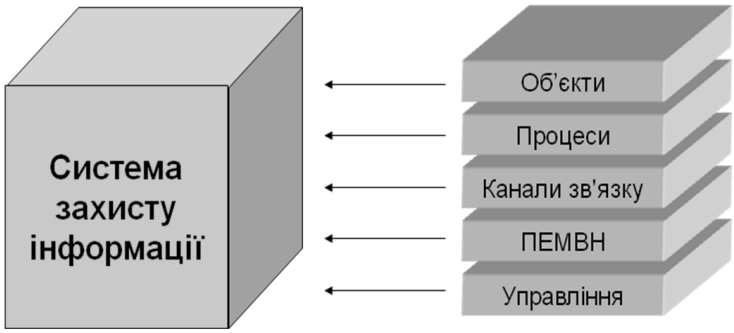

Рис. 3. Напрямки створення та функціонування СЗІ

Рис. 4. Етапи створення та функціонування СЗІ

5. Обрання засобів захисту інформації та їх характеристик;

6. Впровадження і організація використання обраних заходів, способів і засобів захисту;

7. Здійснення контролю цілісності і управління системою захисту.

Оскільки кожен з цих напрямків базується на перерахованих вище основах, «Законодавчу … базу» слід розглядати по усіх напрямках створення СЗІ (див. рис. 5), а саме:

1. Законодавча … база захисту об'єктів ІС;

2. Законодавча … база захисту процесів, процедур і програм…;

3. Законодавча … база захисту каналів зв'язку;

4. Законодавча … база придушення побічних електромагнітних випромінювань;

5. Законодавча … база по контролю і управлінню системою захисту.

Запропонована класифікація

Розглянуто відкриті нормативні документи України, що стосуються систем технічного захисту інформації. В результаті, запропоновано класифікацію нормативних документів за наступними напрямками забезпечення інформаційної безпеки:

1. Законодавчі та загальні положення інформаційної безпеки;

2. Інформаційна безпека організації;

3. Захист інформації від витоку технічними каналами;

4. Захист інформації в обчислювальних системах;

5. Захист інформації в мережах зв’язку і передачі даних;

6. Придушення побічних електромагнітних випромінювань;

7. Криптографічний захист інформації;

8. Спеціальні документи (методи вимірювань і параметри оцінки).

Розділ «Захист інформації в мережах зв’язку і передачі даних» обрано як найбільш важливий в створенні системи інформаційної безпеки Українського сегменту мережі зовнішнього зв’язку і передачі даних космічного ракетного комплексу «Циклон». Представлено список документів в цьому розділі запропонованої класифікації.

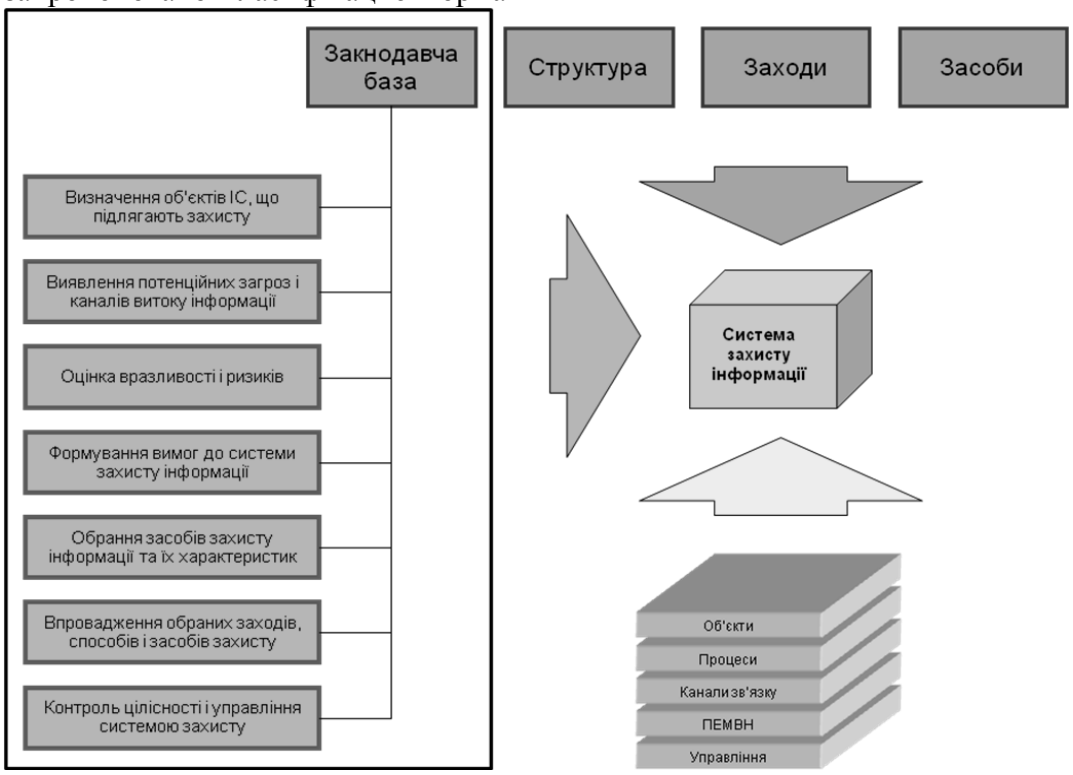

Рис. 5. Розглянута складова СЗІ

Перелік документів найбільш важливого розділу

Список нормативно-правових документів у зазначеному розділі містить закони, нормативні документи і положення України щодо забезпечення інформаційної безпеки:

1. Закон України «Про захист інформації в автоматизованих системах»;
2. Тимчасове положення про категоріювання об'єктів (ТПКО-95);
3. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення;
4. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
5. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;
6. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту;
7. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту;
8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;
9. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт;
10. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;
11. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;
12. Положення про порядок контролю за експортом, імпортом і транзитом окремих видів виробів, обладнання, матеріалів, програмного забезпечення і технологій, що можуть використовуватися для створення озброєння, військової чи спеціальної техніки;
13. Положення про порядок надання суб'єктам зовнішньоекономічної діяльності повноважень на право здійснення експорту, імпорту товарів військового призначення та товарів, які містять відомості, що становлять державну таємницю.

Висновки

Зроблено висновок про потребу узгодження термінології і положень існуючих нормативно-правових документів в області забезпечення інформаційної безпеки з метою підвищення ефективності Української законодавчої бази.

Проведений аналіз нормативних документів дозволив підвищити ефективність забезпечення інформаційної безпеки мережі зовнішнього зв'язку і передачі даних космічного ракетного комплексу «Циклон».

Список літератури

1. Габович А.Г., Головань С.М., Домарев В.В. и др. Основи наукових досліджень – К.: ДУИКТ, 2006. – 173 с.
2. Домарев В.В. Безопасность информационных технологий. Системный подход – К.: ООО «ТИД «ДС», 2004. – 992 с.
3. Домарев В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності – К.: Вид-во Європ. ун-ту, 2006. – 102 с.
4. Материалы юбилейной научно-технической конференции «Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине» – К.: КПИ, 1998. – 280 с.