УДК 621.3.06

О.П. Дóренський, асп.
Кіровоградський національний технічний університет

Особливості класифікації загроз безпеці інформації сучасної інформаційно-телекомунікаційної системи

У статті досліджено особливості класифікації загроз безпеці інформації сучасної інформаційно-телекомунікаційної системи. Проаналізовано існуючі суперечності та запропоновано загальноприйняті технічні загрози виділити у два окремі класи загроз безпеці інформації: апаратні (технічні) і програмні. Обґрунтовано необхідність та доцільність обраного підходу.
інформаційно-телекомунікаційна система, безпека інформації, загрози, класифікація

Сьогодні, не зважаючи на стрімкий розвиток галузі захисту інформації та інформаційної безпеки в цілому, кількість інцидентів безпеки продовжує стрімко зростати [1]. Їх причинами є, зокрема, криза загальносистемних розробок, направлених на розв'язок актуальних задач безпеки інформації, деякі суперечності спеціалістів щодо підходів організації безпеки інформації сучасних інформаційно-телекомунікаційних систем (ІТС) [1] та застарілість нормативної бази, засобів і способів організації систем забезпечення безпеки інформації (СЗБІ).

Аналіз останніх досліджень і публікацій [2-17] показав, що відповідно до сучасних поглядів та, зокрема, результатів дослідження [3], забезпечення безпеки інформації в організаціях, відомствах, підприємствах, у корпоративних і інших ІТС здійснюється на чотирьох рівнях: законодавчому (нормативно-правовому); адміністративному; процедурному (організаційно-технічному); технологічному (програмно-технічному). На кожному з цих рівнів застосовують відповідні підходи (концепції, стратегії) забезпечення безпеки інформації, заходи безпеки інформації [3]. СЗБІ за допомогою набору методів, способів та засобів повинна забезпечити максимальну протидію загрозам безпеці інформації ІТС або повністю унеможливити їх дії на дані ІТС та безпосередньо СЗБІ ІТС [4]. Саме тому дослідження загроз безпеці інформації ІТС за допомогою їх класифікаційного поділу є актуальною задачею, яка має практичну цінність та потребує нагального розв'язку.

Метою роботи є одержання класифікації загроз безпеці інформації сучасної ІТС, дослідження та обґрунтування її особливостей.

Поставлену задачу можливо розв'язати за допомогою вдосконалення існуючих класифікацій шляхом обґрунтування поділу загальноприйнятих і визначених вітчизняними нормативними документами (наприклад, державні стандарти України "Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97", "Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 ", "Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96", "Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва ДБН А.2.2-2-96" і ін.) технічних загроз безпеці інформації ІТС на два окремі класи: апаратні і програмні. Це дасть можливість застосовувати на практиці системний підхід виявлення й дослідження вже існуючих і нових загроз безпеці інформації ІТС та, відповідно, організації високорівневої інформаційної безпеки ІТС [4-6].

Дослідження [2, 4-8] дають підстави стверджувати про наявність на сьогоднішній день кількох класифікаційних поділів загроз безпеці даних інформаційно-

телекомунікаційної системи. Їх детальний аналіз проведено в [8], за результатами якого можна виділити дві основні класифікації: 1) відносно джерел загроз; 2) відносно результатів атаки загроз (збитків). І перший, і другий підхід у відповідних методиках дає позитивні результати, але відсутність єдиної загальноприйнятої класифікації загроз безпеці інформації ще раз підтверджує необхідність нагального розв'язку цієї задачі.

Таким чином, серед розглянутих класифікацій можна виділити три найбільш прийнятні різновиди класифікаційного поділу загроз безпеці інформації:

1) природні (об'єктивні) та штучні (суб'єктивні) [5, 12];

2) технічні, стихійні, антропогенні [1, 2, 7, 12, 13];

3) апаратні, програмні, стихійні (природні), антропогенні (людські) [8].

В досліджені [9] наведено критерії класифікації загроз безпеці інформації ІТС: критерій 1 – інформаційна безпека, проти якої направлені загрози; критерій 2 – компоненти інформаційної системи, на які спрямовані загрози; критерій 3 – спосіб впливу; критерій 4 – розміщення джерела загроз.

Дослідження класифікацій проведемо згідно строгого критерію [5]: загроза має відповідати ознакам (характеристикам) виключного одного класу. Аналіз першої групи (де природні загрози визначено як загрози, які викликані впливом на ІС та її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини, а штучні загрози – загрози ІС, викликані діяльністю людини) повністю відповідає наведеному критерію: не виявлено жодної загрози безпеці інформації, яка б або не відповідали ознакам класифікації, або задовольняли одночасно декільком ознакам. Проте, незважаючи на її універсальність, вона є неефективною у застосуванні. Це пов'язано з тим, що такий поділ вимагає розробки додаткового багаторівневого дерева підкласів, при чому воно буде переважно симетричним. Так, наприклад, загрози безпеці інформації, джерелом яких є програмні засоби, можуть породжуватись як об'єктивними (недосконалість програмного забезпечення, збої [14]), так і суб'єктивними чинниками (шкідливі програмні модулі, віруси, шпигуни [17, 18]). Тобто підкласи дублюються в обох класах. Саме це дало підстави зробити висновок про її неефективність у практичному використанні.

На відміну від першої, дослідження другої і третьої класифікацій показали більш високу практичну цінність. Вітчизняною нормативною документацією систем захисту інформації [2] визначено, що 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. Проте, більшість спеціалістів галузі безпеки інформаційних технологій, досліджень, присвячених захисту інформації [1, 3, 5, 6, 8-13] і методи, проаналізовані в [5], пропонують визначати рівень безпеки інформації ІТС величиною збитку від дії загроз (атак). Цей підхід є найбільш ефективним, оскільки без використання нечіткої логіки чи ймовірнісних показників надійності системи захисту інформації дає точне уявлення про наслідки дії атак загроз безпеці інформації ІТС, які розглядаються. Відповідно, за допомогою методів обчислення величини запобіженого збитку, наприклад, [14, 16] можна оцінити надійність і ефективність системи забезпечення безпеки інформації. Ця оцінка має значно повніше інформаційне навантаження щодо результатів низького рівня захищеності системи і є більш наглядною й простішою для документального опису, ніж відсоткова величина. Таким чином, для проведення класифікації доцільно обрати класифікацію відносно джерела не виникнення загроз безпеці інформації, а джерела безпосередньої дії загрози на інформацію. Саме це дало підстави зробити висновок про раціональність використання класифікацій 2 і 3 [1-2, 7, 8, 12, 13]. Їх аналіз проведено в досліджені [7]. Єдина розбіжність полягає в тому, що більшість вітчизняних фахівців з захисту інформації і існуюча нормативна документація у класі

технічних загроз безпеці інформації ІТС розглядають апаратні і програмні загрози, які в класифікації [8] виділені в окремі два класи.

Дослідження та аналіз класифікацій [7, 8] проведемо за допомогою моделі процесу забезпечення безпеки інформації ІТС [8].

Класифікація [6] типує всі загрози безпеці інформації на три класи, наведені на рисунку 1. При цьому, до складу класу технічних загроз віднесено [6]:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- допоміжні засоби (спеціалізація, телекомунікація і т.і.);
- інші технічні засоби, які використовуються на об'єкті;
- засоби зв'язку;
- мережі інженерних комунікацій;
- транспортні засоби.

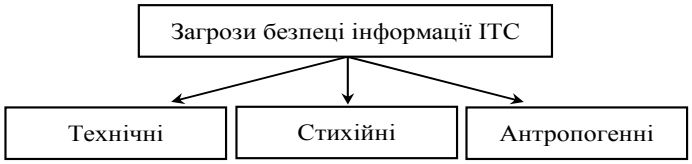

Рисунок 1 – Класифікація загроз безпеці інформації ІТС [7]

Зважаючи на сучасний стан розвитку науки, техніки, інформаційних технологій, пропонується вдосконалення класифікації [7] шляхом поділу класу технічний загроз безпеці інформації ІТС на два окремі класи: апаратні, програмні. На підставі останніх досліджень і публікацій [3-7, 9-19], а також висновків фахівців інформаційної безпеки дають підстави стверджувати про доцільність такого поділу.

За результатами аналізу класифікації [7] можна зробити висновок про її повну відповідність критерію [6]. Звідси випливає, що вдосконалена класифікація [8] також відповідає цим вимогам.

Причиною об'єднання фахівцями програмних та апаратних загроз безпеці інформації у єдиний клас можна вважати нормативну документацію України, затверджену переважно до 2000 року. Згідно неї, захист інформації здійснюється технічними засобами: інженерними, програмно-апаратними [2]. При цьому реалізація автоматизованої системи, згідно [2], здійснюється за допомогою апаратних та програмних засобів. З цього випливає, що складові ІТС складаються з двох видів засобів, а, отже, джерел загроз безпеці інформації також є два. Тож, у зв'язку з розвитком технологій за останні 5-9 років, вітчизняна нормативна база захисту інформації стає не відповідати дійсності і вимагає нагального вдосконалення. Здійснити це можна двома шляхами:

1) Вдосконалити НД технічного захисту інформації, замінивши поняття "технічний захист" на "програмно-технічний" і, відповідно, окремими розділами сформувати вимоги до організації програмного та апаратного захисту інформації;

2) Розробка окремих нормативів програмного захисту автоматизованих систем, вилучивши ці поняття з НД технічного захисту інформації.

Обґрунтувати вірність і доцільність запропонованих шляхів можна за допомогою дослідженнях [12, 14, 18], в яких дослідження цих понять чітко розмежовані, запропоновано різні методи вивчення, діагностики, запобігання апаратних і програмних загроз безпеці інформації ІТС.

Незаперечним доказом автономності класу І і класу ІІ загроз інформації могло б бути доведення незалежності їх джерел. Але особливістю загроз БІ ІТС є те, що вони не є незалежними [14]. На рисунку 2 наведено виявленні в досліджені [8] суб'єктивно-

об’єктивні функціональні міжкласифікаційні зв’язки. При чому, мають неоднакову вагову характеристику. Сумарна величина вагових характеристик, наприклад, класу IV рівна 0,65, що еквівалентно 65% загальної величини збитку ІТС, який завдається у результаті атаки загроз безпеці інформації [10]. Виявлені зв’язки також є цінним надбання з метою подальшого дослідження впливу одного класу загроз на інший. При чому, використовуючи принцип сумарного збитку кожного зв’язку, можна одержати приблизні величини загальних збитків.

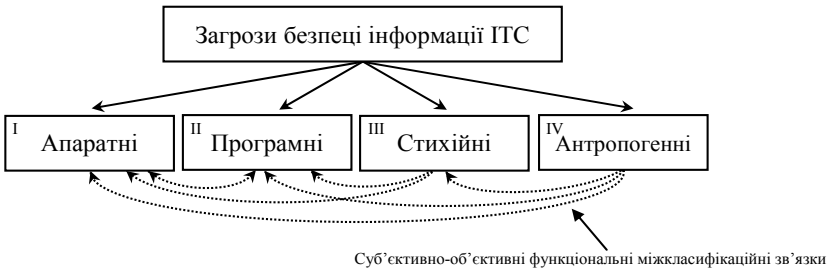

Рисунок 2 – Класифікація загроз безпеці інформації ІТС [8]

Людство вже майже у всіх галузях діяльності накопичену інформацію акумулює та обробляє не за допомогою традиційних інформаційних систем, новітніх цифрових інформаційних технологій, методів, способів обробки, зберігання, передачі цифрових даних, їх зберігання на цифрових носіях. Змінюються також види самої інформації, її властивості, ознаки, носії. Доказом цього є, наприклад, прийнятий закон України “Про електронні документи та електронний документообіг” [21]. В статті 7 цього закону визначено, що оригіналом електронного документа вважається електронний примірник документа з обов’язковими реквізитами, у тому числі з електронним цифровим підписом автора. Тобто, у разі копіювання (надсилання) електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Проте оригіналом звичайного (традиційного) документа, який, як правило, представлений на паперовому носієві, може бути виключно один документ, решта – його копії. Це є досить нетрадиційним і революційним на сьогоднішній день, але щоденно воно продовжує впроваджувати у все нові галузі науки і техніки та розвиватись надшвидкими темпами, демонструючи свою надефективність застосування [20].

Надійність апаратно-технічних засобів на сьогоднішній день сягає високого рівня, тому з їх вдосконаленням ймовірність відмови ІТС саме через апаратний елемент (модуль) протягом номінального терміну застосування надзвичайно мала. Проте це не стосується програмних засобів: нове програмне забезпечення, яке забезпечує обробку даних будь-якої сучасної інформаційно-телекомунікаційної системи є потужним джерелом об’єктивних (ненавмисних) загроз безпеці інформації [14]. Це випливає також з рисунку 3, на якому наведено графік ймовірності відмови програмних засобів та апаратних засобів протягом всього життєвого циклу ІТС.

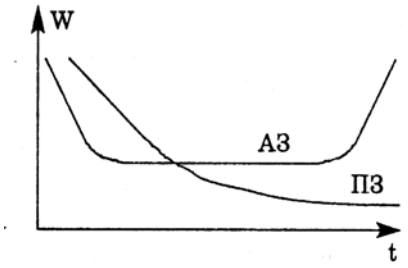

Рисунок 3 – Різниця між надійністю апаратних засобів (АЗ) та програмного забезпечення (ПЗ)

Важливим чинником класифікації загроз безпеці інформації ІТС є сучасна статистика. Згідно звіту корпорації Microsoft в 2007 році приблизно 60% всіх комп'ютерних систем були атаковані програмними суб'єктивними загрозами [18]. Ці дані підтверджено й дослідженнями "Лабораторії Касперського" (Російська Федерація) [11]. Враховуючи атаки об'єктивних програмних загроз [14], ця цифра буде значно вищою. Величини збитку, якими оцінюються як загрози безпеці інформації, так і системи забезпечення інформаційної безпеки, від програмних атак вимірюються млрд. доларів США. Тенденцію їх щорічного зросту наведено на рисунку 4, на основі чого можна зробити припущення про подальший приріст цієї величини. Це, в свою чергу, змушує все більше уваги концентрувати на запобігання саме програмного класу загроз безпеці інформації ІТС.

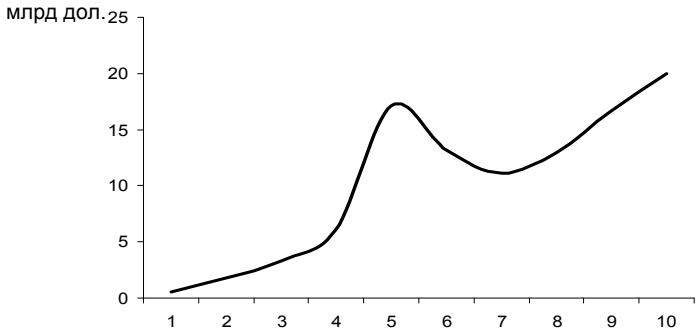

Рисунок 4 – Приріст світового збитку від атак програмних загроз безпеці інформації (1998-2007рр.)

Таким чином, все частіше вітчизняні та зарубіжні фахівці з інформаційної безпеки під час побудови, аналізу й досліджень систем забезпечення безпеки інформації ІТС більшість уваги, коштів і засобів спрямовують на запобігання й унеможливлення атаки саме суб'єктивних (навмисних) програмних загроз безпеці інформації [6, 7, 10, 12, 14, 17-19], які виникають у зв'язку дії суб'єктивного міжкласового зв'язку класу IV. При цьому в більшості випадків апаратні джерела загроз майже не розглядаються. Експерти-розробники інтуїтивно покладаються на достатньо високий рівень надійності сучасних аналогових і цифрових пристроїв та, відповідно, надмалу ймовірність здійснення атаки об'єктивних апаратних загроз. Також враховується і висока надійність загальноприйнятих технічних обмеження безпосереднього доступу людини до ІТС з метою засобів захисту інформації ІС чи ІТС, що майже повністю унеможливлює реалізацію і суб'єктивних апаратних загроз. Це, в свою чергу, дає підстави прогнозувати подальше зменшення впливу апаратних і, відповідно, стрімкий зріст програмних загроз на безпеку інформації ІТС, що вимагає проведення аналізу з подальшим вдосконаленням нормативної бази, принципів побудови і організації сучасних системи забезпечення безпеки інформації ІТС.

З наведених у статті результатів дослідження слідують наступні висновки:

1) Проаналізовано існуючі критерії та класифікації загроз безпеці інформації інформаційно-телекомунікаційної системи.

2) На основі дослідження існуючих класифікаційних поділів загроз безпеці інформації сучасної ІТС запропоновано вдосконалену класифікацію, здійснену відносно джерела безпосереднього впливу на інформацію на чотири класи: апаратні, програмні, стихійні, антропогенні.

3) За допомогою статистичних досліджень та чинних нормативних документів України можна стверджувати нагальну необхідність на теперішньому етапі розвитку ІТС і інформаційних технологій виокремлення з технологічних загроз апаратні і програмні в

окремі класи, що дасть можливість більш ефективно їх вивчати, прогнозувати і запобігати, та, як наслідок, забезпечувати високий рівня безпеки інформації ІТС.

4) Особливості класифікаційного поділу полягають у залежності класів загроз безпеці інформації ІТС, наявності між ними суб'єктивно-об'єктивних функціональних міжкласифікаційних зв'язків, найбільшій вазі (майже у 1,9 разів більша, за класи I-III разом взяті) цих зв'язків і, відповідно, величини збитків антропогенного класу, динамічна тенденція зменшення ваги апаратного класу та стрімкого зростання програмного.

5) У зв'язку зі стрімким розвитком інформаційних технологій та інформаційно-телекомунікаційних систем виникла нагальна необхідність здійснення вдосконалення нормативних документів України у сфері технічного захисту інформації відповідно одержаних до результатів дослідження, прогнозів на їх основі, запропонованої класифікації загроз безпеці інформації ІТС та її особливостей.

Список літератури

1. Захаров А.И. Информационные системы:оценка рисков//Информационная безопасность.– №6, 2005.
2. НД СТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – К.: ДСТСЗІ СБ України, 1999.
3. Потій О.В., Лєншин А.В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки зрілості систем забезпечення безпеки інформації // Радіотехніка. Тематичний випуск "Інформаційна безпека". – Вип. 141. – Х.: Радіотехніка, 2005. – С. 144-160.
4. Смірнов А.О., До́ренський О.П. Оцінювання загального показника якості системи забезпечення безпеки інформації автоматизованої системи // Системи обробки інформації. – Х.: ХУПС, 2007. – №7 (65). – С. 95-99.
5. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО "Тид "ДС", 2004. – 992 с.
6. Галатенко В.А. Стандарты и рекомендации в области информационной безопасности // Информационный бюлетень "Jet Informations", №1-3 (8-10), 1996.
7. Егоров Ф.И., Чирков Д.В. Модель угроз безопасности корпоративных сетей // Матеріали III Міжнародної науково-технічної конференції "Сучасні інформаційно-комунікаційні технології /COMINFO'2007/". – К.: ДУІКТ, 2007. – С. 273-275.
8. До́ренський О.П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу // Збірник наукових праць Кіровоградського національного технічного університету. – Вип. 19. – Кіровоград: КНТУ, 2007. – С. 55-61.
9. Ротштейн А.П. Интелектуальные технологии идентификации. – Вінниця: Вид-во "Універсум-Вінниця", 1999. – 320 с.
10. Галатенко В.А. Основы информационной безопасности. 3-е изд. – М.: "ИУИТ", 2005. – 208 с.
11. А. Прохоров. Вредоносные программы // КомпьютерПресс. – № 3'2006. – М.: ООО "КомпьютерПресс", 2006.
12. Середа С.А. Управление жизненным циклом программных продуктов как фактор сокращения теневого рынка программного обеспечения // Материалы конференции "INFORMATION TECHNOLOGIES - 2003". – Кишенеу: Экономич. академия Республики Молдова, 2003. – С. 38-45.
13. Горбенко И.Д., Потий А.В., Терещенко П.И. Критерии и методология оценки безопасности информационных технологий // Радіотехніка. Тематичний випуск "Інформаційна безпека". – Вип. 141. – Х.: Радіотехніка, 2005. – С. 144-160.
14. Локазюк В.М., Савченко Ю.Г. Надійність, контроль, діагностика. – К.: Видавничий центр "Академія", 2000. – 376 с.
15. Анохин А.М., Глотов В.А., Павельев В.В., Черкашин А.М. Методы определения коэфициентов важности критериев // "Автоматика и телемеханика", 1997. – 335 с.
16. Смірнов А.О., До́ренський О.П. Оцінювання загального показника якості системи забезпечення безпеки інформації автоматизованої системи // Системи обробки інформації. – Х.: ХУПС, 2007. – №7 (65). – С. 95-99.
17. Романов А.Н., Меркулова О.В. Створення підсистем для захисту інформаційних систем від вірусних атак // Інформатика та комп'ютерні технології-2007 / Матеріали III науково-технічної конференції молодих учених і студентів. – Донецьк: ДонНТУ, 2007. – С. 153-155.
18. Беловєд Н.І., Петровська Н.А. Мережні атаки і захист від них // Збірник наукових статтей "Управління розвитком". – Вип. 7'2008. – Х.: ХНЕУ, 2008. – С. 21-22.

19. Бєлозьоров Є.В. Спосіб забезпечення цілісності та безпеки обробки даних користувача в інформаційних системах // Матеріали III Міжнародної науково-технічної конференції “Сучасні інформаційно-комунікаційні технології /COMINFO’2007/”. – К.: ДУІКТ, 2007. – С. 261-264.
20. Каук В.І. Перспективи розвитку дистанційної освіти // Матеріали II науково-практичної конференції “Інформатизація вищих навчальних закладів МВС України”. – Х.: ХНУВС, 2008. – С. 4-6.
21. Закон України “Про електронні документи та електронний документообіг” від 22.05.2003р // Відомості Верховної Ради: Офіц. вид. – Вип. 36. – К.: Парлам. вид-во, 2003. – С. 275.

В статье исследованы особенности классификации угроз безопасности информации современной информационно-телекоммуникационной системы. Проанализированы существующие противоречия и предложены общепринятые технические угрозы выделить в два отдельных класса угроз безопасности информации: аппаратные (технические) и программные. Обоснованно необходимость и целесообразность избранного подхода.

In the article features of classification of threats safety of information of the modern informatively-telecommunication system are investigational. Existent contradictions are analysed and the generally accepted technical threats to select in two separate classes of threats safety of information are offered: vehicle (technical) and programmatic. Grounded necessity and expedience of select approach.