УДК 004.056.5

С. С. Бучик

АНАЛІЗ ОСНОВНИХ ПІДХОДІВ ДО СТВОРЕННЯ КЛАСИФІКАТОРА ЗАГРОЗ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ

У статті проаналізовано основні підходи до визначення рівня інформаційної безпеки та класифікації загроз. Основна увага зосереджена на міжнародних стандартах, чинному законодавстві України та певних специфічних підходах, які є основою побудови класифікатора загроз державним інформаційним ресурсам.

Постановка проблеми. Одними з найбільш важливих нормативно-технічних документів, які стимулюють розвиток захищених інформаційних систем (ІС), мереж і засобів, є документи, що стандартизують вимоги та критерії оцінювання безпеки [1].

Для створення класифікатора загроз державним інформаційним ресурсам (ДІР) актуальним та необхідним є проведення аналізу підходів до визначення рівня інформаційної безпеки (ІБ) та класифікацій загроз.

Огляд останніх досліджень та публікацій. За роки незалежності в Україні значно змінилася та постійно удосконалюється нормативно-правова база в галузі ІБ [2–7]. У зазначених документах та тих, які наведені на рис. 1, розкрито основні стандарти ІБ, технічні специфікації, критерії, функціональні послуги тощо. Значний практичний інтерес становлять законодавчі акти та підходи у сфері інформаційної безпеки провідних держав світу [8–15]. Але саме питання класифікації загроз ДІР у даних роботах та нормативно-правових документах безпосередньо не розглядалося.

Формулювання завдання дослідження. Виходячи з викладеного вище, метою статті є проведення аналізу основних підходів до визначення рівня ІБ та класифікацій загроз для подальшої побудови класифікатора загроз ДІР.

Виклад основного матеріалу. Для побудови класифікації загроз ДІР можна виділити такі основні напрямки аналізу (рис. 1) [2–14]: існуючих доктрин та законів України, які регламентують питання ІБ держави чи захист інформації (ЗІ); оцінних стандартів, направлених на класифікацію ІС та засобів захисту за вимогами безпеки; технічних специфікацій, що унормовують різні аспекти реалізації засобів захисту; інші підходи (найбільш значущі стандарти ІБ виділені сірою заливкою).

Підхід "Помаранчевої книги" як оцінного стандарту. Історично першим оцінним стандартом [1, 8, 15, 16], який набув широкого поширення і дуже вплинув на базу стандартизації ІБ у багатьох країнах, став документ Міністерства оборони Сполучених Штатів Америки (США) "Критерії оцінки довірчих комп'ютерних систем" (Trusted Computer System Evaluation Criteria, TCSEC). Ця праця, яку називають найчастіше за кольором обкладинки "Помаранчевою книгою", була вперше опублікована в серпні 1983 року з метою визначення вимог безпеки, що висуваються до апаратного, програмного і спеціального забезпечення комп'ютерних систем (КС) і вироблення відповідної методології аналізу політики безпеки (ПБ), що реалізується в КС військового

призначення. “Помаранчева книга” дає поняття безпечної системи, яка “керує за допомогою відповідних засобів доступом до інформації так, що тільки належним чином авторизовані особи або процеси, які діють від їх імені, отримують право читати, записувати, створювати і видаляти інформацію”. Очевидно, що абсолютно безпечних систем не існує, тому є сенс оцінювати лише ступінь наданої довіри.

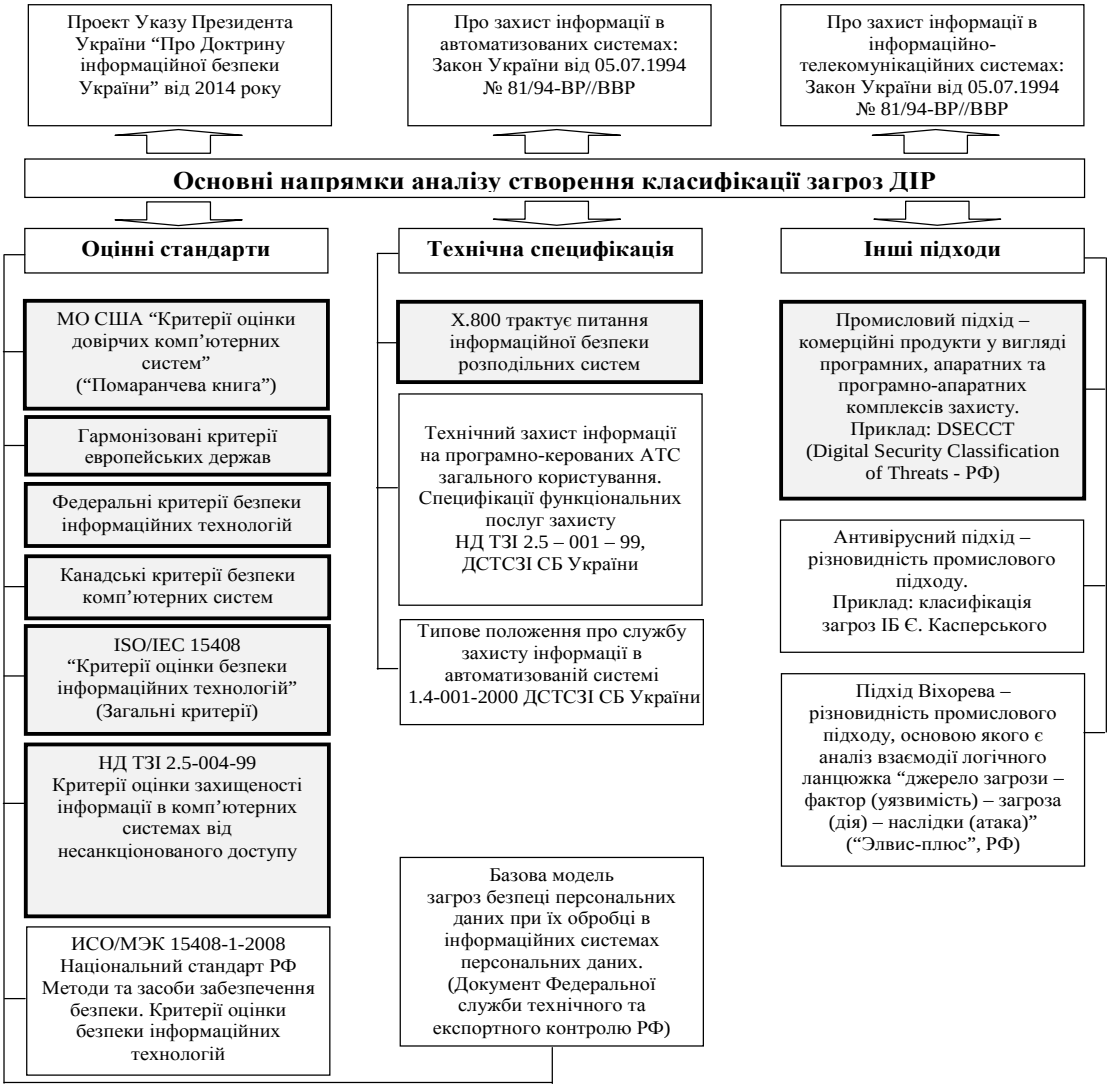

Рис. 1. Основні напрямки аналізу створення класифікації загроз ДІР

У “Помаранчевій книзі” довірча система визначається як “система, що використовує достатні апаратні та програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу”.

У даному стандарті безпека і довіра оцінені виключно з точки зору управління доступом до даних, що є одним із засобів забезпечення конфіденційності й цілісності.

У “Помаранчевій книзі” визначено чотири рівні довіри (безпеки) – D, C, B і A: C – довільне управління доступом; B – примусове управління доступом; A – верифікована безпека, D призначений для систем, визнаних незадовільними. У міру переходу від рівня D до A до систем висуваються все більш жорсткі вимоги (рис. 2). Рівні C і B підрозділяють на класи (C1, C2, B1, B2, B3) з поступовим зростанням міри довіри.

Щоб у результаті процедури сертифікації систему можна було віднести до деякого класу, її ПБ і рівень гарантованості повинні відповідати заданим вимогам.

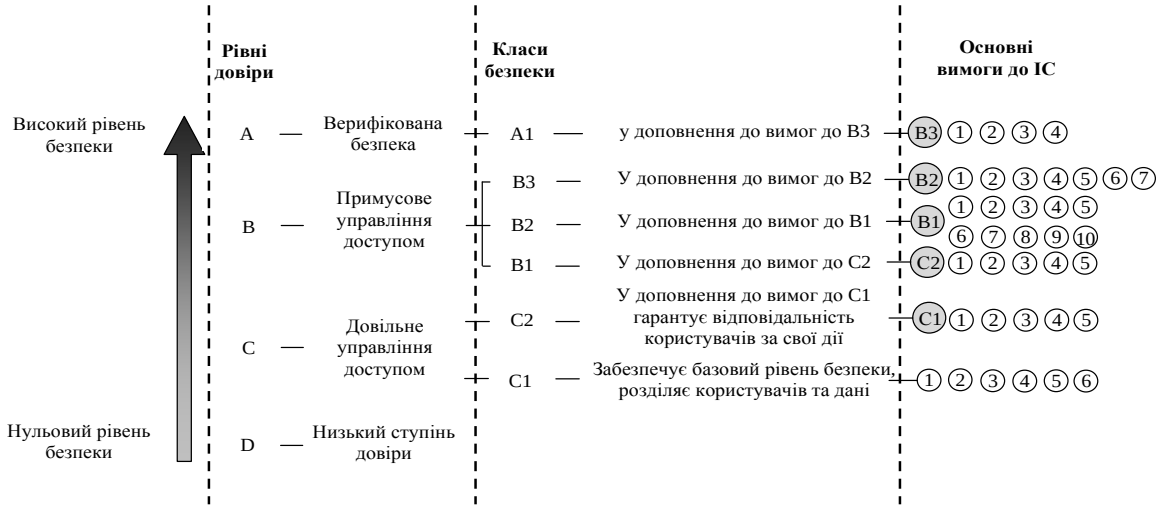

Рис. 2. Залежність рівня інформаційної безпеки від обраного класу безпеки та загальна структура класифікації

"Критерії безпеки комп'ютерних систем" МО США були першою спробою створити єдиний стандарт безпеки, розрахований на розробників, споживачів і фахівців із сертифікації КС. "Помаранчева книга" стала основою для розробників усіх інших стандартів ІБ і досі, з урахуванням доповнень і пояснень, використовується в США як керівний документ при сертифікації КС обробки інформації.

Можна зробити висновок, що дана класифікація побудована, у першу чергу, для оцінювання ступеня забезпечення ІБ в ІС, унаслідок чого питання протидії розглядаються з точки зору саме оцінки, а не рекомендацій для побудови комплексної системи захисту інформації (КСЗІ) ІС.

Основним недоліком такого підходу є те, що одна й та ж реальна загроза або не підходить під жодну із класифікаційних ознак, або, навпаки, відповідає декільком [16].

Слабким місцем "Помаранчевої книги" є недостатня увага вимогам гарантії оцінки [17].

Європейські критерії безпеки інформаційних технологій [Information Technology Security Evaluation Criteria (ITSEC)] – стандарт ІБ, розроблений у країнах Європи (Франція, Німеччина, Нідерланди та Великобританія) у 1991 році. "Європейські критерії" розглядають такі завдання засобів ІБ: захист від несанкціонованого доступу (НСД) з метою забезпечення конфіденційності та цілісності інформації шляхом недопущення її несанкціонованої модифікації або знищення; забезпечення працездатності систем завдяки протидії загрозам відмови в обслуговуванні (доступність).

Для вирішення проблеми визнання засобів захисту ефективними в критеріях уведене поняття гарантій засобів захисту. Гарантії включають два аспекти: ефективність, що відображає відповідність засобів безпеки завданням, які вирішуються, і коректність, що характеризує процес їх розроблення й функціонування. Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту і рівня гарантій їхньої реалізації.

У "Європейських критеріях" сім рівнів гарантій від E0 до E6 у порядку зростання (рис. 3). Рівень E0 означає мінімальні гарантії. При їх перевірці аналізується весь життєвий цикл системи – від початкової фази проектування до експлуатації та супроводження. Рівні гарантій від E1 до E6 розташовані з наростанням вимог ретельності

контролю. Так, на рівні Е1 аналізується тільки загальна архітектура системи, а гарантії засобів захисту підтверджуються функціональним тестуванням. На рівні Е3 до аналізу залучаються вихідні тексти програм і схеми апаратного забезпечення. На рівні Е6 потрібний формальний опис функцій безпеки, загальної архітектури, а також ПБ.

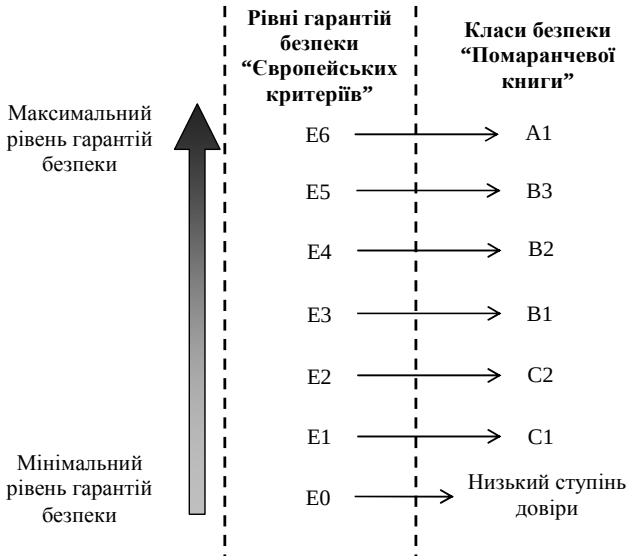

Рис. 3. Залежність рівня ІБ від обраного рівня гарантії безпеки

Рівні безпеки в "Європейських критеріях" використано для характеристики ступеня безпеки системи, зокрема їх визначено три: базовий, середній і високий. Безпека вважається *базовою*, якщо засоби захисту здатні протистояти окремим випадковим атакам; *середньою*, якщо засоби захисту здатні протистояти зловмисникам, які мають обмежені ресурси та можливості. Безпеку можна вважати *високою*, якщо є впевненість, що засоби захисту можуть бути подолані тільки зловмисником з високою кваліфікацією, набір можливостей і ресурсів якого виходить за межі відомого.

"Європейські критерії" покладено в основу багатьох стандартів безпеки КС. На їх основі Державною службою спеціального зв'язку та захисту інформації (ДССЗЗІ) Служби безпеки (СБ) України розроблено нормативні документи (НД) системи технічного захисту інформації (ТЗІ) щодо технічного захисту інформації на програмно-керованих автоматичних телефонних станціях (АТС) загального користування.

Таким чином, у "Європейських критеріях" уперше введено поняття гарантованості та шкалу для їх критеріїв – рівні гарантії. Зокрема, вимогам гарантованості надано навіть більше значущості, ніж функціональним. "Європейські критерії" повністю прийняли класи безпеки "Помаранчевої книги" і ввели ще п'ять додаткових класів [17]. Принципово важливою рисою даного стандарту є відсутність вимог до умов, за яких повинна працювати ІС [8].

Федеральні критерії безпеки інформаційних технологій [Federal Criteria for Information Technology Security (FCITS)] – стандарт ІБ, розроблений Національним інститутом стандартів і технологій (NIST) і Агентством національної безпеки (NSA) США у 90-х роках для використання в американському федеральному стандарті з оброблення інформації (Federal Information Processing Standard), який повинен був замінити "Помаранчеву книгу" [18, 20].

"Федеральні критерії" охоплюють практично весь спектр проблем, пов'язаних із захистом та забезпеченням безпеки, оскільки включають усі аспекти конфіденційності, цілісності та доступності. Основними об'єктами застосування вимог безпеки критеріїв є продукти інформаційних технологій (ІТ-продукти) і системи оброблення інформації. Ключовим поняттям концепції ІБ "Федеральних критеріїв" є поняття профілю захисту.

Головною метою створення "Федеральних критеріїв" було визначення універсального і відкритого для подальшого розвитку набору основних вимог безпеки, що висуваються до сучасних ІТ. Стандарт описує обґрунтований і структурований підхід до розробки вимог безпеки, ІТ, що ставляться до продуктів з урахуванням сфер їх застосування. Даний документ є узагальненням основних принципів забезпечення безпеки ІТ, розроблених у 80-і роки, він забезпечує спадкоємність щодо них з метою збереження досягнень у сфері захисту інформації.

"Федеральні критерії" містять положення, які стосуються тільки окремих ІТ-продуктів. Питання побудови систем обробки інформації з їх набору не є предметом розгляду цього документа.

Гармонізовані критерії європейських країн стали для свого часу передовим стандартом, оскільки створили передумови для появи "Загальних критеріїв".

Відповідно до "Федеральних критеріїв" процес розробки систем оброблення інформації здійснюється у вигляді послідовності таких основних етапів: розроблення та аналіз профілю захисту; розроблення і кваліфікаційний аналіз ІТ-продуктів; компонування й сертифікація системи оброблення інформації.

"Федеральні критерії" регламентують тільки перший етап цієї схеми – розробку та аналіз профілю захисту. Процес створення ІТ-продуктів і компонування систем оброблення інформації залишаються за межами цього стандарту.

Канадські критерії безпеки КС [Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)] – національний стандарт ІБ, розроблений Центром безпеки відомства безпеки зв'язку Канади (Canadian System Security Centre Communication Security Establishment) у 90-х роках [18, 19, 21].

"Канадські критерії" розроблялися для використання як національний стандарт безпеки КС. Він може бути використаний для розробки вимог безпеки, специфікацій засобів захисту й сертифікації програмного забезпечення (ПЗ) робочих станцій (РС) і багатопроцесорних обчислювальних систем (ОС), персональних і багатокористувацьких операційних систем, систем управління базами даних, розподілених, мережевих, вбудованих, об'єктно-орієнтованих тощо.

"Канадські критерії" є добре збалансованим поєднанням "Помаранчевої книги" і "Федеральних критеріїв", посиленим вимогами гарантій реалізації ПБ. Поряд з іншими стандартами вони стали основою для розроблення "Загальних критеріїв" безпеки ІТ.

У розрізі побудови класифікатора загроз ДІР інтерес викликає додаток до "Канадських критеріїв", який включає набір стандартних профілів захисту, що містять типові набори вимог до КС, які використовуються в державних установах. Цей підхід має багато спільного з концепцією профілів захисту, запропонованою у "Федеральних критеріях" США.

Канадські критерії оцінки безпеки КС стали першим стандартом ІБ, у якому на рівні структури документа функціональні вимоги до засобів захисту відокремлені від вимог

гарантії оцінки (адекватності реалізації). У них відкинуто підхід до оцінки рівня безпеки за допомогою універсальної шкали і використано незалежне ранжування вимог за кожним розділом, що забезпечує гнучкість у підході до оцінки безпеки різних типів виробів і систем.

Канадські критерії безпеки КС були покладені в основу Критеріїв оцінки захищеності інформації в КС від НСД [19], розроблених ДССЗЗІ СБ України для державної системи ТЗІ.

Загальні критерії безпеки інформаційних технологій (ISO/IEC 15408). У 1990 році під егідою Міжнародної організації зі стандартизації (ISO) були розгорнуті роботи зі створення стандарту в сфері оцінювання безпеки ІТ. Розробка цього документа переслідувала такі основні цілі [22]: уніфікацію національних стандартів у сфері оцінювання безпеки ІТ; підвищення рівня довіри до оцінювання безпеки ІТ; скорочення витрат на оцінювання безпеки ІТ на основі взаємного визнання сертифікатів.

Поява проекту міжнародного стандарту "Загальні критерії оцінки безпеки інформаційних технологій" (ЗК) стала якісно новим етапом у розвитку відповідної нормативної бази. ЗК узагальнили зміст і досвід використання "Помаранчевої книги", розвинули рівні гарантії оцінки "Європейських критеріїв", втілили в реальні структури концепцію типових профілів захисту "Федеральних критеріїв" США.

У ЗК проведено класифікацію широкого набору вимог безпеки ІТ, визначено структури їх групування і принципи цільового використання. Головні переваги ЗК: повнота і систематизація вимог безпеки, гнучкість у застосуванні та відкритість для подальшого розвитку. У [23] визначено, що за оцінками фахівців у галузі ІБ за рівнем систематизації, повнотою та можливостями деталізації вимог, універсальністю та гнучкістю в застосуванні ЗК є найбільш досконалими із існуючих у теперішній час стандартів. Він має, завдяки особливостям побудови, практично необмежені можливості для розвитку і є базовим стандартом, який містить методологію вироблення вимог і оцінювання безпеки ІТ, а також систематизований каталог вимог безпеки.

ЗК розроблено так, щоб задовольнити потреби трьох категорій користувачів об'єкта оцінки (ОО): споживачів, розробників і оцінювачів. Під ОО розуміють апаратно-програмний продукт або ІС. До таких об'єктів відносять, наприклад, операційні системи, обчислювальні мережі, розподілені системи, прикладні програми.

До аспектів безпеки, що розглядаються в ЗК, належать: захист від НСД, модифікації або втрати доступу до інформації при дії загроз, що є результатом навмисних або ненавмисних дій. Захищеність від цих трьох типів загроз зазвичай називають конфіденційністю, цілісністю і доступністю.

Використання ЗК дозволяє підвищити довіру до засобів захисту та, відповідно, до інформації, яку необхідно захистити. Цього досягають внаслідок гнучкого висування вимог безпеки до засобів ЗІ з урахуванням їх призначення та умов застосування, а також завдяки наявності найбільш повного й обґрунтованого набору вимог безпеки і методології оцінювання. ЗК відкриті й можуть бути розширені, за рахунок чого можна здійснювати уточнення або вводити додаткові вимоги.

Російська Федерація (РФ) перейшла на даний стандарт ще в 2004 році [23]. Російський стандарт ГОСТ Р ИСО/МЭК 15408 "Общие критерии оценки безопасности информационных технологий" є точним перекладом міжнародного стандарту. Поява

цього ГОСТу відображає не лише процес удосконалення російських стандартів з використанням міжнародного досвіду, але й частину урядової програми зі вступу РФ у Світову організацію торгівлі (СОТ).

В Україні робота щодо впровадження даного стандарту також ведеться, але даний процес проходить дуже повільно. ІБ нашої держави залежить від розв'язання проблем формування і керування процесами суспільної свідомості, виробництва та репродукції інформаційних ресурсів і доступу до них, створення цивілізованого ринку інформаційних продуктів та послуг, реалізації прав громадян на інформацію [24].

Технічна специфікація X.800 з'явилася дещо пізніше, ніж "Помаранчева книга", але дуже повно і глибоко трактує питання ІБ розподілених систем. Вона визначає рівні еталонної семирівневої моделі OSI, на яких можуть бути реалізовані функції безпеки, її використовувані механізми, а також адміністрування засобів безпеки [8, 25]. Таким чином, у ній можна виділити специфічні мережеві функції (сервіси) безпеки, а також необхідні для їх реалізації захисні механізми. Зміст загальних функцій (сервісів) безпеки технічної специфікації X.800 зображено на рис. 4.

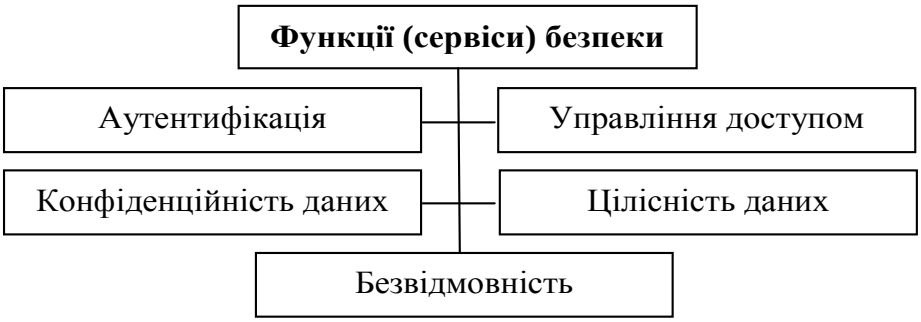

Рис. 4. Загальні функції (сервіси) безпеки технічної специфікації X.800

Серед дій, які стосуються ІС в цілому, зазначимо: забезпечення актуальності ПБ; взаємодію з іншими адміністративними службами; реагування на події, що відбуваються; аудит і безпечне відновлення. Адміністрування сервісів безпеки включає: визначення об'єктів, що захищаються; вироблення правил підбору механізмів безпеки (за наявності альтернатив); комбінування механізмів для реалізації сервісів; взаємодія з іншими адміністраторами для забезпечення узгодженої роботи. Обов'язки адміністратора механізмів безпеки передбачені переліком задіяних механізмів.

Промисловий підхід (класифікація загроз DSECCT (Digital Security Classification of Threats), РФ). Потреба забезпечення необхідної ІБ в ІС корпоративного масштабу з розгалуженою системою передавання даних (СПД) зумовила появу нових комерційних пропозицій і, відповідно, нових комерційних продуктів у вигляді програмних, апаратних і програмно-апаратних комплексів ЗІ. У зв'язку з цим деякими комерційними організаціями для створення реальних промислових комерційних продуктів було розроблено декілька типів класифікацій [15].

У класифікаторі загроз ІБ DSECCT, розробленому фахівцями компанії Digital Security, загрози поділено за характером, видом дії, причиною й об'єктом . Основна мета створення фахівцями Digital Security класифікації загроз – якнайповніший, детальніший розподіл, що описує усі існуючі загрози ІБ, за якими кожна з них потрапляє тільки під одну

класифікаційну ознаку, і тому найкраще може бути застосовний для аналізу ризиків реальних ІС [11].

У цій класифікації усі загрози потрапляють під одну класифікаційну ознаку, таким чином, кожна має бути однозначно віднесена до певного характеру, виду впливу, джерела або об'єкта. Саме тому загрози, які потрапляють під одну кваліфікаційну ознаку, можуть бути нейтралізовані з використанням одних і тих самих методів.

Аналізуючи DSECCT, можна зазначити, що більше уваги приділено загрозам технологічного характеру. У той же час, розглядаючи джерело загроз, яким може бути локальний порушник, не з'ясовано його вплив на канали, протоколи і лінії зв'язку, устаткування в цілому.

Основні результати. У ході дослідження з'ясовано, що існує ціла низка міжнародних стандартів, нормативних документів України, специфічних (спеціальних) підходів, які стосуються визначення рівня ІБ та класифікації загроз в інформаційно-телекомунікаційних системах (ІТС). Чинне законодавство, яке регламентує питання ІБ в ІТС, потребує уточнення та, у зв'язку з прагненням України вступити до Європейського союзу, прискорення переходу на міжнародні стандарти ІБ, що дасть змогу інтегруватися в світові інформаційно-комунікаційні системи та організації на засадах рівноправності, економічної доцільності, кіберзахисту та збереження інформаційного суверенітету. Результати аналізу мають лягти в основу побудови класифікатора загроз ДІР.

Висновок. Таким чином, у статті проаналізовано основні підходи до визначення рівня ІБ та класифікації загроз. Основна увага зосереджена на міжнародних стандартах, чинному законодавстві України та певних специфічних підходах, що є основою побудови класифікатора загроз ДІР.

СПИСОК ЛІТЕРАТУРИ

1. Гармонизированные критерии европейских стран ITSEC [Электронный ресурс]. – Режим доступа : http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/garmonizirovannye_kriterii_evropejskix_stran_itsec/?all.

2. Юдін О. К. Аналіз загроз державним інформаційним ресурсам / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С. 93–99.

3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 81/94-ВР // Вісник Верховної Ради. – 1994. – № 31. – С. 287.

4. Про Доктрину інформаційної безпеки України : проект Указу Президента України від 2014 року [Електронний ресурс]. – Режим доступу : http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025.

5. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту : НД ТЗІ 2.5-001-99 [Електронний ресурс]. – Режим доступу : http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=103243.

6. Про захист інформації в автоматизованих системах : Закон України від 05.07.1994 № 81/94-ВР // Вісник Верховної Ради. – 1994. – № 31. – С. 287.

7. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4-001-00 [Електронний ресурс]. – Режим доступу : http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41657.

8. Галатенко В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. – Режим доступа : http://www.intuit.ru.
9. Вихорев С. В. Классификация угроз информационной безопасности [Электронный ресурс] / С. В. Вихорев. – Режим доступа : http://www.elvis.ru.
10. Касперский Е. Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения [Электронный ресурс] / Е. Касперский // JetInfo. – 2003. – № 12. – Режим доступа : http://jetinfo.isib.ru/2003/12/2/article2.12.2003.html.
11. Классификация угроз Digital Security (Digital Security Classification of Threats) [Электронный ресурс]. – Режим доступа : http://www.dsec.ru/products/grif/fulldesc/classification.
12. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]. – Режим доступа : http://fstec.ru.
13. Элвис-Плюс. Информаториум. Персональные данные [Электронный ресурс]. – Режим доступа : http://www.elvis.ru/competency/informatorium/40/.
14. Классы информационной безопасности в международных стандартах [Электронный ресурс]. – Режим доступа : http://www.arinteg.ru/articles/klassy-informatsionnoy-bezopasnosti-v-mezhdunarodnykh-standartakh-30970.html.
15. Анализ подходов к классификации угроз информационной безопасности [Электронный ресурс]. – Режим доступа : http://infocom.uz/2013/05/01/analiz-podxodov-k-klassifikacii-ugroz-informacionnoj-bezopasnosti.
16. Общие критерии, основные изменения [Электронный ресурс]. – Режим доступа : http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/obschie_kriterii_osnovnye_izmenenija/?all.
17. Общие критерии оценки безопасности информационных технологий [Электронный ресурс]. – Режим доступа : http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/obschie_kriterii_otsenki_bezopasnosti_informatsionnyx_texnol/?all.
18. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення : [підруч.] / О. К. Юдін. – К. : НАУ, 2011. – 640 с.
19. Богуш В. М. Інформаційна безпека держави : [навч. посіб.] / В. М. Богуш, О. К. Юдін. – К. : "МК-Прес", 2005. – 432 с.
20. Федеральные критерии безопасности информационных технологий [Электронный ресурс]. – Режим доступа : http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/federalnye_kriterii_bezopasnosti_informatsionnyx_texnologij/?all.
21. Канадские критерии безопасности компьютерных систем CTCPEC [Электронный ресурс]. – Режим доступа : http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/kanadskie_kriterii_bezopasnosti_kompjuternyx_sistem_ctcpec/?all.
22. Профили защиты на основе "Общих критериев". Аналитический обзор / В. Б. Бетелин, В. А. Галатенко, М. Т. Кобзарь и др. [Электронный ресурс]. – Режим доступа : http://citforum.ru/security/criteria.

23. Россия перешла на “Общие критерии” (ГОСТ Р 15408-2002) [Электронный ресурс]. – Режим доступа : http://www.securitylab.ru/informer/240673.php.
24. Петров О. С. Критерії оцінки захищеності інформації в комп’ютерних системах: порівняння єдиних критеріїв та критеріїв України / О. С. Петров, О. А. Таликін, А. В. Мінін // Вісник Східноукр. нац. ун-ту ім. В. Даля. – Сєвєродонецьк : СНУ, 2005. – № 9 (91). – С. 92–96.
25. Рекомендации X.800 для распределенных систем [Электронный ресурс]. – Режим доступа : http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/rekomendatsii_x_800_dlja_raspredelennyx_sistem/?all.

Подано 15.10.2015

С. С. Бучик

АНАЛИЗ ОСНОВНЫХ ПОДХОДОВ К СОЗДАНИЮ КЛАССИФИКАТОРА УГРОЗ ГОСУДАРСТВЕННЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ

В статье проанализированы основные подходы для определения уровня информационной безопасности и классификации угроз. Основное внимание сосредоточено на международных стандартах, действующем законодательстве Украины и определенных специфических подходах, которые являются основой для построения классификатора угроз государственным информационным ресурсам.

S. S. Buchyk

ANALYSIS OF BASIC APPROACHES ON CREATION OF CLASSIFIER OF THREATS TO STATE INFORMATIVE RESOURCES

The analysis of basic approaches in relation to determination of informative security and classification of threats is conducted in the article. Basic attention is concentrated on realization of the analysis of international standards, current legislation of Ukraine and certain specific approaches, which must underlie the construction of the classifier to threats of state informative resources.