УДК 004.056.5

[1] **Юдін О. К.,** д.т.н.,
[2] **Бучик С.С.,** к.т.н.

АНАЛІЗ КЛАСИФІКАЦІЙ ТИПІВ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

[1]Національний авіаційний університет
[2]Житомирський військовий інститут імені С.П. Корольова
Державного університету телекомунікацій
kszi@ukr.net
s_stbu@ukr.net

Здійснено подальше удосконалення типової схеми захисту інформації з урахуванням розробленого авторами методу «Подвійної трійки захисту». Показано, що дана типова схема захисту може бути прийнята за основу при подальшій розробці систем захисту державних інформаційних ресурсів. Приведена загальна класифікація типів систем захисту інформації з урахуванням проведеного аналізу даного явища, показано необхідність використання принципу комплексності захисту державних інформаційних ресурсів

Ключові слова: система захисту інформації; тип; класифікація; комплексність; державні інформаційні ресурси

Аналіз останніх досліджень і публікацій

Незважаючи на широке коло публікацій та досліджень, які стосуються питання певної класифікації систем захисту інформації (СЗІ), конкретному питанню класифікації їх типів приділяється небагато уваги. Так в роботі Корченко О. Г. [1] приводиться класифікація засобів захисту, комп'ютерних вірусів, атак, апаратних засобів, але виходячи з назви праці не приведена класифікація типів СЗІ. В роботі [2-3] авторів Юдіна О. К., Корченко О. Г. та Конаховича Г. Ф. також не розглядалось дана тематика. Не розглядається дана тематика і в роботах Богуша В. М., Довидькова О. А., Кривуці В. Г. [4], Шаньгина В. Ф. [5]., Грайворонського М. В., Новікова О. М. [6] та інших вчених. Також виходячи з аналізу нормативних документів, які регламентують захист інформації в Україні, не прослідковується класифікація типів СЗІ. В зв'язку з чим розгляд та визначення класифікації типів систем захисту інформації є актуальним.

Постановка задач досліджень

Таким чином, метою статті є представлення типової системи захисту інформації та проведення аналізу класифікацій типів систем захисту інформації на її основі і, як наслідок, створення власної класифікації; обґрунтування на основі цього необхідності використання принципу комплексності захисту державних інформаційних ресурсів (ДІР).

Виклад основного матеріалу

Нормативний документ технічного захисту інформації (НД ТЗІ) 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22, надає визначення поняттю захист інформації в автоматизованій системі (АС), але не надає визначення, що собою представляє система захисту інформації. Існує визначення лише поняття комплексної системи захисту інформації (КСЗІ). Приведемо дані визначення.

Захист інформації в АС – діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Комплексна система захисту інформації – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС (на автономних робочих станціях (АС класу 1) і в комп'ютерних мережах (АС класу 2 і 3)).

Зрозуміло, що так як система визначається як сукупність взаємозв'язаних елементів, то призначення *системи захисту інформації* полягає в тому, щоб об'єднати усі складові елементи захисту в єдине ціле, в якому кожен компонент, виконуючи свою пряму функцію, одночасно забезпечує виконання функцій іншими компонентами і пов'язаний з ними логічно і технологічно [7].

За відсутності окремих компонентів системи або їх неузгодженості між собою неминучі помилки в технології захисту інформації. Отже, захист має бути *системним*, і це є основною умовою захисту інформації.

Для того, щоб забезпечити надійність захисту інформації, потрібна не лише системність захисту, але і її комплексність – один із основних принципів захисту інформації. Таким чином, ми отримуємо перший тип СЗІ – комплексні системи захисту інформації.

Щоб визначитись з іншими типами СЗІ, розкриємо поняття комплексності. В цілому, комплексність представляє собою сукупність предметів і явищ, які пов'язані між собою в одне ціле.

Відповідно до поняття захисту інформації комплексність має три призначення [7]:

1. у об'єднанні локальних систем захисту;

2. у забезпеченні повноти усіх складових системи захисту;

3. у забезпеченні всеосяжності захисту інформації.

Перше призначення полягає у об'єднанні в одне ціле локальних СЗІ, при цьому, вони повинні і функціонувати, як єдине ціле.

Друге призначення комплексності обумовлене призначенням самої системи. Система повинна логічно і технологічно об'єднати усі складові захисту. Але вона не розглядає повноту цих складових, не враховує усіх чинників, які чинять або можуть чинити вплив на якість захисту. Таким чином, якість захисту полягатиме у обиранні необхідних оптимальних варіантів побудови систем (системи) захисту інформації (повинні враховуватися усі параметри уразливості інформації, потенційно можливі загрози її безпеки, охоплюватися усі необхідні об'єкти захисту, використовуватися усі можливі види, методи і засоби захисту і необхідні для захисту кадрові ресурси, здійснюватися усі захисні заходи, що викладені в цілях і завданнях) з урахуванням конкретного призначення системи.

Третє призначення комплексності полягає в тому, що система має забезпечувати безпеку усієї сукупної інформації належному захисту і за будь-яких обставин. Це означає, що повинні захищатися усі носії інформації в усіх компонентах її збору, зберігання, передачі і використання, в будь-який час і при усіх режимах функціонування системи обробки інформації.

В той же час, комплексність не виключає, а навпаки, припускає диференційований підхід до захисту інформації. Тут диференційованість залежить від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умов прояву її уразливості, каналів і методів несанкціонованого доступу до інформації.

Для того, щоб впевнитись у багатоплановості СЗІ достатньо переглянути її типову схему (рис.1) за основу якої взята схема, що представлена в [8], але з урахуванням авторських досліджень та запровадженого методу «Подвійної трійки захисту» [3,9].

Окремо охарактеризуємо виділенні на рис.1 елементи організаційної системи захисту. Розуміння решти елементів для більшості фахівців із захисту інформації не представляє труднощів.

Система організації психологічного захисту інформації являє собою систему, яка використовує допустимі нормами права і моралі методи і засоби вивчення психофізіологічних особливостей і можливостей людей, а також психологічної дії на людей з метою оцінки відповідності їх вимогам для допуску до обробки інформації, що захищається.

Система організації використання морально-етичних норм захисту інформації являє систему, що використовує норми і правила, які не мають юридичної сили, але їх порушення веде до втрати авторитету, виникнення додаткових труднощів і інших негативних наслідків для людини і організації.

Система організації страхування захисту інформації є системою захисту інформації, яка передбачає відшкодування збитків від її знищення або модифікації шляхом отримання страхових виплат.

Як вказано в [8], морально-етичні і психологічні елементи захисту інформації практично в усіх країнах до теперішнього часу розглядалися лише в теорії.

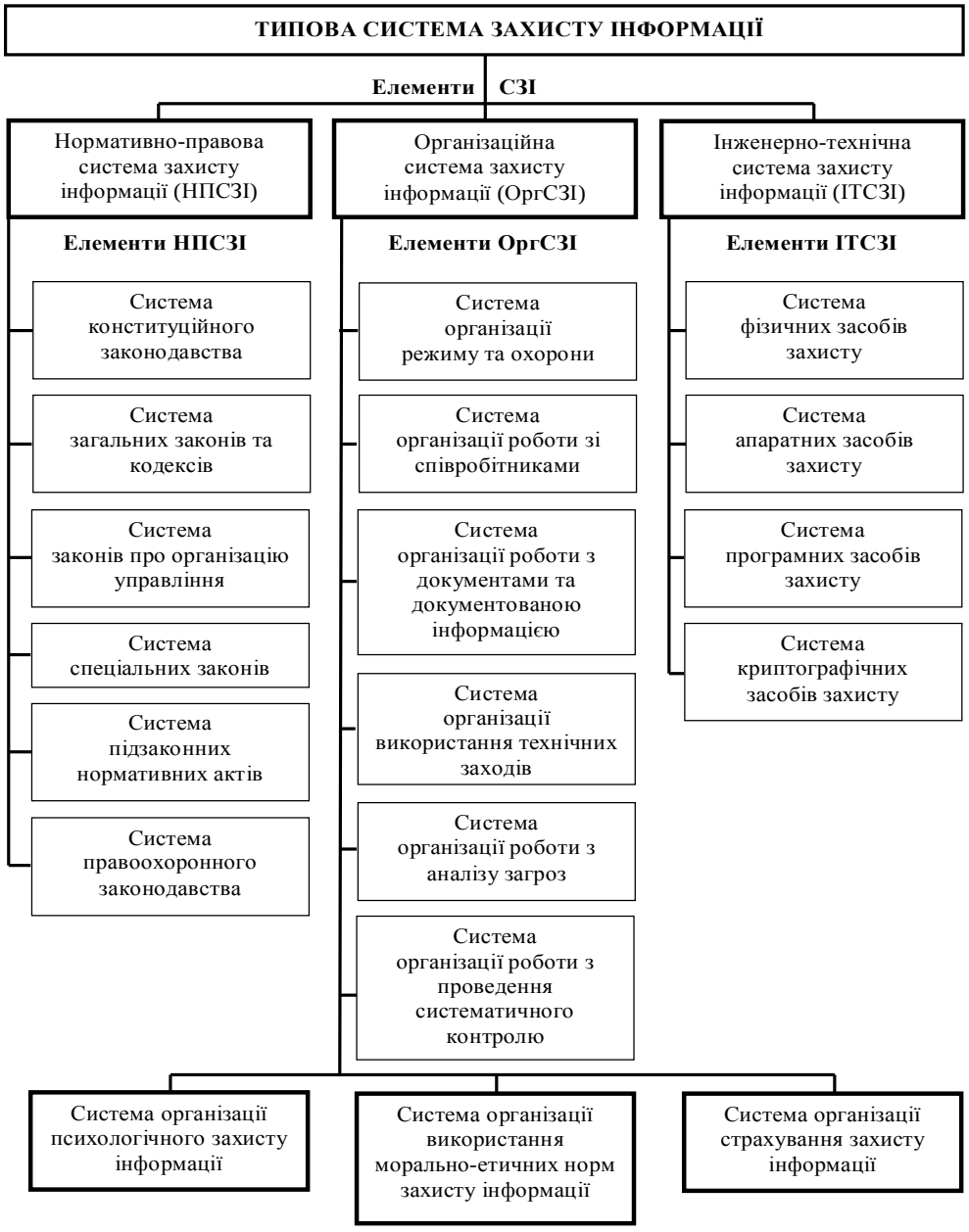

Рис. 1. Типова схема системи захисту інформації

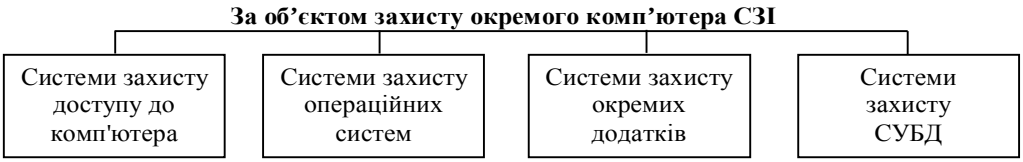

Рис. 6. Класифікація СЗІ за об'єктом захисту окремого комп'ютера

Системи захисту доступу до комп'ютера – передбачає використання апаратно-програмних модулів довіреного завантаження, які шляхом реалізації належного контролю доступу користувачів до технічних засобів автоматизованого робочого місця та виконання завантаження довіреної операційної системи, забезпечують захист інформації від несанкціонованого доступу (здійснюється перевірка цілісності технічних та програмних засобів комп'ютера та апаратна ідентифікація/аутінтифікація користувача).

Системи захисту операційних систем – призначені для ідентифікації та аутентифікації, розмежування доступу користувачів до ресурсів, протоколювання та аудиту самої системи, управління політикою безпеки, виконання криптографічних та мережевих функцій захисту.

Системи захисту окремих додатків – призначені для ідентифікації та аутентифікації, розмежування доступу користувачів до окремих додатків, протоколювання та аудиту роботи з додатками.

Захист баз даних є однією із самих складних задач. Необхідно контролювати доступ працівників до інформації, яка зберігається в базі даних, обмежувати адміністраторів бази даних від можливості читання та зміни чутливих даних, захистити інформацію під час зберігання та при передачі по мережі. В зв'язку з чим забезпечити захист баз даних можливо лише використовуючи комплексний підхід. Таким чином, призначення системи захисту СУБД буде виходити із задач, які необхідно вирішувати [12].

Системи захисту СУБД – призначені для розмежування повноважень всередині бази даних з реалізацією обмеження доступу до даних адміністратором; реалізації мандатного доступу (з використанням міток) до даних; обмеження доступу і контролю виконання команд в залежності від часу, *IP*-адреси, операції, яка виконується; суворої аутентифікації при доступі до бази даних; захисту клієнтського трафіка (*SSL*) при мережевому доступі до баз даних; прозорому шифруванню чутливої інформації в базі даних та її захист на фізичних носіях інформації; захист резервних копій даних; консолідації, зберігання та аналізу аудита різних баз даних.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999) за сукупністю характеристик АС виділено три ієрархічні класи АС, вимоги до функціонального складу комплекс засобів захисту (КЗЗ) яких істотно відрізняються. Виходячи з даних трьох ієрархічних класів АС можна здійснити класифікацію і СЗІ (рис. 7).

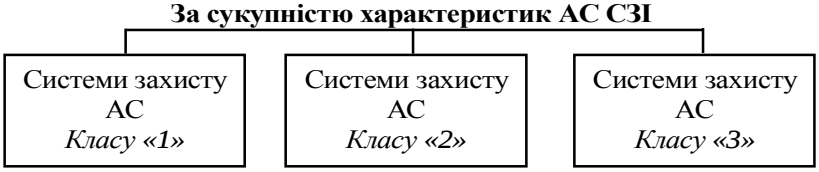

Рис.7. Класифікація СЗІ за сукупністю характеристик АС

Системи захисту АС Класу «1» – призначені для захисту одномашинного однокористувацького комплексу, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

Системи захисту АС Класу «2» – призначені для захисту локалізованого багатомашинного багатокористувацького комплексу, який обробляє інформацію різних ступенів обмеження доступу.

Системи захисту АС Класу «3» – призначені для захисту розподіленого багатомашинного багатокористувацького комплексу, який обробляє інформацію різних ступенів обмеження доступу.

Наступним критерієм нашої класифікації типів СЗІ може виступати інтегральна характеристика захищеної інформаційної системи – *політика безпеки*. Існують два типи політики безпеки: дискреційна й мандатна [2]. В зв'язку з чим, ми можемо здійснити класифікацію типів СЗІ за обраним типом політики безпеки (рис. 8).

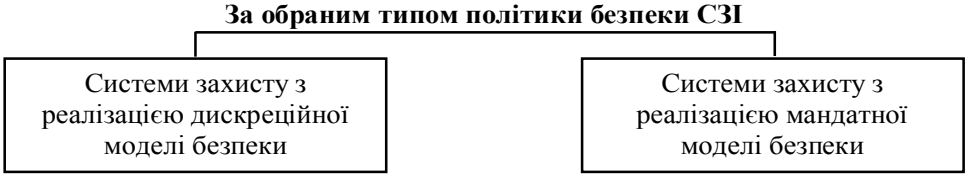

Рис.8. Класифікація СЗІ за обраним типом політики безпеки

Системи захисту з реалізацією дискреційної моделі безпеки – забезпечують дискреційне управління доступом (*Discretionary Access Control – DAC*), що визначається двома властивостями: всі суб'єкти й об'єкти повинні бути ідентифіковані; права доступу суб'єкта до об'єкта системи визначаються на підставі деякого зовнішнього, стосовно системи правила.

Системи захисту з реалізацією мандатної моделі безпеки – забезпечують мандатне управління доступом (*Mandatory Access Control – MAC*), що визначається наступними властивостями: всі суб'єкти й об'єкти системи повинні бути однозначно ідентифіковані; задається лінійно впорядкований набір міток таємності; кожному об'єкту системи привласнена мітка таємності; кожному суб'єктові системи привласнена мітка таємності, що визначає рівень довіри до нього в інформаційній системі; визначено максимальне значення мітки таємності об'єктів, до яких суб'єкт має доступ (мітка таємності суб'єкта називається його рівнем доступу).

Наприкінці наведемо ще одну класифікацію типів СЗІ – це класифікація за відношенням до загальних моделей, які можуть бути реалізовані в даній СЗІ (рис. 9). Як вказано в [13], системну класифікацію загальних моделей в теперішній час здійснити практично неможливо.

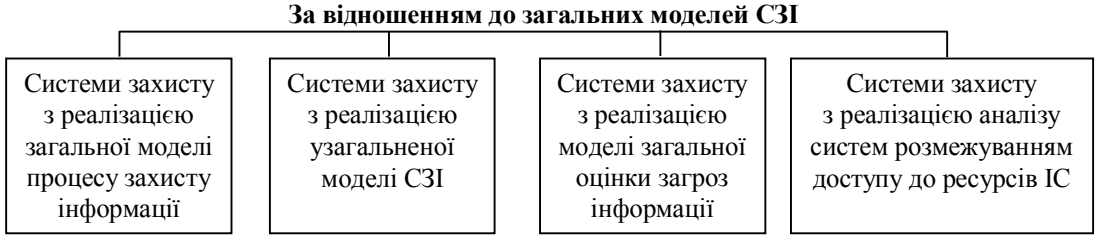

Рис. 9. Класифікація СЗІ за відношенням до загальних моделей

Враховуючи загальну системну класифікацію, яка представлена в [13] та моделі захисту інформаційних ресурсів, які викладені в [2, 14], класифікацію СЗІ за відношенням до загальних моделей можна трактувати наступним чином.

Системи захисту з реалізацією загальної моделі процесу захисту інформації – відображають процес захисту інформації як процес взаємодії дестабілізуючих факторів, які впливають на інформацію, і засобів захисту інформації, що перешкоджають дії цих факторів. Наслідком цієї взаємодії є певний рівень захищеності інформації.

Системи захисту з реалізацією узагальненої моделі СЗІ – відображають основні процеси, які здійснюються в ній з метою раціоналізації та оптимізації процесів захисту. Прикладом побудови таких систем можуть бути системи, які побудовані на основі так званої узагальненої концепції захисту інформації (УКЗІ). В даному випадку УКЗІ – інструментально-методологічна база, що забезпечує оптимальну практичну реалізацію стратегій захисту на регулярній основі з урахуванням мінімальних витрат [2].

Системи захисту з реалізацією моделі загальної оцінки загроз інформації – здійснюється оцінка не лише загроз інформаційним ресурсам, а ще і оцінка тих втрат, які можуть мати місце при виявленні різних загроз. Прикладом таких систем є системи, які побудовані на основі емпіричного підходу щодо захисту інформаційних ресурсів, суть якого полягає в тому, що на основі тривалого збору й обробки даних реальних проявів загроз інформації і розмірів завданого збитку виключно емпіричним шляхом, встановлюються залежності між потенційно можливим збитком і коефіцієнтами, що характеризують частоту прояву відповідної загрози і значення розміру збитку. Також можуть використовуватися і динамічні моделі оцінки потенційних загроз, які також враховують очікувану частоту появи загроз та значення можливого збитку при прояві загрози – дані моделі можуть бути зведені в постановці задач в термінах теорії ігор.

Системи захисту з реалізацією аналізу систем розмежуванням доступу до ресурсів ІС – призначені для забезпечення вирішення задач аналізу та синтезу систем (механізмів) розмежування доступу до різних видів ресурсів. Прикладами таких моделей є СЗІ побудовані на основі класичних мандатних моделей цілісності та розмежування доступу Белла-Лападула, Біба, моделі поширення прав доступу Take-Grant, моделі контролю цілісності Кларка-Вілсона.

Основні результати

До основних результатів, отриманих в статті, можна віднести подальше удосконалення типової схеми захисту інформації з урахуванням розробленого авторами методу «Подвійної трійки захисту». Вказана типова схема може бути прийнята за основу при розробці в подальшому систем захисту ДІР. Приведена загальна класифікація типів СЗІ, показано необхідність використання принципу комплексності захисту ДІР.

Висновки

Розглядаючи сучасний етап розвитку технологій забезпечення інформаційної безпеки, відсутності на ринку реальних продуктів, що дозволяли б реалізувати інтегровані СЗІ, дослідження авторів дозволяє зробити висновок щодо необхідності використання комплексного підходу до побудови системи захисту державних інформаційних ресурсів. Застосування багатокомпонентних, а тим паче, однокомпонентних СЗІ в межах захисту ДІР та з урахуванням сучасної типової системи захисту інформації (рис. 1) не є доцільним або може використовуватися в межах вирішення вузькоспеціалізованих задач.

Список літератури

1. Корченко А. Г. Построение систем защиты информации на нечётких множествах. Теория и практика решения / А. Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

2. Юдін О.К. Захист інформації в мережах передачі даних: підруч. / Г.Ф. Конахович, О.Г. Корченко, О.К. Юдін . – К.: Вид-во ТОВ НВП "ІНТЕРСЕРВІС", 2009. – 714 с.

3. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

4. Богуш В. М. Теоретичні основи захищених інформаційних технологій: навч. посібник / Б. М. Богуш, О. А. Довидьков, В. Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.

5. Шаньгин В. Ф. Информационная безопасность / Владимир Федорович Шаньгин. – М.: ДМК Пресс, 2014. – 702 с.

6. Грайворонський М. В. Безпека інформаційно-телекомунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.

7. Попов В. В. Комплексная защита информации на предприятии. Курс лекций / В. В. Попов. – М.: МАИ, 2009. – 124 с. – Режим доступу: http://www.frela-21.narod.ru/kzip/kzip.doc.

8. Аверченков, В. И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – Брянск: БГТУ, 2007. – 225 с.

9. Юдін О.К. Методологія побудови класифікатора загроз державним інформаційним ресурсам / О. К. Юдін, С. С. Бучик, А. В. Чунарьова, О. І. Варченко // Наукоємні технології.– 2014. №2(22) / Технічні науки. – С. 200–210.

10. Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. – 416 с.

11. Типовая структура комплексной системы защиты информации от несанкционированного доступа. – Режим доступу: http://www.mehatronics.ru/2011/01/типовая-структура-комплексной-систе/

12. Система защиты баз данных. – Режим доступу: http://www.lins-m.ru/index.php?ID=155

13. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ТИД Диа Софт, 2002. – 688 с. – Режим доступу: http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=1284

14. Арьков П. А. Разработка комплекса моделей для выбора оптимальной системы защиты информации в информационной системе организации: дис. кандидата тех. наук : 05.13.19 – Методы и системы защиты информации, информационная безопасность / Арьков Павел Алексеевич. – Волгоград, 2009. – 185 с.

Статтю подано до редакції 12.09.2015