УДК 681.3

НОВА СИСТЕМНА КОНЦЕПЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІНОВАНОГО ДОСТУПУ

Вячеслав Шорошев
ДНДІ МВС України

Анотация: **На основі аналізу існуючих системних підходів та розвитку критеріїв і стандартів інформаційної безпеки провідних країн світу пропонується нова системна Концепція захисту інформації в комп'ютерних системах від загроз несанкціонованого доступу.**
Summary: **On the basis of analysis of existent systems approaches and development of criteria and standards of informative safety after the best experience of leading countries of world new domestic system Conception is offered in relation to the priv in the computers systems from the threats of unauthorized division.**
Ключові слова: **Потенційні загрози, несанкціонований доступ, конфіденційність, цілісність, доступність, спостереженість, функціональні послуги безпеки, гарантійні послуги безпеки, профільні послуги безпеки, антивірусна безпека, ідентифікація, автентифікація.**

I Вступ

Основною метою статті є концептуальне визначення й обґрунтування складу базових (типових) підсистем для побудови архітектури системи захисту інформації в комп'ютерних системах від загроз несанкціонованого доступу (СЗІ НСД). Для цього аналізується кращий досвід провідних країн світу, таких як США, Канада, Англія, Франція, Німеччина, Нідерланди, а також Російська Федерація і Україна щодо пріоритетної вагомості критеріїв захищеності інформації в комп'ютерних системах, насамперед, від загроз несанкціонованого доступу (НСД), а також розглядаються рекомендації Ради Європи про кібезлочинність щодо необхідності міжнародного співробітництва в боротьбі з суспільно небезпечними діяннями.

В запропонованій Концепції потенційними загрозами НСД визначаються наступні порушення: конфіденційності, цілісності, доступності, спостереженості.

II Основна частина

Перші міжнародні концепції одержали найбільше поширення в провідних західних країнах, насамперед, в рамках інвестиційних програм щодо розробки міжнародних критеріїв та стандартів комп'ютерної безпеки (США, Канада, Англія, Франція, Німеччина, Нідерланди), а також в Російській Федерації і в Україні.

Так, згідно з критеріями безпеки комп'ютерних систем TCSEC США (1983 р.), інакше відомими як "Оранжова книга", захищеність інформації в будь-якій комп'ютерній системі в цілому оцінювалась за трьома її класами: С2 - **мінімальний рейтинг** захищеності від несанкціонованого доступу, В2 – **відносно стійкий захист** від несанкціонованого доступу, В3 – **стійкий захист** від несанкціонованого доступу [1].

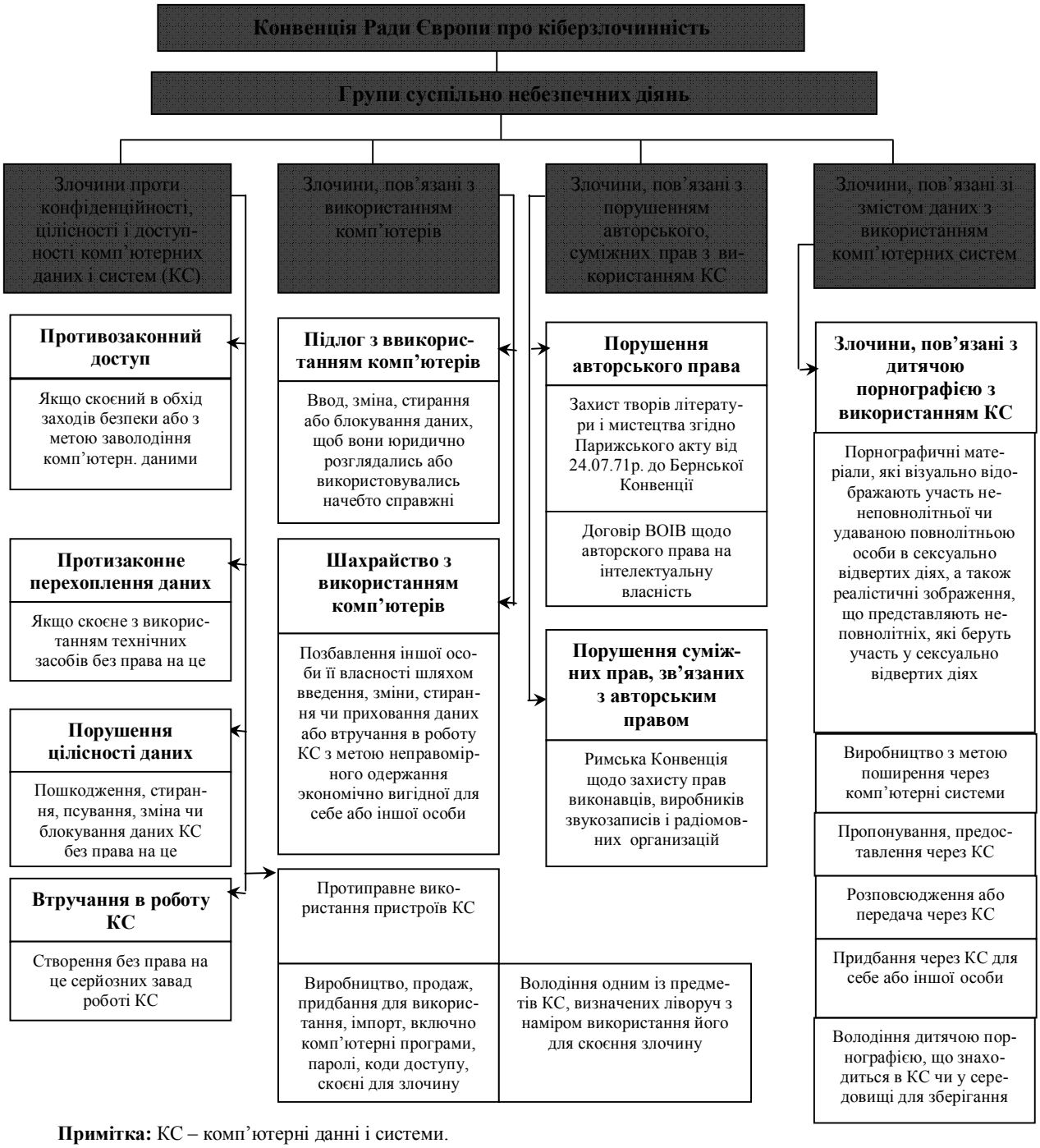
Згідно з європейським критерієм безпеки інформаційних технологій ITSEC (1991 р., країни розробники Німеччина, Франція, Англія, Нідерланди) захищеність інформації в будь-якій комп'ютерній системі в цілому оцінювалась також за трьома її класами: FC-2 **- мінімальний рейтинг** захищеності від несанкціонованого доступу, FB-2 – **відносно стійкий** захист від несанкціонованого доступу, FB-3 – **стійкий захист** від несанкціонованого доступу [1, 2].

Пріоритетність захисту від загроз несанкціонованого доступу одержала подальший розвиток в Єдиних міжнародних критеріях CCITSE (1996 – 1997 роки), потім в міжнародних стандартах ISO 15408, ISO 17799 [3, 4 – 7].

Серед міжнародних нормативно-правових документів особливе місце за вагомістю займає **Конвенція Ради Європи про кіберзлочинність**. На рис. 1 запропонована концептуальна модель політики безпеки комп'ютерних даних і систем за рекомендаціями Конвенції Ради Європи про кіберзлочинність. У цій концепції особливо виділяються чотири вказаних групи суспільно небезпечних діянь, які вимагають міжнародного співробітництва і контролю [8 – 10]. Це злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, злочини, пов'язані з використанням комп'ютерів, злочини, пов'язані з авторськими і суміжними правами та дитячою порнографією.

Конвенція Ради Європи про кіберзлочинність чинна з 7 січня 2001 р. Україна підписала Конвенцію 23 листопада 2001 р., а в 2005 р. її ратифікувала Верховна Рада України. Настав час уважно ознайомитися й усвідомити основні положення цього важливого міжнародно-правового документа, а також виробити заходи,

що забезпечують його виконання в нашій країні і гармонізацію його рекомендацій із законодавчими актами України.



Примітка: КС – комп'ютерні данні і системи.

Рисунок 1 – Концептуальа модель політики безпеки комп'ютерних даних і систем за рекомендаціями Конвенції Ради Європи про кіберзлочинність

Конвенція про кіберзлочинність є комплексним документом, що містить норми, покликані вплинути на різні галузі права: карного, карно-процесуального, авторського, цивільного, інформаційного. Вона ґрунтується на головних принципах міжнародного права: поваги прав людини, співробітництва і сумлінного виконання зобов'язань.

Норми Конвенції спрямовані на регулювання трьох основних блоків питань:

- зближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації;

- зближення національних карно-процесуальних заходів, спрямованих на забезпечення збору доказів при розслідуванні таких злочинів;

- міжнародне співробітництво в карно-процесуальній діяльності, спрямоване на збирання доказів здійснення таких злочинів за кордоном.

Кримінально-правові питання Конвенції. Конвенцією пропонується включити в законодавство країн-учасниць єдині норми про кримінальну відповідальність за "кіберзлочинність", перелік яких включає діяння, спрямовані проти комп'ютерної інформації (як предмета злочинного зазіхання) і які використовують її як унікальне знаряддя здійснення злочину.

Об'єктом кіберзлочинів, відповідно до Конвенції, є широкий спектр охоронюваних нормами права суспільних відносин, що виникають при здійсненні виробництва, збору, обробки, накопичування, збереження, пошуку, передачі, поширення і споживання комп'ютерної інформації.

Серед них, з огляду на підвищену суспільну значущість, нормами права Конвенції вирізняються правовідносини, що виникають у сфері забезпечення ***конфіденційності, цілісності і доступності*** комп'ютерних даних та систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського та суміжного прав на інтелектуальну власність.

Об'єктивна сторона кіберзлочинів характеризується виокремленням чотирьох груп суспільно небезпечних діянь, успішна протидія яким можлива тільки за умови широкого міжнародного співробітництва країн-членів, що підписали Конвенцію Ради Європи.

1. Злочини проти конфіденційності, цілісності і доступності комп'ютерних даних та систем.

Протизаконний доступ – одержання доступу до комп'ютерної системи загалом або до будь-якої її частини без права на те, що може розглядатися як злочин, якщо це вчинено в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними чи з іншим безчесним наміром.

Протизаконне перехоплення комп'ютерних даних, якщо його здійснено з використанням технічних засобів перехоплення без права на це і для не публічних передач комп'ютерних даних у комп'ютерну систему, з неї чи всередині такої системи, в т. ч. електромагнітні випромінювання комп'ютерної системи, що несуть такі комп'ютерні дані, а також якщо це вчинено в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними чи іншим безчесним наміром щодо комп'ютерної системи, з'єднаної з іншою комп'ютерною системою.

Порушення цілісності даних – ушкодження, стирання, псування, зміна або блокування комп'ютерних даних без права на це, у тому числі винятково у випадках, які призвели до серйозних наслідків.

Втручання в роботу (функціонування) системи – створення без права на це серйозних перешкод роботі комп'ютерної системи шляхом уведення, передачі, ушкодження, стирання, псування, зміни чи блокування комп'ютерних даних.

Протиправне використання пристроїв:

виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання в користування: 1) пристроїв, у т. ч. комп'ютерних програм, розроблених чи адаптованих, насамперед для цілей здійснення злочинів; 2) комп'ютерних паролів, кодів доступу або інших подібних даних, за допомогою яких може бути отриманий несанкціонований доступ до комп'ютерної системи загалом чи до будь-якої її частини, з наміром використовувати їх з метою здійснення злочинів; володіння одним із предметів, що згадуються вище, з наміром використовувати його з метою здійснення злочинів .

2. Злочини, пов'язані з використанням комп'ютерів.

Підробка з використанням комп'ютерів – уведення, зміна, стирання чи блокування комп'ютерних даних, що призводять до порушення їх автентичності з наміром, щоб вони розглядалися або використовувалися в юридичних цілях та начебто вони залишаються справжніми, незалежно від того, чи ці дані читаються безпосередньо, чи зрозумілі.

Шахрайство з використанням комп'ютерів – позбавлення іншої особи його власності шляхом уведення, зміни, стирання чи приховання комп'ютерних даних або втручання у функціонування комп'ютера або системи з метою неправомірного одержання економічної вигоди для себе чи для іншої особи.

3. Злочини, пов'язані з порушенням авторських і суміжних прав з використанням комп'ютерних даних і систем.

Порушення авторського права, передбаченого нормами внутрішньодержавного законодавства, з урахуванням вимог Паризького акту від 24 липня 1971 р. до Бернської Конвенції про захист творів літератури і мистецтва, Угоди про пов'язані з торгівлею аспекти прав на інтелектуальну власність і Договори про авторське право Всесвітньої організації інтелектуальної власності (ВОІВ), за винятком будь-яких моральних прав, наданих цими Конвенціями, коли такі дії навмисне відбуваються в комерційному масштабі і за допомогою комп'ютерної системи.

Порушення суміжних прав, пов'язаних з авторським правом, передбачених нормами внутрішньодержавного законодавства, з урахуванням вимог Міжнародної конвенції про захист прав виконавців, виробників звукозаписів і радіомовних організацій (Римська конвенція);

Угоди про пов'язані з торгівлею аспекти прав інтелектуальної власності і Договори ВОІВ про виконавців і звукозаписи, за винятком будь-яких наданих цими Конвенціями моральних прав, коли такі дії відбуваються навмисне в комерційному масштабі і за допомогою комп'ютерної системи.

Установлення як обов'язкової ознаки більш важких наслідків (матеріального збитку, протиправного використання отриманої комп'ютерної інформації тощо) Конвенцією залишено на розсуд держав-учасниць. Загалом норми Конвенції не передбачають обов'язковість настання шкідливих наслідків.

4. Злочин, пов'язані зі змістом даних.

Правопорушення, пов'язані з дитячою порнографією (порнографічними матеріалами, що візуально відображають участь неповнолітньої чи удаваної повнолітньою особи в сексуально відвертих діях, а також реалістичні зображення, що представляють неповнолітніх, які беруть участь у сексуально відвертих діях), а саме:

- виробництво з метою поширення через комп'ютерні системи;
- пропозиція чи надання через комп'ютерні системи;
- розповсюдження чи передача через комп'ютерні системи;
- придбання через комп'ютерну систему для себе чи для іншої особи;

- володіння дитячою порнографією, що знаходиться в комп'ютерній системі або в середовищі для збереження комп'ютерних даних.

Запропоновані концептуальна модель політики безпеки комп'ютерних даних і систем та її тлумачення можуть бути корисними для фахівців при побудові архітектури захищених комп'ютерних систем, а також для гармонізації законодавчих актів України як країни-учасниці щодо сумлінного виконання рекомендацій цієї Конвенції та їх впровадження в практичну діяльність органів внутрішніх справ України як інформаційне забезпечення.

В 1992 р. Держтехкомісія (ДТК) при Президенті Російської федерації опублікувала п’ять Керівних документів щодо захисту від несанкціонованого доступу до інформації [1]. Ці документи чинні і в Україні. Ідейною основою цих документів є "Концепція захисту засобів обчислювальної техніки від несанкціонованого доступу до інформації (НСД)". З точки зору розробників цих документів основна задача засобів безпеки – це забезпечення захисту від несанкціонованого доступу до інформації. Документи ДТК встановлюють дев’ять класів захищеності автоматизованих систем (АС) від НСД (3Б, 3А, 2Б, 2А, 1Д, 1Г, 1В, 1Б, 1А), кожний з яких характеризується певною сукупністю вимог до засобів захисту.

Класи поділяються на три групи (1, 2, 3), що відрізняються специфікою обробки інформації в АС. Група АС визначається на основі наступних ознак або вимог: наявність в АС інформації різного рівня конфіденційності; рівень повноважень користувачів АС на доступ до конфіденційної інформації; режим обробки даних в АС (колективний чи індивідуальний).

Так, третя група включає АС, в яких працює один користувач, допущений до всієї інформації АС, яка розміщена на носіях одного рівня конфіденційності (класи 3Б, 3А).

Друга група включає АС, в яких користувачі мають однакові повноваження доступу до всієї інформації, що обробляється та/або зберігається в АС на носіях різного рівня конфіденційності (класи 2Б, 2А).

Перша група включає багато користувачеві АС, в яких одночасно оброблюється та/або зберігається інформація різних рівнів конфіденційності (класи 1Д, 1Г, 1В, 1Б, 1А).

СЗІ НСД містить чотири типових (базових) підсистеми з наступними основними функціями захисту.

1. Підсистема управління доступом (ідентифікація, перевірка справжності, контроль доступу, управління потоками інформації).

2. Підсистема реєстрації та обліку (реєстрація та облік; облік носіїв інформації; очищення областей пам’яті, що звільнюються; сигналізація щодо спроб порушення захисту).

3. Підсистема криптографічна (шифрування конфіденційної інформації; шифрування інформації, що належить різним суб’єктам доступу або групам доступу з різними ключами).

4. Підсистема забезпечення цілісності (забезпечення цілісності програмних засобів та інформації, що обробляється; фізична охорона засобів обчислювальної техніки та носіїв інформації; наявність адміністратора безпеки інформації; періодичне тестування системи захисту інформації від НСД; засоби відновлення системи захисту інформації від НСД; використання сертифікованих засобів захисту).

До недоліків даного стандарту Російської Федерації відносяться відсутність вимог до захисту від загроз працездатності, орієнтація на протидію загрозам НСД і відсутність вимог до адекватності реалізації політики безпеки. Поняття “політика безпеки” трактується винятково як підтримка режиму таємності і відсутність НСД, що принципово не вірно.

В Україні в 1999 р. було вперше введено в дію вітчизняний пакет із п'яти нормативних документів НД ТЗІ з питань технічного захисту інформації комп'ютерних систем від несанкціонованого доступу.

1. ***НД ТЗІ 1.1-002-99*** "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" (далі Загальні положення). В цьому нормативному документі визначаються та регламентуються:

- постановка проблеми захисту інформації в комп'ютерних системах від несанкціонованого доступу за основними напрямами захисту;
- концепція забезпечення захисту інформації: основні загрози інформації; політика безпеки інформації; комплекс об'єктів комп'ютерної системи і засобів захисту; визначення несанкціонованого доступу; модель порушника;
- основні принципи забезпечення захисту інформації: планування захисту і керування системою захисту; основні принципи керування доступом (безперервний захист, атрибути доступу, довірче й дмініструвне керування доступом, забезпечення персональної відповідальності); послуги безпеки; гарантії безпеки;
- основні принципи реалізації програмно-технічних засобів: функції і механізми захисту; реалізація комплексу засобів захисту; концепція диспетчера доступу.

2. ***НД ТЗІ 2.5-004-99*** "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" (далі Критерії). В цьому нормативному документі визначаються та регламентуються:

- побудова та структура критеріїв захищеності інформації;
- критерії конфіденційності (довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні);
- критерії цілісності (довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні);
- критерії доступності (використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв);
- критерії состереженості (реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, ідентифікація й автентифікація при обміні, автентифікація відправника, автентифікація отримувача);
- критерії гарантій (архітектура, середовище розробки, послідовність розробки, середовище функціонування, документація, випробування комплексу засобів захисту);
- функціональні послуги за окремим Додатком А;
- гарантії і процес оцінки за окремим Додатком Б.

Додаток А визначає принципові положення та обґрунтування критеріїв конфіденційності, цілісності, доступності, спостереженості.

Додаток Б визначає принципові положення та обґрунтування критеріїв гарантії безпеки рівнів Г-1…Г-7 і процес їх оцінки. Цей додаток має принципове значення для визначення і розуміння фахівцями практичних шляхів забезпечення рівнів гарантії безпеки Г-1…Г-7 за трьома їх ознаками: ***показ*** послуги безпеки (послуга є чи ні), ***демонстрація*** послуги безпеки (послуга працює чи ні), ***доказ*** послуги безпеки (послуга ефективна чи ні).

3. ***НД ТЗІ 2.5-005-99*** "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу". В цьому нормативному документі визначаються та регламентуються:

- класифікація автоматизованих систем за трьома їх класами (клас 1 – персональна ЕОМ, клас 2 – локальна обчислювальна мережа), клас 3 – глобальна обчислювальна мережа);
- функціональні профілі захищеності (визначення і призначення, семантика профілю, стандартні профілі);
- стандартні функціональні профілі захищеності для АС класу 1, 2, 3;
- додаток А для вибору профілю захищеності АС залежно від їх призначення – для автоматизації діяльності органів державної влади, автоматизації банківської діяльності, керування технологічними процесами, довідково-пошукових систем.

4. ***НД ТЗІ 3.7-001-99*** "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі" (далі Класифікація АС). В цьому нормативному документі визначаються та регламентуються:

- загальні вимоги до розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (порядок розробки і зміст технічного завдання);
- вимоги до змісту розділів технічного завдання (загальні відомості, мета і призначення КСЗІ, загальна характеристика автоматизованої системи і умов її функціонування, вимоги до КСЗІ в частині захисту від НСД та в частині захисту від витоку інформації технічними каналами);
- вимоги до складу проектної та експлуатаційної документації;

- етапи виконання робіт;
- порядок внесення змін і доповнень до технічного завдання;
- порядок проведення випробувань КСЗІ.

5. ***НД ТЗІ 1.1-003-99*** "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу". В цьому нормативному документі визначаються та регламентуються основні терміни і поняття: властивості інформації і загрози; створення і експлуатація захищених систем; принципи, послуги і механізми забезпечення безпеки.

Приємно вказати, що для практичної реалізації та апробації вимог цих нормативних документів НД ТЗІ, а також для практичного їх використання в навчальному процесі Національної академії внутрішніх справ України, фахівцями НДІ НАВСУ було розроблено програмний Delphi-продукт у вигляді Експертної системи "Торсіон-1" в рамках планової НДР "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" [1]. На Експертну систему "Торсіон-1" одержано Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20. 11. 2005 та позитивний висновок НАВСУ на використання Експертної системи в навчальному процесі академії.

За результатами проведених досліджень пропонується нова та багатофакторно декомпозована концепція побудови архітектури системи захисту інформації в КС, АС від несанкціонованого доступу. Основними перевагами цієї концепції є наступні чинники.

По-перше, відповіднсть вимогам вітчизняних нормативних документів з питань захисту інформації в КС, АС від несанкціонованого доступу.

По-друге, визначення вимог до реалізації профільних послуг безпеки КС, АС підкласів К, Ц, Д, Ц, КД, ЦД, КЦД.

По-третьє, визначення як істотних і типових не тільки технчних, але й організаційних заходів захисту КС, АС від загроз НСД.

На рис. 2 пропонується концептуальа модель системи захисту інформації в комп'ютерних системах від загроз несанкціонованого доступу.

III Висновки

Необхідність та актуальність запропонованої Концепції зумовлена наступними чинниками.

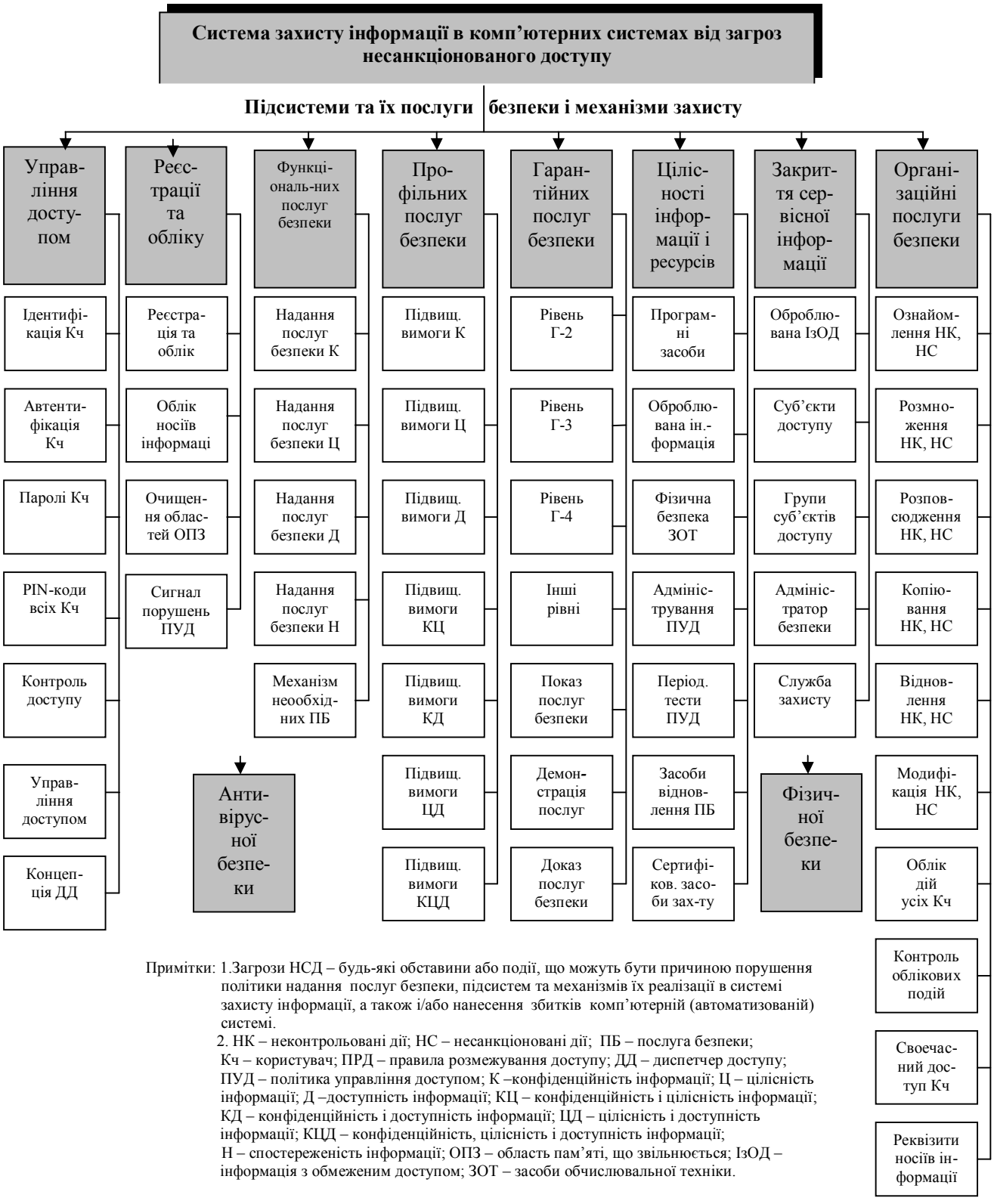
1. Реалізація і впровадження науково-практичних положень нормативного документу НД ТЗІ 2.5-005-99 щодо необхідності визначення окрім класів 1, 2, 3 ще підкласів автоматизованих систем типу К, Ц, Д, КЦ, КД, ЦД, КЦД.

2. Необхідність надання можливості кількісної експертної і тендерної оцінки профільних послуг безпеки автоматизованих систем підкласів К, Ц, Д, КЦ, КД, ЦД, КЦД.

3. Необхідність гармонізації кваліфікаційних ознак злочинів у сфері використання ЕОМ (комп'ютерів), комп'ютерних систем і мереж та мереж електрозв'язку за ст.ст. 361-363 з примами КК України з рекомендаціями Конвенції Ради Європи про кіберзлочинність щодо боротьби зі злочинами проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а також зі злочинами, пов'язаними з використанням комп'ютерів.

4. Необхідність гармонізації послуг безпеки комп'ютерних систем з вимогами міжнародного стандарту ISO 17799 (Практичні правила управління інформаційною безпекою) щодо пріоритетності формування та дотримання положень обраної політики безпеки.

5. Необхідність методичних рекомендацій щодо науково-практичного використання рекомендацій запропонованої нової вітчизняної Концепції. Основна увага акцентується на дотриманні рекомендацій Конвенції Ради Європи щодо боротьби зі злочинами проти конфіденційності, цілісності і доступності комп'ютерних даних і систем.



Примітки: 1.Загрози НСД – будь-які обставини або події, що можуть бути причиною порушення політики надання послуг безпеки, підсистем та механізмів їх реалізації в системі захисту інформації, а також і/або нанесення збитків комп'ютерній (автоматизованій) системі.

2. НК – неконтрольовані дії; НС – несанкціоновані дії; ПБ – послуга безпеки; Кч – користувач; ПРД – правила розмежування доступу; ДД – диспетчер доступу; ПУД – політика управління доступом; К –конфіденційність інформації; Ц – цілісність інформації; Д –доступність інформації; КЦ – конфіденційність і цілісність інформації; КД – конфіденційність і доступність інформації; ЦД – цілісність і доступність інформації; КЦД – конфіденційність, цілісність і доступність інформації; Н – спостереженість інформації; ОПЗ – область пам'яті, що звільнюється; ІзОД – інформація з обмеженим доступом; ЗОТ – засоби обчислювальної техніки.

Рисунок 2 – Концептуальна модель системи захисту інформації в комп'ютерних системах від загроз несанкціонованого доступу

Література: ***1.*** *А. Ю. Ільніцький, В. В. Шорошев, І. Л. Близнюк. Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" (шифр "Торсіон-1"). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді програмного продукту "Торсіон-1". – К.: Видавництво НАВСУ, 2003 р. – 316 с.* ***2.*** *Шорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно европейским "Критериям оценки безопасности информационных технологий ITSEC" (Information Technology Security Evaluation Criteria). Журнал "Бизнес и безопасность" № 3, 1998 г.* ***3.*** *Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 1 1999г. Рекомендации по основам информационной безопасности согласно Единых критериев CCITSE (Common Criteria for Information Technology Security Evaluation), 1996-1997 г.г.* ***4.*** *Стандарт ISO/IEC 17799: 2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.* ***5.*** *Стандарт ISO/1EC 15408: 2000. Information technology - Security techniques -Evaluation criteria for IT security. - Part 1: Introduction and general model.* ***6.*** *Стандарт ISO/IEC 15408: 2000. Information technology - Security techniques Evaluation criteria for IT security. - Part 2: Security functional requirements.* ***7.*** *Стандарт ISO/IEC 15408: 2000. Information technology - Security techniques -Evaluation criteria for IT security. - Part 3: Security assurance requirements.* ***8.*** *Шорошев В. В. Модель угроз для локальних вычислительных сетей по рекомендаціям Конвенции Сонета Европы о кибеопреступности. Науково-виробничий журнал Державної адміністрації зв'язку та інформатизації України "Зв'язок" № 4, 2005. С. 37-42.* ***9.*** *Шорошев В. В., Близнюк И. Л., Балина С. Н. Классификация угроз для компьютерніх данных и систем по рекомендациям Конвенции о киберпреступности Сонета Европы. Бизнес и безопасность № 1, 2005. С. 36-39.* ***10.*** *Шорошев В. В., Близнюк І. Л. Моделі загроз комп'ютерним даним і системам за Конвенцією Ради Європи про кіберзлочинність. // Науковий вісник НАВСУ. – К., 2005. - № 6.- С. 119-128.*

УДК 681.3.06

МНОГОМЕРНЫЙ СТАТИСТИЧЕСКИЙ ТЕСТ ДЛЯ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Михаил Савчук, Виталий Шарапов
Физико-технический институт Национального технического университета Украины "КПИ"

Аннотация: **Строится многомерный статистический критерий проверки качества случайных последовательностей. С использованием слабой сходимости векторных случайных процессов находятся асимптотические распределения статистик. Приводятся формулы, облегчающие практическое использование критерия. Даются рекомендации по выбору параметров.**
Summary: **The multidimensional statistical criterion of quality check of casual sequences is constructed. Weak convergence of vector casual processes is used for research of asymptotic statistics distributions. Formulas facilitating practical use of criterion and recommendations for parameters selection are presented.**
Ключевые слова: **Многомерный случайны процесс, неравновероятные последовательности, сходимость случайных процессов, случайные и псевдослучайные последовательности, статистический критерий.**

I Постановка задачи

Пусть задана последовательность $\varepsilon = \varepsilon_1\varepsilon_2\ldots\varepsilon_s$, $\varepsilon_i \in \{0,1\}$, $i = 1,\ldots,s$, которую рассматриваем как реализацию некоторого случайного дискретного процесса. Необходимо проверить гипотезу H_0 о том, что последовательность ε является реализацией последовательности независимых двоичных знаков, которые с вероятностью p, $0 < p < 1,$ принимают значение 1, иначе говоря, случайные величины ε_i независимы в совокупности и $\forall i = 1,\ldots,s \;\; P(\varepsilon_i = 1) = 1 - P(\varepsilon_i = 0) = p$.

II Построение случайного процесса

Пусть $s = nN$. Введем случайные процессы на интервале $[0,1]$: