Критерий		АКФ	Котельникова	Допустимого отклонения
Фонема	Параметр	f_s=96кГц	$f^к$=12кГц	$f^д$=48кГц
з	M	**0.08319**	0.086393	0.083668
	σ	**0.043433**	0.044923	0.043655
	M-σ	0.076574	0.065944	0.074194
	M+σ	0.089805	0.10684	0.093141
	D	**0.0018864**	0.0020181	0.0019057
	τ_0	0.00175	0.00175	0.00175

Как видно из результатов расчета параметров критерия заданных статистических оценок погрешности определения сигнала на интервале корреляции с рассчитанной частотой дискретизации fs=96кГц для фонем с широкополосным высокочастотным спектром, рассчитанное среднеквадратическое отклонение хуже заданного, т. к. частота дискретизации fs=96кГц меньше рассчитанной (20) fs=158кГц.

Таким образом, при обработке речевых сигналов, дискретизированных с вышеуказанной частотой, целесообразно применять корреляционные алгоритмы. При этом гарантируется заданная статистическая оценка погрешности аппроксимирующего сигнала.

Выводы

Сравнение результатов эксперимента и расчетных исследований позволяет сделать вывод о том, что предложенный критерий оптимизации частоты дискретизации стохастического речевого сигнала, основанный на заданных максимальных статистических оценках погрешности его определения на интервале корреляции, позволяет строго гарантировать точность его цифрового представления.

В связи с тем, что применение данного критерия для сигналов с верхней граничной полосой порядка 10кГц потребует АЦП с высокими граничными частотами, возможно применение АЦП с транскодированием дельта модулированных сигналов в импульсно – кодовую модуляцию и наоборот, которые предложены в авторских свидетельствах [10, 11].

Распространение предложенного критерия на иные виды стохастических сигналов, например с осциллирующей АКФ, требует дополнительных исследований.

*Литература: **1.** Бекман Д. Аутентификация пользователей при подключении к сети. – М.: Радио и связь, 1997. - 256 с. **2.**Новосельский А. Ф., Жариков Ю. Ф. Программный пакет VIS для идентификации по голосу //Тезисы докладов 8-й Международной конференции "Информатизация правоохранительных систем". – М.: 1999. – С 323-324. **3.** Рабинер Л., Шафер Р. Цифровая обработка речевых сигналов. - М.: Радио и связь, 1981. – 496 с. **4.** Вокодерная телефония. Методы и проблемы. Под ред. А. А. Пирогова – М.: Связь, 1974. - 536 с. **5.** Вентцель Е. С., Овчаров Л. А. Теория вероятностей и ее инженерные приложения. – М.: Наука, 1988. - 480 с. **6**. Купер Дж., Макгиллем К. Вероятностные методы анализа сигналов и систем: Пер. с анг. – М.: Мир, 1989. - 376с. **7.** Котельников В. А. Теория потенциальной помехоустойчивости. – М.: Радио и связь, 1998. – 152 с. **8** Основы теории информации и кодирования/ И. В. Кузьмин, В. А. Кедрус. – К.: Вища школа, 1986. – 238 с. **9.** Брандт З. Статистические методы анализа наблюдений. – М.: Мир, 1975. – 312 с. **10.** А. с. 282207 СССР. МКИ НОЗМ 7/32. Цифровой преобразователь импульсно-кодово-модулированных в дельта-модулированные сигналы / В .Н. Журавлев, В. И. Жуковицкий, Г. В. Кузнецов (СССР). -N 3185490/24; Заявлено 04.11.87; Зарегистр. в Гос. реестре изобретений СССР 01.09.88. **11.** А.с. 288569 СССР, МКИ НОЗМ 3/32. Преобразователь дельта-сигма-модулированного сигнала в сигнал с импульсно-кодовой модуляцией / В. И. Жуковицкий, В. Н. Журавлев, Г. В. Кузнецов и др. (СССР). - N 3192864/24-24; Заявлено 01.03.88; Зарегистр. в Гос. реестре изобретений СССР 01.02.89.*

УДК 681.396

МЕТОДИКА АНАЛІЗУ НАДІЙНОСТІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Ігор Павлов

ВІТІ НТУУ "КПІ"

Анотація: **Розглядається методика аналізу надійності комплексних систем захисту інформації в автоматизованих системах під час проектувань. Пропонується алгоритм аналізу надійності.**

Summary: **Considered technique of the reliability analysis of complex systems information protection in the automated systems during development, and also the analysis algorithm of reliability is offered.**
Ключові слова: **Надійність, бар'єр захисту, механізм захисту, комплексна система захисту інформації (КСЗІ), автоматизована система (АС).**

I Вступ

Аналіз надійності – це систематизоване дослідження з метою впливу на надійність об'єкта особливостей конструкції, технологічних процесів виробництва, умов експлуатації, а також визначення досягнутого рівня надійності при виконанні запланованих заходів щодо забезпечення і підвищення надійності та оцінка ефективності [1]. Поняття надійності комплексних систем захисту інформації (КСЗІ) відсутнє в НД ТЗІ, тому в своїй роботі поняття та визначення орієнтовані на [1]. Надійність систем захисту інформації в автоматизованих системах (АС) визначається прийнятими проектними рішеннями на етапі розробки.

Аналіз існуючих публікацій, пов'язаних з проблемою надійності систем захисту інформації, показує недостатнє висвітлення проблеми аналізу надійності КСЗІ в АС. Публікації базуються на оцінках надійності забезпечення захисту інформації окремих методів захисту інформації, в основному програмних та криптографічних, тоді, як КСЗІ – це сукупність організаційних та інженерних мір, програмно-апаратних засобів, які забезпечують захист інформації в АС [2 - 7]. Такий підхід не задовольняє вимогам до автоматизованих систем через те, що в таких системах розглядається ступінь відповідності можливих або отриманих результатів цільового використання системи результатам, які бажано отримати.

В зв'язку з цим виникає об'єктивна необхідність розробки методики аналізу надійності КСЗІ в автоматизованих системах.

II Постановка завдання

Вихідними даними для аналізу надійності КСЗІ в автоматизованих системах є:

— загальна структура системи захисту інформації з повним перекриттям;

— виділені області вразливості системи захисту та бар'єри, які перекривають ці області;

— технічні характеристики бар'єрів – T_m, $T_{\text{В}}$, T_{b_i}.

Необхідно знайти:

1. $P_{\text{Б}d}(t)$ – ймовірність надійного перекриття загроз d-м бар'єром захисту, при $d = \overline{1,D}$;

2. $P_{\text{М}q}(t)$ – ймовірність надійного перекриття загроз механізмом захисту на q шляху впливу загроз, при $q = \overline{1, Q}$;

3. $P_{\text{З}}(t)$ – ймовірність надійного захисту КСЗІ.

Основними обмеженнями при розробці методики є:

— оцінюється якість і технічні умови функціонування КСЗІ на етапі проектування та розробки;

— не враховуються типи загроз, які впливають на КСЗІ;

— не розглядається стійкість роботи механізмів захисту інформації (під стійкістю роботи механізму захисту інформації розуміється спроможність виконувати задачі, які покладені на механізм захисту, під впливом різного типу загроз);

— розрахунки показників надійного захисту інформації більш пристосовані для апаратно-технічних методів захисту інформації у складі КСЗІ;

— потік загроз на систему захисту інформації приймається, як найпростіший, розподілений за законом Пуассона;

— не розглядається вплив загроз на бар'єри з боку суміжних механізмів захисту, бар'єри яких не витримали цей вплив.

III Основна частина

Під надійністю комплексної системи захисту інформації від реалізації загроз в АС розуміється властивість КСЗІ зберігати в часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування [1].

Надійність захисту інформації в АС має ряд особливостей, які впливають на побудову системи захисту інформації [8].

1. Велика різнорідність загроз.
2. Швидкість зміни умов впливу загроз.
3. Велика кількість типів засобів захисту інформації, які використовуються в АС.

4. Значна залежність функціонування систем захисту інформації у складі АС від впливу різного типу загроз.

5. Різні шляхи впливу загроз на АС.

В загальному випадку надійність захисту інформації в АС визначається надійністю механізмів та бар'єрів захисту у складі КСЗІ. Сукупність показників надійності захисту бар'єрів та механізмів захисту, характеризує надійність захисту в АС в цілому [9].

Проведений аналіз особливостей надійного захисту інформації в АС показує, що розрахунок надійності КСЗІ маэ виконуватися поетапно:

1 етап – визначення ймовірності надійного перекриття інформації одним бар'єром у складі механізму захисту;

2 етап – визначення ймовірності надійного перекриття інформації одним механізмом захисту у складі КСЗІ;

3 етап – визначення ймовірності надійного захисту КСЗІ в цілому.

Згідно з [10] в системі захисту інформації типової структури захисту з повним перекриттям виділяються область уразливості системи захисту та бар'єри, які перекривають ці області, як зображено на рис. 1.

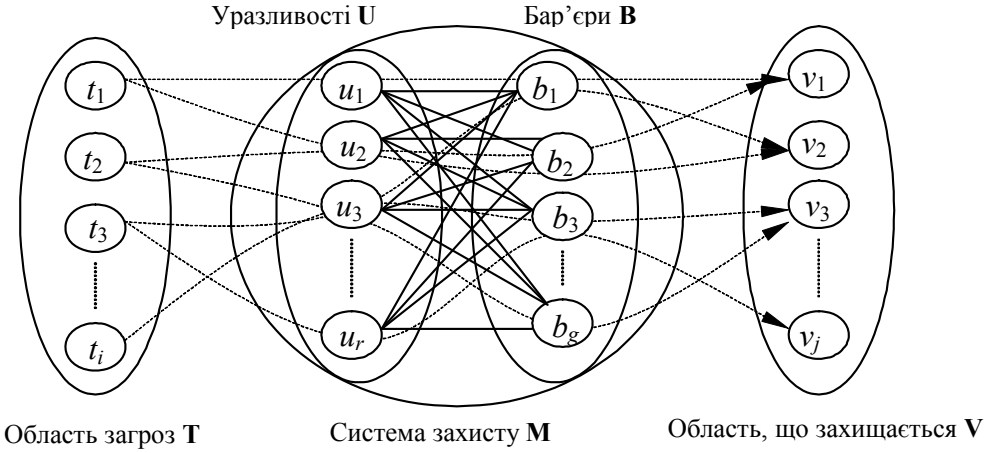

Рисунок 1 – Структура захисту інформації з повним перекриттям загроз з урахуванням внутрішніх взаємозв'язків

Для цієї структури виконується умова:

$$\forall < \text{ti, vj} > \exists < \text{ur, bg} > \in \text{M} \mid f(\text{ti, vj}), \quad (1)$$

де функціонал f(ti, vj) – описує виконання умови забезпечення захисту об'єкта vj при наявності загрози ti..

Система захисту **M** такої структури складається з множини механізмів захисту, які в свою чергу складаються з множини бар'єрів, які перекривають множину уразливих місць системи захисту [11].

$$\mathbf{M} = \{m_k\} = \{\mathbf{U} \times \mathbf{B}\}. \quad (2)$$

У складі механізму захисту може бути декілька бар'єрів захисту, які перекривають вплив загроз в області уразливості системи захисту з визначеною ймовірністю, як зображено на рис. 2.

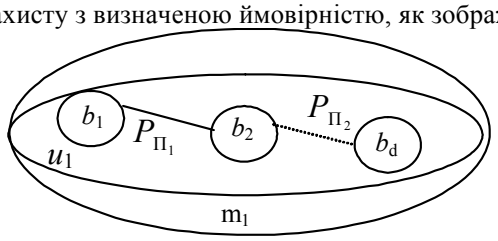

Рисунок 2 – Взаємозв'язок множин системи захисту інформації

Як зображено на рис. 3, на першому етапі необхідно визначити наскільки бар'єр b спроможний надійно захистити область **V** від впливу загроз **T**.

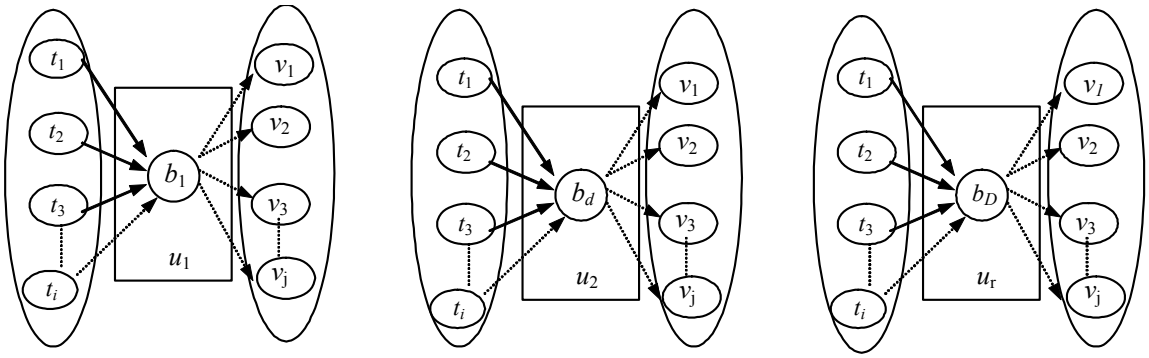

Рисунок 3 – Місце бар'єра в структурі захисту інформації

За показник надійного захисту бар'єром прийнята ймовірність надійного перекриття загроз d-м бар'єром – $P_{Бd}$

$$P_{Б_d}(t) = P_{БР_d}\left(1 - P_{П d}\right), \tag{3}$$

де $P_{БР_d}$ – ймовірність безвідмовної роботи d-го бар'єра, при умові:

$$P_{БР_d} = P_{БР_{d(ОЗ)}} \times P_{БР_{d(АТЗ)}} \times P_{БР_{d(ПЗ)}} \times P_{БР_{d(КЗ)}}, \tag{4}$$

де $P_{БР_{d(ОЗ)}}$ – ймовірність безвідмовної роботи d-го бар'єра при здійсненні організаційних методів захисту інформації;

$P_{БР_{d(АТЗ)}}$ – ймовірність безвідмовної роботи d-го бар'єра при здійсненні апаратно-технічних методів захисту інформації;

$P_{БР_{d(ПЗ)}}$ – ймовірність безвідмовної роботи d-го бар'єра при здійсненні програмних методів захисту інформації;

$P_{БР_{d(КЗ)}}$ – ймовірність безвідмовної роботи d-го бар'єра при здійсненні криптографічних методів захисту інформації;

$P_{П d}$ – ймовірність проходу загрози через d-й бар'єр.

Імовірність безвідмовної роботи бар'єра залежить від технічних характеристик бар'єра

$$P_{БР_d} = K_{Г_d} e^{-\frac{t}{T_m}}, \tag{5}$$

де $K_{Г d}$ – коефіцієнт готовності d-го бар'єра блокувати загрозу;

t – середній час роботи бар'єра;

T_m – середній наробіток бар'єра на відмову.

Коефіцієнт готовності залежить від показників бар'єра, які закладаються ще на етапі розробки бар'єра розробником

$$K_{Г_d} = \frac{T_m}{T_m + T_В}, \tag{6}$$

де $T_В$ – середня тривалість відновлення бар'єра після відмови.

Однак слід підкреслити, що формально оцінка надійності захисту бар'єром від різних шляхів впливу загроз не означає їх функціональну незалежність.

Це обумовлюється тим, що одні і ті ж загрози можуть впливати на одні і ті ж області, які захищаються, тільки різними шляхами [9]. Для цього потрібно враховувати, що використовуючи різні області уразливості будь-які загрози можуть впливати на бар'єри одного механізму захисту, перекриваючи їх. Враховуючи, що потік загроз, які впливають на систему захисту інформації, є найпростішим, використовуючи формулу Ерланга розглянемо якісний показник ймовірності надійного захисту бар'єра –

ймовірність проходу загрози через d-й бар'єр – $P_{\Pi d}$

$$P_{\Pi d} = \frac{\frac{a^n}{n!}}{\sum_{k=1}^{n} \frac{a^k}{k!}}, \quad (7)$$

де a – щільність потоку загроз , які впливають на бар'єр;

n – сумарна кількість загроз, які можуть впливати на бар'єр;

k – умовний розрахунковий порядковий номер загроз.

Приведена щільність потоку загроз на бар'єр враховує частотно-часові характеристики

$$a = \lambda T_{b_i}, \quad (8)$$

де λ – інтенсивність надходження загроз за хвилину;

T_{b_i} – середній час перекриття бар'єром і –ї загрози.

З метою полегшення аналізу надійності і спрощення розрахунків припускається, що потік відмов є простішим. Простіший потік відповідає трьом умовам: стаціонарності, ординарності та відсутності післядії. Простіший потік називають пуассонівським, оскільки для нього ймовірність появи певної кількості подій підпорядковано закону Пуассона. При простішому потоці загроз у системі захисту час між сусідніми загрозами приймається розподіленим за експоненційним законом.

Стаціонарність потоку загроз визначається постійністю його статичних параметрів у часі. Тобто для найпростішого потоку ймовірність $P_{\Pi d}$ проходу загрози в проміжок часу Δt не залежить від розташування цього проміжку на осі часу, а залежить тільки від його величини:

$$P_{\Pi d}(\Delta t_1) = P_{\Pi d}(\Delta t_3) < P_{\Pi d}(\Delta t_2). \quad (9)$$

Ординарність потоку визначається, як ймовірність надходження двох і більше загроз в проміжок часу $\Delta t \to 0$, і є величиною більш малого порядку ніж Δt.

Відсутність післядії в потоці визначає, що ймовірність надходження загроз після довільного моменту часу t_1 не залежить від характеру надходження загроз до цього моменту часу.

Математичне очікування цього процесу дорівнює дисперсії.

Як зображено на рис. 4, на другому етапі необхідно визначити наскільки механізм захисту, який складається із декількох бар'єрів, спроможний надійно захистити область **V** від впливу загроз **T**.

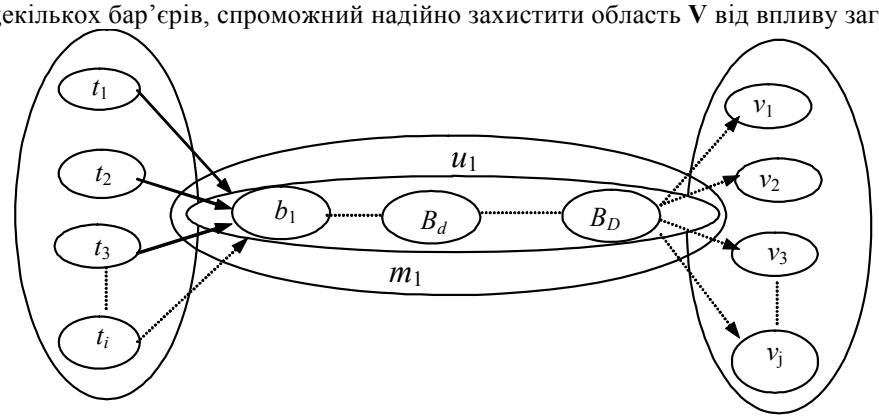

Рисунок 4 – Місце механізму захисту в структурі захисту інформації

За показник надійного захисту механізму захисту приймається ймовірність надійного перекриття загроз механізмом захисту на q-м шляху впливу загроз

$$P_{\text{М}\,q}(t) = 1 - \prod_{b=1}^{D} \left(1 - P_{\text{Б}\,d}(t)\right), \quad (10)$$

де D – кількість бар'єрів у складі механізму захисту.

Як зображено на рис. 5, на третьому етапі визначається, наскільки КСЗІ, що складається із декількох механізмів захисту, спроможна надійно захистити область **V** від впливу загроз **T**.

При оцінці надійності КСЗІ за показник береться ймовірність надійного захисту КСЗІ

$$P_{\text{З}}(t) = 1 - \prod_{m=1}^{Q} \left(1 - P_{\text{М}\,q}(t)\right), \quad (11)$$

де Q – кількість механізмів захисту у складі КСЗІ.

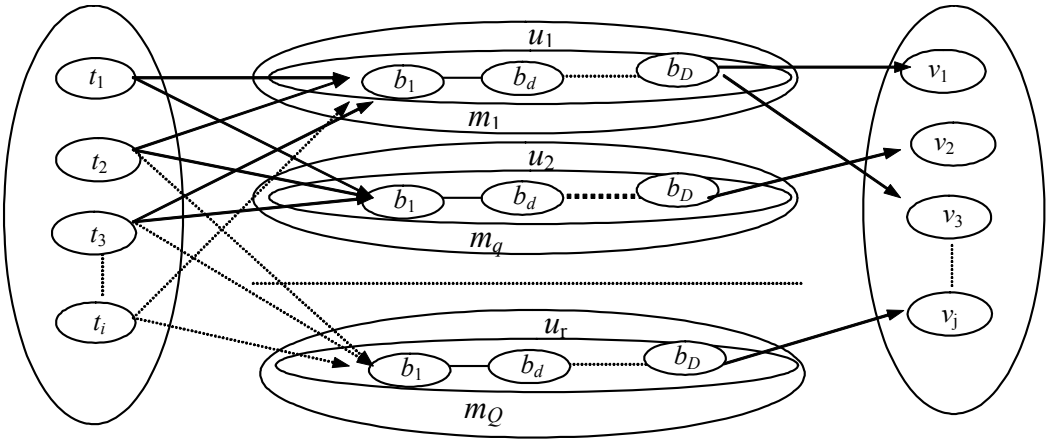

Рисунок 5 – Місце комплексної системи захисту в структурі захисту інформації

Алгоритм, який реалізує запропоновану методику аналізу надійності КСЗІ в АС, поданий на рис. 6, де $\Phi = \{\varphi_i\}$ - значення вихідних параметрів, необхідних для розрахунку надійності КСЗІ.

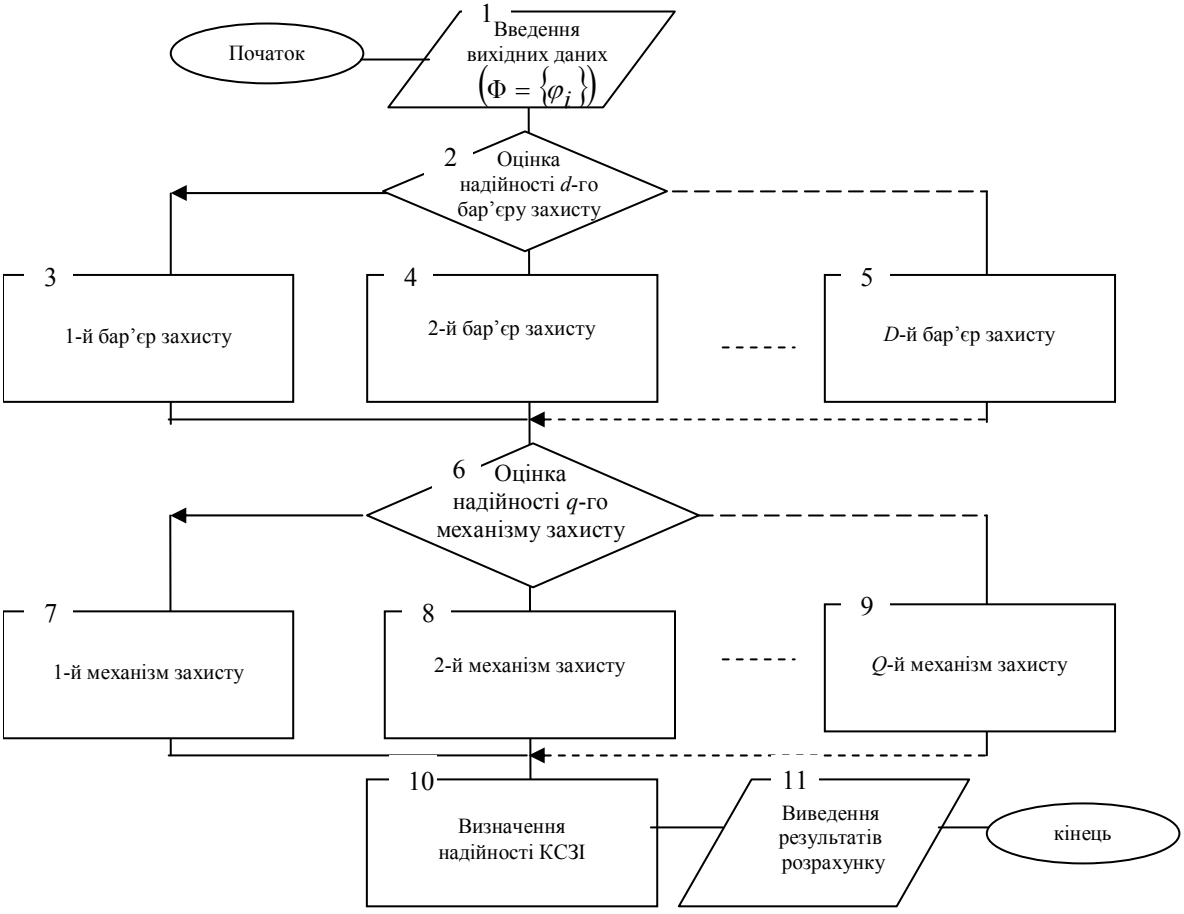

Рисунок 6 – Алгоритм методики оцінки надійності КСЗІ в АС

IV Висновки

В роботі наведено математичний апарат аналізу надійності комплексних систем захисту інформації на основі теорії вірогідності та алгоритм методики проведення аналізу.

Запропонована методика відрізняється від існуючих наступним:

- вона, враховує взаємозв'язки загроз, які впливають на систему, механізмів захисту та областей, що захищаються;
- позволяє враховувати технічний (експлуатаційний) стан механізмів захисту;
- при проведенні оцінки надійності КСЗІ здійснюється поетапний аналіз надійності бар'єрів та механізмів захисту.

Методику доцільно застосовувати під час проектування КСЗІ в АС.

Подальшим напрямком досліджень є оцінка живучості КСЗІ в АС на основі теорії ймовірності.

*Література: **1.** ДСТУ 2860–94. Надійність техніки. Терміни та визначення. //Держстандарт України. – К.: 1994. **2.** НД ТЗІ 1.1–003–99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. // ДСТСЗІ. – К.: 1999. **3.** Курочкин В .В. Оценка надежности комплекса средств защиты информации // Системи обробки інформації. – К.: 2003. – Вип. 2. – С. 87 – 91. **4.** Соломаха В. В., Богдан А.В. Аналіз захищеності інформаційних систем // Вісник Сумського державного університету. 2003. – № 12 (45). – С. 140 - 144. **5.** Хамула С. М., Ковбаса В.С., Кулинич Ю.Р. Формалізація процесів захисту інформації в інформаційно-обчислювальних системах // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К.: 2003. – Вип. 7. – С. 113 — 117. **6.** Щербина Л. П. Основы теории сетей военной связи // – Л.: 1984. – 169 с. **7.** Романов А. И. Телекоммуникационные сети и управление // – К.: 2003. – 246 с. **8.** Селезнев М .Л. Информационно-вычислительные системы и их эффективность // Радио и связь. – М.: 1986. – С. 103 – 112. **9.** Зуев О.В., Хмелько Ю. М., Чирков Д. В. Критерий оценки качества функционирования средств защиты информации // Захист інформації. – К.: 2001. – № 1. – С. 17 – 22. **10.** Романов О. І., Лівенцев С. П., Павлов І. М. Математична модель захисту інформації в автоматизованих мережах спеціального призначення // Науково-методичний збірник ВІТІ НТУУ "КПІ". – К.: 2004. – Вип. 5. – С. 23 – 31. **11.** Романов О.І., Лівенцев С. П., Павлов І. М. Методика оцінки надійності комплексних систем захисту інформації в спеціальних телекомунікаційних системах // Зв'язок. – К.: 2005. – № 2. – С. 38 – 47.*

УДК 339.166.5; 338.462:681.3

ПАТЕНТНО-ПРАВОВА ОХОРОНА ВИНАХОДІВ У ГАЛУЗІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Сергій Войтко, Анастасія Дідович

Національний технічний університет України "Київський політехнічний інститут"

Анотація: **Проаналізовано патентно-правову охорону винаходів у галузі інформаційних технологій. Розглянуто поняття комп'ютерного піратства і його негативний вплив на розвиток сфери інформаційних технологій. Приведені основні поняття у галузі інформаційних технологій, а саме: комп'ютерна програма і база даних. Представлено законодавство інших країн світу щодо захисту комп'ютерних програм. Розглянуто нормативно-правову охорону інформаційних технологій.**

Summary: **In this work a patent-law protection of inventions in the field of informational technologies is analyzed. A conception of computer piracy and its affect on development of informational technologies is considered. Such principal concepts in the field of informational technologies as computer program and data base are also examined. Legislation on protection of computer programs in other countries is analyzed. A legal protection of informational technologies is considered.**

Ключові слова: **Інтелектуальна власність, комп'ютерна програма, винахід, комп'ютерна технологія, піратство, програмний продукт, база даних.**

Вступ

Світова економіка перебуває у фазі розвитку, яку можна назвати "постіндустріально-інформаційна". На даний час за аналізом діяльності великих компаній світу, темпів їх зростання, прибутковості можна зробити висновок, що перші місця посідають компанії, діяльність яких зосереджена у високотехнологічних промислових сферах. Інформаційний бум дещо спадає.

Якщо з власниками ресурсів у індустріальному суспільстві все зрозуміло (природні ресурси належать