1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення системи ТЗІ. Стандартизація, сертифікація та випробовування засобів ТЗІ

УДК 00691 (045)

НОВЫЙ ПОДХОД К ОЦЕНКЕ РАСШИРЕННОЙ НЕОПРЕДЕЛЕННОСТИ РЕЗУЛЬТАТОВ МНОГОКРАТНЫХ ИЗМЕРЕНИЙ ПРИ РАВНОМЕРНО РАСПРЕДЕЛЕННЫХ ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ

Евгений Володарский, Александр Карпенко*

*Национальный технический университет Украины "КПИ", Национальный авиационный университет Украины**

Аннотация: **Предложена статистика для использования при обработке результатов прямых многократных измерений с равномерно распределенными составляющими. Установлены аналитические зависимости, позволяющие оценить эффективность предлагаемого подхода по сравнению с традиционным.**

Summary: **Statistic for using in direct multiple measurement processing is considered where components are uniformly distributed. It was determined an analytical dependency which allows to estimate efficiency of suggested method comparing with traditionally used one.**

Ключевые слова: **Расширенная неопределенность, равномерный закон, многократные измерения.**

I Введение

Основным показателем качества измерений, согласно нормативного документа Международной Организации по Стандартизации (ISO) "Руководство по выражению неопределенности измерений" [1] (далее Руководство), является неопределенность полученных результатов. Составляющие неопределенности сгруппированы в две категории, основанные на методе их расчета, типы "А" и "В". Оценка неопределенности по типу А основана на статистическом анализе серии наблюдений, а оценка по типу В – на использовании других методов, отличных от статистического анализа серии наблюдений. Стандартную неопределенность типа А определяют на основании функции плотности распределения вероятностей, которую, в свою очередь, получают из распределения частот, в то время как стандартную неопределенность по типу В получают из предполагаемой функции плотности распределения вероятности, т. е. на основании априорной информации. В данной статье мы остановимся на методике расчета расширенной неопределенности при многократных измерениях, т. е. когда в основе лежит статистическая обработка экспериментальных данных. Целью работы является изложение результатов исследований, имеющих как теоретическое, так и практическое значение.

II Основная часть

Остановимся кратко на методике оценки расширенной неопределенности для прямых и косвенных многократных измерений [2]. Предположим, что в результате эксперимента была получена выборка значений измеряемой величины $X : x_1 ... x_n$, где n объем выборки. В качестве наилучшей оценки математического ожидания величины $X,$ которая рассматривается как оценка результата прямого многократного измерения, принимается среднее арифметическое значение $\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i$. Рассеивание значений $\bar{x}$ характеризуется дисперсией $\sigma^2(\bar{x})$, которая имеет связь с дисперсией наблюдаемых

значений измеряемой величины на основании выражения $\sigma^2(\bar{x}) = \sigma^2(x_i)/n$. Наилучшей оценкой этого соотношения выступает выражение $S^2(\bar{x}) = S^2(x_i)/n$, где $S^2(\bar{x})$ – экспериментальная дисперсия среднего значения, а $S^2(x_i) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2$ – экспериментальная дисперсия наблюдаемых значений измеряемой величины. Экспериментальное среднеквадратическое отклонение среднего $S(\bar{x})$ количественно характеризует насколько хорошо $\bar{x}$ оценивает математическое ожидание $M(X)$ и используется как мера сомнения о действительном соотношении $\bar{x}$ и $M(X)$. Стандартная неопределенность прямых многократных измерений оценивается как $u(x_i) = S(\bar{x})$. Расширенную неопределенность рассчитывают как $U_P = k_P(v) \cdot u(x_i)$, где $k_P(v)$ - коэффициент Стьюдента для $v = n-1$ степеней свободы и доверительной вероятности P. В случае косвенных многократных измерений, например с функциональной зависимостью $Y = X_1 + X_2$, наилучшей оценкой математического ожидания $M(Y)$ выступает значение $y = \bar{x}_1 + \bar{x}_2$. Оценка дисперсии при отсутствии корреляции рассчитывается как $S^2(y) = S^2(\bar{x}_1) + S^2(\bar{x}_2)$, а оценка среднеквадратического отклонения, соответствующая комбинированной неопределенности u_c, может быть найдена из выражения $u_c = \sqrt{S^2(\bar{x}_1) + S^2(\bar{x}_2)}$. В соответствии с [1] (Приложение G.4.1.) распределение случайной величины $\frac{y - M(y)}{u_c}$ не является распределением Стьюдента, поэтому при расчете расширенной неопределенности в случае косвенных многократных измерений $U_P = k_P(v_{eff}) \cdot u_c$ используют коэффициент Стьюдента для эффективного количества степеней свободы v_{eff}, который находят из формулы Вэлча-Саттервэйта:

$$v_{eff} = \frac{u_c^4}{\sum_{i=1}^{N} \frac{u_i^4}{v_i}}$$

где N количество аргументов функциональной зависимости, а u_i стандартные неопределенности прямых измерений.

Таким образом, отмечаем, что в Руководстве в качестве наилучшей оценки результата измерения рассматривается среднее арифметическое, а в качестве стандартной неопределенности используется оценка среднеквадратического отклонения среднего арифметического. При расчете расширенной неопределенности используется распределение Стьюдента, для косвенных измерений учитывают эффективное количество степеней свободы.

В процессе исследований вероятностно-нечеткого перехода и возможностей использования функций принадлежности [3, 4] было установлено, что для равномерно распределенных случайных величин рассеивание граничных значений выборок, т. е. минимального или максимального значения выборки, меньше, чем рассеивание среднего арифметического значения этих выборок. Исходя из этого можно сделать вывод, что рассеивание случайной величины

$$m_i = \frac{\min(x_i) + \max(x_i)}{2},$$

будет также меньше рассеивания среднего арифметического. Такие выводы приводят к необходимости исследования распределения случайной величины :

$$K = \frac{(m_i - M(m_i))}{S(m_i)},$$

где $M(m_i)$ - математическое ожидание, а $S(m_i)$ - оценка среднеквадратического отклонения величины m_i, найденная на основании выборочных экспериментальных данных, $i = 1 \ldots n$, где n - объем выборки.

Как можно заметить, в отличие от распределения Стьюдента, основанного на среднем арифметическом, используемом в качестве наилучшей оценки результата измерения, используется среднее арифметическое граничных значений выборки для построения распределения величины K. Таким образом, можно ожидать, что распределение рассматриваемой случайной величины K будет иметь те же свойства, что и распределение Стьюдента, но при этом исследуемое распределение будет у́же и, как следствие, позволит находить более узкие доверительные интервалы при тех же уровнях доверительной вероятности. Отличительным свойством распределения Стьюдента является его независимость от среднеквадратического отклонения выборки. Это достигается за счет наличия связи между СКО выборки и СКО среднего арифметического $\sigma(\bar{x}_i) = \sigma(x_i)/\sqrt{n}$. В результате оценка СКО среднего арифметического $S(\bar{x}_i)$, найденная на основании экспериментальных данных, рассчитывается через экспериментальное СКО выборки $S(x_i)$ и таким образом, распределение Стьюдента не зависит от $S(x_i)$. Следовательно, можно рассчитывать, что наличие связи между $S(m_i)$ и $S(x_i)$ также приведет к независимости распределения величины K от СКО. В результате проведенных исследований было установлено, что связь между $\sigma(x_i)$ и $\sigma(m_i)$ линейна $\sigma(m_i) = p\sigma(x_i)$ и коэффициент p зависит только от объема выборки. В таблице 1 представлены значения этого коэффициента для различных n.

Таблица 1 ─ Соответствие между значением p и объемом выборки n.

	n=10	*n*=15	*n*=20	*n*=25	*n*=30	*n*=50	*n*=70	*n*=90
p	0.2132	0.1486	0.1139	0.0924	0.0778	0.0475	0.0343	0.0268

На основании этих данных с помощью МНК получено аналитическое выражение зависимости $p(n)$:

$$p = \frac{1}{0.4078 \cdot n + 0.6229}, \tag{1}$$

О качестве аппроксимации при помощи выражения (1) можно судить по рис. 1.

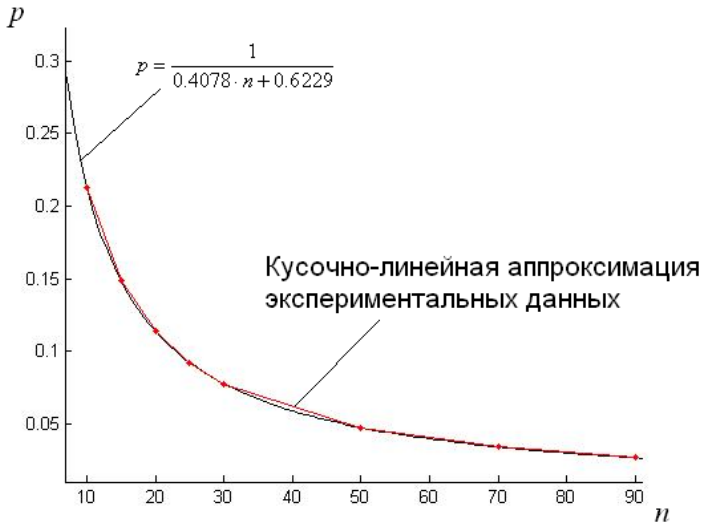

Рисунок 1 ─ Оценка качества аппроксимации аналитической зависимости $p(n)$

Таким образом, приходим к выводу, что предлагаемая статистика K может быть представлена как

$$K = \frac{(m_i - M(m_i))}{p \cdot S(x_i)}.$$

Следующим этапом была проверка независимости функции принадлежности от СКО для рассматриваемой случайной величины. Для этого построим и исследуем функции принадлежности при различных значениях СКО. Результаты приведены на рис. 2.

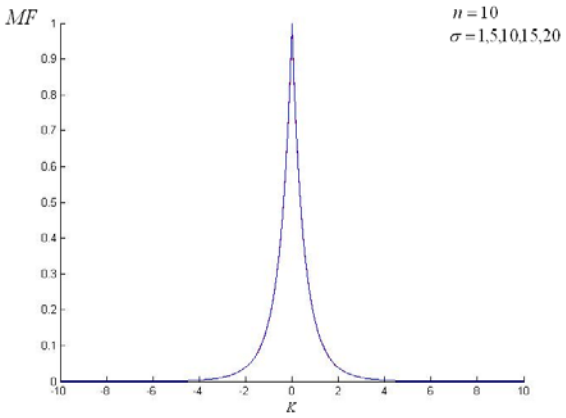

Рисунок 2 — Функции принадлежностей, построенные на основании распределения величины K при различных СКО. Объем выборки $n=10$. Количество экспериментов 1000000

Представленные на рис. 2 функции принадлежностей для различных СКО совпадают, тем самым, подтверждая независимость величины K от СКО. Следствием этого является вывод о независимости от СКО распределения величины K для функции случайных величин $f(X_1, X_2, ...X_N)$. Более того, как было установлено, распределение величины K для линейной функции случайных величин имеет такую же форму, как и распределения этой величины для входных аргументов (при условии одинаковых объемов выборок). Распределение величины K, также как и распределение Стьюдента, зависит только от объема выборки. Данные выводы подтверждаются результатами, полученными при моделирующем эксперименте (рис. 3). С увеличением объема выборки распределение величины K сужается, что не противоречит теоретическим представлениям. На рис. 3 приведена также функция принадлежности для распределения Стьюдента при $n=10$. Сравнение ее с функцией принадлежности распределения величины K при том же объеме выборки показывает, что использование последней приведет к более узким интервалам при тех же уровнях доверительной вероятности.

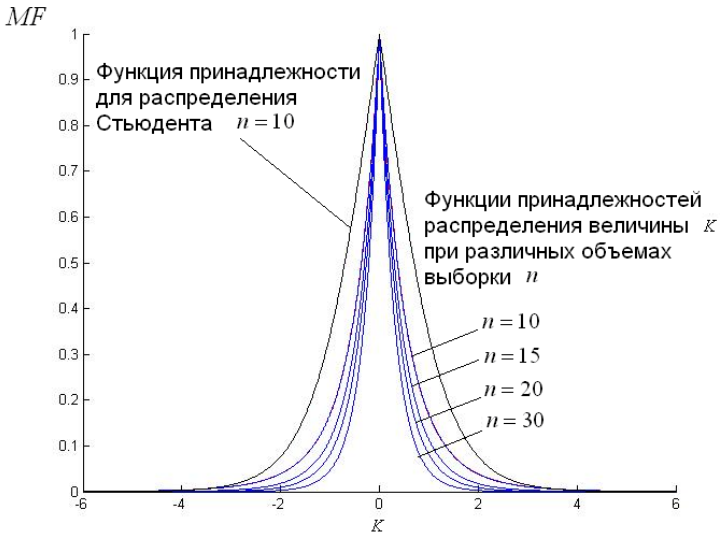

Рисунок 3 — Функции принадлежностей распределения величины K при различных объемах выборки n. Количество экспериментов 1000000

Исследуем эффективность использования распределения величины K при оценке расширенной неопределенности. Для этого рассмотрим объединение двух равномерно распределенных независимых

величин X_1 и X_2: $Y = X_1 + X_2$. В качестве оценки результата объединения (косвенного измерения) используем выражение :

$$m = \frac{\min(x_{1i}) + \min(x_{2i}) + \max(x_{1i}) + \max(x_{2i})}{2}$$

Находим экспериментальные СКО для входных выборок S_1 и S_2, на основании которых рассчитываем оценку СКО величины Y: $S_Y = \sqrt{S_1^{\,2} + S_2^{\,2}}$, которая используется для нахождения оценки СКО величины m: $S_m = S_Y \cdot p$, где p коэффициент, который находим из полученной ранее зависимости (1). Введем интервал I_P, аналогичный расширенной неопределенности U_P, границы которого определяются как $y \pm k_P(n) \cdot S_m$, где $k_P(n)$ коэффициент, найденный для требуемого уровня доверительной вероятности по распределению величины K. Если провести аналогию с традиционным поиском расширенной неопределенности, то коэффициент p можно сравнивать с $1/\sqrt{n}$, а коэффициент $k_P(n)$ соответствует коэффициенту Стьюдента. В процессе проведения моделирующего эксперимента были сгенерированы различные выборки x_{1i} и x_{2i} объема n, на основании которых рассчитаны предлагаемым способом значения I_P и традиционным путем U_P (при расчете U_P для поиска количества степеней свободы используется выражение Вэлча-Саттервэйта). При этом варьировалось соотношение $\sigma(x_{1i})/\sigma(x_{2i})$, а также изменялся объем выборок n. Параллельно подсчитывались частоты попадания математического ожидания $M(Y) = M(X_1) + M(X_2)$ в интервал I_P. Это позволяет оценить достоверность исследуемого метода, разделив частоты попадания в интервал I_P на общее количество экспериментов, тем самым рассчитав относительные частоты W. Для одной пары значений n и $\sigma(x_{1i})/\sigma(x_{2i})$ проводилось 100000 экспериментов. Соотношение ширины интервалов I_P и U_P позволяет оценить эффективность предложенного метода. Результаты экспериментов представлены на рис. 4.

Из представленного на рисунке следует, что относительная частота W, выступающая в качестве оценки доверительной вероятности, не выходит за пределы допустимых уровней, т. е. 0.997, 0.95 и 0.90. Это свидетельствует о том, что с помощью предложенного метода действительно получаем доверительные интервалы с необходимой доверительной вероятностью. Что касается эффективности, то отметим, что она увеличивается с ростом объема выборки и с понижением уровня доверительной вероятности. Данный подход дает выигрыш и при малых объемах выборки и эффективность практически не зависит от соотношения СКО составляющих.

Соотношения I_P / U_P, представленные на рис. 4, были получены экспериментальным путем. Однако эти значения можно получить аналитически как соотношение полуширин доверительных интервалов, т. е. $\frac{k_P(n) \cdot p \cdot S_Y}{k_S(v) \cdot S_Y / \sqrt{n}} = \frac{k_P(n) \cdot p \cdot \sqrt{n}}{k_S(v)}$, здесь берется $k_S(v)$ - коэффициент Стьюдента для $v = n - 1$ степеней свободы. Как уже было показано, $k_S(v)$ не зависит от значений $\sigma(x_{1i})$ и $\sigma(x_{2i})$, поэтому при рассмотрении величины $\sigma(x_{1i})/\sigma(x_{2i})$ соотношение I_P / U_P следует принимать как константу. Данный результат был подтвержден при проведении дополнительных исследований. Однако, как видно из зависимостей, представленных на рис. 4, наблюдается некоторый наклон этих зависимостей, т. е. имеет место влияние соотношения $\sigma(x_{1i})/\sigma(x_{2i})$ на I_P / U_P.

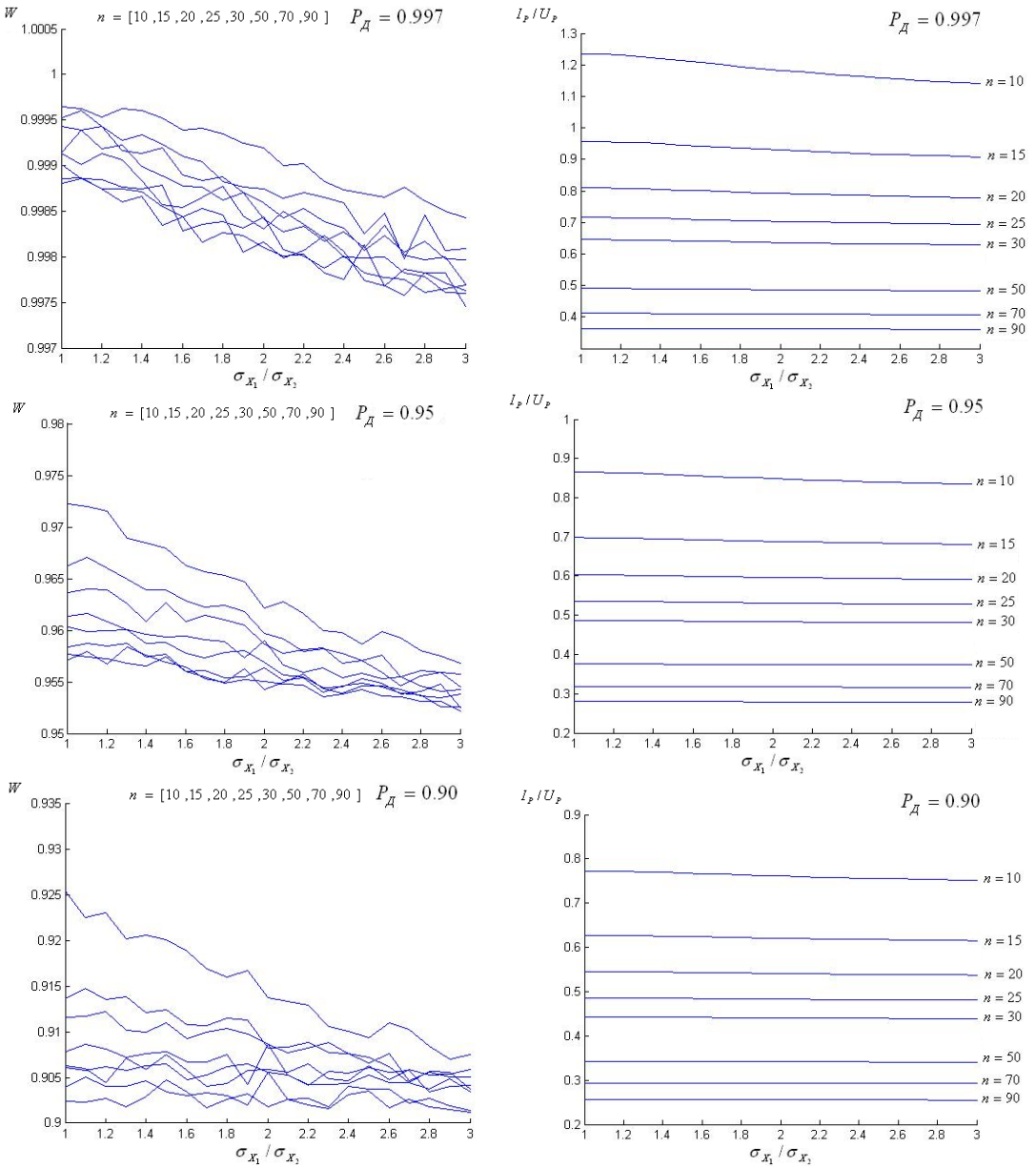

Рисунок 4 — Результаты экспериментов по оценке достоверности и эффективности предлагаемого метода

Это обусловлено тем, что при расчете v_{eff} по формуле Вэлча-Саттервэйта используются $\sigma(x_{1i})$ и $\sigma(x_{2i})$. Необходимо отметить, что эффективность предложенного подхода не зависит от количества объединяемых составляющих.

III Заключение

Проведенный анализ показал эффективность предлагаемого подхода оценки расширенной неопределенности по сравнению с традиционным, рассмотренным в Руководстве [1]. Показано, что при прямых и косвенных измерениях при равномерно распределенных случайных величинах расширенная неопределенность будет меньше при том же уровне доверительной вероятности. Получены аналитические зависимости, позволяющие оценить введенный показатель расширенной неопределенности, достоверность которого подтверждена результатами математического моделирования. Приведенные аналитические выражения позволяют оценить эффективность предложенного подхода по сравнению с традиционным при расчете расширенной неопределенности.

Литература: ***1.*** *Guide to the Expression of Uncertainty in Measurement: First Edition.- ISO, Switzerland, 1993.- 101 p.* ***2.*** *Ціделко В. Д., Яремчик Н. А. Невизначеність вимірювання. Обробка даних і подання результату вимірювання: Монографія.-К.:ІВЦ "Видавництво <Політехніка>", 2002.-176с.* ***3.*** *G. Mauris, V. Lasserre, L. Foulloy. A Fuzzy approach for the expression of uncertainty in measurement. Measurement, 29, 2001.- Elsevier,- p.165-177.* ***4.*** *Е. Т. Володарский, Л. А. Кошевая, А. Н. Карпенко "Взаимосвязь вероятностного подхода и нечеткой логики при оценке неопределенности измерений"// Системи обробки інформації.- Харків, 2006.-с. 19-22. N7.*

УДК 65.012.8

ЩОДО МЕТОДИКИ РЕАЛІЗАЦІЇ ПРОЦЕДУРИ ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО СЕКРЕТНОЇ

Олександр Архипов, Валерій Ворожко *

*Національний технічний університет України „КПІ", *Інститут захисту інформації з обмеженим доступом Національної академії СБ України*

Анотація: **Розглянуто методичні аспекти реалізації процедури віднесення інформації до секретної, зокрема, виконано формалізацію цієї процедури з представленням її чотириетапною схемою обробки вихідної інформації.**

Summary: **Methodical aspects of realization of information classification procedure to state secret are considered, in particular, there is made formalization of this procedure with its representation by four-stage scheme of the initial information processing.**

Ключові слова: **Державна таємниця, секретна інформація.**

I Вступ

Інформатизація світового суспільства, глобальне розповсюдження нових інформаційних технологій стимулюють загально цивілізаційний процес утворення світового інформаційного простору. Інтеграційні тенденції цього процесу мають спиратися на зростаючу інформаційну відкритість його учасників. Але реалії розвитку та становлення світового інформаційного суспільства вказують на наявність в процесах інформатизації ряду складних та суперечливих тенденцій.

З точки зору розвитку та поширення електронного бізнесу, культурного обміну, технологій дистанційного навчання, доступу до загальносвітових наукових, технічних і культурологічних ресурсів новітні інформаційні та телекомунікаційні технології – це очевидний позитив. Однак одночасно вони – виклик існуючій системі захисту інтелектуальної власності та сегменту національних інформаційних ресурсів, який за своїм характером не є загальнодоступним. Однією з найсуттєвіших складових цього сегменту є державна таємниця (ДТ) – категорія секретних відомостей, умови віднесення інформації до якої чи захист цієї інформації здійснюється відповідно до закону [1]. Процес глобальної інформатизації суспільства приніс для ДТ, як і інших видів інформації з обмеженим доступом (ІзОД), певні проблеми, пов'язані з особливостями захисту ДТ в умовах нового інформаційного середовища.

Для незалежної України, як і для інших держав, що утворилися в пострадянському просторі на початку 90-х років, ці проблеми мали специфічний характер. Справа в тому, що більшість розвинутих країн світу питання регулювання відносин в сфері охорони ДТ розв'язує в межах правового поля, утвореного прийняттям відповідних законодавчих актів. На відміну від цих країн в СРСР не існувало закону про охорону ДТ (як і про регулювання інформаційних відносин взагалі). Практичні питання захисту державних секретів регламентувалися підзаконними нормативними актами, а перелік відомостей, що за своїм змістом мали належати до ДТ, був секретним документом [2]. Фактично мало місце відчуження інституту секретності від суспільства, внаслідок чого не розглядалися та не обговорювалися публічно принципи діяльності цього інституту, його організаційна структура та витрати на функціонування, критично не аналізувався механізм та методи охорони ДТ, їх ефективність та дієвість.

Радикальні зміни політичного та економічного устрою, що сталися в Україні на початку 90-х років та отримали своє законодавче закріплення в різних сферах життєдіяльності особи, суспільства та держави, не обминули і сфери інформаційних відносин. У 1992 р. було прийнято Закон України „Про інформацію", який заклав правові основи інформаційної діяльності. У січні 1994 р. введено в дію Закон України „Про державну таємницю", а в серпні 1995 р. опубліковано „Звід відомостей, що становлять державну таємницю України" (ЗВДТ). З появою цих відкритих документів процес створення механізму віднесення інформації до ДТ можна