УДК 621.391+519.72

Попов А.А., к.т.н. (*Центральный НИИ вооружения и военной техники ВС Украины*)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНФОРМАЦИОННЫХ СООТНОШЕНИЙ ПРИ ВЗАИМОДЕЙСТВИИ СИГНАЛОВ В ПРОСТРАНСТВАХ С РАЗЛИЧНЫМИ АЛГЕБРАИЧЕСКИМИ СВОЙСТВАМИ

Попов А.О. Порівняльний аналіз інформаційних співвідношень при взаємодії сигналів в просторах з різними алгебраїчними властивостями. Розглянуто інформаційний парадокс взаємодії сигналів у лінійному просторі сигналів. Встановлені алгебраїчні властивості простору сигналів, в якому можлива взаємодія сигналів без інформаційних втрат. Визначені основні інформаційні співвідношення, які характеризують взаємодію сигналів в таких просторах. В залежності від якісного змісту цих інформаційних співвідношень на якісному рівні розмежовані види взаємодії між сигналами в просторах сигналів.

Ключові слова: ПРОСТІР СИГНАЛІВ, ВЗАЄМОДІЯ СИГНАЛІВ, РЕШІТКА, КІЛЬКІСТЬ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНИЙ ПАРАДОКС

Попов А.А. Сравнительный анализ информационных соотношений при взаимодействии сигналов в пространствах с различными алгебраическими свойствами. Рассматривается информационный парадокс взаимодействия сигналов в линейном пространстве сигналов. Установлены алгебраические свойства пространства сигналов, в котором возможно взаимодействие сигналов без информационных потерь. Определены основные информационные соотношения, характеризующие взаимодействие сигналов в таких пространствах. В зависимости от количественного содержания этих информационных соотношений, на качественном уровне разграничены виды взаимодействия между сигналами в пространствах сигналов.

Ключевые слова: ПРОСТРАНСТВО СИГНАЛОВ, ВЗАИМОДЕЙСТВИЕ СИГНАЛОВ, РЕШЕТКА, КОЛИЧЕСТВО ИНФОРМАЦИИ, ИНФОРМАЦИОННЫЙ ПАРАДОКС

Popov A.O. The comparative analysis of informational relations on signals interaction in spaces with different algebraic properties. The informational paradox of stochastic signals interaction in linear signal space is being considered. It is being established the algebraic properties of physical signal space, where the signals interaction accompanies without losses of information. It is being determened the main informational relations, which characterize the signals interaction in signal spaces with different algebraic properties. Subject to quantity content of this informational relations, on the quality level it is being differentiated the sorts of signals interaction in signal spaces.

Keywords: SIGNAL SPACE, SIGNALS INTERACTION, LATTICE, INFORMATION QUANTITY, INFORMATIONAL PARADOX

В большей части известной литературы задачи обработки сигналов на фоне помех (шумов) формулируются в линейном пространстве сигналов $\mathcal{LS}$, в котором результат взаимодействия x полезного сигнала s и помехи n описывается операцией сложения аддитивной коммутативной группы: $x=s+n$ [1…4]. Между тем ряд авторов допускает общую постановку задачи обработки сигналов на фоне помех (шумов) по отношению к виду их взаимодействия [5…7]: $x=\Phi(s,n)$, где $\Phi(s,n)$ – некоторая детерминированная функция.

Результаты синтеза конкретных устройств обработки сигналов получают на основе тех или иных критериев оптимальности, как правило, в предположении аддитивного (в терминологии линейного пространства) взаимодействия x сигнала s и помехи n: $x=s+n$. При этом не исследуется вопрос “оптимальности” по отношению к виду взаимодействия сигналов. Насколько модель такого аддитивного взаимодействия сигналов в устройстве обработки близка по своему содержанию к оптимальной? Могут ли быть достигнуты более высокие показатели качества обработки сигналов при их взаимодействии друг с другом, которое отличается от аддитивного, т.е., в случае, если пространство сигналов не является линейным? Может ли быть решена задача синтеза устройства оптимальной обработки сигналов в самом общем виде, в предположении, что свойства пространства сигналов, в котором осуществляется взаимодействие сигналов вида $x=\Phi(s,n)$, не определены? Другими словами, может ли быть найдена неизвестная функция $\Phi(s,n)$, определяющая вид взаимодействия полезного сигнала s и помехи n в ходе решения какой-либо конкретной задачи синтеза устройства обработки сигналов, на основе известных критериев оптимальности? Если в такой постановке задача синтеза не имеет решения, то можно попытаться получить такое решение в случае использования различных критериев оптимальности, во-первых, для определения вида взаимодействия сигналов $\Phi(s,n)$ на входе устройства обработки, и, уже во-вторых, для синтеза устройства оптимальной обработки.

Ведь когда будут определены алгебраические свойства пространства сигналов, в котором имеет место «наилучшее» взаимодействие сигналов $\Phi(s,n)$ соответствующего вида, требование детерминированности для функции $\Phi(s,n)$, используемое для последующего синтеза устройств оптимальной обработки, уже не покажется слишком жестким ограничением. Для того чтобы ответить на эти и другие смежные вопросы, необходимо с единых позиций подойти к анализу информационных соотношений, имеющих место при взаимодействии сигналов в пространствах с различными алгебраическими свойствами.

Здесь следует подчеркнуть одно весьма важное обстоятельство. Классическая теория информации не допускает понятия *количества информации*, содержащейся в сигнале вообще, в ней бессмысленна сама постановка вопроса: «Сколько информации содержится в сигнале a?», поскольку понятие «количества информации» имеет смысл только применительно к паре сигналов [8]. В этом случае допустимо поставить вопрос только так: «Сколько информации содержит в себе сигнал b о сигнале a?». Это значит, что классическая теория информации оперирует только с понятием «относительного количества информации», которое применимо исключительно к паре сигналов. Поэтому, с помощью классической теории информации можно лишь оценить относительное количество информации $I[x,a]$, которое содержится в сигнале x о сигнале a, если, например, сигнал x есть результат аддитивного взаимодействия двух сигналов a и b: $x=a+b$ в линейном пространстве сигналов $\mathcal{LS}$. Однако оценить величину потерь информации, которые имеют место при таком взаимодействии, не представляется возможным. Нельзя сравнить сумму I_a $+I_b$ количества информации, которая содержится в сигналах a и b в отдельности, и количество информации I_x, содержащееся в сигнале x, который является результатом взаимодействия указанной пары сигналов a и b. Причина та же — в классической теории информации величины I_x, I_a, I_b, соответствующие количеству информации, которая содержится в каждом сигнале x, a, b в отдельности просто не определимы.

Целью данной статьи является дальнейшее развитие подхода к оценке информационных соотношений между сигналами, начатое в работах [9…11], для проведения сравнительного анализа информационных свойств пространств сигналов с различными алгебраическими свойствами, которые обусловлены особенностями взаимодействия сигналов в этих пространствах. В данной статье поставлены и решены две задачи. Во-первых, определены основные информационные соотношения между сигналами до и после их взаимодействия в пространствах сигналов с различными алгебраическими свойствами. Во-вторых, в зависимости от количественного содержания этих информационных соотношений, на качественном уровне разграничены виды взаимодействия между сигналами в пространствах сигналов.

1. Информационный парадокс аддитивного взаимодействия сигналов в линейном пространстве сигналов. Понятие идеального взаимодействия сигналов. В работе [9] были введены понятия физического и информационного пространств сигналов, и соответственно, понятия физического взаимодействия и информационных взаимосвязей между сигналами. Если информационные взаимосвязи между сигналами непосредственным образом не влияют на результат их физического взаимодействия, то напротив, физическое взаимодействие сигналов накладывает свои особенности на информационные соотношения между ними и результат их взаимодействия. Рассмотрим эти особенности на примере аддитивного взаимодействия двух стационарных статистически независимых гауссовских случайных процесса $a(t)$, $b(t)$ с нулевыми математическими ожиданиями в линейном (гильбертовом) пространстве $\mathcal{LS}$, $a(t)$, $b(t)\in\mathcal{LS}$, опираясь на основные идеи работ [9…11]:

$$x(t)=a(t)+b(t),\quad t\in T. \qquad \textbf{(1)}$$

Пусть случайные процессы (далее сигналы) $a(t)$ и $b(t)$ характеризуются дисперсиями D_a, D_b и тождественными нормированными корреляционными функциями $r_a(\tau)=r_b(\tau)=$

$r(\tau) \geq 0$ соответственно. Тогда корреляционная функция $R_x(\tau)$ аддитивной смеси $x(t)$ (1) этих двух сигналов равна $R_x(\tau) = D_a\, r_a(\tau) + D_b\, r_b(\tau) = (D_a + D_b) r(\tau)$, а ее нормированная корреляционная функция $r_x(\tau)$ тождественно равна нормированной корреляционной функции сигналов $a(t)$ и $b(t)$: $$r_x(\tau) = r_a(\tau) = r_b(\tau) = r(\tau). \quad \textbf{(2)}$$

Для гауссовского случайного сигнала нормированная корреляционная функция однозначно определяет его нормированную функцию статистической взаимосвязи (НФСВ), введенную в [10]. Поэтому из равенства (2) в соответствии с формулой [10;(1)] следует тождественность НФСВ $\psi_x(\tau)$, $\psi_a(\tau)$, $\psi_b(\tau)$ сигналов $x(t)$, $a(t)$, $b(t)$:

$$\psi_x(\tau) = \psi_a(\tau) = \psi_b(\tau), \quad \textbf{(3)}$$

откуда вытекает тождественность плотностей распределения информации (ПРИ) $i_x(\tau)$, $i_a(\tau)$, $i_b(\tau)$ сигналов $x(t)$, $a(t)$, $b(t)$ (см. формулу [10; (6)]):

$$i_x(\tau) = i_a(\tau) = i_b(\tau). \quad \textbf{(4)}$$

Напомним, что на основе сформулированного в [9] аксиоматического утверждения 1, в зависимости от вида сигнатурных отношений между образами A, B сигналов $a(t)$, $b(t)$ в информационном пространстве сигналов $\mathbf{\Omega}$, построенном на обобщенной булевой алгебре $\mathbf{B}(\mathbf{\Omega})$ с мерой m сигнатуры $(+, \cdot, -, \mathbf{O})$, $A \in \mathbf{\Omega}$, $B \in \mathbf{\Omega}$, определены следующие основные виды количества информации: количество абсолютной информации I_A, I_B, количество взаимной информации I_{AB} и количество общей информации I_{A+B}, определяемые следующими соотношениями соответственно:

$$I_A = m(A);\ I_B = m(B); \quad \textbf{(5а)} \qquad I_{AB} = m(AB); \quad \textbf{(5б)}$$

$$I_{A+B} = m(A+B) = m(A) + m(B) - m(AB) = I_A + I_B - I_{AB}, \quad \textbf{(5в)}$$

причем образы A и B соответствующих сигналов $a(t)$ и $b(t)$, связанны с ПРИ $i_a(\tau)$, $i_b(\tau)$ этих сигналов отображением [9; (16)].

Тождество (4) в соответствии с формулой [11;(3)] означает, что на интервале времени T сигналы $x(t)$, $a(t)$, $b(t)$ несут одно и то же количество абсолютной информации:

$$I_X = I_A = I_B. \quad \textbf{(6)}$$

Однако, учитывая статистическую независимость сигналов $a(t)$ и $b(t)$ (т.е. I_{AB}=0), легко сделать вывод о том, что содержание информации, переносимое этими сигналами совершенно различно, несмотря на количественное равенство $I_A = I_B$. Поэтому количество общей информации I_{A+B}, переносимое сигналами $a(t)$ и $b(t)$ вместе должно быть равно сумме I_A и I_B, и в соответствии с соотношениями (5в), (6) равно:

$$I_{A+B} = I_A + I_B = 2I_X. \quad \textbf{(7)}$$

Сравнивая соотношения (6) и (7), совершенно естественно поставить вопрос: почему количество общей информации I_{A+B}, переносимое двумя независимыми гауссовскими сигналами $a(t)$ и $b(t)$ с тождественными нормированными корреляционными функциями в два раза превышает количество абсолютной информации I_X, содержащейся в аддитивной смеси $x(t)$ сигналов $a(t)$ и $b(t)$, несмотря на интуитивно кажущееся правильным строгое равенство между ними: $I_{A+B} = I_X$?

Тем не менее, при аддитивном взаимодействии (1) двух стационарных статистически независимых сигналов $a(t)$, $b(t)$ с нулевыми математическими ожиданиями в линейном пространстве $\mathcal{LS}$ с произвольными НФСВ $\psi_a(\tau)$, $\psi_b(\tau)$ (и соответственно ПРИ $i_a(\tau)$, $i_b(\tau)$) всегда справедливо информационное неравенство:

$$I_X < I_{A+B} = I_A + I_B. \quad \textbf{(8)}$$

Данное соотношение (8) будем называть *информационным парадоксом (информационным неравенством) аддитивного взаимодействия сигналов* в линейном пространстве, суть которого заключается в неэквивалентности ($I_{A+B} \neq I_X$, $I_{A+B} > I_X$) количества общей информации $I_{A+B} = I_A + I_B$ двух статистически независимых сигналов $a(t)$ и $b(t)$ и количества абсолютной информации I_X, содержащейся в их аддитивной сумме $x(t)$.

На качественном уровне можно пояснить данный парадокс потерями информации ΔI, которые сопровождают аддитивное взаимодействие статистически независимых сигналов $a(t)$ и $b(t)$, и обусловлены разрушением части информации, содержащейся в них:

$$\Delta I = I_A + I_B - I_X.$$

Пример 1. В случае взаимодействия двух гауссовских статистически независимых случайных сигналов с тождественными нормированными корреляционными функциями $r_a(\tau) = r_b(\tau) = r(\tau)$ (т.е. $I_A = I_B = I_X$) и произвольными дисперсиями D_a, D_b, величина потерь ΔI составляет половину от суммы количества информации, переносимого обоими сигналами:

$$\Delta I = (I_A + I_B)/2 = I_A = I_B = I_X.$$

Таким образом, взаимодействие сигналов в линейном пространстве $\mathcal{LS}$ сопровождается потерями информации, которая в них содержится.

В работе будем различать соответствующие виды количества информации, определяемые для информационного $\mathbf{\Omega}$ и физического $\mathbf{\Gamma}$ пространств сигналов. При этом для количества абсолютной информации, количества взаимной информации и количества общей информации, определяемых в информационном пространстве сигналов $\mathbf{\Omega}$, сохраним обозначения, принятые в работах [10,11] соответственно: I_A, I_B; I_{AB}; I_{A+B}. Эти же понятия, определяемые в физическом пространстве сигналов $\mathbf{\Gamma}$, при взаимодействии в нем сигналов $a(t)$, $b(t)$ вида $x(t) = a(t) \oplus b(t)$, где $\oplus$ – некоторая бинарная операция в $\mathbf{\Gamma}$, будем обозначать как I_a, I_b; I_{ab}; $I_{a\oplus b}$ соответственно.

Проблема возникновения потерь информации при взаимодействии сигналов в физическом пространстве сигналов $\mathbf{\Gamma}$ вообще, и, в частности, при их аддитивном взаимодействии (1) в линейном пространстве $\mathcal{LS}$, носит отнюдь не тривиальный характер. В физических пространствах сигналов, отличающихся по своей алгебраической структуре от обобщенной булевой алгебры, перестают выполняться информационные соотношения между взаимодействующими сигналами, которые получены в работе [9] для информационного пространства сигналов $\mathbf{\Omega}$. Это означает, что физическое взаимодействие сигналов негативным образом сказывается на величине некоторых видов количества информации, определяемых для физического пространства сигналов $\mathbf{\Gamma}$. В частности, в общем случае, изменяются количество общей информации $I_{a\oplus b} \neq I_{A+B}$ и количество взаимной информации $I_{ab} \neq I_{AB}$, соответствующих паре взаимодействующих сигналов $a(t)$, $b(t)$. Между тем, остается без изменений количество абсолютной информации, содержащееся в каждом сигнале в отдельности:

$$I_a = I_A, \; I_b = I_B. \quad \textbf{(9)}$$

Таким образом, количество абсолютной информации не нуждается в уточнении, так как определяется безотносительно к другим сигналам физического пространства сигналов, данное понятие введено исключительно по отношению к отдельному сигналу.

Теперь информационное неравенство (8) для физического пространства сигналов $\mathbf{\Gamma}$ с определенной на ней бинарной операцией $\oplus$, можно записать в виде:

$$I_{a\oplus b} \leq I_{A+B} = I_A + I_B - I_{AB}, \quad \textbf{(10)}$$

где $I_{a\oplus b}$ – количество общей информации, содержащееся в паре сигналов $a(t)$, $b(t)$ в физическом пространстве **Γ**, равное количеству абсолютной информации $I_x = I_X$, которое содержится в результате их взаимодействия $x(t) = a(t) \oplus b(t)$: $I_{a\oplus b} = I_x$;

I_{A+B} – количество общей информации, содержащееся в паре сигналов $a(t)$, $b(t)$ в информационном пространстве **Ω**;

I_{AB} – количество взаимной информации, содержащееся в паре сигналов $a(t)$, $b(t)$ в информационном пространстве **Ω**;

$I_A = I_a$, $I_B = I_b$ – количество абсолютной информации, содержащееся в каждом сигнале $a(t)$, $b(t)$ в отдельности.

Неравенство (10), в отличие от неравенства (8), является нестрогим, что, в общем случае, допускает существование физических пространств сигналов, в которых взаимодействие сигналов осуществляется без потерь информации.

Для всякого физического пространства сигналов **Γ** с произвольными алгебраическими свойствами найдется такая пара сигналов $a(t)$, $b(t)$, для которых информационное неравенство (10) переходит в тождество. Информационные свойства таких сигналов вводятся следующим определением.

Определение 1. Два сигнала I_b, физического пространства сигналов **Γ**, $a(t), b(t) \in \mathbf{\Gamma}$, называются *тождественными в информационном смысле*, если для них неравенство (10) переходит в тождество $I_{a\oplus b} = I_{A+B} = I_A = I_B$, причем образы A, B этих сигналов $a(t)$, $b(t)$ в информационном пространстве **Ω** являются тождественными: $A \equiv B$.

Как следует из определения 1, в частном случае, всякий сигнал $a(t)$ является тождественным в информационном смысле самому себе. Например, для случая аддитивного взаимодействия в линейном пространстве, сигналы $a(t)$, $b(t)$ являются тождественными в информационном смысле, если они между собой связаны линейной зависимостью вида: $a(t) = \beta b(t)$, где β=const.

В соответствии со сформулированным информационным неравенством (10) можно поставить следующие вопросы.

1. Почему при взаимодействии сигналов в линейном пространстве $\mathcal{LS}$ возникают потери информации?
2. Во всех ли пространствах взаимодействие сигналов сопровождается потерями информации?
3. Если ответ на второй поставленный вопрос утвердителен, то в каких пространствах сигналов такие потери минимальны? Если ответ на второй вопрос отрицателен, то в каких именно пространствах возможно взаимодействие сигналов без потерь информации?

Ответить на поставленные вопросы можно, если ввести следующее понятие.

Определение 2. Под *идеальным взаимодействием* $x(t) = a(t) \oplus b(t)$ двух статистически независимых сигналов $a(t)$, $b(t)$ в физическом пространстве **Γ**, в котором определены две бинарные операции сложения ⊕ и умножения ⊗, будем понимать бинарную операцию ⊕, при которой понятия количества общей информации $I_{a\oplus b}$, I_{A+B}, содержащейся в паре сигналов $a(t)$, $b(t)$, определяемые для физического **Γ** и информационного **Ω** пространств сигналов соответственно, эквивалентны:

$$I_{a\oplus b} = I_{A+B}. \quad \textbf{(11)}$$

Здесь и далее бинарные операции сложения ⊕ и умножения ⊗ понимаются как абстрактные операции некоторой алгебраической структуры. Выясним, какими алгебраическими свойствами должно характеризоваться физическое пространство сигналов, чтобы в нем имело место тождество (11), которое определяет основные информационные свойства такого взаимодействия сигналов. Ответ на данный вопрос дает следующая теорема.

Теорема 1. *Для того, чтобы в физическом пространстве сигналов* $\mathbf{\Gamma}$, *в котором определены две бинарные операции сложения* $\oplus$ *и умножения* $\otimes$, *было справедливо тождество (11), необходимо и достаточно, чтобы физическое пространство сигналов* $\mathbf{\Gamma}$ *было обобщенной булевой алгеброй* $\mathbf{B}(\mathbf{\Gamma})$ *с мерой* m_Γ.

Доказательство необходимости. Тождество (11) можно записать в более подробном виде:

$$I_{a\oplus b}=I_x=I_X=I_{A+B}=I_A+I_B-I_{AB}=I_a+I_b-I_{ab}. \quad \textbf{(12)}$$

В соответствии с (9) справедливы тождества между количествами абсолютной информации сигналов $a(t)$, $b(t)$, определяемыми для физического $\mathbf{\Gamma}$ и информационного $\mathbf{\Omega}$ пространств сигналов соответственно: $I_a=I_A$, $I_b=I_B$. Тогда справедливо тождество $I_{ab}=I_{AB}$ между количествами взаимной информации I_{ab}, I_{AB}, определяемыми для физического $\mathbf{\Gamma}$ и информационного $\mathbf{\Omega}$ пространств сигналов соответственно. Тогда мера m_Γ элементов (сигналов) $\{a(t), b(t), \ldots\}$ физического пространства $\mathbf{\Gamma}$ изоморфна мере m информационного пространства сигналов $\mathbf{\Omega}$: т.е. для каждого $c(t)\in\mathbf{\Gamma}, \exists C\in\mathbf{\Omega}$, $C=\varphi[c(t)]$: $m_\Gamma[c(t)]=m(C)$ [12,13], а отображение φ: $\mathbf{\Gamma}\to\mathbf{\Omega}$ определяет изоморфизм пространств $\mathbf{\Gamma}$ и $\mathbf{\Omega}$ друг на друга: т.е. $\forall\varphi, \exists\varphi^{-1}:\varphi^{-1}$: $\mathbf{\Omega}\to\mathbf{\Gamma}$. Потому физическое пространство сигналов $\mathbf{\Gamma}$, в котором справедливо тождество (11), является такой же алгебраической структурой, как и информационное пространство сигналов $\mathbf{\Omega}$, т.е. обобщенной булевой алгеброй $\mathbf{B}(\mathbf{\Gamma})$ с мерой m_Γ сигнатуры $(\oplus,\otimes,-,\mathbf{O})$. □

Доказательство достаточности. Если физическое пространство сигналов $\mathbf{\Gamma}$ является обобщенной булевой алгеброй $\mathbf{B}(\mathbf{\Gamma})$ с мерой m_Γ сигнатуры $(\oplus,\otimes,-,\mathbf{O})$, то отображение φ, определяемое соотношениями [9;(16)]: φ: $\mathbf{\Gamma}\to\mathbf{\Omega}$, является гомоморфизмом, сохраняющим все сигнатурные операции, в том числе справедливо:

$$\varphi[a(t)\oplus b(t)]=\varphi[a(t)]+\varphi[b(t)]; \quad \textbf{(13.а)} \qquad \varphi[a(t)\otimes b(t)]=\varphi[a(t)]\cdot\varphi[b(t)], \quad \textbf{(13.б)}$$

где $x(t)=a(t)\oplus b(t)$, $\tilde{x}(t)=a(t)\otimes b(t)$; $\varphi[a(t)]=A$, $\varphi[b(t)]=B$, $\varphi[a(t)\oplus b(t)]=X$, $\varphi[a(t)\otimes b(t)]=\tilde{X}$; $a(t), b(t), x(t), \tilde{x}(t)\in\mathbf{\Gamma}$; $A, B, X, \tilde{X}\in\mathbf{\Omega}$.

В соответствии с (9) справедливы тождества между количеством абсолютной информации сигналов $a(t), b(t), x(t)$, определяемые для физического $\mathbf{\Gamma}$ и информационного $\mathbf{\Omega}$ пространств сигналов соответственно: $I_a=I_A$, $I_b=I_B$, $I_x=I_X$, $I_{\tilde{x}}=I_{\tilde{X}}$. Эти тождества определяют изоморфизм мер m_Γ, m физического $\mathbf{\Gamma}$ и информационного $\mathbf{\Omega}$ пространств сигналов: $m_\Gamma[a(t)]=m(A)$, $m_\Gamma[b(t)]=m(B)$, $m_\Gamma[x(t)]=m(X)$, $m_\Gamma[\tilde{x}(t)]=m(\tilde{X})$. Тогда отображение φ: $\mathbf{\Gamma}\to\mathbf{\Omega}$ является изоморфизмом, сохраняющим меру, причем $m_\Gamma[x(t)]=m(X)$ $\Rightarrow I_x=I_X\Rightarrow I_{a\oplus b}=I_{A+B}$. □

Заметим, что здесь мера $m_\Gamma[\tilde{x}(t)]$ сигнала $\tilde{x}(t)=a(t)\otimes b(t)$ имеет смысл количества взаимной информации I_{ab}, содержащейся и в сигнале $a(t)$ и в сигнале $b(t)$, которое впоследствии будем также обозначать $I_{a\otimes b}$, указывая отношение данной меры к бинарной операции $\otimes$ пространства $\mathbf{\Gamma}$.

Итак, основное содержание теоремы 1 состоит в том, что при взаимодействии $x(t)=a(t)\oplus b(t)$ сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{\Gamma}$ в виде обобщенной булевой алгеброй с мерой, меры соответствующих видов количества информации, определяемые для физического $\mathbf{\Gamma}$ и информационного $\mathbf{\Omega}$ пространств сигналов соответственно, изоморфны, т.е. выполняются тождества:

$$I_a = I_A,\quad I_b = I_B,\quad I_x = I_X,\quad I_{\tilde{x}} = I_{\tilde{X}},\quad I_{a\oplus b} = I_{A+B},\quad I_{ab} = I_{a\otimes b} = I_{AB}.$$

Тогда ответы на поставленные выше вопросы будут звучать следующим образом.

1. При взаимодействии сигналов в линейном пространстве возникают потери информации. Наличие таких потерь информации обусловлено тем, что линейное пространство $\mathcal{LS}$ не изоморфно обобщенной булевой алгеброй с мерой.

2. Взаимодействие сигналов сопровождается потерями информации не во всех пространствах. Исключение составляют пространства со свойствами обобщенной булевой алгебры с мерой.

К сожалению, теорема 1 не дает конкретных рекомендаций для получения пространств сигналов с указанными свойствами. Требование выполнения информационного тождества (11) для практического воплощения в действительность (по крайней мере, на сегодняшний день), может оказаться слишком жестким ограничением. В таком случае вполне достаточно потребовать, чтобы количество взаимной информации $I_{ax} = I_{a\otimes x}$, $I_{bx} = I_{b\otimes x}$, содержащееся в сигналах $a(t)$, $b(t)$ и результате их взаимодействия $x(t) = a(t) \oplus b(t)$, было тождественно равно количеству абсолютной информации I_a, I_b, которое содержится в этих сигналах соответственно:

$$\begin{cases} I_{a\otimes x} = I_a; \\ I_{b\otimes x} = I_b. \end{cases}$$

На основе сформулированного подхода можно привести более приближенную к прикладным аспектам обработки сигналов и несколько расширенную в алгебраическом плане формулировку понятия, определяющего такой вид взаимодействия сигналов в физическом пространстве сигналов, который по своим информационным свойствам отличается от идеального взаимодействия.

Определение 3. Под *квазиидеальным взаимодействием* $x(t) = a(t) \oplus b(t)$ двух сигналов $a(t)$, $b(t)$ в физическом пространстве **Г**, в котором определены две бинарные операции сложения $\oplus$ и умножения $\otimes$, будем понимать бинарную операцию $\oplus$, при которой количество взаимной информации $I_{a\otimes x}$, $I_{b\otimes x}$, содержащееся в сигналах $a(t)$, $b(t)$ и результате их взаимодействия $x(t) = a(t) \oplus b(t)$, тождественно равно количеству абсолютной информации I_a, I_b, которое содержится в этих сигналах соответственно:

$$\begin{cases} I_{a\otimes x} = I_a; & (14/1) \\ I_{b\otimes x} = I_b; & (14/2) \\ x(t) = a(t) \oplus b(t). & (14/3) \end{cases} \qquad \mathbf{(14)}$$

Выясним, какими алгебраическими свойствами должно характеризоваться физическое пространство сигналов **Г**, чтобы в нем была справедлива система уравнений (14), которая определяет основные информационные свойства взаимодействия сигналов данного вида. Ответ на данный вопрос дает следующая теорема.

Теорема 2. *Для того, чтобы в физическом пространстве сигналов **Г**, в котором определены две бинарные операции сложения $\oplus$ и умножения $\otimes$, была справедлива система уравнений (14) достаточно, чтобы физическое пространство сигналов* **Г** *было алгебраической решеткой с операциями верхней грани $\oplus$ и нижней грани $\otimes$ с мерой m_Γ.*

Доказательство. Если физическое пространство сигналов **Г** является алгебраической решеткой с операциями верхней $a(t) \oplus b(t)$ и нижней $a(t) \otimes b(t)$ гранями, то для него справедливы следующие соотношения:

$$\begin{cases} a(t) \otimes x(t) = a(t); & (15/1) \\ b(t) \otimes x(t) = b(t); & (15/2) \\ x(t) = a(t) \oplus b(t), & (15/3) \end{cases} \qquad \mathbf{(15)}$$

где $a(t)\oplus b(t)=\sup_{\mathbf{\Gamma}}\{a(t),b(t)\}$; $a(t)\otimes b(t)=\inf_{\mathbf{\Gamma}}\{a(t),b(t)\}$.

Тождества (15/1), (15/2) определяют аксиомы поглощения решетки [13, 14]. Если физическое пространство сигналов **Г** является решеткой с мерой m_Γ, то система (15) определяет следующие тождества:

$$\begin{cases} m_\Gamma(a(t)\otimes x(t))=m_\Gamma(a(t)); & (16/1)\\ m_\Gamma(b(t)\otimes x(t))=m_\Gamma(b(t)); & (16/2)\\ x(t)=a(t)\oplus b(t), & (16/3)\end{cases} \quad \mathbf{(16)}$$

где $m_\Gamma(a(t)\otimes x(t))=I_{a\otimes x}$, $m_\Gamma(b(t)\otimes x(t))=I_{b\otimes x}$, $m_\Gamma(a(t))=I_a$, $m_\Gamma(b(t))=I_b$.

Итак, для выполнения тождеств (14/1), (14/2) системы (14), достаточно, чтобы физическое пространство сигналов **Г** было решеткой с мерой. □

Таким образом, для выполнения тождеств (14/1), (14/2) системы (14), т.е. для того, чтобы в физическом пространстве сигналов **Г** имело место квазиидеальное взаимодействие, достаточно, чтобы физическое пространство сигналов **Г** было решеткой **Г**(∨, ∧) с операциями верхней и нижней граней соответственно: $a(t)\vee b(t)=\sup_{\mathbf{\Gamma}}\{a(t),b(t)\}$, $a(t)\wedge b(t)=\inf_{\mathbf{\Gamma}}\{a(t),b(t)\}$. Тогда для взаимодействия двух сигналов $a(t), b(t)$ в физическом пространстве сигналов **Г** со свойствами решетки вида: $x(t)=a(t)\vee b(t)$ или $\tilde{x}(t)=a(t)\wedge b(t)$ исходное требование (14) можно записать в несколько расширенном виде, вследствие дуальности свойств операций решетки, с помощью двух систем уравнений соответственно:

$$\begin{cases} I_{a\wedge x}=I_a; & (17/1)\\ I_{b\wedge x}=I_b; & (17/2)\\ x(t)=a(t)\vee b(t). & (17/3)\end{cases};\quad \mathbf{(17)} \qquad \begin{cases} I_{a\vee \tilde{x}}=I_a; & (18/1)\\ I_{b\vee \tilde{x}}=I_b; & (18/2)\\ \tilde{x}(t)=a(t)\wedge b(t). & (18/3)\end{cases}. \quad \mathbf{(18)}$$

Здесь следует заметить, что в физическом пространстве сигналов **Г**, в котором имеет место идеальное взаимодействие сигналов (т.е. справедливо тождество (11), безусловно справедливы соотношения (14/1), (14/2), и, соответственно, имеет место квазиидеальное взаимодействие сигналов. Это поясняется тем, что физическое пространство сигналов **Г**, являющееся обобщенной булевой алгеброй **B(Г)** с мерой m_Γ сигнатуры $(\oplus,\otimes,-,\mathbf{O})$, является также и решеткой сигнатуры $(\oplus,\otimes)$ с операциями верхней и нижней граней соответственно:

$$a(t)\oplus b(t)=\sup_{\mathbf{\Gamma}}\{a(t),b(t)\};\qquad a(t)\otimes b(t)=\inf_{\mathbf{\Gamma}}\{a(t),b(t)\}.$$

На основе определения 3 можно привести другой вариант формулировки понятия квазиидеального взаимодействия, который непосредственным образом не отражает информационные свойства взаимодействия данного вида, делая акцент лишь на его алгебраических свойствах.

Определение 4. *Квазиидеальным взаимодействием* $x(t)=a(t)\oplus b(t)$ полезного $a(t)$ и помехового $b(t)$ сигналов в физическом пространстве сигналов **Г**, в котором определены две бинарные операции сложения ⊕ и умножения ⊗, будем называть такую бинарную операцию между ними ⊕, при которой из результата взаимодействия $x(t)$ можно выделить полностью известный сигнал $a(t)$ без каких-либо потерь информации, таким образом, что справедливо тождество:

$$\hat{a}(t)\otimes x(t)=a(t), \quad \mathbf{(19)}$$

где $\hat{a}(t)$ – некоторая детерминированная функция от известных сигналов $a(t), x(t)$.

Выясним, какими алгебраическими свойствами должно характеризоваться физическое пространство сигналов **Г**, чтобы в нем выполнялось тождество (19), которое определяет основные алгебраические свойства взаимодействия сигналов данного вида. Также установим вид функции $\hat{a}(t)$, удовлетворяющей уравнению (19). Ответ на данный вопрос дает следующая теорема.

Теорема 3. *Для того, чтобы в физическом пространстве сигналов* **Γ**, *в котором определены две бинарные операции сложения* ⊕ *и умножения* ⊗, *выполнялось тождество (19), достаточно, чтобы физическое пространство сигналов* **Γ** *было решеткой сигнатуры* $(\oplus,\otimes)$ *с операциями верхней и нижней граней соответственно:*

$$a(t)\oplus b(t)=\sup_{\mathbf{\Gamma}}\{a(t),b(t)\},\quad a(t)\otimes b(t)=\inf_{\mathbf{\Gamma}}\{a(t),b(t)\}.$$

Доказательство. Из определения 4 следует, что для случая квазиидеального взаимодействия $x(t)=a(t)\oplus b(t)$ полностью известного полезного сигнала $a(t)$ с помеховым $b(t)$ в физическом пространстве сигналов **Γ** существует такая бинарная операция ⊗, при которой с помощью оценки $\hat{a}(t)$ сигнала $a(t)$ с полностью известными параметрами ($\hat{a}(t)=a(t)$) из результата взаимодействия $x(t)$ можно получить полезный сигнал $a(t)$ без потерь информации:

$$y(t)=\hat{a}(t)\otimes x(t)=a(t)\otimes(a(t)\oplus b(t))=a(t). \qquad \textbf{(20)}$$

Последнее соотношение определяет тождество поглощения для решетки с операциями верхней и нижней граней, соответственно:

$$a(t)\oplus b(t)=\sup_{\mathbf{\Gamma}}\{a(t),b(t)\},\ a(t)\otimes b(t)=\inf_{\mathbf{\Gamma}}\{a(t),b(t)\}.$$

Это означает, что для того, чтобы в физическом пространстве сигналов **Γ** могло существовать определенное выше квазиидеальное взаимодействие полезного $a(t)$ и помехового $b(t)$ сигналов, достаточно, чтобы пространство сигналов **Γ** было решеткой сигнатуры $(\oplus,\otimes)$. □

Здесь заметим, что для пространства сигналов **Γ** со свойствами решетки сигнатуры $(\oplus,\otimes)$ для дуального взаимодействия сигналов вида $\tilde{x}(t)=a(t)\otimes b(t)$, справедливо соотношение, дуальное равенству (20):

$$\tilde{y}(t)=\hat{a}(t)\oplus\tilde{x}(t)=a(t)\oplus(a(t)\otimes b(t))=a(t). \qquad \textbf{(21)}$$

Полезность введенного понятия квазиидеального взаимодействия проиллюстрируем следующими примерами.

Пример 2. Рассмотрим модель взаимодействия сигнала $s_i(t)$ из множества детерминированных сигналов $S=\{s_i(t)\}$, $i=1,...,m$ и помехи $n(t)$ в пространстве сигналов со свойствами решетки $\mathbf{\Gamma}(\vee,\wedge)$ с операциями верхней $a(t)\vee b(t)$ и нижней $a(t)\wedge b(t)$ граней соответственно: $a(t)\vee b(t)=\sup_L\{a(t),b(t)\}$, $a(t)\wedge b(t)=\inf_L\{a(t),b(t)\}$; $a(t),b(t)\in\mathbf{\Gamma}(\vee,\wedge)$:

$$x(t)=s_i(t)\vee n(t),\ t\in T_s,\ i=1,...,m, \qquad \textbf{(22)}$$

где $T_s=[t_0,t_0+T]$ – область определения сигнала $s_i(t)$; t_0 – известное время прихода сигнала $s_i(t)$; T – длительность сигнала $s_i(t)$; $m\in\mathbf{N}$, $\mathbf{N}$ – множество натуральных чисел.

Будем полагать, что помеха $n(t)$ характеризуется произвольными вероятностно-статистическими свойствами. При условии наличия в наблюдаемом процессе $x(t)$ сигнала $s_k(t)$, $s_k(t)\in S$, $1\le k\le m$: $x(t)=s_k(t)\vee n(t)$, $t\in T_s$ решение задачи различения сигнала $s_k(t)$ из множества детерминированных сигналов $S=\{s_i(t)\}$, $i=1,...,m$ на фоне помехи $n(t)$ заключается в формировании оценки $\hat{s}_k(t)$, равной принимаемому сигналу $s_k(t)$, причем структурообразующая функция алгоритма оптимальной обработки сигналов имеет вид $\hat{s}_k(t)\wedge x(t)$, а результат оптимальной обработки $y_k(t)$ в соответствии с аксиомой поглощения решетки, тождественно равен принимаемому сигналу $s_k(t)$:

$$y_k(t)=\hat{s}_k(t)\wedge x(t)=s_k(t)\wedge[s_k(t)\vee n(t)]=s_k(t).$$

Таким образом, вне зависимости от условий параметрической и непараметрической неопределенности, и, соответственно, вероятностно-статистических свойств помехи, различитель детерминированных сигналов в пространстве сигналов со свойствами решетки безошибочно осуществляет различение сигналов из заданного множества $S=\{s_i(t)\}$, $i=1,...,m$.

Пример 3. Следствием теоремы Шеннона о пропускной способности канала связи с аддитивным белым гауссовским шумом является существование нижнего предельного значения отношения E_b/N_0 энергии E_b, приходящейся на один бит передаваемой сигналом информации, к величине спектральной плотности мощности шума N_0, называемого пределом Шеннона. Данное значение E_b/N_0, равное $\ln 2$, устанавливает предел, при котором ни при какой скорости нельзя осуществить безошибочную передачу информации [15]. Из предыдущего примера следует, что при решении задачи различения детерминированных сигналов на фоне помехи в пространстве сигналов со свойствами решетки, значение E_b/N_0 может быть сколь угодно мало, равно как и вероятность ошибки приема сигнала $s_i(t)$ из множества детерминированных сигналов $S=\{s_i(t)\}$, $i=1,...,m$. Это, однако, не означает, что в таких пространствах сигналов можно достигать неограниченых значений пропускной способности канала передачи информации с шумом.

2. Информационные соотношения при взаимодействии сигналов в пространствах сигналов с различными алгебраическими свойствами. Для того чтобы с единых позиций подойти к анализу информационных соотношений, имеющих место при взаимодействии сигналов в пространствах с различными видами взаимодействия, а значит, с различными алгебраическими свойствами, воспользуемся следующим соображением.

Положение работы [16] о том, что всякая пара случайных процессов представляет собой частично упорядоченное множество может быть обобщено на физическое пространство сигналов в целом. Действительно, всякое физическое пространство сигналов $\mathbf{\Gamma}$ можно рассматривать как частично упорядоченное множество, в котором в каждый момент времени $t\in T$ между двумя мгновенными значениями (отсчетами) a_t, b_t сигналов $a(t),b(t)\in\mathbf{\Gamma}$ определено отношение порядка $a_t\le b_t$ (или $a_t\ge b_t$). Тогда частично упорядоченное множество $\mathbf{\Gamma}$ является решеткой с операциями верхней и нижней граней соответственно: $a_t\vee b_t=\sup_{\mathbf{\Gamma}}\{a_t,b_t\}$, $a_t\wedge b_t=\inf_{\mathbf{\Gamma}}\{a_t,b_t\}$ и если $a_t\le b_t$, то $a_t\wedge b_t=a_t$ и $a_t\vee b_t=b_t$ [14]:

$$a_t\le b_t\Leftrightarrow\begin{cases}a_t\wedge b_t=a_t;\\ a_t\vee b_t=b_t.\end{cases}$$

Итак, пусть a_t,b_t – мгновенные значения (отсчеты) случайных сигналов $a(t),b(t)\in\mathbf{\Gamma}$ с симметричными одномерными плотностями распределения вероятностей ПРВ $p_a(u),p_b(v)$ вида: $p_a(u)=p_a(-u)$; $p_b(v)=p_b(-v)$.

В работе [16] определением 3 введена величина $\nu_{\mathbf{P}}(a_t,b_t)$, называемая вероятностной мерой статистической взаимосвязи (ВМСВ) между парой отсчетов a_t, b_t случайных сигналов $a(t),b(t)$ в физическом пространстве сигналов $\mathbf{\Gamma}$: $a(t),b(t)\in\mathbf{\Gamma}$:

$$\nu_{\mathbf{P}}(a_t,b_t)=3-4\mathbf{P}[a_t\vee b_t>0], \qquad \mathbf{(23)}$$

где $\mathbf{P}[a_t\vee b_t\ge 0]$ – вероятности того, что случайная величина $a_t\vee b_t$, равная верхней грани отсчетов a_t,b_t, принимает значения больше нуля.

Далее, при рассмотрении информационных соотношений, имеющих место при взаимодействии сигналов в пространствах сигналов с различными алгебраическими свойствами, в существенной мере будут использоваться понятие ВМСВ, а также материал, излагаемый в работе [16].

Итак, определениями 2, 3 были введены понятия идеального и квазиидеального взаимодействия между сигналами соответственно, причем оговаривается, что физическое пространство сигналов **Г**, где эти виды взаимодействия имеют место, обязательно должно иметь две бинарные операции — сложения ⊕ и умножения ⊗, через которые определяются понятия количества общей информации $I_{a\oplus b}$ и количества взаимной информации $I_{ab}=I_{a\otimes b}$ соответственно. Последние равны количеству абсолютной информации $I_x, I_{\tilde{x}}$, которое содержится в результатах этих бинарных операций $x(t)=a(t)\oplus b(t)$, $\tilde{x}(t)=a(t)\otimes b(t)$ между сигналами $a(t)$, $b(t)$ соответственно:

$$I_x = I_{a\oplus b}; \qquad I_{\tilde{x}} = I_{a\otimes b} . \tag{24}$$

Здесь, однако, следует заметить, что не во всяком физическом пространстве сигналов **Г** могут быть определены сразу две указанные бинарные операции сложения ⊕ и умножения ⊗. Исключение, например, составляет широкое множество пространств сигналов со свойствами группы (полугруппы), где определена лишь одна бинарная операция над сигналами, или сложения ⊕, или умножения ⊗. При этом возникает теоретическая сложность следующего характера, которую рассмотрим на примере физического пространства сигналов **Г** со свойствами аддитивной группы линейного пространства, в которой определена только одна бинарная операция между сигналами – сложения ⊕. В таком пространстве сигналов указанным соотношениями (24) способом, можно определить только количество общей информации $I_{a\oplus b}$, содержащееся в результате их взаимодействия $x(t)=a(t)\oplus b(t)$. Определить подобным образом количество взаимной информации I_{ab}, содержащееся и в сигнале $a(t)$, и в сигнале $b(t)$, не представляется возможным. Для того, чтобы с единых позиций подойти к анализу информационных соотношений, имеющих место при взаимодействии сигналов в пространствах с различными алгебраическими свойствами, необходимо определить понятие количества взаимной информации I_{ab}, содержащегося и в сигнале $a(t)$, и в сигнале $b(t)$, способом, приемлемым для пространств сигналов с минимальным количеством бинарных операций между сигналами. Очевидно, что такое минимальное число операций равно одной, и эта единственная бинарная операция характеризует взаимодействие сигналов в физическом пространстве сигналов со свойствами группы (полугруппы). С другой стороны, определение величины I_{ab} необходимо осуществить таким образом, чтобы введенное вновь понятие не вошло в противоречии с уже полученными результатами. Необходимый подход к формулировке понятия количества взаимной информации I_{ab}, взаимоприемлемый для пространств сигналов с произвольными алгебраическими свойствами, дает следующее определение.

Определение 5. Для стационарных, стационарно связанных случайных сигналов $a(t)$, $b(t)$, которые взаимодействуют в физическом пространстве сигналов **Г** с произвольными алгебраическими свойствами, *количеством взаимной информации*, которая содержится в сигналах $a(t)$, $b(t)$, будем называть величину I_{ab}, равную:

$$I_{ab} = \nu_{ab}\min(I_a, I_b), \tag{25}$$

где $\nu_{ab}=\nu_{\mathbf{P}}(a_t, b_t)$ – ВМСВ между парой отсчетов a_t, b_t случайных сигналов $a(t), b(t)$ в физическом пространстве сигналов **Г**, определяемая выражением (23).

С помощью определения 5 для произвольного сигнала $a(t)$ в физическом пространстве сигналов **Г** с произвольными алгебраическими свойствами вводится мера количества информации m_Γ, определяемая соотношением (25):

$$m_\Gamma[a(t)] = I_{aa} = \nu_{aa}\min(I_a, I_a) = I_a .$$

Здесь заметим, что, как было показано в [16], для физического пространства сигналов **Г** со свойствами группы понятия ВМСВ (определение 3) и нормированной меры статистической взаимосвязи (НМСВ) (определение 1) совпадают, между тем для пространства сигналов **Г** со свойствами решетки данные понятия имеют различное содержание. В данной работе последующий анализ информационных соотношений между сигналами, взаимодействующими в физическом пространстве сигналов **Γ** с различными алгебраическими свойствами, будет выполнен на основе понятия количества взаимной информации (25), причем последнее будет использоваться на основе ВМСВ ($\nu_{ab}=\nu_{\mathbf{P}}(a_t,b_t)$), хотя, безусловно, количество взаимной информации I_{ab} может быть определено через НМСВ ($\nu_{ab}=\nu(a_t,b_t)$).

В начале статьи отмечалось, что в радиотехнических задачах синтеза и анализа практически повсеместно, за редким исключением, рассматривается аддитивное взаимодействие полезного сигнала и помехи. В ряде случаев, например, представляет интерес их мультипликативное взаимодействие [17]. Эти и другие виды взаимодействия сигналов в физическом пространстве сигналов, принципиально отличающиеся по своим информационным свойствам от двух рассмотренных выше видов взаимодействия, в работе будут отнесены к большой группе взаимодействий с «обычными» информационными свойствами с помощью следующего определения, которое опирается на введенное определением 5 понятие количества взаимной информации.

Определение 6. Под *обычным взаимодействием* $x(t)=a(t)\oplus b(t)$ двух сигналов $a(t)$, $b(t)$ в физическом пространстве **Γ** со свойствами полугруппы будем понимать бинарную операцию ⊕, при которой количество взаимной информации I_{ax}, I_{bx}, содержащееся в сигналах $a(t)$, $b(t)$ и результате их взаимодействия $x(t)=a(t)\oplus b(t)$, строго меньше количества абсолютной информации I_a, I_b, которое содержится в этих сигналах соответственно:

$$\begin{cases} I_{ax} < I_a; & (26/1) \\ I_{bx} < I_b; & (26/2) \\ x(t)=a(t)\oplus b(t). & (26/3) \end{cases} \qquad \textbf{(26)}$$

Напомним, что все приведенные в работе [9] определения видов количества информации основаны на аксиоматическом утверждении, согласно которому виды количества информации полностью определяются видом бинарной операции между образами A, B сигналов $a(t), b(t)$ в информационном пространстве сигналов **Ω**, построенном на обобщенной булевой алгебре $\mathbf{B}(\mathbf{\Omega})$ с мерой m сигнатуры $(+,\cdot,-,\mathbf{O})$. Между тем, определением 5 вводится знакомое понятие количества взаимной информации, но уже иным образом, а именно, через ВМСВ и количество абсолютной информации, которое содержится во взаимодействующих сигналах $a(t)$, $b(t)$. Проверим, насколько хорошо определение 5, во-первых, согласуется с соответствующим понятием статьи [9], и, во-вторых, позволяет учитывать особенности информационных соотношений между сигналами, которые взаимодействуют друг с другом в физическом пространстве сигналов **Γ** с произвольными алгебраическими свойствами.

Для идеального взаимодействия $x(t)=a(t)\oplus b(t)$ пары сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов **Γ** со свойствами обобщенной булевой алгебры $\mathbf{B}(\mathbf{\Gamma})$ с мерой m_{Γ} сигнатуры $(\oplus,\otimes,-,\mathbf{O})$ справедливы следующие основные информационные соотношения:

$$\begin{cases} I_a + I_b - I_{ab} = I_x; & (27/1) \\ I_{ax} = I_a; & (27/2) \\ I_{bx} = I_b, & (27/3) \end{cases} \qquad \textbf{(27)}$$

где $I_a = m_{\Gamma}[a(t)] = I_A = m(A)$, $I_b = m_{\Gamma}[b(t)] = I_B = m(B)$, $I_x = m_{\Gamma}[x(t)] = I_X = I_{A+B} = \; = m(A+B)$, $I_{ab} = \; m_{\Gamma}[a(t)\otimes b(t)] = I_{AB} = m(AB)$; m – мера информационного пространства сигналов **Ω**, изоморфная мере m_{Γ} физического пространства сигналов **Γ**.

Здесь равенство (27/1) представляет собой информационное тождество идеального взаимодействия (11), (12), а равенства (27/2), (27/3) представляют собой информационные тождества квазиидеального взаимодействия (14/1), (14/2), поскольку последние имеют место при идеальном взаимодействии сигналов. Фигурирующие во всех уравнениях системы (27) величины количеств взаимной информации I_{ab}, I_{ax}, I_{bx} понимаются уже в смысле определения 5, причем тождества (27/2), (27/3) являются следствием аксиомы поглощения решетки (15/1), (15/2).

На основе уравнений системы (27) можно получить следующую систему уравнений:

$$\begin{cases} \dfrac{I_{ax}}{I_x}+\dfrac{I_{bx}}{I_x}-\dfrac{I_{ab}}{I_x}=1; & (28/1) \\ I_{ax}=I_a; & (28/2) \\ I_{bx}=I_b. & (28/3) \end{cases} \quad \textbf{(28)}$$

Для квазиидеального взаимодействия $x(t)=a(t)\oplus b(t)$ пары сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{\Gamma}$ со свойствами решетки с мерой m_{Γ} справедливы следующие основные информационные соотношения:

$$\begin{cases} I_a+I_b-I_{ab}>I_x; & (29/1) \\ I_{ax}=I_a; & (29/2) \\ I_{bx}=I_b, & (29/3) \end{cases} \quad \textbf{(29)}$$

где $I_a=m_{\Gamma}[a(t)]=I_A=m(A)$, $I_b=m_{\Gamma}[b(t)]=I_B=m(B)$, $I_x=m_{\Gamma}[x(t)]=I_X=m(X)$, $I_{ab}=\nu_{ab}\min(I_a,I_b)$; m – мера информационного пространства сигналов $\mathbf{\Omega}$; m_{Γ} – мера физического пространства сигналов $\mathbf{\Gamma}$ со свойствами решетки.

Здесь неравенство (29/1) представляет собой информационное неравенство (10), а равенства (29/2), (29/3) представляют собой информационные тождества квазиидеального взаимодействия (14/1), (14/2). Фигурирующие во всех уравнениях системы (29) количества взаимной информации I_{ab}, I_{ax}, I_{bx} также понимаются в смысле определения 5, причем тождества (29/2), (29/3) вытекают из результатов [16;(39а)], [16;(39б)] теоремы 17 [16].

На основе соотношений системы (29) можно получить следующую систему уравнений:

$$\begin{cases} (I_{ax}+I_{bx}-I_{ab})/I_x>1; & (30/1) \\ I_{ax}=I_a; & (30/2) \\ I_{bx}=I_b. & (30/3) \end{cases} \quad \textbf{(30)}$$

Для аддитивного взаимодействия $x(t)=a(t)+b(t)$ пары случайных сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{\Gamma}$ со свойствами группы (линейного пространства сигналов $\mathcal{LS}$) справедливы следующие основные информационные соотношения:

$$\begin{cases} \nu_{\mathbf{P}}(a_t,x_t)+\nu_{\mathbf{P}}(b_t,x_t)-\nu_{\mathbf{P}}(a_t,b_t)=1; & (31/1) \\ \nu_{\mathbf{P}}(a_t,x_t)<1; & (31/2) \\ \nu_{\mathbf{P}}(b_t,x_t)<1, & (31/3) \end{cases} \quad \textbf{(31)}$$

где $\nu_{\mathbf{P}}(a_t,x_t)$, $\nu_{\mathbf{P}}(b_t,x_t)$, $\nu_{\mathbf{P}}(a_t,b_t)$ – ВМСВ соответствующих пар отсчетов a_t, x_t; b_t, x_t; a_t, b_t случайных сигналов $a(t), b(t), x(t)$.

Здесь равенство (31/1) представляет собой результат [16;(11)] теоремы 5 [16], а неравенства (31/2), (31/3) представляют собой следствия неравенств (26/1), (26/2) определения 6. С учетом соотношения (25) определения 5, систему (31) можно переписать в следующем виде:

$$\begin{cases} \dfrac{I_{ax}}{I_a} + \dfrac{I_{bx}}{I_b} - \dfrac{I_{ab}}{\min[I_a, I_b]} = 1; & (32/1) \\ I_{ax} < I_a; & (32/2) \\ I_{bx} < I_b, & (32/3) \\ \dfrac{I_a}{I_x} + \dfrac{I_b}{I_x} - \dfrac{I_{ab}}{I_x} > 1, & (32/4) \end{cases} \quad \textbf{(32)}$$

где $I_a = I_A = m(A)$, $I_b = I_B = m(B)$, $I_x = I_X = m(X)$, $I_{ab} = \nu_{ab}\min(I_a, I_b)$, $I_{ax} = \nu_{ax}\min(I_a, I_x)$, $I_{bx} = \nu_{bx}\min(I_b, I_x)$; m – мера информационного пространства сигналов $\mathbf{\Omega}$.

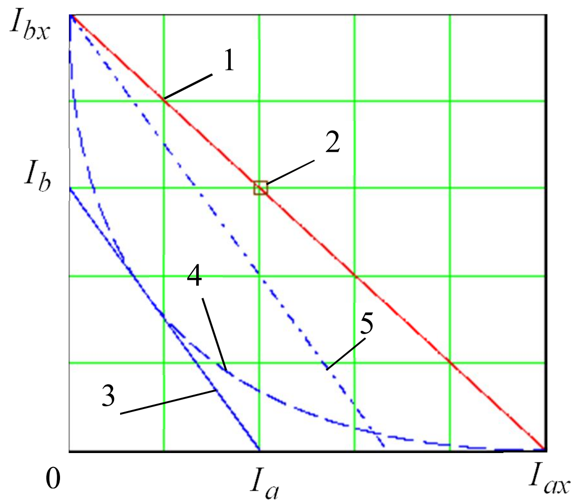

Рис. 1

Здесь равенство (32/1) является следствием совместного выполнения соотношений (31/1) и (25), неравенства (32/2), (32/3) являются следствием неравенств (26/1), (26/2) определения 6, а неравенство (32/4) представляет собой информационное неравенство (10).

На рис. 1 показаны зависимости $I_{bx}(I_{ax})$ количества взаимной информации I_{bx}, содержащейся в сигнале $x(t)$ о сигнале $b(t)$, от количества взаимной информации I_{ax}, содержащейся в сигнале $x(t)$ о сигнале $a(t)$: 1 – для случая идеального взаимодействия; 2 – для случая квазиидеального взаимодействия; 3 – для случая обычного взаимодействия статистически независимых сигналов в линейном пространстве сигналов (при I_{ab}=0); 4 – для случая обычного взаимодействия статистически независимых сигналов в линейном пространстве сигналов, при $I_{bx}(I_{ax}) \leq \sup\limits_{I_a + I_b = \text{const}} [I_{bx}(I_{ax})]\Big|_{I_{ab}=0}$; 5 – для случая обычного взаимодействия статистически зависимых сигналов в линейном пространстве сигналов, построенные на основе соотношений (28), (30), (32), соответственно.

Для идеального взаимодействия $x(t) = a(t) \oplus b(t)$ пары сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{\Gamma}$ со свойствами обобщенной булевой алгебры $\mathbf{B}(\mathbf{\Gamma})$ сигнатуры $(\oplus, \otimes, -, \mathbf{O})$ зависимость 1 определяется уравнением прямой (28/1), причем I_{bx}=0 при $I_{ax} = I_a + I_b$, а I_{ax}=0, при $I_{bx} = I_a + I_b$. Зависимость 1 определяет верхнюю предельно достижимую границу возможных значений количеств взаимной информации I_{ax}, I_{bx} взаимодействующих сигналов $a(t), b(t)$, причем ни один из видов взаимодействия сигналов не позволяет достичь лучших информационных соотношений при фиксированной сумме $I_a + I_b$=const. Для квазиидеального взаимодействия $x(t) = a(t) \oplus b(t)$ пары сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{\Gamma}$ со свойствами решетки зависимость 2 определяется точкой: $I_{ax} = I_a$, $I_{bx} = I_b$, что соответствует тождествам (29/2), (29/3). Для аддитивного взаимодействия $x(t) = a(t) + b(t)$ пары статистически независимых сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{\Gamma}$ со свойствами группы линейного пространства сигналов $\mathcal{LS}$ зависимость 3 определяется уравнением прямой (32/1), проходящей через точки (I_a,0), (0,I_b) соответственно, причем для независимых сигналов $a(t)$, $b(t)$ количество взаимной информации I_{ab} равно нулю: I_{ab}=0. Зависимость 3 определяет нижнюю предельно достижимую границу возможных значений количеств взаимной информации I_{ax}, I_{bx} взаимодействующих сигналов $a(t)$, $b(t)$, причем как бы не взаимодействовали сигналы друг с другом, невозможно достичь более худших информационных соотношений при фиксированной сумме $I_a + I_b$=const. Зависимость 4 – $\sup\limits_{I_a + I_b = \text{const}} [I_{bx}(I_{ax})]\Big|_{I_{ab=0}}$ определяет верхнюю предельно достижимую границу возможных значений количеств взаимной информации I_{ax}, I_{bx} аддитивно взаимодействующих в линейном пространстве сигналов $a(t)$, $b(t)$, причем как бы не взаимодействовали сигналы друг с другом, невозможно достичь лучших информационных соотношений при фиксированной сумме $I_a +$ I_b=const. Данная функция определяется соотношением:

$$\sup\limits_{I_a + I_b = \text{const}} [I_{bx}(I_{ax})]\Big|_{I_{ab=0}} = \left(\sqrt{I_a + I_b} - \sqrt{I_{ax}}\right)^2. \quad \textbf{(33)}$$

Для аддитивного взаимодействия $x(t) = a(t) + b(t)$ пары статистически зависимых сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{Г}$ со свойствами группы линейного пространства сигналов $\mathcal{LS}$ зависимость 5 определяется уравнением прямой (32/1), проходящей через точки (kI_a,0), (0,kI_b) соответственно, где k равно:

$$k = 1 + [I_{ab} / \min(I_a, I_b)], \quad \textbf{(34)}$$

причем для зависимых сигналов $a(t)$, $b(t)$ количество взаимной информации I_{ab} ограничено величиной: $I_{ab} \le [\min(I_a, I_b)]^2 / \max(I_a, I_b)$.

Зависимость 5 определяет верхнюю предельно достижимую границу возможных значений количеств взаимной информации I_{ax}, I_{bx} статистически зависимых сигналов $a(t)$, $b(t)$, взаимодействующих аддитивно в линейном пространстве сигналов, причем как бы не взаимодействовали сигналы друг с другом, в линейном пространстве сигналов невозможно достичь лучших информационных соотношений при фиксированной сумме $I_a + I_b$=const. В случае, если взаимодействующие сигналы $a(t)$, $b(t)$ являются тождественными в информационном смысле (см. определение 1), т.е. характеризуются одинаковым количеством информации $I_a = I_b$, причем информация, содержащаяся в этих сигналах является одинаковой по содержанию, тогда значение коэффициента k, определяемого соотношением (34) становится равным двум: $k = 2$. В этом (и только в этом) случае зависимости 5 и 1 совпадают.

Таким образом, геометрическое место прямых, характеризующих зависимость (32/1) для аддитивного взаимодействия $x(t) = a(t) \oplus b(t)$ пары сигналов $a(t)$, $b(t)$ в физическом пространстве сигналов $\mathbf{Г}$ со свойствами группы (линейного пространства сигналов $\mathcal{LS}$) заключено между кривыми 1 и 3 на рис. 1.

Резюмируя вышесказанное, можно сделать следующие выводы.

1. Не во всех физических пространствах сигналов взаимодействие сигналов сопровождается потерями некоторого количества общей информации. Исключение составляют пространства сигналов со свойствами обобщенной булевой алгебры с мерой. Взаимодействие сигналов в пространствах этого типа характеризуется сохранением количества общей информации, которая содержится в паре взаимодействующих сигналов, при этом выполняется информационное тождество (12).

2. При взаимодействии сигналов в физическом пространстве сигналов, не изоморфном обобщенной булевой алгебре с мерой, неизбежно возникают потери некоторого количества общей информации. На качественном уровне эти потери в количестве общей информации, которая содержится в паре взаимодействующих сигналов, описываются

информационным неравенством (10). Поэтому взаимодействие сигналов в линейном пространстве $\mathcal{LS}$ всегда сопровождается потерями части количества общей информации, которая в них содержится.

3. Также не во всех физических пространствах сигналов взаимодействие сигналов сопровождается потерями некоторого количества взаимной информации между сигналами до и после их взаимодействия. Исключение составляют пространства сигналов со свойствами решетки. Взаимодействие сигналов в пространствах этого типа характеризуется сохранением количества взаимной информации, которое содержится как в одном из взаимодействующих сигналов ($a(t)$ или $b(t)$), так и в результате взаимодействия $x(t) = a(t) \oplus b(t)$, при этом выполняются информационные тождества (14/1), (14/2).

4. При взаимодействии сигналов в физическом пространстве сигналов, не изоморфном решетке, неизбежно возникают потери некоторого количества взаимной информации, которая содержится как в одном из взаимодействующих сигналов ($a(t)$ или $b(t)$) так и в результате взаимодействия $x(t) = a(t) \oplus b(t)$. На качественном уровне эти потери в количестве взаимной информации, описываются информационными неравенствами (24/1), (24/2). Поэтому взаимодействие сигналов в линейном пространстве $\mathcal{LS}$ всегда сопровождается потерями части количества взаимной информации, которое содержится как в одном из взаимодействующих сигналов, так и в результате их взаимодействия.

5. В зависимости от качественных соотношений между количеством общей информации $I_{a\oplus b}$ или количеством взаимной информации I_{ab}, с одной стороны, и количеством абсолютной информации I_a, I_b, содержащейся во взаимодействующих сигналах $a(t), b(t)$, с другой, различаются следующие виды взаимодействия между сигналами в физическом пространстве сигналов: идеальное, квазиидеальное и обычное, введенные определениями 2, 3 и 6 соответственно.

6. При идеальном взаимодействии сигналов в физическом пространстве сигналов со свойствами обобщенной булевой алгебры выполняются информационные соотношения (28).

7. При квазиидеальном взаимодействии сигналов в физическом пространстве сигналов со свойствами решетки выполняются информационные соотношения (30).

8. При аддитивном взаимодействии сигналов в физическом пространстве сигналов со свойствами линейного пространства выполняются информационные соотношения (32).

9. Зависимости 1,3, определяемые равенствами (28/1), (32/1), устанавливают верхний и нижний теоретические пределы соответственно, которые ограничивают информационные соотношения между сигналами, взаимодействующими в пространствах сигналов с различными алгебраическими свойствами.

10. Информационное пространство сигналов является на сегодняшний день пока лишь абстрактным понятием, позволяющим оценивать потенциально возможные информационные соотношения между сигналами, взаимодействующими в реальном физическом пространстве сигналов. Между тем, если будет найдена физическая среда, в котором взаимодействие сигналов будет обладать свойствами идеального взаимодействия, определенного в работе, то в таком физическом пространстве сигналов будут получены предельно достижимые характеристики качества обработки сигналов. В отличие от пространств сигналов с идеальным взаимодействием сигналов, физическое пространство сигналов со свойствами решетки может быть реализовано уже сегодня. Необходимые предпосылки возможности получения такого пространства сигналов и его взаимосвязи с линейным пространством сигналов заданы уравнениями [14; §XIII.3; (14)], [14; §XIII.4; (22)].

Литература

1. Амиантов И.Н. Избранные вопросы статистической теории связи / И.Н. Амиантов. – М.: Сов. Радио, 1971. – 416 с.
2. Миддлтон Д. Введение в статистическую теорию связи. Том 1. / Д. Миддлтон. – М.: Сов. радио, 1961. – 782 с.
3. Френкс Л. Теория сигналов / Л. Френкс. – М.: Сов. радио, 1974. – 344 с.

4. Сосулин Ю.Г. Теория обнаружения и оценивания стохастических сигналов / Ю.Г. Сосулин. – М.: Сов. радио, 1978. – 320 с.

5. Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М.: Радио и связь, 1989. – 656 с.

6. Теория обнаружения сигналов / [П.С. Акимов, П.А. Бакут, В.А. Богданович и др.] ; под ред. П.А. Бакута. – М.: Радио и связь, 1984. – 440 с.

7. Тихонов В.И. Статистический анализ и синтез радиотехнических устройств и систем / В.И. Тихонов, В.Н. Харисов. – М.: Радио и связь, 1991. – 608 с.

8. Шеннон К. Математическая теория связи // В кн. «Работы по теории информации и кибернетике». – С. 243-332. / К. Шеннон. – М.: ИИЛ, 1963. – 832 с.

9. Попов А.А. Информационные соотношения между элементами пространства сигналов, построенного на обобщенной булевой алгебре с мерой / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2007. – Т.5, № 2. – С.175-184.

10. Попов А.А. Вероятностно-статистические и информационные характеристики случайных процессов, инвариантные относительно группы взаимнооднозначных функциональных преобразований / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2007. – Т.5, № 1. – С. 52-62.

11. Попов А.А. Мера количества информации в пространстве сигналов, построенном на обобщенной булевой алгебре с мерой / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2007. – Т.5, № 3. – С.253-261.

12. Сикорский Р. Булевы алгебры / Р. Сикорский. – М.: Мир, 1969. – 376 с.

13. Общая алгебра. Т. 2 / [В.А. Артамонов, В.Н. Салий, Л.А. Скорняков и др.]; под общ. ред. Л.А. Скорнякова. – М.: Наука, 1991. – 480 с.

14. Биркгоф Г. Теория решеток / Г. Биркгоф. – М.: Наука, 1984. – 568 с.

15. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

16. Попов А.А. Инварианты групп отображений мгновенных значений случайных сигналов в метрическом пространстве со свойствами *L*-группы / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2013. – № 1. – С.28-38.

17. Харкевич А.А. Борьба с помехами / А.А. Харкевич. – М.: Наука, 1965. – 276 с.

УДК 681.3.067

Яремчук Ю.Є., к.т.н. (*Вінницький національний технічний університет*)

ОЦІНЮВАННЯ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ПРОТОКОЛІВ ШИФРУВАННЯ БЕЗ ПОПЕРЕДНЬОГО РОЗПОДІЛУ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Яремчук Ю.Є. Оцінювання обчислювальної складності протоколів шифрування без попереднього розподілу ключів на основі рекурентних послідовностей. В даній роботі проведено оцінювання обчислювальної складності протоколу шифрування інформації без попереднього розподілу ключів на основі V_k- та U_k-послідовностей і отримано його мінімальні та максимальні оцінки складності. Проведено порівняння отриманих оцінок з оцінками складності відомого протоколу шифрування без попереднього розподілу ключів Шаміра. Результати порівняння показали, що протокол шифрування на основі рекурентних послідовностей має меншу складність обчислень для будь-якого k, причому не менше ніж у 100 разів і при цьому забезпечує достатній рівень криптостійкості.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, КРИПТОГРАФІЯ, ШИФРУВАННЯ, РОЗПОДІЛ КЛЮЧІВ, ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ АЛГОРИТМІВ, РЕКУРЕНТНІ ПОСЛІДОВНОСТІ

Яремчук Ю.Е. Оценивание вычислительной сложности протоколов шифрования без предварительного распределения ключей на основе рекуррентных последовательностей. В данной работе