К ВОПРОСУ ОЦЕНИВАНИЯ ЭНТРОПИИ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лившиц И.И.[1], Неклюдов А.В.[2]

Для создания современных систем обеспечения информационной безопасности важно обеспечить «баланс интересов» различных компонентов, определяющих устойчивость функционирования защищаемых активов различных типов. Для решения данной задачи могут применяться различные методики, которые подразумевают получение оценки энтропии информационных систем. Однако в настоящее время не создано единого подхода к расчету энтропии для информационных систем, что не позволяет в должной мере реализовать безопасное функционирование систем безопасности в общем и систем обеспечения информационной безопасности в частности. В данном исследовании предпринята попытка анализа систем обеспечения информационной безопасности с позиции определения полной энтропии информационной системы. Учтены показатели систем аудитов ИБ как «системной оболочки». Представлен пример оценки диссипативных систем в терминах термодинамической теории И. Пригожина. Показана возможность рассмотрения современных систем обеспечения информационной безопасности как диссипативных систем, у которых компонента «производства энтропии» отрицательна на продолжающейся вправо шкале.

Ключевые слова: *система управления, интегрированная система менеджмента; информационная система; энтропия, диссипативная система; информационная безопасность.*

DOI: 10.21681/2311-3456-2017-5-30-41

Введение

При создании современных систем обеспечения информационной безопасности (СОИБ) представляется важным обеспечение не только заданных технологических режимов и параметров контроля объектов (в данном случае информационных систем – ИС), но и достижение цели устойчивого безопасного функционирования ИС в составе сложного промышленного объекта (СлПО). Применительно к специфике объекта ИС особое значение приобретает не только обеспечение устойчивости, но и проблема обеспечения информационной безопасности (ИБ). Расширенное понятия ИБ (не ограниченное только «классической триадой» конфиденциальности, целостности и доступности в терминах ISO серии 27001) нашло свое практическое применение и в иных стандартах IEC (серии 61508 и 61511) с позиции обеспечения функциональной безопасности (ФБ). В частности, обеспечение ИБ (security) трактуется как часть более общей задачи – обеспечение ФБ (safety) для СлПО. В данном аспекте постановка задачи сформулирована как разработка подхода к оцениванию энтропии СОИБ.–

Обзор существующих методик

В настоящее время для решения поставленной задачи применяются различные методики, часть из которых подразумевает учет различных компонент – внутренних и внешних подсистем и мониторинг энтропии ИС. Описание существующих подходов приведены в работах Агуреева [1–3], Зеленцова, Потрясаева, Охтилева, Соколова, Юсупова [4 – 7] и ряда зарубежных ученых [8–10].

В работе [4] отмечается, что «*в современных условиях характерным требованием, предъявляемым к процессам управления СТО, является требование оперативности*». Для СлПО применяются расширенные требования к СОИБ, в частности: «*наиболее актуальные задачи СУ с точки зрения их функциональности решаются до сих пор, в большинстве случае, в ручном режиме и с учетом отдельных аспектов функционирования СТО, в том числе – выявление, локализация и ликвидация сбоев, отказов*…». В работе [5] подтверждается, что «*мониторинг, прогнозирование и управление СлО на практике автоматизировано лишь частично*» и что «*операторам предоставляется информация, в лучшем случае, лишь частично о состоянии элементов, но не объектов контроля в целом*». Дополнительно отмечается важность обеспечения безопасности как «*катастрофоустойчивости*». Соответственно, задача обеспечения безопасности СлПО в целом решается и с учетом требований ФБ (safety).

В современных риск-ориентированных стандартах (например, ISO серии 27001, 22301, 55001,

1 Лившиц Илья Иосифович, доцент, кандидат технических наук, Университет ИТМО, г. Санкт-Петербург, Россия. E-mail: Livshitz.il@yandex.ru

2 Неклюдов Андрей, ведущий инженер, ООО «Газинформсервис», г. Санкт-Петербург, Россия. E-mail: nav7ad@mail.ru

9001) введен специальный термин, описывающий влияние внутренних и внешних компонентов – «контекст». В известных работах поддерживается тезис, что «*мониторинг энтропии в информационной системе целесообразен для поддержания устойчивой работы*», в частности, в работе Андриановой [11]. В работе Кудж [12] поясняется, что, в частности «*математическую теорию Шеннона, написанную в 1948, нельзя в современных условиях считать адекватной теорией информации*». В работах Игонина [13, 14] представлен тезис, что «*в процессе объединения отдельных наук актуальны вопросы создания критериев комплексной оценки при проявлении кризисов различного рода (катаклизмов)*», и авторы полагают одной из основных целей создания современных СОИБ как раз противодействие таким «кризисам». Также в ряде изданий отмечается, что «*энтропия в информационных системах имеет физический смысл и может быть рассчитана и измерена косвенными методами*» [11, 12, 15, 16].

Рассмотрим кратко требования стандарта IEC 61508, в котором отмечается: «*компьютерные системы (обычно называемые программируемыми электронными системами), применяемые во всех прикладных отраслях для выполнения функций, не связанных с безопасностью, во все более увеличивающихся объемах используются для выполнения функций обеспечения безопасности*». Далее даются уточнения по применению в СлПО в тех случаях, «*когда одна или несколько таких систем включают в себя электрические, электронные, программируемые электронные элементы*» (п. 1.2 а) и/или «*требует рассмотрения злонамеренных и непредусмотренных действий во время анализа отказов и рисков. Сфера анализа включает в себя все стадии жизненного цикла системы безопасности*» (п. 1.2 k). В стандарте IEC 61511 отмечено, что «*в большинстве ситуаций безопасность лучше всего может быть достигнута с помощью проектирования безопасного в своей основе процесса. При необходимости он может быть дополнен системами защиты или системами, с помощью которых достигается любой установленный остаточный риск*». Отдельно подчеркивается, что учитываются требования по проектированию, эксплуатации и техническому обслуживанию систем безопасности в области промышленных процессов различных отраслей, включая химическую, нефтеперерабатывающую, нефтегазодобывающую, неядерную энергетику (п. 1.2. e). Далее под открытой системой понимается СОИБ, в состав которой входят ИС, для которых необходимо обеспечение ИБ, в том числе – обеспечение ФБ (в терминах [12, 13, 17]). Однако в ряде публикаций отмечается, что в ИС диссипация (рассеяние информации) в «чистом виде» не существует [11, 16]. Этот факт может означать, что в настоящее время «чистые» ИС не рассматриваются с должным вниманием к протекающим процессам, в том числе – с точки зрения обеспечения безопасности (как ФБ (safety), так и ИБ (security), в частности). Соответственно, для СОИБ в настоящее время не предложено описание потоков энергии и уравнения полной энергии, в том числе с учетом диссипативного характера.

Формирование пространства состояний для открытых систем

Современный этап развития теории управления включает в себя не только моделирование физических аспектов функционирования СОИБ (насколько это необходимо для создания адекватной модели), но и учет экономических факторов. Вторая (экономическая) часть СОИБ необходима для учета внешних аспектов любой открытой системы и разнородной структуры требований. Влияние указанных аспектов позволяет осуществить учет как внешних аспектов открытой системы, так и разнородной структуры требований безопасности. Отметим, что в работе [6] дано полезное уточнение: «*под средой понимается не физическое окружение объектов, а абстрактная модель совокупности факторов, о которых у нас нет достоверной информации*» и далее: «*если неопределенные факторы удается описать в виде случайных величин (в нашем случае можно говорить о переменных), с известной функцией распределения, то говорят, что возмущающие действия статистически распределены*».

Заметим, что аналогичный подход с 2012 г. изложен во всех риск-ориентированных стандартах, в которых в явном виде требуется определить «контекст» («*context*»). На основании этого базового требования представляется возможным не «пересчитывать» полностью все множество свойств технических систем («*СТС*» в нотации [6]), как «*неизученные и/или неизвестные ранее*». Применение современных риск-ориентированных стандартов позволяет обеспечить за счет гибких обратных связей (в частности – процессов аудита ИБ) оптимальное управление и пересчет векторов оптимального управления как «*изучающего приращения управления*» (в нотации [6]) для корректировки более точной модели в данном конкретном случае представляется избыточными.

Формирование интегральной оценки диссипативных систем

В работах Аюрова [17, 18] отмечается, что функционирование диссипативных систем всегда связано с преобразованием в них энергии, и это преобразование предполагает наличие взаимодействия диссипативной системы с окружающими ее объектами реального «внешнего» мира. В этой связи авторами предложен подход, при котором второй компонент диссипативной системы рассматривается как оценка системы формирования добавленной стоимости для СОИБ. В литературе по теории качества часто применяется схожее понятие «добавленная стоимость аудита». В данном случае авторы предлагают учитывать метрику «добротности функционирования» для оценки в рамках СОИБ. В данное понятие вкладывается следующий смысл: чем выше уровень «качества преобразования» энергии в СОИБ и чем ниже уровень собственных потерь такой СОИБ, тем выше «*качество функционирования*» [11]. Авторы вкладывают в базовый термин «потерь» Андрианова дополнительно потери от инцидентов ИБ, оказавших негативное влияние на функционирование СлПО.

В работах [4-10, 11, 18] отмечается, что реальные условия функционирования диссипативных систем таковы, что они все имеют в своем составе соответствующие «системные оболочки». Это положение авторы полагают безусловно верным, иначе говорить об управляющих воздействиях на СлПО и обеспечении ИБ для объекта во внешней среде не приходится. Рассмотрим благоприятные условия функционирования СОИБ, поскольку ее структура, состав функций, режимы работы и прочее не могут быть постоянны во времени (для неконсервативных систем), а должны оптимизироваться [1, 15, 19]. Соответственно, владелец СлПО вправе ожидать, что при достижении целей управления, «системная оболочка» обеспечит снижение затрат на свое собственное функционирование, не повышая значимость рисков управления в аспекте ИБ (см. рисунок 1 – в пределах контура ИСМ и внутреннего интерфейса).

В предложенной модели ИСМ (см. рисунок 1) в «системной оболочке» предусмотрена реализация важнейшего преимущества всех современных риск-ориентированных стандартов – управление рисками. В практическом аспекте это означает, что под контроль ИСМ попадают (и соответственно, должны быть компенсированы определенными мерами и средствами обеспечения ИБ) риски ИБ ([20],[21]).

На основании общего подхода, предложенного в [11], применим специальную метрику Q – «инте-

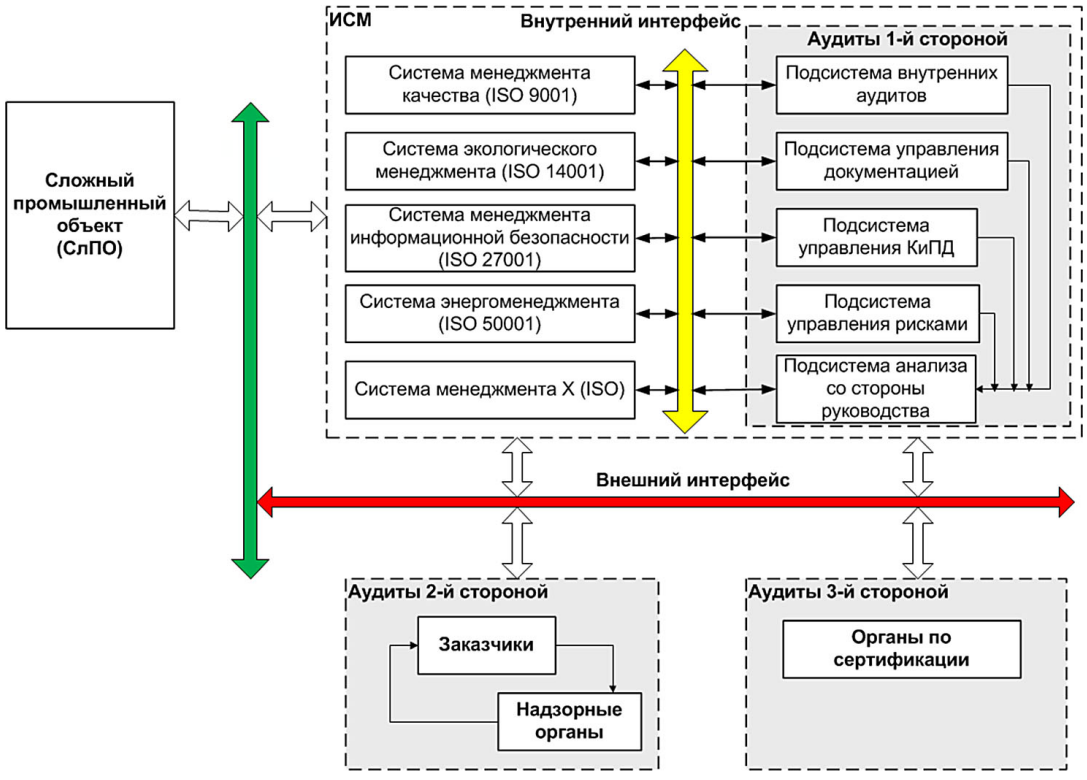

***Рис.1** – Базовая модель аудитов ИСМ*

гральную добротность функционирования», которую определим для решения поставленной задачи следующим образом:

$$Q = \frac{dK_{ext}}{dt} / \frac{dK_{int}}{dt}, \quad (1)$$

где: $\frac{dK_{ext}}{dt}$ – компонент, характеризующий изменение внешнего поведения системы (внешние аспекты контекста, $\frac{dK_{int}}{dt}$ – компонент, характеризующий изменение «системной оболочки» (внутренние аспекты контекста). В работах Игонина отмечается, что трактовка ИС как диссипативной системы требует специально организованных процессов, и важно, что «*организованная техническая система является человекомерной*» [13, 14]. Соответственно, на этом множестве требований возможно описать внешнее поведение системы (СлПО), как показано на общей модели ИСМ для обеспечения безопасности СлПО и оценить первый компонент формулы (1): $\frac{dK_{ext}}{dt}$.

В экономическом аспекте Q показывает соотношение затрат двух основных компонент, в том числе косвенно учитывается и «зрелость системной оболочки» как системы обеспечения ИБ. Необходимо подчеркнуть, что изменение компонентов, характеризующих «системную оболочку», может быть равно нулю, а внешние изменения остаются значимыми. В практике управления СлПО это может означать различные ситуации, в частности, при изменении вектора внешних воздействий СОИБ, ЛПР может увеличить издержки на внутренний компонент – на «системную оболочку», что, в свою очередь, снизит рентабельность функционирования объекта управления.

Часто на практике наблюдается ситуация, когда ЛПР жестко ограничивает затраты на «системную оболочку» (ИСМ), что приводит к парированию только определенных выборочных требований регуляторов (см. рисунок 1) [20, 21, 22]. Например, по оценкам авторов, такая ситуация наблюдается для объектов критической инфраструктуры при реализации только мер защиты из набора, рекомендованного ФСТЭК России (Приказ № 31, приложение № 2 или NIST SP 800). Также наблюдается и обратная ситуация: при стабилизации внешних воздействий (на практике – «положительный риск» в терминах ISO), ЛПР не стремится оперативно снизить издержки на «системную оболочку» (ИСМ), что приводит к «запаздыванию» реакции СОИБ, дисбалансу затрат и не позволяет управлять полной энтропией системы с требуемой оперативностью. Это также означает, что добиться отрицательного значения энтропии по вкладам всех компонент для выполнения условия диссипативной системы не удается.

Пример расчета интегральной добротности функционирования

Рассмотрим пример расчета Q (в нотации [11]) на основании формулы (1) как отношение двух основных количественных метрик – внешней (как количество выявленных несоответствий N_{ext}) и внутренней (как размер затрат на механизм внутренних аудитов ИБ в «системной оболочке» S_{int}). Таким образом, Q для СОИБ приобретает новый вид (с учетом, соответственно, замены и подстановки N_{ext} и S_{int}):

$$Q = \frac{dN_{ext}}{dt} / \frac{dS_{int}}{dt}, \quad (2)$$

Рассмотрим пример «А», для которого наблюдается снижение в течение года количества несоответствий N_{ext} и также наблюдается существенное снижение затрат S_{int} на обеспечение аудитов ИБ в ИСМ. Мониторинг СОИБ выполняется ежеквартально, результаты приведены в таблице 1. Совокупные затраты S по варианту «А» составят 300 условных единиц.

Графическое представление компонент расчета интегральной добротности функционирования системы Q_A по варианту «А» приведено на рисунке 2.

Рассмотрим пример «Б», для которого также наблюдается снижение в течение года количества несоответствий и незначительное постоянное снижение затрат на обеспечение аудитов ИБ в ИСМ. Мониторинг СОИБ выполняется ежеквартально, результаты приведены в таблице 2. Сово-

Таблица 1.

Расчет интегральной добротности функционирования (вариант «А»)

Период, T	Количество несоответствий, N_{ext}	$\frac{dN_{ext}}{dt}$	Затраты на аудит, S_{int}	$\frac{dS_{int}}{dt}$	$Q = dN_{ext} / dS_{int}$
1	14	-6	100	-10	0,600
2	8	-3	90	-20	0,150
3	5	-1	70	-30	0,033
4	4	-1	40	-40	0,025

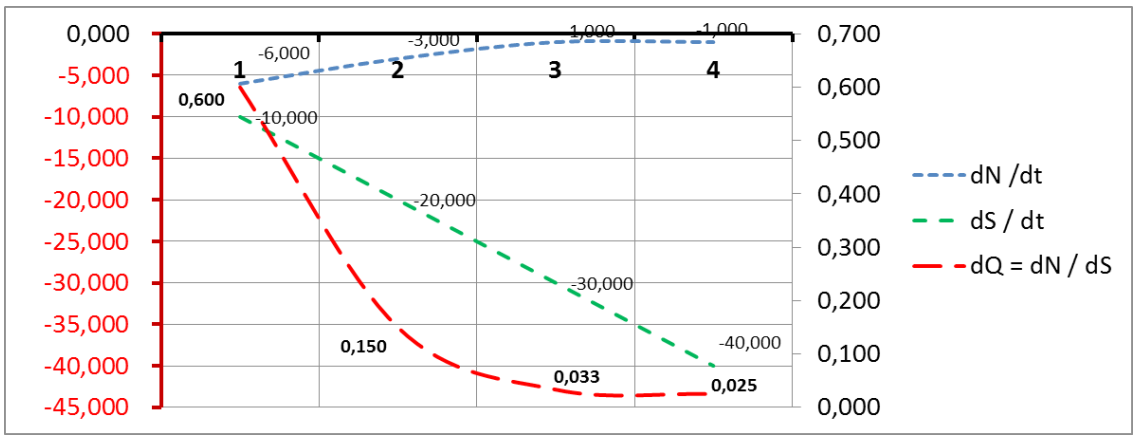

***Рис. 2** – Интегральная добротность функционирования (по варианту «А»)*

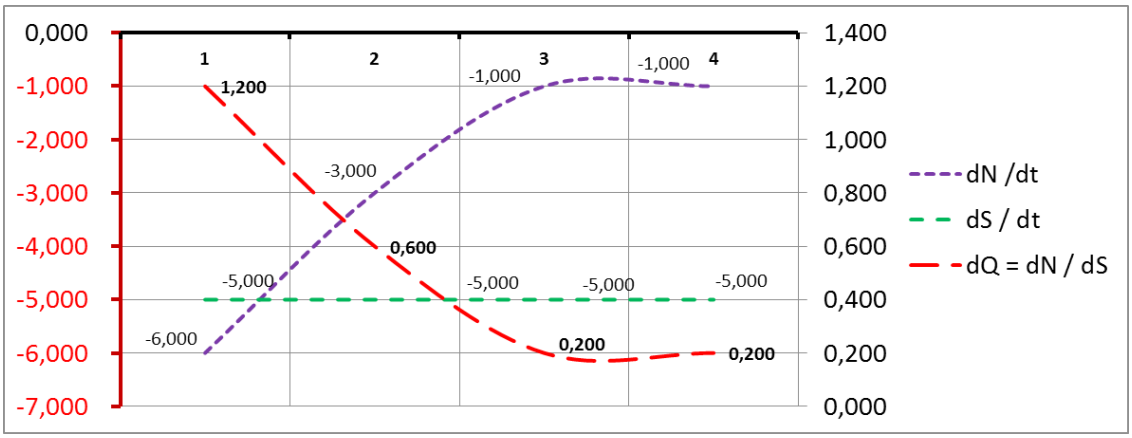

***Рис. 3** – Интегральная добротность функционирования (по варианту «Б»)*

купные затраты S по варианту «Б» составят 450 условных единиц.

Графическое представление компонент интегральной добротности функционирования системы Q_B по варианту «Б» приведено на рисунке 3.

Обратим внимание на соотношение Q_A и Q_B при одном и том же значении dN_{ext} и различных значениях dS_{int}. Как видно из рисунка 2 и рисунка 3, в случае для варианта «А» значение интегральной добротности функционирования Q_A при одном и том же значении dN_{ext} в каждой точке расчета Т значительно ниже Q_B:

$$\frac{dS_{int\,A}}{dt} < \frac{dS_{int\,B}}{dt} <=> Qa < Qb$$

То есть компонента «системной оболочки», обеспечивающая в модели ИСМ практический механизм внутренних аудитов ИБ (рисунок 2), в варианте «А» требовала значительно меньших затрат, чем в варианте «Б», «обходилась дешевле» при выполнении сопоставимой аналогичной «внешней работы» СОИБ (300 условных единиц против 450). Авторы полагают, что в качестве параметров, непосредственно влияющих на Q, ЛПР могут быть дополнительно приняты также:

1. Коэффициенты изменения затрат на «системную оболочку»;
2. Коэффициенты изменения рисков ИБ;
3. Коэффициенты изменения стоимости надзорных аудитов ИБ;

Таблица 2.

Расчет интегральной добротности функционирования (вариант «Б»)

Период, Т	Количество несоответствий, N_{ext}	$\frac{dN_{ext}}{dt}$	Затраты на аудит, S_{int}	$\frac{dS_{int}}{dt}$	$Q = dN_{ext} / dS_{int}$
1	14	-6	100	-5	1,200
2	8	-3	95	-5	0,600
3	5	-1	90	-5	0,200
4	4	-1	85	-5	0,200

4. Коэффициенты изменения требований отраслевых регуляторов.

Расчет энтропии в сложных системах

Более подробно остановимся на диссипативных системах, для которых, согласно работам И. Пригожина, характерно убывание энтропии [23]. Очевидно, что СОИБ могут быть отнесены к типу «открытых систем», так как любые СОИБ создаются для удовлетворения определенных потребностей ЛПР, принимают запросы (входные данные) и выдают управляющие воздействия (результаты). Соответственно, для обеспечения устойчивости безопасного управления (safety) для СлПО важно оценить существующий порядок внутренних процессов. В открытых системах, при установившемся обмене с внешней средой, изменение энтропии представляется в виде суммы двух компонентов, первый из которых определяет происходящие внешние процессы (поток энтропии), а второй обусловлен внутренними системными процессами (производство энтропии) [11, 16]:

$$\frac{dS}{dt} = \frac{dS_1}{dt} + \frac{dS_2}{dt}, \quad (3)$$

где: $\frac{dS_1}{dt}$ – поток энтропии, $\frac{dS_2}{dt}$ – производство энтропии.

В ряде работ отмечается, что для открытых систем значение энтропии может быть любого знака, несмотря на то, первый компонент может быть больше или равен нулю, а второй компонент может принимать значения как меньше, так и больше нуля [11, 16, 23]. Соответственно, в открытых системах (под которыми авторы понимают и СОИБ) за счет второго компонента общее изменение энтропии может быть отрицательным. Ситуация, при которой общее изменение энтропии в открытой системе меньше нуля, характеризует «диссипативную структуру» в терминологии И. Пригожина [23]. Такую ситуацию ЛПР необходимо дополнительно анализировать, чтобы понять причины и обеспечить условия уменьшения «хаоса» в реальных СОИБ (security). В частности, необходимо специфицировать безопасные и устойчивые рабочие режимы, которые позволяют обеспечить СОИБ (security) на практике требуемый уровень безопасности для СлПО в целом (safety).

Именно целостность ИСМ позволяет реализовать общую задачу обеспечения ФБ (и ИБ в том числе) для СлПО. Мониторинг изменения энтропии необходим и целесообразен для поддержания устойчивости СОИБ на контролируемом временном интервале. В работе Андриановой ([11]) дается уточнение, что в математической литературе самостоятельно термин «диссипация» используется достаточно редко и обычно используется понятие «диссипативная система» (в частности у Пригожина [23]). На основании [11] определим диссипативную систему как:

$$\frac{d\bar{y}}{dt} = \bar{f}\,(t, y),$$

в том случае, если все решения $\bar{y}\,(t, t_0, \bar{y}_0)$ бесконечно продолжаемы вправо и существует $R > 0$ такое что:

$$\overline{lim}_{t\to 0} \;\; || \bar{y}(t, t_0, \bar{y}_0) || < R \quad (4)$$

и для каждого решения $\bar{y}\,(t, t_0, \bar{y}_0)$ существует такой момент времени $t_1 = t_0 + T\,(t_0,\ \bar{y}_0) \geq t_0$, после которого выполняется $||\ y\ || < R$ или $|| \bar{y}(t, t_0, \bar{y}_0) || < R$ при $t_1 \leq t < \infty$. [15, 28].

В работе Андриановой ([11]) отмечается, что примера *«чистого рассеивания» информации, аналогичного рассеиванию энергии в физических системах, в ИС найти не удается»*. Также приводится пример, что при дословном простейшем толковании данного понятия применительно к программным (банковским) системам «диссипация» может означать простое исчезновения (уничтожение) записей о банковских операциях. Для СОИБ рассмотрим примеры «негативного преобразования информации», конкретно: необратимого чистого рассеивания информации. Хотя авторы и признают разумность приведенного выше примера с банковским ПО, тем не менее, известны и иные решения, подтверждающие применимость данного понятия в аспекте ФБ (safety), например, разработка программных систем по методике SDL (Security Development Lifecycle) и пр.

Рассмотрим простую модель СОИБ, в которой, допустим, внутреннее состояние ИБ описывается двумя параметрами: N (количество несоответствий) и S (затраты на аудит). Также допустим, что эти два параметра отражаются в двумерном (фазовом) пространстве. На основании уравнения (3) рассмотрим два параметра, которые позволят описать изменение энтропии в реальной открытой системе в виде суммы двух компонент: N (поток энтропии за счет изменения количества несоответствий) и S (производство энтропии за счет затрат на аудит ИБ). Рассмотрим два варианта поведения модели СОИБ в аспекте ФБ. В варианте «А» наблюдается стабильное снижение количества несоответствий (поток энтропии N снижается) и значительный рост затрат на поддержание данного состояния ИБ (производство энтропии S повышается). Общий результат – пол-

Таблица 3.
Расчет энтропии СОИБ по варианту «А»

Время, T	Кол-во н/с, ***N***	D_{int} = d***N***/dt	Затраты на аудит, ***S***	D_{ext} = d***S***/dt	Q = D_{ext} + D_{int}
1	14	-2	100	5	3
2	12	-3	105	10	7
3	9	-4	115	15	11
4	5	-5	130	20	15

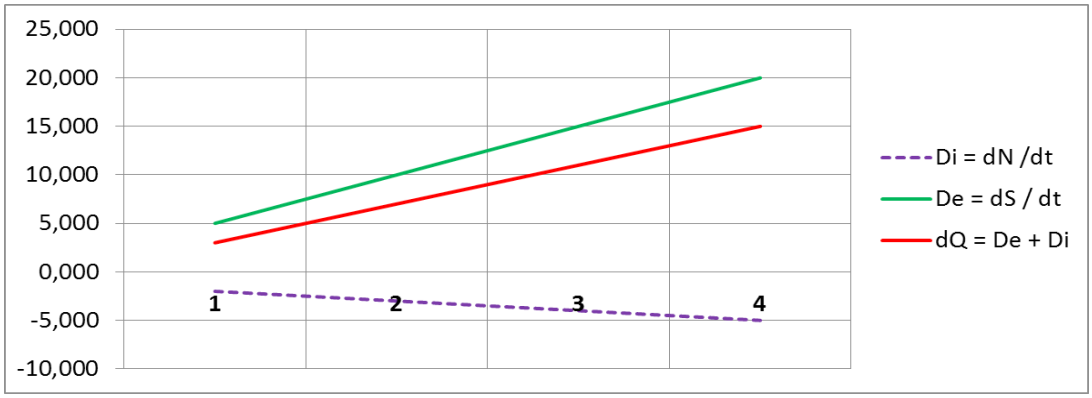

Рис. 4 *– Результаты расчета энтропии СОИБ по варианту «А»*

ная энтропия СОИБ возрастает (таблица 3). Такая ситуация имеет место на практике, когда в рамках различных несогласованных действий наблюдается «рассогласование» по векторам управления ИБ в ИСМ [11, 21].

Графическое представление результатов расчета энтропии СОИБ по варианту «А» приведено на рисунке 4.

В варианте «Б» наблюдается также стабильное снижение количества несоответствий (поток энтропии *N* снижается) и неравномерное снижение затрат на поддержание данного состояния ИБ (производство энтропии *S* снижается). Общий результат – полная энтропия системы снижается (таблица 4).

Графическое представление результатов расчета энтропии СОИБ по варианту «Б» приведено на рисунке 5.

Таблица 4.
Расчет энтропии СОИБ по варианту «Б»

Время, T	Кол-во н/с, ***N***	D_{int} = d***N***/dt	Затраты на аудит, ***S***	D_{ext} = d***S***/dt	Q = D_{ext} + D_{int}
1	14	-2	100	-5	-7
2	12	-3	95	-10	-13
3	9	-4	85	-15	-19
4	5	-5	70	-20	-25

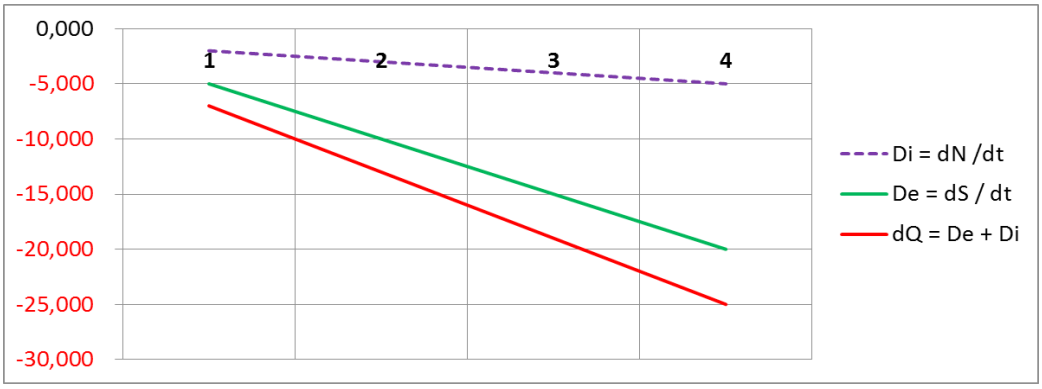

Рис. 5 *– Результаты расчета энтропии СОИБ по варианту «Б»*

В примере «А» показано, что первый компонент показывает отрицательную динамику, что достаточно часто наблюдается для реально функционирующих СОИБ. В тоже время следует заметить, что $D_{int} = 0$ означает полное отсутствие несоответствий внутри любой реальной СОИБ, и что, по мнению авторов, на практике маловероятно. Второй компонент в примере «А» D_{ext} демонстрирует увеличение затрат на поддержание целостности и устойчивости СОИБ, в частном случае – затраты на выполнение функции аудита ИБ (что представляется нерациональным, так как количество несоответствий все же снижается). Поскольку $D_{ext} > 0$ и $D_{ext} > D_{int}$, в примере «А» общая энтропия СОИБ $Q > 0$.

В примере «Б» показано, что D_{int}, также как в примере «А», демонстрирует отрицательную динамику (наблюдается снижение количества несоответствий). В тоже время D_{ext} отражает снижение затрат на выполнение функции аудита ИБ, что может иметь место в зрелых СОИБ, в которых эффективно действуют различные контуры обратной связи и оптимизации (рисунок 1). Поскольку и $D_{ext} < 0$ и $D_{int} < 0$, в примере «Б» обеспечивается общая энтропия СОИБ $Q < 0$. В соответствии с формулой (3) и условием (4) это характеризует диссипативную систему, имеющую практическую реализацию при наличии «зрелой» СОИБ.

Сопоставление полученных результатов оценки энтропии

Представляет определенный интерес сопоставление полученных авторами выше результатов при расчете энтропийных характеристик СОИБ (вариант «А» и «Б») с результатами, полученными в рамках классических подходов по расчету информационно-энтропийной меры (например, Шеннона) в рамках вероятностного подхода. Однако это сопоставление может быть применимо только при возможности выявлении несоответствий в СОИБ СлПО, и в частности, не применимо для анализа систематических отказов (например, вызванных ошибками проектирования), т.е., не имеющих вероятностной меры.

Известно, что задача максимизации «интегральной добротности» системы может быть сведена к оцениванию ее энтропии [24]. Энтропия в этом случае связана с распределением вероятностей количества несоответствий в системе (например, Шеннона):

$$S = -\sum_{j=1}^{n} P_j \log P_j, \quad (5)$$

где j – номер несоответствия, а $P_j(r_j)$ – вероятность появления несоответствия, которую можно вычислить из накопленной (апостериорной) статистики. Однако на практике затруднительно получить достоверное распределение вероятности появления того или иного конкретного несоответствия (отказа) для СлПО (см. IEC 61508 и IEC 61511). В частном случае, если принять, что все события отказов равновероятны, возможно рассмотреть зависимость только от количества несоответствий и затрат на обеспечение аудитов.

Этот тезис также дополнительно подтверждается и требованиями стандартов в области ФБ (safety), в частности:

- Интенсивность опасных отказов для СОИБ должна быть подтверждена анализом надежности, выполненным с использованием признанной процедуры или данными по надежности из промышленной базы данных по оборудованию (например, IEC 61508, п. 7.5.2.6 a);
- СОИБ должна быть независимой от иных (исполнительных) систем, связанных с безопасностью, и других средств снижения риска (например, IEC 61508, п. 7.5.2.6 d);
- Для систем с тяжелым последствиям в случае отказа должны быть приняты особые меры предосторожности по отношению к маловероятным событиям по общей причине, например, авиационным катастрофам или землетрясениям (например, IEC 61508, п. 7.6.2.7).

В этом случае формула (5) значительно упрощается и совпадает с формулой Хартли [25]:

$$H = \log_2 N \quad (6)$$

где N – количество несоответствий.

Таким образом, для различных состояний СлПО между оценками энтропии в представлениях Хартли и Шеннона существуют тесные связи, которые указывают на сходство данных величин между собой [25]. В свою очередь, частные виды информационной энтропии могут быть представлены в определенной реализации на практике как в форме (5), так и в форме (6).

Рассмотрим известные ранее варианты «А» и «Б», в которых энтропия представлена дополнительно формулой Хартли. При увеличении затрат на поддержание ИБ происходит снижение энтропии Q за счет, прежде всего, явного уменьшения количества несоответствий D_{int} (см. таблицу 5 и таблицу 6 соответственно).

Графическое представление результатов рас-

Таблица 5.
Расчет энтропии СОИБ по варианту «А» (Хартли)

Время, T	Кол-во н/с, ***N***	D_{int} = d***N***/dt	D_{int} (по Хартли)	Затраты на аудит, ***S***	D_{ext} = d***S***/dt	D_{ext} (по Хартли)	Q = D_{ext} + D_{int}	Q = D_{ext} + D_{int} (по Хартли)
1	14	-2	3,81	100	5	6,64	3	10,45
2	12	-3	3,58	105	10	6,71	7	10,30
3	9	-4	3,17	115	15	6,85	11	10,02
4	5	-5	2,32	130	20	7,02	15	9,34

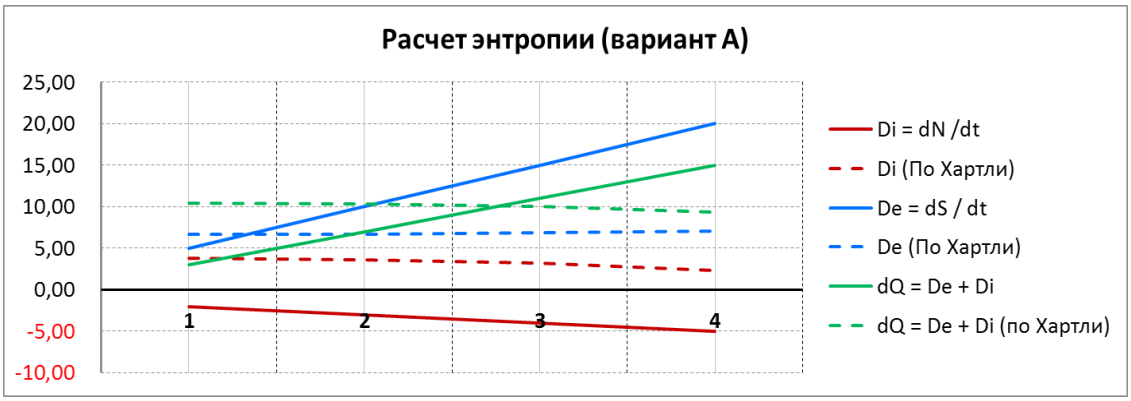

Рис. 6 *– Результаты расчета энтропии СОИБ по варианту «А» (Хартли)*

чета энтропии СОИБ по варианту «А» (Хартли) приведено на рисунке 6.

Графическое представление результатов расчета энтропии СОИБ по варианту «Б» (Хартли) приведено на рисунке 7.

Как видно из полученных результатов, в зависимости от состояния СлПО, можно обосновать принцип применения расчета энтропии и сопоставить различные виды расчета энтропии СОИБ. Однако предложенная авторами методика оце-

Таблица 6.
Расчет энтропии СОИБ по варианту «Б» (Хартли)

Время, T	Кол-во н/с, ***N***	D_{int} = d***N***/dt	D_{int} (по Хартли)	Затраты на аудит, ***S***	D_{ext} = d***S***/dt	D_{ext} (по Хартли)	Q = D_{ext} + D_{int}	Q = D_{ext} + D_{int} (по Хартли
1	14	-2	3,81	100	-5	6,64	-7	10,45
2	12	-3	3,58	95	-10	6,57	-13	10,15
3	9	-4	3,17	85	-15	6,41	-19	9,58
4	5	-5	2,32	70	-20	6,13	-25	8,45

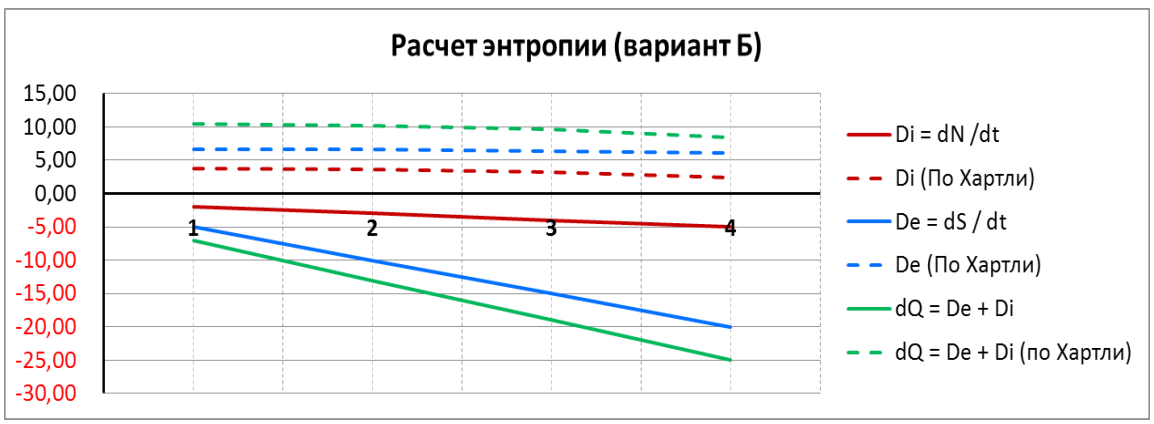

Рис. 7 *– Результаты расчета энтропии СОИБ по варианту «Б» (Хартли)*

нивания энтропии в СОИБ представляется более предпочтительной, поскольку демонстрирует результаты более точной оценки динамики изменения различных компонент СОИБ. В частности, применение «классической» информационно-энтропийной меры Шеннона (5) и формулы Хартли (6) предоставляет ЛПР менее качественный анализ. Это можно объяснить тем, что меры Шеннона и Хартли основаны на функции логарифма, а не оценки динамики приращений, что не всегда удобно для практического применения на всем диапазоне возможных аргументов конкретных СОИБ (например, при общем числе несоответствий ИСМ менее 50).

Вывод

На основании учета различных аспектов различной природы предложен подход к формированию оценки энтропии в СОИБ. Показана возможность рассмотрения современных СОИБ как диссипативных систем с целью достижения устойчивого функционирования и обеспечения требуемого уровня ИБ для СлПО.

***Рецензент**: Молдовян Александр Андреевич, доктор технических наук, профессор, заведующий научно-исследовательским отделом проблем информационной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук», Санкт-Петербург, Россия. E-mail: maa1305@yandex.ru*

Литература

1. Агуреев И.Е., Денисов М.В. Математическое описание динамики пассажирских транспортных систем // Мир транспорта и технологических машин. 2011. Вып. 1. С. 15-22.
2. Агуреев И.Е., Богма А.Е., Пышный В.А. Динамическая модель транспортной макросистемы // ИзвестияТулГУ. Технические науки. 2013. Вып. 6. Ч. 2. С. 139-145.
3. Агуреев И.Е., Гладышев А.В. Динамика производства и спроса в диссипативной модели логистической системы // ИзвестияТулГУ. Технические науки. 2013. Вып. 6. Ч. 2. С. 152-160.
4. Охтилев М.Ю., Соколов Б.В Новые информационные технологии мониторинга и управления состояниями сложных технических объектов в реальном масштабе времени //Труды СПИИРАН. – 2005. – Вып. 2. – т. 2 – С. 249 – 265.
5. Охтилев М.Ю., Соколов Б.В, Юсупов Р.М. Теоретические и технологические основы концепции проактивного мониторинга и управления сложными объектами // Известия ЮФУ. Технические науки. 2015. – № 1. – С. 162 – 174
6. Соколов Б.В., Потрясаев С.А., Малышева И.В., Назаров Д.И. Алгоритм адаптации моделей управления структурной динамикой сложной технической системы к воздействию возмущающих факторов // Всероссийская научная конференция по проблемам управления в технических системах. – 2015. – № 1. – С. 3-6.
7. Бураков В.В., Зеленцов В.А., Потрясаев С.А., Соколов Б.В. Оценивание и выбор перспективных технологий автоматизированного управления активными подвижными объектами на основе комплексного моделирования // Доклады ТУСУР № 3 (34) 2014. – С. 155 – 165
8. Baumgarte J. Stabilization of constraints and integrals of motion in dynamical systems // Comp. Math. Appl. Mech. Eng. 1972. No. 1. P. 1-16.
9. Ascher U.M., Hongsheng Chin, Petzold L.R., Reich S. Stabilization of constrained Mechanical systems with DAEs and invariant manifolds // J. Mechanics of Structures and Machines. 1995. Vol. 23. P. 135-158.
10. Amirouche F. Fundamentals of Multibody Dynamics. Theory and Applications. Birkhauser, Springer, 2005. 684 p.
11. Андрианова Е.Г., Мельников С.В., Раев В.К. Диссипация и энтропия в физических и информационных системах. Фундаментальные исследования. 2015. Вып. 8. С. 233 – 238
12. Кудж С.А., Цветков В.Я. Особенности развития направлений информатики // Перспективы науки и образования. 2013. Вып. 6. С. 11.
13. Игонин В.И. Технологические особенности энергообследования зданий, сооружений и инженерных сетей. // Курс лекций. – Вологда: ВоГТУ. 2012. 104 с.
14. Игонин В.И. Методология научных исследований и научно-техническое развитие «субъекта» // Методическое пособие для магистров. – Вологда. ВоГТУ. 2013. 111с.
15. Шеннон К. Работы по теории информации. – М.: Изд-во иностранной литературы. 1966.88 с.
16. Маркин А.А., Мельников С.В. Философский и естественнонаучный аспекты понятия информационной энтропии // Труды российской научной конференции «Инновационные стратегии развития науки, техники и общества», Минобрнауки РФ, МГТУ МИРЭА. М., 2014. С. 98–102.
17. Аюров В.Д. Круговорот товаров и физика денег. Неделя горняка - 2003. - ГИАБ, Изд-во МГГУ. 2003. Вып. 5. с. 90
18. Аюров В.Д. Синергетика экономики. М.: Изд-во МГГУ. 2005. 124 с.: ил.
19. Лившиц И.И. Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22–34.
20. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. 2014. Вып. 6. С. 72–94.
21. Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. 2015. Вып. 3. С. 10-15.

22. Лившиц И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. 2015. Вып. 6. С. 272 – 300.
23. Пригожин И., Гленсдорф П. Термодинамическая теория структуры, устойчивости и флуктуаций. М.: МИР. 1973. 124 с.
24. Малюк А.А. Энтропийный подход к моделированию систем и процессов защиты информации // Безопасность информационных технологий. – 2011. – № 4. – С. 15-19.
25. Аверин Г.В., Звягинцева А.В. О взаимосвязи статистической и информационной энтропии при описании состояний сложных систем // Научные ведомости. Серия математика. Физика. 2016. № 20 (241). – Выпуск 44. – С. 105-116

ASSESSMENT OF ENTROPY OF INFORMATION SECURITY SYSTEMS

Livshitz I.I. [3]***, Neklydov A.V.*** [4]

To create modern information security systems, it is important to ensure 'the balance of interests' of various components, which define stability of operation of various types of protected assets. Various methods can be used to solve this task, which assume assessment of the information system entropy. However, there is no common approach to calculating entropy for the information systems, which does not allow for implementing safe operation of the security systems as far as necessary in general and information security systems in particular. This research attempts to analyze information security systems from the point of view of defining full entropy of the information system. It takes into account the indicators of the IS audit systems as a 'system shell'. It provides an example for assessing dissipative systems in terms of the thermodynamic theory of I. Prigozhin. It shows that it is possible to consider modern information security systems as dissipative systems, which 'production of the entropy' element is negative on the scale that proceeds to the right.

Keywords: *Management system, Integrated Management System; Information System; Entropy, Dissipative system; Information Security.*

References

1. Agureev I., Denisov M. [Mathematical description of the dynamics of passenger transport systems]. Mir Transporta. 2011. Vol. 1. pp. 15-22 (In Russ).
2. Agureev I., Bogma A., Pyshni'V. [Dynamic model of the transportation macrosystem]. Izhvestiay TulGU. Technicheskie nauki. 2013. Vol. 6. pp. 139-145 (In Russ).
3. Agureev I., Gladyshev A. [The Dynamics of production and demand in dissipative model of logistic system]. Izhvestiay TulGU. Technicheskie nauki. 2013. Vol. 6. pp. 152-160. (In Russ).
4. Okhtilev M.Y., Sokolov, B.V. [New information technology of the monitoring and control of complex technical objects in real time] // SPIIRAS Proceedings. Issue 2, vol. 2. — SPb.: Nauka, 2005. – Pp. 249 – 265. (In Russ).
5. Okhtilev M.Y., Sokolov B.V., Yusupov R.M. Conception of complex objects proactive monitoring management and control: theoretical and technological foundations // YFU Proceedings. – 2015. – 1. – Pp. 162-174. (In Russ).
6. Sokolov B.V., Potryasaev S.A., Malysheva I.V., Nazarov D.I. [Algorithm of dynamical multiple criteria model of integrated adaptive planning and scheduling for complex technical system] // Vserossi'skaya konferncia po problemam upravleniya v tehnicheskih systemah. – 2015. – 1. Pp. 3 – 6. (In Russ).
7. Burakov V.V., Zelentsov V.A., Potryasaev S.A., Sokolov B.V. [Evaluation and choice of automatic control technology for active moving objects on the basis of integrated Modeling] // TUSUR Proceeding. – 2014. – vol. 3 (34). – Pp. 155-165. (In Russ).
8. Baumgarte J. Stabilization of constraints and integrals of motion in dynamical systems. Comp. Math. Appl. Mech. Eng. 1972. Vol. 1. pp. 1-16.
9. Ascher U.M., Hongsheng Chin, Petzold L.R., Reich S. Stabilization of constrained Mechanical systems with DAEs and invariant manifolds. J. Mechanics of Structures and Machines. 1995. Vol. 23. pp. 135-158.
10. Amirouche F. Fundamentals of Multibody Dynamics. Theory and Applications. Birkhauser, Springer. 2005. 684 pages.
11. Andrianova E., Mel'nikov S., Raev V. [Dissipation and entropy in the physical and information systems. Fundamental research]. 2015. Vol. 8. pp. 233-238. (In Russ).

3 Ilya Livshitz, Ph.D., Associate Professor, ITMO University, Saint-Petersburg, Livshitz.il@yandex.ru
4 Adrew Neklydov, Lead Engineer JSC «Gazinformservice, Saint-Petersburg , nav7ad@mail.ru

12. Kudzh S.A., Cvetkov V.Ja. [Features of the development of Informatics]. Perspektivy nauki i obrazovanija. 2013. Vol. 6. p. 11. (In Russ).
13. Igonin V. [Technological features energy survey of buildings, structures and engineering networks]. Vologda. VoGTU. 2012. p. 104. (In Russ).
14. Igonin V. [The methodology of scientific research and technological development «of the subject»]. Vologda. VoGTU. 2013. p. 111. (In Russ).
15. Shennon K. [Work on the theory of information and Cybernetics]. M.: Izd-vo inostrannoj literatury. 1966. 88 p. (In Russ).
16. Markin A.A., Melnikov S.V. [Philosophical and scientific aspects of the concept of information entropy]. Trudy rossijskoj nauchnoj konferencii «Innovacionnye strategii razvitija nauki, tehniki i obshhestva», Minobrnauki RF, MGTU MIRJeA. M., 2014. pp. 98–102. (In Russ).
17. Ayurov V. [The circulation of goods and the physics of money]. GIAB. MGTU. 2003. vol. 5. p.90.
18. Ayurov V. [Synergetic economy]. M.: MGU. 2005. p. 124. (In Russ).
19. Livshitz I. [Practical purpose methods for ISMS evaluation]. Menedzhment kachestva – Quality Management. 2013. Vol. 1. pp. 22–34 (In Russ).
20. Livshitz I. [Approaches to the application of the integrated management system model for carrying out audits for complex industrial facilities – airport complexes]. SPIIRAS Proceedings. 2014. Vol. 6, pp. 72–94. (In Russ).
21. Livshitz I. [The technique of performing complex audits of industrial facilities to ensure the effective implementation of energy management systems]. Energobezhopasnost' i energosberezhenie. 2015. Vol. 3. pp. 10-15. (In Russ).
22. Livshitz I. [The formation of the concept of instantaneous audits of information security]. SPIIRAS Proceeding. 2015. Vol. 6. pp. 272-300. (In Russ).
23. Prigozhin I., Glensdorf P. [Thermodynamic theory of structure, stability and fluctuations]. M.: MIR. 1973. p. 124. (In Russ).
24. Malyuk A.A. [Entropy Approach to Modeling Information Security Systems and Processes] // Information Technology Security. – 2011. – Vol.4. – pp. 15-19. (In Russ).
25. Averin G.V., Zviagintseva A.V. [The statistical and information entropy relationship when describing the complex systems state] // Science proceeding. Mathematics. Physics. – 2016. – vol. 20 (241). – pp. 105-116. (In Russ).