СОВРЕМЕННОЕ СОСТОЯНИЕ ФИЛОСОФИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

А.П. Баранов
доктор физико-математических наук, Заместитель Генерального директора ФГУП «Главный научно-исследовательский вычислительный центр ФНС России»

Адрес: 125373, г. Москва, Походный проезд, вл. 3, стр. 1
E-mail: baranov.ap@yandex.ru

Статья посвящена разработке философской концепции понятия «эффективность управления информационной безопасностью». Основой концепции является представление информации как содержания отображения взаимодействующих систем. Данный подход позволяет рассматривать с единых позиций вопросы обеспечения защиты информации для технических, компьютерных, а также общественно-политических систем. Ключевым моментом концепции является формулирование целей взаимодействия систем, которые для разных сторон взаимодействия могут быть принципиально различными.

Понятие управления информационной безопасностью предлагается интерпретировать как управление состоянием достаточности обеспечения движения информации, возникающей при взаимодействии систем. Такое определение является частным случаем традиционного понятия управления системой, если в качестве системы рассматривать взаимодействующие объекты, осуществляющие процесс отображения.

Предлагаемый подход расширяет традиционный взгляд на управление информационной безопасностью, содержащийся в стандартах различных российских и международных организаций. Стандартный подход оказывается частным случаем, основанным на оценках рисков или выполнении рекомендаций регуляторов. В свою очередь, к оценке эффективности процесса управления информационной безопасностью, как и в общем случае оценки эффективности управления системой, оказывается применимым закон У.Эшби.

На основе этого подхода выявляются возможности повышения эффективности управляющей системы для оперативного управления. Рассматривается пример функционирования портала госуслуг как взаимодействующих систем государственного органа и населения. Делается вывод о слабой информационной защищенности системы населения при осуществлении взаимоотображений государственного органа и общества. Как вариант повышения эффективности управления предлагается использовать потенциал саморегулируемых организаций.

Ключевые слова: философия, отражение, информация, безопасность взаимодействия, информационная безопасность, эффективность управления, закон У.Р. Эшби, регуляторы, саморегулируемые организации.

1. Введение

Развитие информационных технологий в современном мире сопровождается повышением значения и роли защиты информации на всех этапах ее существования. Объемы исследований и затраты, направляемые на разработку методов защиты, увеличиваются вместе с расширением областей применения компьютерной техники. Становясь неотъемлемой частью производственных, хозяйственных и общественных функций, информационные технологии зачастую оказывают решающее влияние на функционирование жизненно важных процессов существования государств, включая критические технологии [1].

Предметом применения компьютерной техники является информация, которую, в частности, требуется защищать, поэтому понятие «информационная безопасность» необходимо соотнести со всей совокупностью аспектов безопасности функционирования общественно-экономических и технических систем.

Мы будем придерживаться принципа вторичности термина «информационная безопасность» по отношению к понятию общей безопасности системы. Аналогично, управление информационной безопасностью будем рассматривать как частный случай управления системой. При этом сразу возникают два вопроса: что такое «безопасность» и что мы понимаем под термином «информация».

В настоящее время в литературе сформулирован ряд определений понятия «информация» ([2; 3; 4] и др.). Мы будем основываться на представлении информации как содержания отражения взаимодействующих систем. Причиной выбора такого подхода является, во-первых, возможность вывести из него другие, косвенные признаки, характеризующие понятие информации, во-вторых, этот подход не противоречит другим определениям.

Используя материалистическое понимание взаимодействия и моделирования систем [5], можно с любой степенью подробности описать современные общественные и технические процессы [6]. Применение формальной теории систем для моделирования процессов с целью дальнейшей оптимизации результатов взаимодействия в зависимости от целей существования и функционирования отдельных систем стало насущной и естественной практикой анализа и прогнозирования развития ситуаций. В настоящей работе мы не будем рассматривать методы теории систем, ограничимся лишь философским содержанием взаимодействия и отражения, непосредственно приводящим к понятию информации.

Отражение двух взаимодействующих систем заключается в том или ином воспроизведении одной системой (называемой отражающей) другого объекта или системы (называемых отражаемыми). Свойства отражения и характер его проявления зависят от целей взаимодействия систем, их самореализации, а также среды, разделяющей системы, если таковая имеется.

Таким образом, мы сразу отмечаем, что отражение носит направленный характер: от отражаемого объекта к отражающему.

Будем исходить из определения информации как содержания отражения и направления ее движения от отражаемого объекта к отражающему. Поскольку содержание отражения зависит от цели взаимодействия, то и содержание, а также направление движения информации определяется этой целью. Следовательно, информация существует только в движении, и это заключение, на первый взгляд, противоречит «здравому смыслу», когда речь идет о хранении информации на материальных носителях – книгах, дисках и пр. Однако, «противоречие» легко устраняется при рассмотрении основных форм движения информации, которые будут нам полезны, когда в дальнейшем мы будем исследовать понятие безопасности информации в той или иной форме движения.

Различают четыре основные формы движения информации [7]:

1. Восприятие (или использование) информации отражающей системой, направленное на изменение внутреннего содержания отражающей системы путем воспроизводства содержания отражаемого объекта.

2. Передача и предоставление информации от одного объекта к другому через определенную промежуточную среду, в ходе взаимодействия разнесенных в пространстве систем.

3. Хранение информации отражаемой системой с целью ее дальнейшего предоставления некоторой, возможно, и не точно известной, отражающей системе. Хранение можно рассматривать как передачу информации во времени.

4. Переработка и порождение информации отражающей системой с целью предоставления результата переработки или порождения другой отражающей системе, когда бывшая ранее отражающей система станет отражаемой.

Мы добавили к этим традиционным формам движения информации еще одну:

5. Добыча (разведка) информации, которая возникает в случае, если отражаемая система в ходе взаимодействия либо препятствует, либо контролирует объемы и характер своего передаваемого содержания отражающей системе.

2. Управление информационной безопасностью

Рассмотрим содержание понятия «безопасность», имея в виду различные формы движения информации. Прежде всего, отметим, что каждая из перечисленных форм движения соответствует своим целям взаимодействия систем, причем цели взаимодействия отражаемых и отражающих систем в общем случае различны.

Общее определение безопасности процесса, системы или взаимодействия систем сформулируем как состояние обеспечения целевой функции существования указанных объектов. Такое определение, по крайней мере, не противоречит принятому определенной группой философов [8; 9]. Тогда логично определить информационную безопасность как состояние обеспечения движения информации в процессе отражения систем, соответствующего цели взаимодействия. Очевидно, что при двухстороннем взаимодействии информационная безопасность общей системы, включающая в себя две взаимодействующие системы, будет объединением двух отдельных состояний информационной безопасности. Понятно также, что безопасность движения информации будет различна для различных форм движения.

Сформулируем теперь определение понятия управления информационной безопасностью. Под термином «управление системой, процессом, состоянием» будем понимать совокупность воздействий на указанные объекты для достижения наилучшей реализации поставленной цели.

В частном случае управления информационной безопасностью объектом регулирования или управления является состояние достаточной обеспеченности движения информации, необходимого для взаимодействия систем. Однако, даже в случае одного и того же типа и характера взаимодействия задачи управления могут быть различны. Например, при передаче информации, содержащей государственную тайну, важнейшим аспектом может быть обеспечение конфиденциальности; при передаче аутентификационной, или командной, информации главной задачей может являться целостность и достоверность и т.д.

В свою очередь, несмотря на наличие объекта регулирования или управления в виде состояния, непосредственные воздействия возможны на отдельные части системы взаимодействия. Таким образом, управляющие воздействия для достижения цели обеспечения состояния информационной безопасности могут быть отнесены на отражающие или отражаемые системы, а также на сам процесс их взаимодействия.

Рассмотрим более подробно со сформулированных позиций содержание состояния информационной безопасности, а затем и управление этим состоянием. Характеристики состояния определяются требованием к обеспечению процесса взаимодействия и соответствующей форме движения информации. Например, при хранении договоров купли-продажи недвижимости требуется обеспечить конфиденциальность персональных данных, неизменность документов, доступность к ним только определенных лиц, а также нотариальную (юридическую) значимость, из которой вытекает невозможность аннулирования сделки ее участниками. Указанные требования должны выполняться в соответствии с Законом № 125-ФЗ от 22.10.2004 года «Об архивном деле в Российской Федерации» при временном хранении в государственных органах или муниципальных образованиях в течение 75 лет. Затем документы передаются на постоянное хранение, где также должен быть обеспечен необходимый уровень состояния информационной безопасности.

Состояние информационной безопасности в общем виде традиционно характеризуется свойствами конфиденциальности, целостности и доступности. При этом легко привести примеры ситуаций, когда необходимо выполнение любого из подмножеств этого множества свойств.

Мы отметили выше, что состояние информационной безопасности может быть отнесено к отдельным субъектам взаимодействия и быть различным для отражающей системы и отражаемого объекта. В примере с хранением договоров купли-продажи основные требования предъявляются к процессу хранения у объекта отражения. К отражающей системе, запрашивающей информацию о сделке купли-продажи, требования оказываются проще, необходима только строгая аутентификация запроса. Вместе с тем, если информация передается по каналу связи, то возникает целый комплекс требований по обеспечению

надежности аутентификации запроса и конфиденциальности передачи ответа.

Управляющие воздействия на систему имеют различия, проистекающие из многообразия состояний информационной безопасности по отношению к отражаемой или отражающей системам, а также целям взаимодействия и формам движения информации. Эти воздействия можно разделить на два больших класса:

1. Выполнение регламентных требований регуляторов.

2. Выработка оптимальных методов обеспечения выполнения цели взаимодействия на основе оценки рисков для отражающей и отражаемой систем.

Первый подход обязателен для государственных структур. Зачастую он приводит к необходимости весьма больших затрат, однако способствует перенесению ответственности при нарушении целей взаимодействия на регулятора.

Второй подход оптимизирует затраты, однако требует весьма тщательного анализа процесса отражения при взаимодействии, что не всегда возможно при создании, например, больших компьютерных систем в силу низкого качества проектной документации или отсутствия контакта с разработчиком. Следует отметить, что возможность реализации второго подхода при создании государственных систем с 2013 года разрешается и регламентируется Приказом №17 ФСТЭК РФ от 12.02.2013 г., а также Приказом №21 ФСТЭК РФ от 18.02.2013 г.

Таким образом, мы видим, что вариаций методов управления информационной безопасностью взаимодействия систем весьма много. Рассмотрим один из возможных методов оценки эффективности управления.

3. Применение закона У.Р. Эшби для оценки эффективности управления

Закон необходимого разнообразия У.Р.Эшби [10] утверждает, что информационная емкость или разнообразие (Rz) состояний регулятора должны быть не меньше, чем разнообразие возмущений (Rv), сопровождающих существование управляемой системы.

Другими словами, если $Rz = |Mz|$ – мощность конечного множества Mz дискретных состояний регулятора, равная числу различных элементов множества состояний регулятора, а $Rv = |Mv|$ – мощность множества Mv внешних или внутренних воздействий на регулируемый объект, то для эффективной работы регулятора необходимо, чтобы хотя бы $|Mz|$ было больше или равно $|Mv|$.

У.Р. Эшби использовал понятие «разнообразие», которое можно по-разному интерпретировать в случае континуальных (неконечных) множеств Mz и Mv. Мы не будем развивать здесь направления применения закона Эшби для разных типов множеств управления. Оказывается, что даже для дискретных множеств Mz и Mv можно получить интересные следствия.

Следствие1. Любой нетривиальный регулятор с минимальным разнообразием Rz , большем или равном 2, может управлять возмущениями любого конечного разнообразия.

Доказательство. Пусть $Rz = 2$, а $Rv = 2^n$, где n – произвольное фиксированное число, $n > 1$. Произведение n – множеств Mz имеет размерность n и мощность 2^n.

Следовательно, на каждое возмущение из Mv могут быть образованы цепочки реакций длины n. Таким образом, за счет удлинения времени реакции в n раз регулятор может соответствовать закону Эшби. Множество Mz фактически характеризует компетентность регулятора.

Вывод. Малокомпетентный регулятор может быть эффективным за счет уменьшения скорости реакции или увеличения времени реагирования на воздействие.

Следствие2. Если $Rz > Rv$, то это еще не гарантирует эффективности управления.

Действительно, построим пример неэффективного управления, удовлетворяющего условиям Следствия 2. Пусть $Rv = 2$, а Rz – произвольное конечное или бесконечное число. Однако, все элементы Rz не оказывают влияния на управляемую систему, то есть не управляют ею. Тогда фактически все элементы из Rz эквивалентны одному элементу, заключающемуся в отсутствии управления. Обозначим его через $Mz(1)$. Таким образом, по отношению к понятию управления все элементы Mz тождественны, и по отношению к управлению реальная мощность управляющего множества равна 1, то есть для $|Mz(1)| = 1 < Rv$. Следовательно, такое управление не может быть эффективным.

Таким образом, мы видим, что оценка эффективности управления зависит не только от мощности управляющего множества, но и от факторизации этого множества по отношению к воздействию на систему.

В системе управления средствами защиты информации возмущающие воздействия состоят в факторах нарушения условий взаимодействия систем, определяющих, в свою очередь, требования к безопасности осуществления отражения как к отражающей системе, так и к отражаемому объекту. Объем так называемого алфавита (вариантов) нарушений достаточно велик, в чем можно убедиться, рассмотрев перечень угроз для персональных данных, разработанный регуляторами – ФСБ РФ и ФСТЭК РФ. Цепочки же нарушений тем более создают большое пространство воздействий, то есть множество *Mv* имеет большое значение *Rv*. Таким образом, для того, чтобы адекватно и своевременно реагировать на возмущения (нарушения), множество управляющих воздействий обеспечения информационной безопасности также должно быть, по закону Эшби, достаточно развитым: *Rz* больше или равно *Rv*.

Все приведенное выше относится к непосредственному, так сказать, оперативному управлению системой безопасности или системой защиты информации. Следующим уровнем управления является управление информационной безопасностью в целом как при создании системы, так и при ее эксплуатации. Другими словами, управление состоянием отражения при взаимодействии двух или более систем с целью обеспечения надлежащего информационного содержания отражения, отвечающего целевому предназначению отражения. Информационное содержание отражения заключается в реализации движения информации в форме, требуемой целью взаимодействия. Следовательно, управление информационной безопасностью (УИБ) взаимодействия систем осуществляется в целях обеспечения заданной формы движения информации, а требования к форме определяются целью отражения.

4. Априорное и апостериорное управление

Из предложенного понимания содержания УИБ вытекают два вида воздействия на процесс взаимодействия систем – априорное и апостериорное. Априорное воздействие или управление заключается в формировании спектра условий и мер, обеспечивающих требуемый уровень взаимодействия при организации и дальнейшей реализации процесса отражения. Апостериорное УИБ заключается в коррекции условий реализации процесса по итогам уже осуществляемого отображения. Апостериорное УИБ почти всегда дешевле реализовать, но оно, как правило, осуществляется после завершения инцидентов нарушений. Реализация локализации и компенсации потерь от произошедших инцидентов нарушения информационной безопасности может иметь дополнительную цену, и тогда решение о применении апостериорного метода УИБ следует принимать на основе оценки соответствующих рисков.

Априорное УИБ обеспечивает требуемый уровень взаимодействия, но, как правило, приводит к осуществлению весьма дорогостоящих мер, цена которых может определяться как стоимостью оборудования или реализации условий, так и ограничениями, накладываемыми на процесс взаимодействия, сужая его возможности по реализации отражения. Особенность априорного УИБ заключается в безусловном выполнении требований государственных органов и может реализовываться как комплекс мер по итогам разработки модели угроз информационной безопасности на основе рекомендаций регуляторов. Указанные рекомендации охватывают актуальное множество угроз, зачастую избыточных, для конкретных систем. Проекция широкого спектра угроз на конкретную систему и обоснование незначительности их отдельных составляющих для защищаемого отражения является непростой задачей. Поэтому в ряде случаев разработчики мер защиты идут по пути стандартного выполнения требований регуляторов, что приводит к существенному удорожанию проектов защиты информации.

В случае использования оценок рисков и применения мер, приводящих к блокированию неприемлемых угроз, реальный уровень безопасности повышается и обеспечивает надлежащий характер взаимодействия. Особенностью подобного подхода является возложение ответственности за обеспечение информационной безопасности полностью на разработчика системы.

Как при прямом выполнении административных регламентов, так и при использовании оценок рисков происходит воздействие на организацию отражения систем, что и составляет содержание управления состоянием информационной безопасности взаимодействия. Некоторая попытка систематизации действий при реализации УИБ изложена в стандартах ISO/IEC 27000-27006 и ICO/IEC 13335. Перевод указанных документов на русский язык содержится в ГОСТ РИСО/МЭК 27001-27006 и ГОСТ Р МЭК 13335, имеющих рекомендательный к исполнению характер.

Описанная схема понимания УИБ взаимодействия применима к техническим, включая компьютерные, к общественным, а также к смешанным системам.

Если применение вышеизложенного подхода к создаваемым или эксплуатируемым компьютерным системам не вызывает противоречий со сложившейся практикой обеспечения информационной безопасности, то рассмотрение взаимодействия общественных систем под «техническим» углом зрения составляет определенную «новеллу».

Остановимся на варианте УИБ взаимодействия системы «Портал госуслуг (ПГУ)» и отдельных граждан. Очевидно, что взаимодействие и отражение здесь имеют двухсторонний характер. С одной стороны, ПГУ получает запросы, предложения и пожелания от граждан, то есть отражает в определенной степени значительную часть населения. В этом отражении ПГУ и государственные организации, взаимодействующие с ПГУ, изменяют свое содержание, отражая запросы общества. ПГУ – отражающая система, граждане – отражаемая система. С другой стороны, граждане получают требующиеся им сведения о деятельности государственных органов и определенный вид услуг, отражающих через ПГУ деятельность государства. В этом взаимодействии и соответствующем отражении отражаемая система – ПГУ, а отражающая система – граждане. И в том, и в другом взаимодействии обе стороны, являющиеся отражающими и отражаемыми, подвергаются внутреннему изменению, используя содержание отражения – информацию, движущуюся от ПГУ к гражданам и обратно. Цель взаимодействия ПГУ и граждан отражена в Законе №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 г., глава 5 (далее – Закон №210).

Закон №210 формулирует требования со стороны государства к ПГУ по выполнению функций взаимодействия как отражаемой, так и отражающей стороны. Требований к гражданам, осуществляющим взаимодействие с ПГУ, найти в Законе №210 не удалось. Таким образом, если мы рассматриваем УИБ-системы «ПГУ – граждане» только на основании Закона №210, то будем вынуждены сконцентрироваться на обеспечении информационной безопасности ПГУ. Информационная безопасность граждан в этом взаимодействии остается задачей самих граждан, без широко доступных для реализации инструкций по использованию ими средств защиты информации, адаптированных к технологии и особенностям функционирования ПГУ. Между тем, во взаимодействии граждан с ПГУ присутствует весь спектр угроз, перечисленных, например, в Приказе ФСБ №795 от 27.12.2011 г. Выбор гражданами адекватных мер защиты собственной информации весьма затруднен в силу отсутствия специальных знаний в этой области среди основной части общества. Подводя итог, мы можем констатировать, что в системе «ПГУ – граждане» УИБ носит односторонний характер, что не способствует развитию системы в целом и является явным сдерживающим фактором в предоставлении через ПГУ юридических значимых, то есть принимаемых в суде, документов и услуг.

В целом, регулирование различных сторон взаимодействия элементов государства и общества возложено на более чем 20 государственных органов. Наблюдается дальнейший рост числа регуляторов. Такую тенденцию можно объяснить стремлением системы «Государство – Общество» улучшить управление, то есть в соответствии с Законом У.Р. Эшби увеличить Rz – мощность множества управляющих воздействий в быстро развивающейся области – информатизации всех сторон жизни, а именно, в увеличивающемся множестве вариантов воздействий Mv, $Rv = |Mv|$. Напомним, что согласно закону У.Р. Эшби, Rz должно быть больше, чем Rv. Однако, такой путь развития ведет либо к увеличению госаппарата, либо к увеличению времени реакции государства на вызовы общества.

5. Заключение

Выявленные проблемы могут быть решены либо за счет кардинального и непрерывного повышения квалификации сотрудников органов управления, либо за счет передачи части функций регулирования самому обществу, путем стимулирования деятельности саморегулируемых организаций и признания регуляторами их необходимости. Последнее становится возможным в силу формирования в современной России значительной группы высококвалифицированных специалистов в различных областях обеспечения информационной безопасности. Привлечение широкого круга специалистов значительно, в десятки раз, увеличивает значение величины Rz и позволяет обеспечить выполнение закона У.Р.Эшби. Принципиально, подобный подход может обеспечить уменьшение рутинной нагрузки на специалистов госаппарата, сняв с них часть несвойственных административным сотрудникам экспертных инженерно-технических функций. ■

Литература

1. Указ Президента РФ от 15.01.2013 г. №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства Российской Федерации, 2013. № 3. Ст. 178.
2. Переслегин С.Б. Новые карты будущего или Анти-Рэнд. М.: Аст, 2009. 701 с.
3. Урсул А.Д. Отражение и информация. М.: Мысль, 1973. 232 с.
4. Гуревич И.М., Урсул А.Д. Информация – всеобщее свойство материи. Характеристики, оценки, ограничения, следствия. М.: Либроком, 2012. 312 с.
5. История русской философии / Маслин М.А. и [др.] М.: КДУ, 2008. 640 с.
6. Бусленко Н.П. Моделирование сложных систем. М.: Наука, 1978. 400 с.
7. Рябов О.А. Моделирование процессов и систем: Учебное пособие. Красноярск, 2008. 122 с.
8. Смирнов С.Н. Диалектика отражения и взаимодействия в эволюции материи. М.: Наука, 1974. 382 с.
9. Рыбалкин Н.Н. Философия безопасности: Учебное пособие. М.: МПСИ, 2006. 296 с.
10. Романович А.Л., Урсул А.Д. Устойчивое будущее (глобализация, безопасность, ноосферогенез). М.: Жизнь, 2006. 512 с.
11. Эшби У.Р. Введение в кибернетику. М.: ЕЕ Медиа, 2012. 425с.

CURRENT STATE OF INFORMATION SECURITY MANAGEMENT PHILOSOPHY

Alexander BARANOV
Deputy CEO, Federal State Unitary Enterprise «Main Research Computing Center (GNIVC) of Federal Tax Service of Russia»
Address: property 3, bdg. 1, Pohodnyi proezd, Moscow, 125373, Russian Federation
E-mail: baranov.ap@yandex.ru

The paper elaborates a philosophical vision of the «information security management efficiency» concept. The concept is based on presentation of information as content of interacting systems' reflection. This approach allows considering from a unified point of view the issues of information protection for technical, computer, social and political systems. The key point of the concept is formulation of systems' interaction goals that may by profoundly different for different parts of the interaction.

The concept of information security management is proposed to be interpreted as management of the state of sufficiency of ensuring of information transfer that occurs during interaction of the systems. This definition is a special case of the traditional concept of system management, if the system is considered as a set of interacting objects performing the reflection process.

The approach expands the traditional view on information security management presented in the standards of various Russian and international organizations. The common approach appears to be a special case based on risk assessment or statutory regulations. In turn, the W.R. Ashby's law appears to be applicable for evaluation of the information security management process, as a particular case of the system management process.

The approach allows discovering new possibilities to improve managing system efficiency for operative level of management. An example of the Portal for Government Services as government agency's systems interaction with citizens is discussed. The conclusion about weak information protection of the people's system in the process of mutual reflection of a government agency and society has been drawn. As a possible way to increase management effectiveness it is recommended to employ the potential of the self-regulatory organizations.

Key words: philosophy, reflection, information, security of interaction, information security, management efficiency, W.R. Ashby law, regulators, self-regulated organizations.

References

1. President of Russian Federation (2013) Ukaz *«O sozdanii gosudarstvennoj sistemy obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'juternyh atak na informacionnye resursy Rossijskoj Federacii»* [Executive Order «On establishment of government system of detection, prevention and liquidation of consequences of computer attacks targeting on information resources of Russian Federation»], January 15, 2013, No. 31c. Collection of Legislation of Russian Federation, 2013, no. 3, art. 178. (in Russian)
2. Pereslegin S.B. (2009) *Novye karty budushhego ili Anti-Rjend* [New maps of future or Anti-Rand]. Moscow: Ast. (in Russian)
3. *Ursul A.D. (1973) Otrazhenie i informacija* [Reflection and information]. Moscow: Mysl'. (in Russian)
4. Gurevich I.M., Ursul A.D. (2012) *Informacija – vseobshhee svojstvo materii. Harakteristiki, ocenki, ogranichenija, sledstvija* [Information – the common feature of matter. Characteristics, estimations, limitations, consequences]. Moscow: Librokom. (in Russian)
5. Maslin M.A. et al (2008) *Istorija russkoj filosofii* [History of Russian philosophy]. Moscow: KDU. (in Russian)
6. Buslenko N.P. (1978) *Modelirovanie slozhnyh sistem* [Complex systems modeling]. Moscow: Nauka. (in Russian)
7. Rjabov O.A. (2008) *Modelirovanie processov i sistem* [Processes and systems modeling]. Krasnojarsk. (in Russian)
8. Smirnov S.N. (1974) *Dialektika otrazhenija i vzaimodejstvija v jevoljucii materii* [Reflection and interaction dialectics in evolution of matter]. Moscow: Nauka. (in Russian)
9. Rybalkin N.N. *Filosofija bezopasnosti* [Philosophy of security]. Moscow: MPSI (in Russian), 2006.
10. Romanovich A.L., Ursul A.D. (2006) *Ustojchivoe budushhee (globalizacija, bezopasnost', noosferogenez)* [Stable future (globalization, security, noospherogenesis)]. Moscow: Zhizn'. (in Russian)
11. Ashby W.R. (2012) *Vvedenie v kibernetiku* [An introduction to cybernetics]. Moscow: EE Media. (in Russian)