004.75, 004.41

К вопросу о формулировании системного подхода к исследованиям в области цифровых платформ, распределенных реестров и цифровых активов

D.I. Pravikov, A.V. Gleym, V.I. Egorov, A.A. Ryazanova, A.Yu. Shcherbakov

On the Formulating a Systematic Approach to Research in the Field of Digital Platforms, Distributed Ledgers and Digital Assets

Abstract. *The article is devoted to the formation of a systematic approach to research in the field of digital platforms that combine technologies of distributed ledgers, digital assets and other relevant modern technologies, including machine learning and artificial intelligence technologies. It is shown that the integration of platform levels is possible from the cyber-physical level and the level of quantum communications to the level of storage systems implemented using a distributed ledger and the level of various business processes associated with the target function of the platform. The partial applicability of subject-object models of computer systems for describing platforms and their information security systems is shown, measures of integration level and security degree of platforms are introduced.*

Keywords: *platform, service model, platform-service model, platform integration, distributed ledger, certification authority, infrastructure, cyber-physical system, quantum network, quantum keys, quantum cryptography, quantum communications, control and monitoring subsystem, trusted nodes, digital coin, zero knowledge, electronic signature, authentication code, blockchain, electronic signature, trusted key storage module, random number generator.*

Д.И. Правиков[1]
А.В. Глейм[2]
В.И. Егоров[3]
А.А. Рязанова[4]
А.Ю. Щербаков[5]

[1]Кандидат технических наук, руководитель Научно-образовательного центра новых информационно-аналитических технологий РГУ нефти и газа (НИУ) имени И.М.Губкина.
E-mail: dip@gubkin.pro
[2]Кандидат технических наук, начальник Департамента квантовых коммуникаций ОАО «РЖД».
GleymAV@center.rzd.ru
[3]Кандидат физико-математических наук, заместитель директора Национального центра квантового Интернета.
E-mail: viegorov@itmo.ru
[4]Научный сотрудник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН.
E-mail: a.ryazanova@c3da.org
[5]Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), президент Ассоциации специалистов в области развития криптовалют и цифровых финансовых активов.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена формированию системного подхода к исследованиям в области цифровых платформ, объединяющих технологии распределенных реестров, цифровых активов и других актуальных современных технологий, включая технологии машинного обучения и искусственного интеллекта. Показано, что интеграция в рамках платформы возможна от киберфизического уровня и уровня квантовых коммуникаций до уровня систем хранения, реализованных при помощи распределенного реестра, и уровня бизнес-процессов различного рода, связанных с целевой функцией платформы. Показана частичная применимость субъектно-объектных моделей компьютерных систем для описания платформ и систем их информационной безопасности, а также введены меры степени интеграции и защищенности платформ.*

Ключевые слова: *платформа, сервисная модель, платформенно-сервисная модель, интеграция платформ, распределенный реестр, удостоверяющий центр, инфраструктура, киберфизическая система, квантовая сеть, квантовые ключи, квантовая криптография, квантовые коммуникации, подсистема управления и мониторинга, доверенные узлы, цифровая монета, нулевое разглашение, электронная подпись, код аутентификации, блокчейн, модуль доверенного хранения ключей, датчик случайных чисел.*

ВВЕДЕНИЕ

В тематике исследований в области цифровой трансформации, связанной не в последнюю очередь с применением механизмов распределенного реестра для создания системы сбора, хранения и анализа данных от различных отраслей экономики, в настоящее время как в российской, так и мировой науке явно прослеживаются некоторые признаки стагнации. В первую очередь это связано с исчезно-

вением из большинства исследований системного подхода, связанного с диалектическим взглядом на проблемы цифровой сферы как развивающейся сущности, имеющей иерархическую природу.

Существенным индикатором неразработанности фундаментальных основ в области цифровой трансформации является, в том числе, наличие множества отдельных бизнес-моделей, функционирующих на основе современных информационных технологий, которые упрощают доступ потребителей к товарам и услугам, предоставляют возможность извлечения полезных элементов из персональных данных и предпочтений пользователей системы. Однако кардинальные изменения практически во всех областях экономики под влиянием развития цифровых технологий четко выявляют необходимость детального системного осмысления и применения базовых методов фундаментальных научных исследований.

Кроме того, приоритетные направления научно-технологического развития России на ближайшие 10-15 лет, приведенные в указе Президента РФ «О Стратегии научно-технологического развития Российской Федерации» (с изменениями на 15 марта 2021 года), обуславливают необходимость в исследованиях, которые «позволят получить научные и научно-технические результаты и создать технологии, являющиеся основой инновационного развития внутреннего рынка продуктов и услуг, устойчивого положения России на внешнем рынке, и обеспечат переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта» [1, 2].

Для осмысления природы цифровой трансформации необходимо учитывать основные понятия, описывающие степень влияния информационных технологий на процессы общественного производства. Если цифровизация – это оптимизация бизнес-процессов при помощи цифровых технологий, то цифровая трансформация касается в большей степени уже изменения устоявшихся моделей и форматов взаимодействия между участниками информационных процессов. Таким образом, наблюдается качественный, иногда кардинальный сдвиг от применения цифровых технологий как вспомогательных инструментов в сторону изменения принципов и основ функционирования системы, для которой они используются.

В данной статье предлагается взглянуть на проблему цифровых платформ и цифровой трансформации с точки зрения «живой» развивающейся системы, подчиненной диалектическим законам, как на синтез различных взаимосвязанных задач, направлений и областей науки и техники.

СВОЙСТВО НЕЗАМКНУТОСТИ СИСТЕМЫ. ПЕРЕХОД К ПЛАТФОРМЕННОЙ МОДЕЛИ И НОВОЙ ПАРАДИГМЕ БЕЗОПАСНОСТИ

В первую очередь хотелось бы отметить, что любая компьютерная система в рамках субъектно-объектной модели представляется совокупностью субъектов и объектов. Принципиальная особенность современных КС – их незамкнутость и переход к платформенной модели, когда эта незамкнутость постулируется особо и в систему включаются средства разработки, предназначенные для ее расширения и совершенствования. В целом к проблематике платформ можно обратиться в классических работах [3, 4].

Таким образом, сейчас происходит смена парадигмы как представления информационной и компьютерной системы, так и информационной безопасности, когда наравне с замкнутыми системами появляются незамкнутые системы, для которых в любой заданный момент времени нельзя однозначно перечислить субъекты и объекты. Как следствие, для незамкнутых (разомкнутых) систем не применимы или не в полной мере применимы субъектно-объектные модели, основой которых является администрирование таблиц разграничения прав доступа (теоретически, например, каждый раз при удалении или добавлении субъекта возможно мгновенно пересматривать таблицу разграничения прав доступа, но, как представляется в случае больших систем, этот процесс относится только к умозрительным сущностям). Поэтому

сейчас основная задача — изменить само понятие безопасности, о чем в частности упоминалось в статьях [5, 6].

ПАРАДИГМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В РАМКАХ КОНЦЕПЦИИ МНОГОУРОВНЕВОЙ ПЛАТФОРМЫ

Вне зависимости от понимания свойств безопасности любая сложная социотехническая система может быть представлена как многоуровневая система, верхние уровни которой реализуют бизнес-процессы, а более нижние уровни — как обеспечение свойств безопасности, так и обеспечение работоспособности или надежности системы на киберфизическом уровне.

Определим уровень (слой), реализующий правила безопасности, как базовый. Тогда все, что выше данного слоя (бизнес-уровни), не должно противоречить механизмам обеспечения безопасности. Условно говоря, если вводится правило (элемент политики безопасности), что по отношению к сведениям, составляющим коммерческую тайну, есть допущенные или не допущенные лица, то не должно быть бизнес-процесса, передающего коммерческую тайну не допущенным лицам или вовне системы бесконтрольно.

Уровни, расположенные ниже уровня бизнес-процессов, должны обеспечивать механизмы реализации безопасности. Например, таблица разграничения прав доступа не должна находиться в открытом виде на внешних хранилищах данных. Таким образом, появляется стек технологий, в котором уровни более высокого порядка должны быть обеспечены однозначной поддержкой со стороны ниже лежащих уровней.

В данной работе системный подход и сервисная модель представлены именно в этом ключе, когда задача обеспечения некоторой функции делится на слои, при этом нижележащий слой предоставляет сервис заданного уровня качества для решения задач более высокого слоя.

При описании некоторого стека технологий, объединенных общим понятием платформы, целесообразно разделить его на смежные сегменты, представление которых позволит выделить именно понимание платформы как таковой. Итак, как было сказано выше, существует базовый уровень стека, реализующий механизмы обеспечения информационной безопасности. Все, что ниже, будем называть обеспечивающими уровнями, которые на базовом уровне позволяют реализовывать механизмы безопасности и не допускают легальными (штатными) возможностями платформы или ее элементов вмешиваться в работу базового слоя. Говоря другими словами, не существует возможности в рамках стека обратиться к нижестоящим обеспечивающим уровням таким образом, чтобы данное обращение повлияло на обеспечение или управление информационной безопасностью. Выше базового уровня располагаются уровни автоматической реализации функциональных процессов, которые требуют использования механизмов безопасности. Еще выше — уровни автоматизированной реализации, когда часть данных или управляющих воздействий может поступать от операторов или пользователей системы.

Представляется, что в рамках одной платформы могут быть реализованы несколько бизнес-процессов. Более того, свойства платформы должны поддерживать включение и реализацию новых бизнес-процессов, что отражает суть цифровой трансформации.

В качестве примера рассмотрим процесс переписи населения. Ранее гражданами в присутствии переписчиков от руки заполнялись бумажные бланки, после чего данные с этих бланков вводились в различные системы (в том числе автоматизированные) статистического учета. Реализация переписи населения в текущем году, при которой переписчик использует для ввода данных персональный компьютер или мобильное устройство, по сути является автоматизацией функции переписи, а возможность самостоятельного заполнения формы и направления гражданином данных через сайт Госуслуг уже имеет признаки цифровой трансформации, поскольку меняется сама модель бизнес-процесса. В данном случае сайт Госуслуг выступает в качестве цифровой платформы, которая обеспечила реализацию нового бизнес-процесса.

На данном примере хорошо видно, что компьютерная система, в том числе и в понимании платформы, имеет целевую функцию (верхнего уровня), описывающую задачу, для которой она создана. Целевая функция декомпозируется (раскладывается) на целый спектр бизнес-процессов, находящихся уровнем абстракций выше классического прикладного уровня, поскольку прикладная задача как субъект или совокупность субъектов, связанных общими данными-объектами, составляет только часть некоторого бизнес-процесса. Таким образом, БП является совокупностью взаимосвязанных прикладных задач, относящихся к прикладному уровню КС.

В приведенном выше примере целевой функцией является перепись населения. Данная целевая функция разбивается на бизнес-процессы: сбор данных о гражданах, хранение данных, уточнение данных, верификация данных, построение взаимосвязей данных, аналитическая обработка данных. Прикладной задачей в этом спектре является, например, ввод данных через мобильное устройство переписчика или гражданином через сайт Госуслуг.

Из приведенных рассуждений очевидно, что понятие БП является интегративным. Ниже показано, что интеграция возможна на всех уровнях платформы. В качестве отдельной активной сущности в рамках современных платформ можно рассматривать смарт-контракты, которые, с одной стороны, могут реализовывать свойство расширяемости платформ, а с другой – реализовывать механизмы информационной безопасности и интеграции платформ.

В данном случае смарт-контракты являются интересным примером, как бизнес-процесс из слоя автоматизированной реализации переведен в слой автоматической реализации.

Рассмотрим уровни представления процессов в системе в виде нисходящей схемы (см. рис.1) – уровни абстракций от верхнего – бизнес-процессов до нижнего – аппаратного уровня через прикладной и программный.

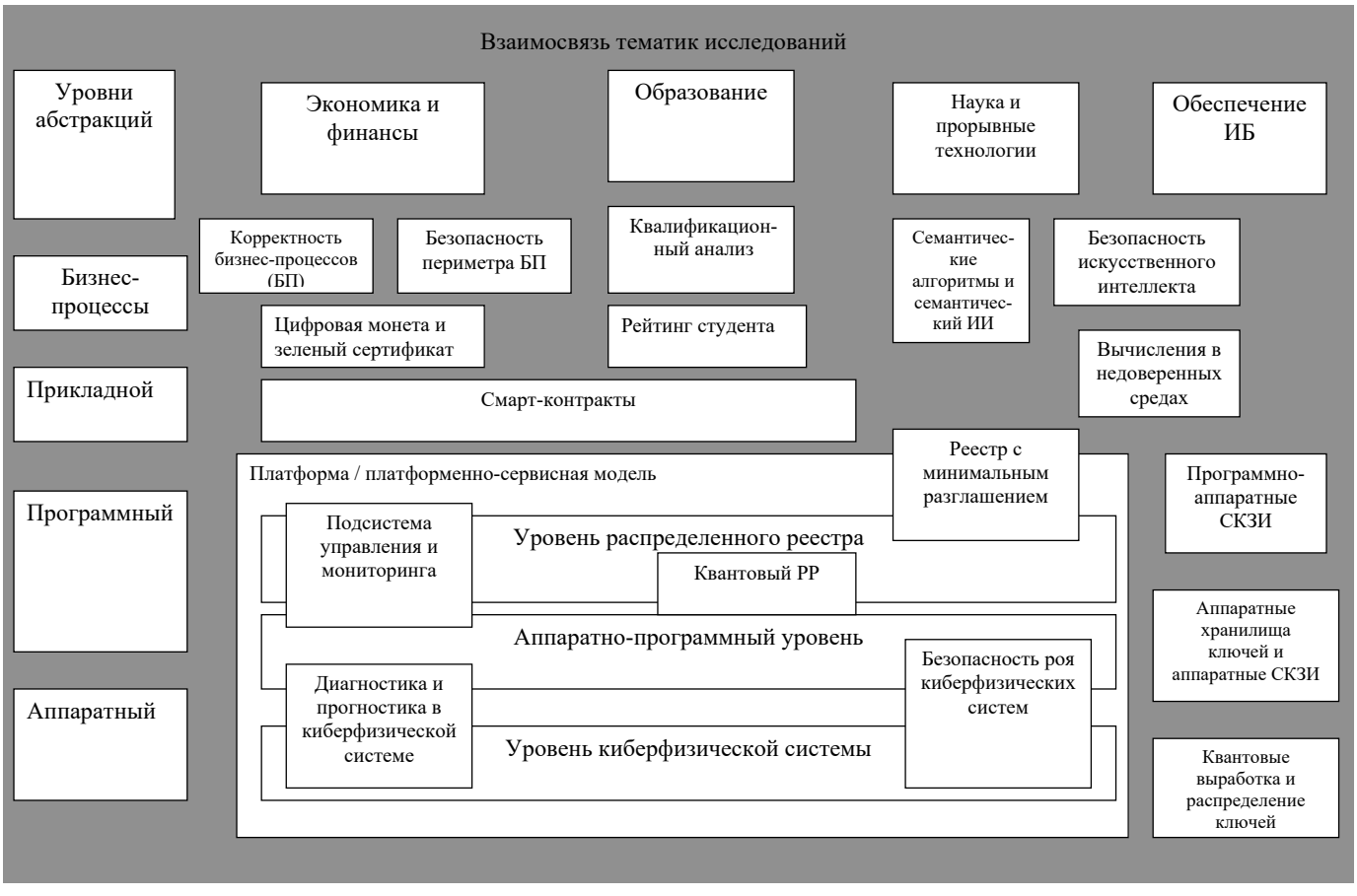

Рис. 1. Взаимосвязь тематик исследований в области перспектив развития технологий цифровых финансовых активов и распределенных реестров

Необходимо заметить, что одной из важных методологических проблем является необходимость рассмотрения платформы с функциями обеспечения безопасности, как киберфизической системы. Вопросы описания функционирования киберфизических систем были подробно изучены в работах [7, 8, 9], в которых показано, что негативное воздействие на киберфизическую систему можно выявить по степени отклонения от стационарных характеристик, описываемых квазианалитической зависимостью.

В соответствии с выводами по результатам типового эксперимента, для киберфизических систем характеристики имеют, как правило, периодическую или псевдопериодическую зависимость. «Киберфизичность» системы или платформы важна не только с точки зрения циркуляции или обработки в ней информации. Аппаратная компонента платформы сама является киберфизической системой. Например, сбор, контроль и обработка данных о состоянии питающих трансформаторов ЦОД или источников бесперебойного питания отдельных серверов необходимы для обеспечения надежности и работоспособности платформы в целом, поскольку от стабильности электропитания зависит не только технологическая работоспособность, но и безопасность хранения данных, включая дисковые массивы и криптографические ключи в специальных хранилищах.

Важно отметить, что рассматриваемое ниже квантовое распределение ключей для территориально-распределенной платформы также относится к киберфизическим процессам. Кроме того, работа обозначенной на рис.1 подсистемы управления и мониторинга с одной стороны может быть предназначена для сбора данных киберфизического уровня (например, о пропускной способности каналов оптоволоконной связи), а с другой – для мониторинга и управления другими элементами платформы (возможно и выше киберфизического уровня), в том числе и относящимися к уровням обеспечения безопасности и поддержания функционирования платформы. Наличие подсистемы удаленного управления и мониторинга является важнейшим свойством развитых территориально распределенных платформ.

С правой стороны рисунка расположены уровни обеспечения информационной безопасности платформы. Здесь мы также опускаемся от обеспечения безопасности ИИ и вычислений в недоверенных средах до аппаратно-программных СКЗИ, нижнего уровня аппаратного хранения ключей и их исходного нижнеуровневого распределения с использованием квантовых технологий.

Квантовое распределение ключей и их последующее неизвлекаемое хранение как «основа» информационной безопасности были предложены в работах [10, 11, 12, 13] и описывают новый подход к обеспечению ИБ, связанный с квантовым распределением, аппаратным хранением ключей и использованием симметричных криптоалгоритмов.

Метод «подъема» ключей и процедур криптографической защиты на уровень платформы или в прикладные задачи и бизнес-процессы происходит также в рамках новой платформенно-сервисной модели [14], когда процессы квантовой или физической выработки и распределения ключей передают сервисам и бизнес-процессам ключевую информацию в виде различного рода криптографически-защищенных контейнеров.

Сервисная модель позволяет выстроить и основные процессы коммерциализации платформы, обеспечивая в первую очередь процессы биллинга. Вторая, не менее важная задача сервисной модели – обеспечение требований регуляторов по периоду смены ключей по времени и/или объему трафика, либо требованию неповторяемости криптографических ключей для различных сервисов, клиентов или БП. Объединяясь с платформенными компонентами, сервисная модель эволюционирует в настоящее время в платформенно-сервисную [14].

Связь сервисной и платформенно-сервисной модели с бизнес-процессами на платформе в полной мере иллюстрируется работами, касающимися как обеспечения корректности (как расширения понятия безопасности) бизнес-процессов [15], так и прикладными аспектами их реализации в части цифровых активов (токенов и цифровых монет) и цифровых финансов в целом [16].

Позитивный вклад современных техноло-

гий, опирающихся на сервисные модели, в технологии образования достаточно полно проиллюстрирован в работах [17, 18].

ВЗАИМОСВЯЗЬ ТЕХНОЛОГИЙ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ С ТЕХНОЛОГИЯМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ

На современном технологическом уровне весьма важной задачей является синтез технологий хранения данных и их обработки в рамках платформы.

Если говорить о технологиях искусственного интеллекта как максимально перспективных и эффективных процессах обработки информации (бизнес-процесса) на платформе, то их развитие зависит от наличия большого количества данных, необходимых для обучения моделей ИИ [19, 20]. При этом хранение и обработка используемых данных должны производиться с соблюдением требований приватности и конфиденциальности, целостности и достоверности, что обеспечивается применением криптографических инструментов в распределенном реестре [21].

В частности, весьма обоснованно использование доказательств с нулевым разглашением с целью фильтрации и получения бизнесом и учеными нужной информации без раскрытия персональных данных ее владельцев. Применение доказательств с нулевым разглашением детально рассмотрено в статьях [22, 23].

Продолжая тему конструирования хранилищ данных и технологий с минимальным разглашением, нельзя не упомянуть работу в области развития методологии создания доверенных и защищенных информационных систем, построенных с использованием технологии распределенных реестров [24], а также статью [25], иллюстрирующую подход, близкий к задачам «нулевого» разглашения.

Один из лидеров в области технологий искусственного интеллекта Трент МакКонахи в своей статье [26] отметил, что синтез технологий распределенных реестров и искусственного интеллекта является сочетанием надежного и корректного хранения данных с алгоритмами их превращения в ценный продукт (то есть их анализа) как необходимого условия функционирования рынка данных на основе распределенной базы данных планетарного масштаба.

Поскольку решения, принимаемые системой искусственного интеллекта, до сих пор часто не поддаются четкому объяснению, необходима возможность возвращаться в исходную точку неизменяемых данных, которые в ней используются, т.е. отслеживать работу алгоритма последовательно от решения вниз к исходным данным. Распределенный реестр позволяет в неизменном виде фиксировать путь к решению задачи и, таким образом, повысить доверие к технологиям и моделям искусственного интеллекта.

На наш взгляд, одной из основных задач, которую может решить распределенный реестр в сочетании с технологиями ИИ, является обеспечение надежности его работы и формирование технологических подходов к обеспечению его безопасности. На рис. 1 в правой верхней части схемы проиллюстрирована взаимосвязь технологий безопасности искусственного интеллекта, вычислений в недоверенных средах и семантических технологий.

Обратимся к теме семантических технологий. На сегодняшний день понятие семантической технологии в первую очередь отождествляется с технологиями семантического поиска, связанными с качественной обработкой поисковых запросов и разрабатываемыми, в том числе, такими лидерами в области информационных технологий, как Google. Эти технологии интерпретируют поисковые запросы пользователей, упрощая их, затем применяют их к базам данных, то есть система автоматической обработки поисковых произвольных запросов переводит их в вид, понятный для базы данных.

Однако на современном уровне техники небезосновательно утверждение, что назначением семантических технологий является переход от извлечения данных и документов к извлечению знаний и их автоматической обработке [27].

Данное утверждение отражает новый подход к развитию семантических технологий в качестве инструментов интеллектуальной обработки информации. В частности, целесоо-

бразно включать в область семантических технологий семейство алгоритмов обработки текстовой информации различного уровня структурированности, связанные с индексированием и сравнением текстов независимо от языка представления, статистическим анализом текстов, выявлением смысла и в перспективе – созданием систем искусственного интеллекта.

В процессе работы семантических алгоритмов с целью оптимизации поиска и отбора релевантной информации происходят семантические преобразования фрагментов текстов. Семантические инструменты предлагают эффективный способ интеграции информационных процессов (передачи потоков данных, распознавания языка представления данных, трансформации и преобразования данных) в рамках платформы и платформ между собой.

Для достижения высокой степени соответствия заданным критериям запрашиваемой участником платформы информации, в целях общего повышения эффективности процессов обработки информации может использоваться методика выделения семантического ядра массива неструктурированных данных. При этом уровень соответствия запросу определяется мерой конгруэнтности, или мощностью пересечения текстов, детально рассмотренной в работе [28]. Анализ частоты встречаемости слов, их соответствия тематике, совместного употребления и вероятностного распределения, может дать корректные результаты в рамках масштабируемой, тиражируемой и расширяемой платформы.

Семантические алгоритмы вполне могут рассматриваться как отдельный слой бизнес-процессов, связанный с реализацией технологий искусственного интеллекта [29].

Как было отмечено выше, одной из основных проблем функционирования ИИ является его «непрозрачность», а, следовательно, отсутствие полного доверия к принятым с его помощью решениям, в том числе с точки зрения управления бизнес-процессами. Сочетание ИИ с распределенным реестром позволит провести обучение ИИ в рамках процедуры записи в РР данных на основании консенсуса. На начальном этапе решения о подтверждении записи в РР принимаются группой экспертов и ИИ, который должен «попадать» в совокупное мнение экспертов. По мере увеличения количества внесенных в РР данных предполагается, что доля решений, совпадающих у ИИ и группы экспертов, будет увеличиваться. По достижении определенного уровня группа экспертов может полностью передать свои полномочия ИИ, при этом в РР останется последовательность принятых решений по различным вопросам, а значит, появится возможность оценить качество и корректность его обучения.

В заключение данного раздела необходимо заметить, что затронутая проблема «непрозрачности» работы ИИ, в первую очередь реализованного в виде нейросетей и нейросетевых технологий, во-первых, методологически связана с парадигмой «имитации» [30], а во-вторых, по меньшей мере частично решается при помощи семантических технологий. Например, параметры процедур сравнения семантических конструкций, лежащие в основе семантического ИИ, могут быть рассмотрены экспертами в рамках описанного выше консенсуального обучения ИИ, либо обратно деконструированы при анализе работы систем ИИ.

ЭФФЕКТИВНОСТЬ ИНТЕГРАЦИИ ПОДСИСТЕМ ПЛАТФОРМЫ

Обратимся снова к рис. 1. Каждый элемент рисунка, представляющий собой подсистему (подмножество) всей платформы, может иметь связи по передаче информации между другими подсистемами или бизнес-процессами. В общем случае связь представляет собой поток информации, направленный к подсистеме или от нее. В некоторых случаях поток принципиально отсутствует. Например, для пары элементов «Квантовые выработка и распределение ключей» и «Аппаратные хранилища ключей» поток возможен только от первого элемента ко второму, если учитывать постулат о свойстве технической сингулярности, при котором загрузка криптографических ключей и криптографически значимой информации происходит только внутрь аппаратного хранилища.

Предположим, что в платформе имеется N подсистем. Тогда параметр S = N(N-1) оценива-

ет сложность или «насыщенность» платформы, он оценивает сверху максимально возможное количество связей между подсистемами платформы (как было отмечено ранее, реальное число связей, зависящее от свойств подсистем или бизнес-процессов, во всех случаях не будет превосходить этой величины, а практически всегда будет меньше).

Пусть {T} – множество реально существующих связей между подсистемами платформы, а мощность этого множества T – число реально существующих связей между подсистемами платформы, T=|{T}|. Тогда соотношение Kn=T/S назовем коэффициентом насыщенности платформы. Из общих соображений можно считать, что коэффициент насыщенности оценивает эффективность интеграции подсистем одной и той же платформы между собой. Например, при низком коэффициенте насыщенности можно полагать, что большая часть подсистем не связана и не интегрирована между собой, что указывает на необходимость пересмотра и доработки архитектуры платформы, которая с точки зрения системного анализа как раз представляет совокупность подсистем и их взаимосвязей.

Нельзя также оставить без внимания тот факт, что связи подсистем могут быть направлены вовне или извне, соединяя данную платформу с другими.

СТЕПЕНЬ ЗАЩИЩЕННОСТИ ПЛАТФОРМЫ

С точки зрения информационной безопасности часть связей из множества реально существующих может быть описана свойством «быть защищенным». Например, связь может быть криптографически защищенной или контролироваться правилами разграничения доступа, либо должны быть выполнены разрешения связи подсистем при выполнении некоторых условий.

Пусть {Z} – множество защищенных связей, а Z – количество таких связей, Z=|{Z}|.

Из технического задания на платформу или требований регулирующего органа может вытекать необходимость обязательной защиты подмножества {R} связей подсистем платформы. При этом можно постулировать, что если {R} является подмножеством {Z}, то платформа может быть названа защищенной при требованиях R.

В противном случае платформа будет являться частично защищенной. Разность множества {R} и пересечения {Z} и {R} в этом случае опишет подмножество незащищенных связей платформы.

Надо отметить, что подход, предложенный в новом документе ФСТЭК [31], методологически достаточно близок к описанному в данной статье. С точки зрения применения криптографических механизмов в рамках платформ подход описан также в [32].

ВЫВОДЫ

Предлагаемая интеграционная модель защищенной цифровой платформы, включающая вертикальное разделение по уровням абстракций представления данных и уровням обеспечения информационной безопасности и содержащая основной стек технологий, определенных Направлениями стратегического развития РФ, а также оценки уровня интеграции и защищенности предлагаемой модели, может служить основой построения и развития технологий цифровых платформ в целях их применения для цифровой трансформации и цифровизации различных отраслей экономики и общественного производства Российской Федерации.

В данной статье взаимодействие предметных областей научных исследований с отсылками к публикациям описано в соответствии с результатами работ по теме 0003-2019-007 (государственное задание Министерства науки и образования РФ (2019-2021гг.): «Исследования в области перспектив развития технологий цифровых финансовых активов (криптовалют) и распределенных реестров (блокчейн) для их применения в сфере цифровой трансформации технологий и экономики Российской Федерации».

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ «О Стратегии научно-технологического развития Российской Федерации». URL: http://static.kremlin.ru/media/acts/files/0001201612010007.pdf (Дата обращения: 27.11.2021).

2. Указ Президента РФ от 15.03.2021 N 143 "О мерах по повышению эффективности государственной научно-технической политики". URL: https://inecon.org/docs/2021/Ukazy_GNTP_20210315.pdf (Дата обращения: 27.11.2021).

3. Рязанова А.А. Обоснование свойств цифровых платформ в рамках субъектно-объектной модели компьютерных систем // Вестник современных цифровых технологий. 2021. № 7. С. 26-33.

4. Рязанова А.А. Концепция цифровых платформ как подход к интеграции научно-информационных процессов // Научно-техническая информация, сер. 2 Информационные процессы и системы. 2020. №12. С. 9-15.

5. Правиков Д.И., Щербаков А.Ю. Изменение парадигмы информационной безопасности // Системы высокой доступности. 2018. Т. 14. № 2. С. 35-39.

6. Правиков Д.И., Щербаков А.Ю. Концепция информационной безопасности «роя» киберфизических систем // Вестник современных цифровых технологий. 2021. №7. С. 39-44.

7. Правиков Д.И., Тихоненко О.О., Щербаков А.Ю. Прогностика и предиктивная аналитика технических систем как элемент технологической безопасности. Новые подходы // Вестник современных цифровых технологий. 2020. № 3. С. 22-30.

8. Гриняев С.Н., Правиков Д.И., Щербаков А.Ю., Фомин А.Н. Основы общей теории киберпространства // Электронные финансы и новая экономика. Автономная некоммерческая организация "Центр стратегических оценок и прогнозов", Москва. ISBN: 978-5-906661-22-7

9. Правиков Д.И., Щербаков А.Ю., Корнеев Н.В., Тихоненко О.О. Комплексная безопасность систем промышленного оборудования // Вестник современных цифровых технологий. 2020. № 2. С. 30-35.

10. Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Об одном способе хранения и управления ключами в системах квантовых коммуникаций // Вестник современных цифровых технологий. 2020. № 2. С. 14-20.

11. Гриняев С.Н., Правиков Д.И., Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра // Научно-техническая информация, сер. 2 Информационные процессы и системы. 2020. №1. С. 11-18.

12. Верещагина Е.В., Егоров В.И., Сантьев А.А., Хоружников С.Э., Щербаков А.Ю. Современное состояние методологии построения защищенной квантовой сети // Вестник современных цифровых технологий. 2021. № 7. С. 6-14.

13. Володин А.И., Разгуляев К.А., Хан Д.В., Щербаков А.Ю. Принципы и протокол регистрации и распределения квантовых ключей в мультинодовых квантовых сетях // Вестник современных цифровых технологий. 2021. №8. С. 17-22.

14. Рязанова А.А., Щербаков А.Ю. К формулированию положений платформенно-сервисной модели для информационно-телекоммуникационных систем // Научно-технический сборник "Научно-техническая информация", сер. 2 Информационные процессы и системы, 2021. № 5. С.17-20.

15. Касперская Н.И., Кузьменко В.В., Мананников Д.А., Хайретдинов Р.Н., Щербаков А.Ю. К проблеме оценки и обеспечения корректности бизнес-процессов // Безопасность информационных технологий, том 26. № 3. 2019. С. 8-21.

16. Бородулина С.А., Селионов И.А., Тюменцев А.А., Черкашин П.А., Щербаков А.Ю. Принципы создания прототипа универсальной цифровой монеты // Вестник современных цифровых технологий. 2021. № 7. С. 34-38.

17. Щербаков А.Ю., Булыгин А.И., Рябков В.Е., Елизарова А.С. Исследование вопросов применения технологий цифровизации на примере цифрового рейтинга студента // Вопросы кибербезопасности. 2019. №3 (30). С. 33-38.

18. Рязанова А.А., Анисимова А.Э. О методике сравнительного квалификационного анализа требований к профессиональным навыкам с целью коррекции национальных образовательных программ // Научно-технический сборник "Научно-техническая информация", сер. 2 Информационный процессы и системы, 2019. № 2. С. 29-35.

19. Николаев А. Блокчейн и искусственный интеллект. URL: https://vc.ru/u/739868-andrey-nikolaev/238947-blokcheyn-i-iskusstvennyy-intellekt (Дата обращения: 24.11.2021).

20. Привалов А. Блокчейн стартапы в области искусственного интеллекта https://cryptochill.ru/ai-blockchain-cryptocurrency/ (Дата обращения: 24.11.2021).

21. Танг Динх, Ми Тай. Искусственный интеллект и блокчейн: идеальная пара. URL: https://www.osp.ru/os/2018/04/13054611 (Дата обращения: 24.11.2021).

22. Запечников С.В. Доказательства с нулевым разглашением и их применения при обработке информации в недоверенных средах // Вестник современных цифровых технологий. 2021. № 6. С. 11-22.

23. Запечников С.В., Щербаков А.Ю. Конфиденциальное машинное обучение с нулевым разглашением // Вестник современных цифровых технологий. 2021. № 7. С. 15-25.

24. Гостев С.С., Гриняев С.Н., Щербаков А.Ю., Правиков Д.И. К развитию методологии создания доверенных и защищенных информационных систем, построенных с использованием технологии распределенных реестров // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 3-2. С. 10-15.

25. Касперская Н.И., Кузьменко В.В., Хайретдинов Р.Н., Щербаков А.Ю. О подходах к созданию универсального доверенного распределенного реестра, обеспечивающего неразглашение данных о системе // Безопасность информационных технологий = IT Security. Том 26. № 1. 2019. С. 6-19.

26. Трент МакКонахи. Чем может блокчейн помочь искуственному интеллекту? https://bitjournal.media/28-09-2017/ot_ii_do_blokchejna_ot_blokchejna_k_dannym_vstrechajte_ocean/ (Дата обращения: 24.11.2021).

27. Berners-Lee T., Hendler J., Lassila O. The Semantic Web // Scientific American Magazine. – May, 2001.

28. Рязанова А.А., Щербаков А.Ю. К вопросу о метриках сходства текстов для методов их автоматизированного сравнения // Приоритетные задачи и стратегии развития технических наук. Выпуск II. Сборник научных трудов по итогам международной научно-практической конференции (25 мая 2017 г.), г. Тольятти. С. 66-69.

29. Рязанова А.А., Щербаков А.Ю. Архитектура искусственных интеллект-помощников и мега-интернет // Актуальные проблемы технических наук в России и за рубежом Сборник научных трудов по итогам международной научно-практической конференции. 2016. С. 172-175.

30. Рязанова А.А., Щербаков А.Ю. Искусственный интеллект как феномен имитации // Вестник современных цифровых технологий. 2019. №1. С. 56-61.

31. Методический документ. Методика оценки угроз безопасности информации. URL: https://fstec.ru/component/attachments/download/2919 (Дата обращения: 27.11.2021).

32. Щербаков А.Ю. Перспективы современной криптографии // Проектирование будущего. Проблемы цифровой реальности. 2020. № 1 (3). С. 227-233.