

## ЕДИНАЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ ПЛАТФОРМА НА БАЗЕ ЗАЩИЩЕННЫХ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ КОСМИЧЕСКИХ ВОЙСК

**Холод Иван Иванович,**

г. Санкт Петербург, Россия, ivan.holod@nicetu.spb.ru

**Беляев Сергей Алексеевич,**

г. Санкт Петербург, Россия, beliaev@nicetu.spb.ru

**Вайнтрауб Анатолий Изидорович,**

г. Санкт Петербург, Россия, wai@nic.spb.ru

**Аннотация.** В данной статье описывается построения облачной платформы для интеграции информационных систем эксплуатируемых в космических войсках на базе защищенных технологий. Такой подход позволяет интегрировать информацию по средствам ПРН, ККП, НАКУ и возможными перспективными системами. Такая интеграция позволит применять к ней современные методы анализа и решить качественно новые аналитические задачи.

**Ключевые слова:** облачные технологии, защищенная облачная платформа, интеллектуальный анализ данных, data mining.

**Сведения об авторах:** Холод И.И., к.т.н., доцент кафедры вычислительная техника Санкт Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина) Заместитель главного конструктора АО «НИЦ СПб ЭТУ»;

Беляев С.А., к.т.н., доцент кафедры МО ЭВМ Санкт Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина);

Вайнтрауб А.И., к.в.н, доцент, заместитель главного конструктора АО «НИЦ СПб ЭТУ»

---

### Введение

В настоящее время в космических войсках (КВ) функционируют несколько автоматизированных информационно-аналитических систем, разработанных в рамках различных ОКР. Данные системы разрабатывались разными предприятиями, в разные годы и в результате имеют существенные различия, в части:

- аппаратных платформ: используются ПЭВМ и сервера закупленные в период с 90-х годов прошлого века, до настоящего времени;
- операционных систем (ОС): используются ОС семейства Windows (Windows NT, 2000 и др.), MS BC, AstraLinux и др.
- систем управления базами данных (СУБД): используется Oracle, PostgreSQL, Линтер и др.;
- архитектур: клиент-серверные, терминальные, «настольные», тонкого клиента и др.
- протоколов взаимодействия: FTP, SOAP и др.

Независимая разработка каждой системы приводит к дублированию в них:

- информационной составляющей в части: нормативно-справочной информации, характеристик объектов и т.п.
- прикладной составляющей в части: сбора и ведения информации, решения функциональных задач, подготовки аналитических отчетов и др.

Такая ситуация приводит к следующим проблемам в эксплуатации систем:

- сложность замены (модернизации) как аппаратных, так и программных средств в связи с их разнородностью;

- повышенные требования к квалификации эксплуатирующего персонала в связи с необходимостью знаний различных технологий (ОС, СУБД и др.);
- быстрое устаревание аппаратной составляющей и не возможность ее замены в связи с сильной зависимостью от программного обеспечения;
- сложность обеспечения безопасности информации в связи с использованием различных средств безопасности и различным уровнем сертификации;
- не равномерная загрузка вычислительных средств;
- высокое электропотребление при простоях систем;
- невозможность получения аналитики по совокупности информации, хранящейся в разных системах.

Проблемы усугубляются с разработкой каждой новой системы, т.к разрабатываются они, как правило, независимо от уже существующих, тем самым внося свою лепту в разнородность используемых средств.

### Мировой и отечественный опыт

В мировой практике для решения данных проблем применяют бурно развивающиеся технологии облачных вычислений. Эти технологии представляет собой модель обеспечения доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, вычислительным серверам, устройствам хранения данных, системам и сервисам — как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и/или обращениями к поставщику [1]:

В настоящее время выделяют несколько основных моделей облачных вычислений [1].

- программное обеспечение как услуга (SaaS — Software as a Service);
- платформа как услуга (PaaS — Platform as a Service);
- инфраструктура как услуга (IaaS — Infrastructure as a Service);
- рабочее место как услуга (WaaS — Workplace as a Service).

Среди мировых лидеров в области разработки технологий облачных вычислений можно назвать компании: Amazon [2], Google Inc [3], Microsoft [4] и др.

Они построены на платформе Apache Hadoop [5] и предоставляют масштабируемую инфраструктуру для выполнения созданных пользователем (по определенным правилам) приложений.

Существуют решения на базе облачных вычислений и для министерства обороны США. В качестве примера можно привести систему Army Private Cloud (APC2) [6]. Данная система на базе облачных вычислений предоставляет сервисы по заключению и отслеживанию выполнения контрактов с МО США. Данный сервис доступен как подразделениям МО, так и частным компаниям.

Из отечественных решений можно выделить национальную облачную платформу [7] — комплекс интегрированных информационных систем, предназначенный для предоставления органам исполнительной власти различного уровня, органам местного самоуправления, коммерческим организациям и физическим лицам прикладные сервисы в сфере здравоохранения, образования, безопасности, жилищно-коммунального хозяйства, имущественно-земельных отношений. Для предприятий малого и среднего бизнеса созданы сервисы для организации работы офиса, управления взаимоотношениями с клиентами, учёта торговых и производственных операций.

Все перечисленные облачные сервисы обладают двумя существенными недостатками:

1. требуют загрузку данных в свое хранилище, что потенциально повышает гриф информации и требования к обеспечению безопасности;
2. используют программные средства, не разрешенные для использования в государственных структурах и в особенности МО РФ.

Эти недостатки делают невозможным их применение для разработки в области государственных структур и в частности в военной технике.

Однако принципы и технологии, заложенные в них, можно успешно использовать при построении защищенного «облака» в интересах МО РФ. Примером такого развития являются проекты Глобус [8] разработки компаний ОАО Северное конструкторское бюро и проект SeaCloud компании ОАО «Си-Проект» [9].

Глобус – защищенная облачная платформа, построенная на базе ОС Astra Linux Special Edition и системы с открытым кодом OpenStack. Данное решение позволяет строить облачные платформы уровня IaaS для виртуализации в них различных АС.

SeaCloud – платформа также ориентирована на предоставления сервисов уровня IaaS. Использует защищенную ОС Astra Linux Special Edition. Концепция SeaCloud предполагает создание виртуальных образов функционирующих рабочих мест и серверов и размещение их в «облаке». За счет фиксации контрольных сумм снятых образов предполагается сохранение целостности и валидности полученных на эти системы сертификатов.

Обе системы, несмотря на использование ОС Astra Linux Special Edition имеют общие недостатки:

- на данный момент не сертифицированы (не имеют сертификатов по НДВ ни по одному классу защищенности);
- не решают проблемы разграничения доступа к информации с различным уровнем защиты;
- ограничиваются уровнем IaaS не предоставляя пользователю дополнительных сервисов (например, аналитических сервисов).

### Архитектура защищенной облачной платформы

Построение защищенной облачной платформы должно решать следующие задачи:

- размещение существующих и вновь разрабатываемых АС на вычислительных ресурсах облака в защищенной среде;
- централизованный доступ к единой НСИ, актуальным характеристикам контролируемой информации и др.;
- проверка доступа, достоверности и др. виды обработки едиными унифицированными алгоритмами;
- решение аналитических и расчетных задач, в том числе статический и интеллектуальный анализ для выработки рекомендаций;
- разграничение доступа к информации в зависимости от грифа информации и уровня доступа пользователя и др.

Первая задача во многом решается существующими средствами систем Глобус и SeaCloud. Остальные задачи требуют новых решений. Для этого предлагается построение защищенной облачной платформы с единым информационным пространством в соответствии с архитектурой, представленной на рисунке 1.

Данная платформа будет включать в себя два уровня:

- физический уровень;
- виртуальный уровень.

На физическом уровне будет размещаться аппаратно-программное обеспечение, реализующее необходимые функции для работы виртуального уровня.

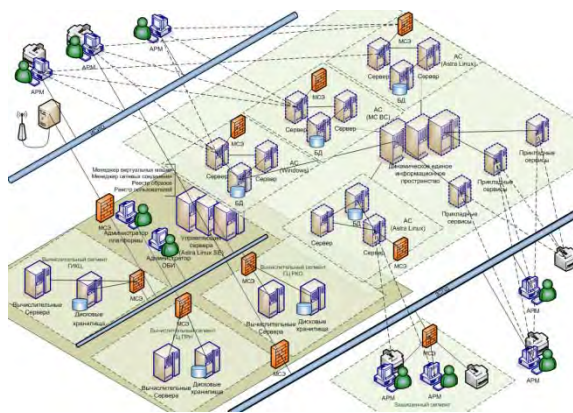


Рис. 1. Архитектура интегрированной информационно-аналитической защищенной платформы.

Аппаратное обеспечение будет включать в себя следующие элементы:

- управляющие сервера – предназначенные для работы на них специального программного обеспечения (СПО) обеспечивающего работу платформы (в качестве такого СПО может быть использована платформа Глобус);
- рабочее место администратора платформы – отвечающего за управление всей платформой;
- рабочее место администратора ОБИ - отвечающего за настройку прав доступа к ресурсам платформы;
- вычислительные сегменты – предназначенные для выполнения на них виртуальных машин с системами эксплуатирующимися в ГИКЦ, ГЦ ПРН, ГЦ РКО и др.

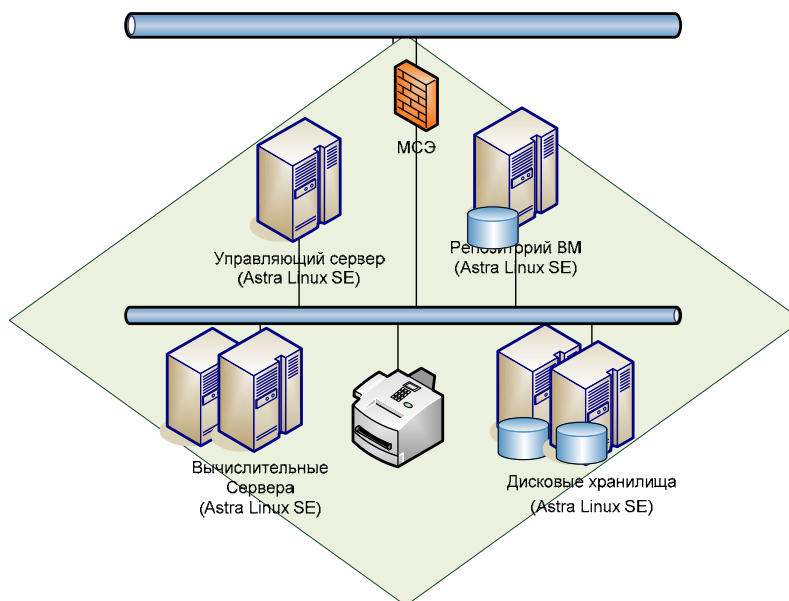


Рис. 2. Архитектура вычислительного сегмента

Каждый вычислительный сегмент (рис. 2) должен включать в себя:

- межсетевой экран – обеспечивающий разграничение доступа к ресурсам сегмента;
- управляющий сервер – отвечающий за управление виртуальными машинами внутри сегмента;
- репозиторий виртуальных машин – хранящий образы виртуальных машин с системами эксплуатируемыми в отдельном центре соответствующий данному сегменту;
- вычислительные сервера, на которых будут выполняться виртуальные машины с системами эксплуатируемыми в отдельном центре соответствующий данному сегменту;
- дисковые хранилища, на которых будет сохраняться информация систем выполняющихся в данном сегменте.

Виртуальный уровень будет включать в себя виртуальные машины, выполняющиеся на доступных вычислительных серверах. Такие виртуальные машины могут быть как образами уже эксплуатируемых систем, так и виртуальными машинами, созданными по требованиям для вновь разрабатываемых систем.

Для сохранения функционирования существующих систем они должны быть перенесены в «облако» на виртуальные машины, настроенные в соответствии с требованиями предъявляемыми данными системами к аппаратной части. Для обеспечения целостности, а также актуальности сертификатов выданных на системы, они должны сниматься целиком в виде виртуальных образов. При этом виртуализации должны подвергаться серверные машины: сервера приложений, базы данных, межсетевые экраны и т.п. Сетевая конфигурация между реальными машинами так же должна сохраняться и воспроизводиться на виртуальном уровне в «облаке».

С клиентских машин доступ к ним будет осуществляться (в зависимости от архитектуры системы) или в терминальном режиме или через протоколы, реализованные в системах. При этом доступ от клиентских рабочих мест к соответствующим виртуальным машинам должен будет регламентироваться как на виртуальном уровне (в соответствии с политикой безопасности, определенной для данной системы), так и на физическом уровне, с точки зрения доступа пользователей в соответствующие вычислительные сегменты. Для систем, работающих с грифом информации «С» и выше, рабочие места должны подключаться к облаку или через выделенные каналы или через защищенную систему передачи данных (ЗСПД).

Для прозрачности доступа к ним с рабочих мест виртуальные машины должны сохранять IP адреса. Таким образом, конечные пользователи будут осуществлять работу без изменения.

При таком подходе абонентами «облака» будут выступать подчиненные подразделения. Они будут являться как поставщиками информации в «облако», так и ее потребителями. Таким образом, в «облаке» будет интегрироваться вся информация, относящаяся к КВ. При этом физически информация будет размещаться на разных сегментах облака, но объединенных высокоскоростными каналами (за счет их локального компактного размещения). Такая интеграция дает возможность значительно повысить аналитические возможности облака.

### Динамическое информационное пространство

Интеграция информации из систем, эксплуатируемых в ГИКЦ, ГЦ ПРН и ГЦ РКО позволит решить следующие задачи:

- оценивание технического состояния и возможностей своих сил и средств;
- генерирование возможных сценариев действий (боевых действий) и отбор среди них нескольких наилучших и предъявление их командованием для принятия решения;
- оценивание состава (боевого состава) и возможностей (боевых возможностей) орбитальных группировок основных иностранных государств;
- разведка космической обстановки как в стратегической космической зоне (СКЗ) в целом, так и в оперативных космических зонах;
- выявление разведывательных усилий основных иностранных государств по территории и объектам РФ с помощью космических средств;
- оперативное выявление изменений в составе деятельности орбитальных группировок;
- информационное обеспечение боевых задач поражения и подавления КА противника и применения средств защиты отечественных КА;
- моделирование космической обстановки и динамики ее развития в соответствии с разработанными сценариями боевых действий в космосе;
- организация взаимодействия между соединениями, эксплуатирующими средства ККП (ПРН) и НАКУ:
  - при возникновении опасности столкновений иностранных КА или фрагментов космического мусора с действующими отечественными КА;
  - при преднамеренных сближениях иностранных КА с отечественными КА;
  - при захватах, повреждениях и разрушениях отечественных космических аппаратов;
  - оценки военно-космической деятельности (ВКД) для оперативного информирования высшего военно-политического руководства государства и принятия решения на применение сил и средств в различных условиях стратегической, оперативной и тактической обстановки, а именно:
    - предупреждения о подготовке и начале боевых действий в космосе и из космоса;
    - оповещения об опасных ситуациях для космических и наземных объектов, включая информацию оповещения о пролетах иностранных разведывательных ИСЗ;
    - информационного обеспечения боевых действий взаимодействующих систем и войск;
    - контроля за соблюдением международных договоров по использованию космического пространства, в том числе в интересах правовой защиты космических аппаратов (КА) Российской Федерации;
    - информационного обеспечения дальнейшего освоения Российской Федерацией и другими государствами околоземного космического пространства и безопасности полетов КА;

- обеспечения эталонными данными информационных средств;
- информационного обеспечения действий по управлению силами и средствами соединений, входящих в Космические войска.

Для решения перечисленных задач в единое информационное пространство КВ должна поступать следующая информация:

От НАКУ:

- информация о составе, состоянии и качестве функционирования отечественных космических систем;
- информация о перспективных космических программах и сроках их выполнения;
- информация о состоянии и программ действия отечественных космических полигонов и трасс вывода КА на орбиту;
- тактические, технические, весогабаритные и специальные характеристики отечественных КА, ракет-носителей и разгонных блоков;
- координатная и некоординатная информация от подчиненных средств наблюдения за космическими объектами (НАКУ и КОС);
- информация по предстоящим и выполненным запускам и маневрам отечественных КА;
- информации о параметрах движения отечественного КА
- информация по разрушениям отечественных КА (причина разрушения, район разрушения, степень загрязнения космического пространства продуктами разрушения и другая информация);
- информации о прекращении функционирования отечественного КА

От средств ККП и ПРН

- информация об общей космической обстановке;
- информация о космических системах иностранных государств, их характеристиках и боевых возможностях;
- информация о запусках, параметрах движения, маневрах и прекращении функционирования КА (КО);
- координатная и некоординатная информация от подчиненных средств наблюдения за космическими объектами;
- результаты расчетов и выявления следующих фактов изменения космической обстановки:
  - воздействия на отечественный КА;
  - опасные ситуации, создаваемые КА противника наземным объектам;
  - запуск нового космического объекта;
  - изменение орбиты КА (маневр КА);
  - изменение состояния КА, при этом даётся оценка возможности воздействия на КА наземного либо космического средства поражения;
  - прекращение существования КА: вход в плотные слои, разрушение, увод КА с орбиты, сход с орбиты и посадка.

Для решения перечисленных задач, с учетом физически разделенного хранения информации, предлагается построение динамического единого информационного пространства на виртуальном уровне (рис. 1). Такое пространство не будет аккумулировать всю информацию в одном месте. Информация будет храниться в исходных местах. Динамическое пространство будет выполнять роль посредника между ними и аналитическими сервисами, запрашивающими необходимую информацию. Решение данной задачи осложняется следующим проблемами, которые возникают при интеграции информации из нескольких гетерогенных источников:

- неоднозначность – в разных системах одни и те же сущности имеют различные способы кодирования (например, номера КА), используют различные единицы измерений и т.д.
- дублирование – наличие одинаковой информации в разных источниках;
- противоречие – наличие различной информации в разных источниках об одном объекте или событии;
- разнородность информации – информация, хранящаяся в разных источниках, имеет разные форматы, принципы представления и хранения.

При создании классических хранилищ данных [10] для решения данных проблем используются технологии извлечения, преобразования и загрузки данных (ETL – Extract Transform Load) [11]. Стандартные ETL системы извлекают информацию из исходной базы данных, преобразуют ее в формат,

поддерживаемый интегрированным хранилищем, а затем загружают в него преобразованную информацию. При этом конфигурация и настройки извлечения, преобразований и загрузки описываются заранее и хранятся в виде метаданных процесса трансформации. Они включают в себя следующее:

- конфигурация извлечения – список данных подлежащих извлечению, правила извлечения (например, порядок) и т.п.;
- конфигурация преобразований – алгоритмы преобразований (например: очистка, нормализация, пересчеты единиц измерений и т.п.), настройки преобразований и т.п.;
- конфигурация загрузки – правила сопоставления атрибутов исходной информации и атрибутов принимающего хранилища.

В отличие от стандартного ETL процесса для построения динамического информационного пространства предлагается замена последнего этапа, загрузки данных, на этап запроса данных. На этом этапе формируется запрос на получения данных в формате (в терминах) приемника. Данный запрос должен преобразовываться (переводиться) к запросу в терминах источника информации. Извлеченная в соответствии с данным запросом информация должна быть извлечена и преобразована в соответствии с заданными настройками, как и в стандартном процессе.

Процесс извлечения и преобразования будет описываться для каждого источника информации. Таким образом, работа динамического информационного пространства для КВ будет выглядеть, так как она представлена на рисунке 3.

Для работы с несколькими БД на этапе формирования запроса, должны выполняться следующие действия:

- разделение запроса – формирование на основе запроса пользователя нескольких запросов к нескольким источникам данных;
- перевод запроса с терминологии приемника на терминологию соответствующего источника;
- слияние результатов – объединение результатов полученных в результате извлечения и преобразования от каждого источника.

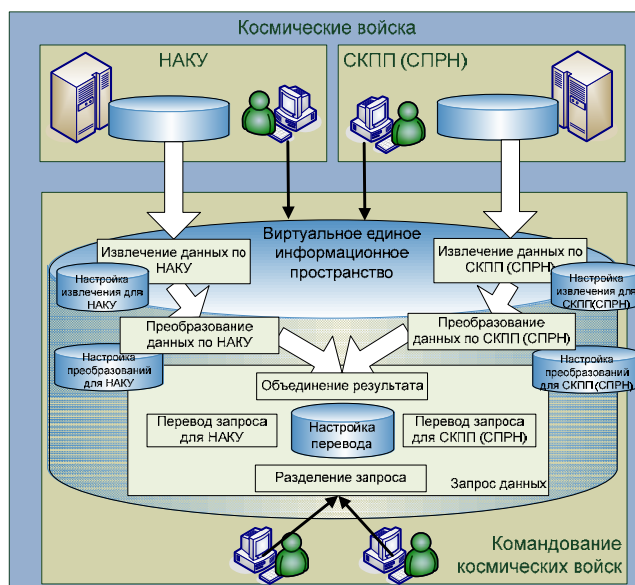


Рис. 3. Архитектура единого-информационного пространства КВ

Динамическое единое информационное пространство будет включать в себя программное обеспечение выполняющее формирование запросов к источникам информации, извлекающее данные из них и преобразующее извлеченную информацию. Для каждого источника должны разрабатываться свои модули: извлечения данных, преобразования данных и перевода запросов. Они должны работать в соответствии с настройками заданными для этих источников. Модули разделения запросов и объединения

результатов должны быть общими для всех источников информации и работать в соответствии с настройками перевода.

Основным недостатком такого подхода является низкая скорость выполнения запросов. Задержки возможны вследствие, преобразования запросов, преобразования данных, передачи данных по сетям. Однако в случае, когда источники информации размещаются в «облаке» данная проблема нивелируется.

### Заключение

В статье описывается архитектура облачной платформы, построенной на базе защищенных средств для космических войск. Описывается подход виртуализации эксплуатируемых автоматизированных информационных систем и их размещение в облаке. Для выполнения аналитических задач над объединенной информацией предлагается создание динамического информационного пространства, осуществляющего трансформацию запросов пользователей к нему в запросы к исходным источникам информации. Это позволяет решить проблемы с разграничением хранения информации имеющей различные грифы и относящейся к разным центрам, а также проблемы с её актуализацией. За счет размещения исходных информационных систем в едином вычислительном кластере устраняется основной недостаток такого подхода – низкая скорость доступа к данным.

### Литературы

1. Mell Peter, Grance Timothy. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. Gaithersburg. 2011.
2. Amazon Elastic MapReduce. Developer Guide. <http://s3.amazonaws.com/awsecs/ElasticMapReduce/latest/emr-dg.pdf>.
3. Google Developers. Google BigQuery. <https://developers.google.com/bigquery/what-is-bigquery?hl=ru>.
4. SQL Server Data Mining. Home. <http://www.sqlserverdatamining.com/ssdm/> [электронный ресурс].
5. Tom White. Hadoop: The Definitive Guide. T. White. USA.: O'Reilly Media, 2009. pp 526.
6. Army Private Cloud (APC2) <http://h10131.www1.hp.com/public/contract-vehicles/apc2/>
7. Национальная облачная платформа. <https://www.o7.com/#main> [электронный ресурс]
8. <http://лаборатория50.рф> [электронный ресурс].
9. <http://www.seaproject.ru/products/seacloud>.
10. Ralph Kimball, Joe Caserta. The Data Warehouse ETL Toolkit. Wiley Press, 2004.
11. Анализ данных и процессов. / А.А.Барсегян, М.С.Куприянов, И.И.Холод, М.Д.Тесс, С.И.Елизаров. СПб.: БХВ-Петербург, 2009. 512 с.: ил.



## UNIFIED INFORMATION AND ANALYTICAL PLATFORM BASED ON SECURE CLOUD TECHNOLOGY FOR SPACE FORCES

**Kholod Ivan Ivanovich,**

St.Petersburg, Russian, ivan.holod@nicetu.spb.ru

**Belyaev Sergey Alekseevich,**

St.Petersburg, Russian, beliaev@nicetu.spb.ru

**Vaintraub Anatoly Isidorovich,**

St.Petersburg, Russian, wai@nic.spb.ru

**Abstract.** This article describes how to build a cloud platform for the integration of information systems operated in the space forces based on a protected technology. This approach enables the integration of information by means of PRN, PSC, NACU and possible future systems. This integration will allow to apply the modern methods of analysis and to solve new analytical problems.

**Keywords:** cloud computing, secure cloud platform, intellectual data analysis, data mining.

### References

1. Mell Peter, Grance Timothy. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. Gaithersburg, 2011.
2. Amazon Elastic MapReduce. Developer Guide. <http://s3.amazonaws.com/awsdocs/ElasticMapReduce/latest/emr-dg.pdf>.
3. Google Developers. Google BigQuery. <https://developers.google.com/bigquery/what-is-bigquery?hl=ru>.
4. SQL Server Data Mining. Home. <http://www.sqlserverdatamining.com/ssdm/>
5. Tom White. Hadoop: The Definitive Guide. T. White. USA.: O'Reilly Media, 2009. 526 p.
6. Army Private Cloud (APC2) <http://h10131.www1.hp.com/public/contract-vehicles/apc2/>
7. National cloud platform. <https://www.o7.com/#main> [электронный ресурс].
8. <http://лаборатория50.рф> [электронный ресурс].
9. <http://www.seaproject.ru/products/seacloud> [электронный ресурс].
10. Ralph Kimball, Joe Caserta. The Data Warehouse ETL Toolkit. Wiley Press, 2004.
11. Analyze of data and processes. /A.A.Bargesyan, M.S. Kuprijanov, I.I.Kholod, M.D. Tess, S.I. Elizarov. SPb.: BHV: Petersburg, 2009. 512 p.

**Information about authors:** Kholod I.I., PhD, Associate Professor SPbSETU imeni V.I. Ulyanova (Lenina) Deputy Chief Designer of AO «NIC SPB ETU»;  
Belyaev S.A., PhD, Associate Professor SPbSETU imeni V.I. Ulyanova (Lenina);  
Vaintraub A.I., PhD, Associate Professor, Deputy Chief Designer of AO «NIC SPB ETU»;