

ПЕРСПЕКТИВЫ СОЗДАНИЯ ЕДИНОЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ БАЗЫ С ИСПОЛЬЗОВАНИЕМ ЗАЩИЩЕННЫХ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ПРОВЕДЕНИЯ РАЗВЕДЫВАТЕЛЬНЫХ ОПЕРАЦИЙ

PROSPECTS FOR CREATING A UNIFIED INFORMATION AND ANALYTICAL BASE USING SECURED CLOUD TECHNOLOGIES FOR INTELLIGENCE OPERATIONS

V. Moiseenko

Summary. The article discusses the prospects for creating a unified information and analytical base using secure cloud technologies for conducting intelligence operations. The relevance of the development of cloud technologies in the military sphere is substantiated. Cloud storage models are described. The structure of the information and analytical base for the purpose of conducting intelligence operations has been determined. It is concluded that the creation of a unified information and analytical base using secure cloud technologies for conducting reconnaissance operations in the future should be represented at the level of data collection by heterogeneous means of communication (ground, air, space, tactical) into a single global network of uninterrupted data transmission via a unified protocol, the level of automated management of the collection, processing, storage, assessment of intelligence data with geospatial reference, formalization by objects and bringing them to the tactical group and the level of a single information space in which information is processed and analyzed.

Keywords: cloud technologies, information and analytical base, information security, infrastructure, data, data center.

Моисеенко Вадим Олегович

Военнослужащий в войсковой части, г. Новочеркасск
moiseenko.business@mail.ru

Аннотация. В статье рассматриваются перспективы создания единой информационно-аналитической базы с использованием защищенных облачных технологий для проведения разведывательных операций. Обоснована актуальность развития облачных технологий в военной сфере. Описаны модели облачного хранилища. Определена структура информационно-аналитической базы в целях проведения разведывательных операций. Сделан вывод о том, что создание единой информационно-аналитической базы с использованием защищенных облачных технологий для проведения разведывательных операций в перспективе должно быть представлено на уровне сбора данных разнородными средствами связи (наземными, воздушными, космическими, тактическими) в единую глобальную сеть бесперебойной передачи данных по единому протоколу, уровне автоматизированного управления сбора, обработки, хранения, оценки разведывательных данных с геопространственной привязкой, формализацией по объектам и доведение их до тактических групп и уровне единого информационного пространства, в котором происходит обработка и анализ информации.

Ключевые слова: облачные технологии, информационно-аналитическая база, защита информации, инфраструктура, данные, дата-центр.

По данным компании Selectel, в конце 2022 года рост российского рынка облачных технологий составил 44 % по сравнению с 2021 годом.

Оценка RuVDS показала, что если в 2022 году 32 % компаний — пользователей облачных сервисов относились к иностранным клиентам, то в последнем квартале 2023 года этот показатель достиг 37 %, при этом основными клиентами стали Европа, Восток и Средняя Азия. Рост спроса на услуги российских провайдеров в 2023 году составил 20–30 %. Основным направлением развития ИТ-сферы является развитие облачных мощностей, активное внедрение решений и архитектур, построенных на разных облачных платформах. При этом более половины запросов от частных компаний к провайдерам были направлены на подключение IaaS (инфраструктура

как услуга) и включали требования разнообразия архитектуры, индивидуальные решения, усиление информационной безопасности, устойчивости от кибератак [7].

Отмечается рост спроса на услуги облачные ресурсы хранения персональных данных и виртуальных машин, на которые можно устанавливать операционную систему, периферические устройства, одним из преимуществ которых является гибкость управления сценариями переключения, возможность устанавливать на один ПК несколько виртуальных машин.

Таким образом, рост ИТ-рынка ориентирован в целом на отказ от модели локального развертывания программного обеспечения на базе инфраструктуры непосредственно компании и сосредоточении на возможностях «облака».

По данным Stack Group и M1Cloud, к концу 2023 года рынок облачных технологий составил более 40 % всего ИТ-рынка. При этом основная концентрация усилий представлена в сфере логистических и облачных решений, проектирование и создание альтернативных платформ для разных сегментов рынка [6].

Правительственные организации, в частности, учреждения Министерств обороны разных стран, не являются исключением в своем стремлении обладать облачным потенциалом. Например, США использует облачное хранилище с целью планирования развертывания ресурсов, которые ранее находились стационарно в центрах обработки данных. Такой подход обеспечил достижение трех целей: согласованность действий и принятия решения, повышение управляемости и осведомленности в едином пространстве. Китай, Индия, Иран, Япония вкладывают достаточно большие инвестиции в разработку военных НИОКР, технологии применения искусственного интеллекта и облачных хранилищ. В Японии и Южной Корее масштабность милитаризации привела к военному партнерству государства и частных компаний в сфере ИТ, космоса, логистики, робототехники, энергетики, а также био- и нано-разработок. В целом развитие ИТ-рынка показывает, что вопросы национальной безопасности и повышение обороноспособности посредством применения новых технологий становятся на первое место.

В традиционном понимании облачные технологии представляют собой технологии обработки данных, где информационные ресурсы предоставляются пользователю в Интернете в качестве сервиса, при этом инфраструктура, программное обеспечение и операционные системы хранятся у поставщика услуги [3; 9].

На сегодняшний день сущность облачных технологий базируется на предоставлении услуг вычислительных компаний через Интернет (так называемое «облако») посредством хранилищ данных, серверов, программного обеспечения, аналитики и интеллектуального анализа. На данный момент представлены три модели облачных вычислений:

1. Модель IaaS: поставщик услуг предоставляет физическое пространство для хранения информации, при этом в зоне ответственности владельца баз данных лежит программное обеспечение, включая приложения и сами данные, а также его безопасность.
2. Модель PaaS: поставщик облачных услуг обслуживает операционную систему, программное и аппаратное обеспечение. При этом разработчик получает доступ к инфраструктуре и инструментам для разработки, тестирования и развертывания приложений. Владелец оплачивает услугу и отвечает за данные и приложения.

3. Модель SaaS: поставщик услуг отвечает за всю инфраструктуру, приложения и доступ к ним через Интернет [1].

Кроме того, постоянное развитие технологий способствует появлению новых типов сервисов, например, EaaS или XaaS — «Все как сервис», которая заключается в предоставлении поставщиком услуг облака в виде единого сервиса (приложения, инфраструктура, бизнес-процессы).

Учитывая модели облачного хранилища, следует обозначить, что в целях разведывательных операций модель должна носить либо локальный характер развертывания, либо гибридный, когда облачная инфраструктура совмещает публичное и локальное облако. При этом должны быть определены:

1. требования и задачи хранения, обработки, обмена разными видами данных теми или иными участниками (Минобороны, командиры, штабы, разведывательные группы и др.);
2. выбор облачного провайдера с точки зрения требований безопасности, доступности, масштабируемости [2];
3. проектирование и разработка архитектуры системы с учетом принципов безопасности, включая сетевые конфигурации, уровни доступа, шифрование данных в покое и в движении, а также резервное копирование и восстановление данных;
4. требования к управлению ключами и инструментами для шифрования;
5. проектирование и разработка приложений и сервисов, обслуживающих базу данных и совместимых с облачной инфраструктурой;
6. уровни настройки системы мониторинга и анализа угроз: отслеживание аномалий, подозрительной активности, потенциальных угроз [8];
7. регулярность проведения тестирования и аудита безопасности: выявление слабых мест, наличие уязвимостей, устранение потенциальных проблем [7];
8. обновляемость облачных технологий и уровней их защиты;
9. обучение сотрудников пользованию сервисами, приложениями, хранению паролей, способам управления безопасностью и выявлению угроз [5].

Исходя из анализа сущности, задач, содержания и тенденций развития облачных технологий, целесообразно определить структуру информационно-аналитической базы в целях проведения разведывательных операций:

1. Закрытое облачное хранилище служебных и секретных данных в рамках сети территориально распределенных центров обработки данных

(ЦОД). В целях разведывания обстановки в ЦОД размещаются электронные карты и 3D-модели местности. Принцип работы ЦОД заключается в использовании, обработке и передаче больших данных посредством системы высокопроизводительных вычислений. В рамках сети оптимальным вариантом является электронная почта, включая отдельную сеть с грифом «секретно». Закрытые каналы позволяют получать геопрограммную информацию, в частности, карты, в условиях подавления тех или иных систем связи (например, спутниковой). Облачные технологии позволяют оперативно получить актуальную, достоверную цифровую информацию. Внедрение сегмента по генерированию 3D-моделей местности будет способствовать эффективному взаимодействию группировок войск и штабов для проведения разного рода разведывательных действий и разработке операций [4]. Такой подход направлен на оценку местности, определение угроз со стороны противника и эффективное управление подготовкой и проведением операций. Получение цифровых карт из облака в условиях разведывательных операций позволяет решать следующие задачи:

- отсутствие необходимости печати карт: командир получает обновленные карты практически мгновенно, при этом четкая ориентация на местности позволяет точно определить место дислокации, районы, которые должны занять войска. Наличие возможности просмотра карты местности в реальном режиме времени направлено на повышение управляемости передвижения войсками;
- возможность оперативного обращения к топографическому онлайн-хранилищу отдельных разведывательных групп, в том числе и тех, которые находятся в тылу противника.

Внедрение в облачное хранилище платформ, направленных на решение следующих задач:

- возможность перехода от цифровой карты к реалистичному изображению местности с функцией привязки целей разведки к координатам;
- автоматизированное создание 3D-макета местности в онлайн-режиме с учетом доступности среды противника (город, горы, море и др.) и возможностью определять цели противника;
- широкое использование спутниковых систем для мониторинга, разведки, дешифрирования объектов, оценки перевозимых грузов и др.;
- развертывание GIS-систем на всех уровнях данных дистанционного зондирования Земли (ДЗЗ) с целью поддержки функций проведения мониторинга, разведки и военных операций в защищенных вычислительных средах, в том числе для работы в облачном хранилище в запрещенных, отключен-

ных, прерывистых средах и средах с низкой пропускной способностью. При этом становится возможным использование таких методов обработки данных как машинное чтение, нейронных сетей, гравиметрии (данные о строении Земли), фотограмметрии (определение реальных размеров объекта по его характеристикам) и т.д.;

- аналитического дата-центра, который способен сверхбыстро и сверхточно обрабатывать информацию и позволяет проводить аналитику в онлайн-режиме для оперативного принятия решения.
2. Дата-центр, где компьютеры защищены от внешнего воздействия посредством следующих действий: высокий уровень надежности помещений, автономное электропитание, наличие системы охлаждения и пожарной безопасности, защита от подключения внешних носителей, доступ к информации только по запросу.

Следует отметить, что каждый сегмент представляет собой закрытый автономный центр обработки данных, где задействованы большие данные. В рамках сегмента целесообразно развернуть электронный обмен данными на базе защищенной передачи информации без стандартного доступа в Интернет. Кроме того, доступ к дата-центру имеет строгую ограниченность, компьютеры должны работать исключительно на российском программном обеспечении и защищены от подключений внешних носителей данных. При этом задача центра — шифрование информационных потоков, разбивка на несколько пакетов и передача данных, а также постоянное создание резервных копий в целях недопущения искажения, уничтожения информации.

3. Актуальность пользования топографической информацией в полевых условиях. Для этой цели наиболее оптимальным вариантом целесообразно считать автоматизированную систему электронных карт и 3D-моделей местности высокой точности, в основе которых лежит постоянно обновляемая информация оптических, инфракрасных, лазерных и радиолокационных датчиков, установленных с целью разведывательных операций на беспилотниках, боевых самолетах, кораблях, спутниках.
4. Распределение аналитических данных на базовую и текущую информацию. Первая должна формироваться заблаговременно, однако ее актуализация на месте и получение текущей (оперативной) информации должно осуществляться средствами разведывательных групп (воздушной, космической, наземной, тактической) [6]. В этой связи оперативная формализация данных по объектам должна проводиться со стороны мобильного пункта планирования и координации данных по опре-

деленным зонам. При этом взаимодействие между тактическими войсками и разведывательными группами должна носить автоматизированный характер с контролем доступа по конкретным объектам, однако штабной пункт командования на местности должен иметь возможность вхождения в другие подсистемы разведки с автоматическим включением полученных разведывательных данных по объектам в единую базу. В таком случае сокращается время принятия решения по конкретному объекту поражения. Такой подход обеспечивает эффективное функционирование единой информационно-аналитической базы связано не только с защищенными облачными технологиями, но и комплексным взаимодействием по планированию, обработке данных внутри каждой подсистемы и обмену данными.

Итак, создание единой информационно-аналитической базы с использованием защищенных облачных технологий для проведения разведывательных операций в перспективе должно быть представлено на следующих уровнях:

1. Уровень сбора данных разнородными средствами связи (наземными, воздушными, космиче-

скими, тактическими) в единую глобальную сеть бесперебойной передачи данных по единому протоколу.

2. Уровень автоматизированного управления сбора, обработки, хранения, оценки разведывательных данных с геопространственной привязкой, формализацией по объектам и доведение их до тактических групп. Такой подход позволяет обеспечить территориально-распределительную сеть автоматизированных систем, позволяющую не только обращаться к разным видам данных, но выполнять бизнес-процессы.
3. Уровень единого информационного пространства, в котором происходит обработка и анализ информации, создание на ее основе новой информации для принятия решений разными группами разведки, войск и командованием. Тем самым происходит создание совместное использование информационных ресурсов, объединенных в единую сеть, позволяющих увеличить детальность полученной информации, точность координат объектов поражения, ее корректировку, дальность разведки, сокращение времени на принятие решения командным пунктом.

ЛИТЕРАТУРА

1. Антипка А.В. Облачные вычисления. Модели развертывания систем облачных вычислений / А.В. Антипка // Молодой ученый. 2023. № 6 (453). С. 9–10.
2. Бойкова А.В. Подход к технико-экономическому обоснованию выбора модели облачных технологий для вооруженных сил РФ // Экономика и бизнес: теория и практика. 2023. №8 (102). С. 22–24.
3. Гаврилов В.В., Кузнецов С.В. Интеллектуальный анализ данных. М.: ФИЗМАТЛИТ, 2018. — 448 с.
4. Геоинформационные системы военного назначения: теория и практика применения: материалы IX Респ. науч.-практ. конф., Минск, 12 мая 2023 г. / Белорус. гос. ун-т; редкол.: А.М. Бахарь (гл. ред.) [и др.]; под общ. ред. А.С. Черенко. Минск: БГУ, 2023. С. 98–102.
5. Ковалев А.А., Кудайкин Е.И. Информационные технологии в обеспечении военной безопасности государства // Управленческое консультирование. 2017. №5 (101). С. 20–27.
6. Матвеевский М.М., Сафонов М.А. Организация и ведение разведки в интересах боевого применения ракетных войск и артиллерии в современных операциях // Военная Мысль. 2017. № 10.
7. Мизгирева К.А. Обеспечение кибербезопасности в военной сфере РФ // Седьмые юридические чтения: государство и право в эпоху информатизации. Сборник статей. Том Часть 2. 2020. С. 85–91.
8. Скиба В.А. Синтез информационно-коммуникационного пространства эргатических систем военного назначения // Военная мысль. 2018. №11. С. 39–43.
9. Черпанов С.П. Достоинства и недостатки аппаратных решений систем обработки больших данных // Современные наукоемкие технологии. 2020. № 8. С. 86–89.

© Моисеенко Вадим Олегович (moiseenko.business@mail.ru)

Журнал «Современная наука: актуальные проблемы теории и практики»