Өндірілген пропантты іске асыру нәтижесінде алынған техникалық нәтиже – эксплуатациялық өнімділігі жоғары және құны төмен пропант бөлшектерін алу және оны қолдану арқылы қабаттағы сұйықты өндіру құнын төмендету. Проппант туралы ақпарат, яғни тығыздығы, химиялық құрамы, сфералылығы және беріктілік қоры сияқты ақпарат ұсынылады. Ұсынылған технология жеңіл салмақты (яғни төменгі тығыздықпен), ұшпа күлдің айтарлықтай үлесін қамтитын керамикалық проппанта материалдарына қатысты. Сонымен қатар проппантты дайындау үшін ұшпа күлді пайдаланудың артықшылықтары туралы мәліметтер келтіріледі. Тығыздығы аз және беріктілігі жоғары боксит, ұшпа күл, кварц құмы және балшық негізіндегі проппантты дайындау әдісі сипатталады.

Түйін сөздер: *проппант, беріктілік, қаттылығы, боксит, ұшпа-күл, қабаттың гидравликалық жарылуы , сығылу кернеуі.*

MANUFACTURING PROPPANTS ON THE BASIS OF VOLATILE ASH

A. Shokanov, B. Suleimenov, E. Smikhan

This article describes the methods for the production of proppants - proppants used in the extraction of oil and gas by the method of hydraulic fracturing. The technical result obtained by the implementation of the developed proppant is to obtain proppant particles with high performance and low cost, the use of which leads to a decrease in the cost of the produced fluid. Presents information about proppants. The proposed technology relates to materials of ceramic proppant with a lighter weight (i.e. lower density), containing a significant proportion of fly ash. The data on the advantages of using fly ash as a material for the manufacture of proppants are given. Outlines methods for producing proppant based on bauxite, fly ash, silica sand and clay, having a low specific weight and high strength.

Key words: *proppant, strength, hardness, bauxite, volatile ash, hydraulic fracturing, compressive stress.*

МРНТИ: 50.41.23

Б.Ж. Молдабеков[1], К.У. Зенкович[2]
[1]Алматинский университет энергетики и связи имени Г. Даукеева
[2]Университет имени Шакарима города Семей

МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СОТОВЫХ СЕТЯХ

Аннотация: *Рост мобильных устройств охватывает многие аспекты безопасности, начиная от защиты пользовательской информации, и заканчивая защитой провайдеров мобильной связи от мошеннического использования их услуг: клонирование SIM-карт, маршрутизация зарубежного трафика через собственные серверы злоумышленников и т.д. Основными требованиями к постепенно и неизбежно растущим мобильным сотовым сетям являются: высокая пропускная способность; низкие затраты капитала; низкие операционные расходы. Эти аспекты продиктованы требованиями высокоскоростного доступа к услугам связи за небольшие деньги. Поэтому технологии радиодоступа и сотовые сети постоянно развиваются и пытаются достичь более эффективного использования радиоресурсов.. Одним из таких решений является обнаружение аномалий. В данной статье рассмотрены проблемы информационной безопасности Big Data в сетях оператора сотовой связи. А также особенности применения выявления аномалий в сотовых сетях.*

Ключевые слова*: Обнаружение аномалий, информационная безопасность, Big Data, сотовая связь, сигнатуры обнаружения.*

Постоянный рост мобильных устройств охватывает многие аспекты безопасности, начиная от защиты пользовательской информации, и заканчивая защитой провайдеров мобильной связи от мошеннического использования их услуг: клонирование SIM-карт, маршрутизация зарубежного трафика через собственные серверы злоумышленников и т.д. Основными требованиями к постепенно и неизбежно растущим мобильным сотовым сетям являются: высокая пропускная способность; низкие затраты капитала; низкие операционные расходы. Эти аспекты продиктованы требованиями высокоскоростного доступа к услугам связи за небольшие деньги. Поэтому технологии радиодоступа и сотовые сети постоянно развиваются и пытаются достичь более эффективного использования радиоресурсов [1]. Однако, несмотря на растущее количество подобных угроз, большинство мобильных

операторов реагируют на угрозы уже после их реализации, а не действуя на опережение. Тем не менее, в последнее время становится все более популярной разработка систем обнаружения аномалий, которые бы предлагали значительное количество преимуществ над существующими решениями.

Одной из отраслей, где обнаружение аномалий является действительно актуальной проблемой является телекоммуникационная сфера, а именно – сети операторов сотовой связи. Сигнатурные методы обнаружения угроз не позволяют вовремя обнаружить утечку трафика, поскольку это не является прямой атакой на сеть оператора. Факты такого воровства трафика можно обнаружить уже постфактум, что приносит значительные убытки компаниям [1].

В данной статье рассмотрены проблемы информационной безопасности Big Data в сетях оператора сотовой связи.

Обеспечение информационной безопасности при работе с большими данными не существенно отличается от обычной защиты данных. Но различия имеются и они зависят от следующих факторов:

– данные, которые собираются, объединяются и анализируются средствами и инструментами Big Data;

– инфраструктура, обеспечивающая хранение и размещение крупных данных;

– технологии, которые применяются для анализа структурированных, полу-структурированных и неструктурированных больших данных.

Так как обычно основным приоритетом является скорость обработки большого объема информации, то некоторыми аспектами безопасности часто пренебрегают, в основном потому, что нет четкой классификации данных, которые будут храниться и передаваться [2].

В случае оператора сотовой связи Big Data может использоваться для следующих задач:

– увеличение объема хранилищ данных;
– оптимизация услуг;
– адаптивное внедрения электронных услуг (e-service);
– предоставление услуг в реальном времени;
– аналитика данных;
– создание моделей прогнозирования для систем поддержки принятия решений;
– оценка рисков.

Операторы сотовой связи постоянно ищут пути развития инновационных услуг, основанных на данных, которые могут стать источником прибыли в случае анализа огромного количества данных, которые генерируются их инфраструктурой. Для операторов сотовой связи Big Data – это бизнес-решение, которое касается не только оптимизации внутренних процессов. У них есть многочисленные возможности разработки приложений Big Data используя инфраструктуру, предлагая эти услуги другим индустриям, таким как: продажа, финансовые услуги, здравоохранение, маркетинг и т. То есть операторы сотовой связи выступают не только пользователями, но и поставщиками.

В Big Data много применений в сфере телекоммуникаций. Одним из таких является аналитика данных для управления телекоммуникационной инфраструктуры. Информация собирается для определения трендов и анализа поведения сети. Анализ данных также является полезным для внутренних сервисов (управление ресурсами, управление доходами, поставками и т.д.), которые обрабатывают данные, постоянно генерируются и интегрируют техники Big Data для оптимизации внутренних процессов, операций или для более эффективной продажи продуктов.

Также, с использованием Big Data, информация, возникающая внутри сотовой сети, особенно данных о геолокацию, результат анализа позволяет выявить тренды и шаблоны с целью лучшего понимания поведения пользователей, основываясь на событиях, которые возникают непрерывно в течение года. Информация собирается и объединяется по выделенным интерфейсам сетевого оборудования (базовые станции, антенны, сетевые контроллеры).

Основные проблемы информационной безопасности:

1) Проверка источника и фильтрация информации.

Объединение персональных данных, циркулирующих в сотовых сетях, обусловливает возникновение важных проблем безопасности, а именно контроль происхождения данных. Одной проблемой является то, что фреймворк приложений Big Data собирает информацию, которая генерируется в оборудовании сотовой сети, в которой используются технологии различных производителей. Оператор сотовой связи должен проверять и доверять компонентам инфраструктуры – как аппаратному, так и программному обеспечению – которые создают данные и события, собираются фреймворками Big Data и быть уверенными в корректности защищенного происхождения данных.

2) Защита программного обеспечения.

Необходимо использование защищенных версий программного обеспечения. Иногда, использование open-source технологий, которые могут быть экономически выгодным решением, может стать причиной возникновения уязвимостей.

3) Контроль доступа и аутентификация.

Должны быть внедрены механизмы контроля и аутентификации для различных ролей (пользователь / клиент), которые будут пользоваться услугой. Тем не менее, самой большой проблемой может стать тот факт, что аутентификация пользователей и доступ к данным может осуществляться с различных локаций. Данный процесс не всегда может эффективно контролироваться через использование децентрализованной модели и многочисленных взаимодействий между системами.

В частности, в регулируемых отраслях защита доступа привилегированного пользователя должно быть главным приоритетом. Определенным пользователям должен быть предоставлен доступ к высокочувствительных данных в конкретных бизнес-процессах, но предотвращения потенциальном мошенничества с данными может быть проблематичным.

Защита доступа привилегированного пользователя требует четко определенных политик безопасности и контроля, внедряющих доступ, основанный на ролях.

4) Защита цепочки поставок.

Использование в сотовых сетях различных устройств (как смартфонов, так и обычных мобильных) приводит проблему безопасности цепочки поставок, поскольку контроль за устройствами возлагается на организации, чья деятельность связана с предоставлением услуг или доставкой товаров.

5) Защищенное управление данными.

В случае предоставления услуг Big Data, безопасность должна рассматриваться в качестве части системы. Защита хранилищ данных должно быть первоочередной задачей, которая, впрочем, зависит от выбранной бизнес-модели услуги могут предоставляться только собственными силами или некоторые элементы будут приобретены (арендованные) в третьей стороны.

6) Защита инфраструктуры.

Защита инфраструктуры должно охватывать не только кибер-физические системы (например, сенсорные сети), но и терминалы конечного пользователя, независимо, это будет портативным устройством или нет. Большое количество ненадежных устройств может быть подключена к сети компании в любое время, на которых будут циркулировать критические данные, что приводит к необходимости «конечного» шифрования.

7) Использование защищенного «облака».

С использованием Big Data в «облаке», нужно принимать во внимание специфические категории рисков относительно облачных технологий: привязка к поставщику, нарушение целостности и управления данными.

На рисунке 1 изображена модель, усовершенствованная методами Big Data.

Рисунок 1 – Усовершенствованная методами Big Data модель

Входные данные в параллельном режиме подаются на два модуля, в каждом из которых первым начинает работать главный узел (Master Node), который распределяет нагрузку между рабочими узлами (Slave), на которых происходит двухшаговая реализация метода MapReduce, на выходе получается полезная информация, которая затем проверяется условиями и тогда результатом будет либо решение системы о нормальности данных, или классифицирована угроза или неизвестная активность.

Литература

1. Бондаровець С.С. Сучасні методи виявлення аномалій / С.С. Бондаровець // «ITSEC»: VI міжнар. наук.-техн. конф.: тези доп. – К.: НАУ, 2016.– С. 76-77.
2. Feldman R. Techniques and applications for sentiment analysis / R. Feldman. – USA: Communications of the ACM, 2013. – P. 82-89.

ҰЯЛЫ ЖЕЛІНІҢ АНОМАЛИЯСЫН АНЫҚТАУ ӘДІСТЕРІ

Б.Ж. Молдабеков, К.У. Зенкович

Ұялы құрылғылардың өсуі пайдаланушының ақпаратын қорғаудан бастап, ұялы байланыс операторларын олардың қызметтерін жалған пайдаланудан қорғауға дейін: SIM карталарын клондау, зиянкестердің жеке серверлері арқылы сыртқы трафикті бағыттау және т.б. қауіпсіздіктің көптеген аспектілерін қамтиды. Біртіндеп және сөзсіз дамып келе жатқан ұялы байланыс желілеріне қойылатын негізгі талаптар: өткізу қабілеті жоғары; капитал шығындарының аздығы; төмен шығындар. Бұл аспектілер аз ақшаға байланыс қызметтеріне жоғары жылдамдықты қол жетімділіктің қажеттілігімен түсіндіріледі. Сондықтан радиоға қол жеткізу технологиялары мен ұялы желілер үнемі дамып келеді және радио ресурстарын тиімді пайдалануға қол жеткізуге тырысады.Осы шешімдердің бірі – ауытқуларды анықтау. Бұл мақалада ұялы байланыс операторларының желілеріндегі Big Data ақпараттық қауіпсіздігі мәселелері талқыланады. Ұялы желілерде аномалияны анықтаудың ерекшеліктері.

Түйін сөздер: *Аномалды анықтау, ақпараттық қауіпсіздік, Big Data, ұялы байланыс, анықтау қолдары.*

CELL NETWORK ANOMALY DETECTION METHODS

B. Moldabekov, K. Zenkovich

The growth of mobile devices covers many aspects of security, from protecting user information to protecting mobile providers from fraudulent use of their services: cloning SIM cards, routing foreign traffic through intruders' own servers, etc. The main requirements for the gradually and inevitably growing mobile cellular networks are: high bandwidth; low capital costs; low operating costs. These aspects are dictated by the requirements of high-speed access to communication services for little money. Therefore, radio access technologies and cellular networks are constantly evolving and are trying to achieve a more efficient use of radio resources. One of these solutions is the detection of anomalies. This article discusses the problems of information security Big Data in the networks of a mobile operator. As well as features of the application of anomaly detection in cellular networks.

Key words: *Anomaly detection, information security, Big Data, cellular, detection signatures.*

МРНТИ: 65.09.03

Б.Е. Сулейменова, Ж.К. Молдабаева
Университет имени Шакарима города Семей

КАЧЕСТВО ПШЕНИЧНОГО ХЛЕБА В ГОРОДЕ СЕМЕЙ

Аннотация: *Хлеб представляет собой весьма калорийный продукт, в состав которого входит около 50% углеводов. В хлебе содержатся важные пищевые вещества, необходимые человеку. Среди них белки (до 12,5 %), углеводы (до 75 %), витамины (B1, B2, PP), минеральные вещества (Ca, K, P, Na, Mg), пищевые волокна. За счет потребления хлеба человек почти на половину удовлетворяет свою потребность в углеводах, на треть – в белках, более чем на половину – в витаминах группы В, солях фосфора и железа. В статье приведены результаты исследования основных показателей качества пшеничного хлеба, выпускаемого в городе Семей Восточно-Казахстанской области. Дана сравнительная характеристика качества хлеба, вырабатываемого производителями в городе Семей.*

Ключевые слова: *мука, пшеница, пшеничный хлеб, органолептическая экспертиза, физико-химическая экспертиза.*