КВАНТОВЫЙ КРИПТОАНКЛАВ ДЛЯ РЕАЛИЗАЦИИ НЕКОМПРОМЕТИРУЕМЫХ ДОВЕРЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Елисеев В. Л.[1]

DOI: 10.21681/2311-3456-2025-3-99-104

Цель исследования: *разработка и обоснование архитектуры квантово-криптографической системы защиты доступа в центр обработки данных с высокими требованиями к конфиденциальности обрабатываемой информации, принадлежащей различным субъектам, на примере задачи федеративного обучения.*

Метод(ы) исследования: *системный анализ.*

Результат(ы) исследования: *рассматривается задача обеспечения конфиденциальности данных, принадлежащих различным субъектам, при их совместной обработке. Исследуется концепция криптоанклава как эффективного подхода для реализации поставленной задачи. Проводится анализ современных и перспективных угроз для криптографических методов защиты информации. Предлагается концепция квантового криптоанклава, сочетающего технологии криптографической защиты информации и квантового распределения ключей. Приводится пример возможной реализации квантового криптоанклава для решения задачи федеративного обучения.*

Научная новизна: *предложена архитектура квантового криптоанклава – центра обработки данных с криптографической защитой доступа с помощью сети квантового распределения ключей с доверенными промежуточными узлами.*

Ключевые слова: *криптоанклав, доверенные вычисления, федеративное обучение, квантовое распределение ключей, сеть квантового распределения ключей.*

Введение

Одним из следствий значительного развития информационных и коммуникационных технологий, наблюдающегося на протяжении нескольких десятков лет, стал существенный рост ценности информации, представленной в форме, доступной для цифровой обработки. Обладание информацией на протяжении всей истории человечества давало приоритет, однако только в наше время стало возможным конвертировать большие данные в коммерческий успех. Множество интернет-компаний, от поисковиков до социальных сетей, существуют исключительно благодаря возможности анализировать и продавать агрегированные данные о своих пользователях в форме рекомендательных и статистических моделей, обеспечивающих другим компаниям рост продаж их товаров и услуг. Феномен успеха интернет-магазинов связан не только с удобством выбора товаров и доставки, но и с возможностью точного таргетирования рекламы. Традиционные экономические субъекты, такие как банки и страховые компании, также повышают эффективность своей работы за счёт анализа больших данных. Весьма характерным выражением этой тенденции является крылатая фраза «данные – это новая нефть».

Развитие производительных вычислительных средств обеспечивает гигантский прогресс в обработке больших данных. Например, феномен больших языковых моделей является синергетическим эффектом больших данных (текстов и других видов информации), эффективных алгоритмов глубокого обучения и быстродействующих вычислительных платформ. Можно смело сказать, что чем больше данных удаётся собрать для обучения глубокой модели, тем более эффективной, мощной и полезной окажется такая модель.

Одним из ярких примеров понимания важности накопления, актуализации и использования больших данных во благо экономики государства является национальный проект «Экономика данных», объединяющий несколько прорывных направлений, каждое из которых в той или иной степени связано с обработкой информации.

Подобно любой ценности, данные тщательно охраняются. Для их защиты разработаны различные технические и криптографические методы, а также развитая правовая и регуляторно-нормативная база. Однако никакая защита не может считаться абсолютно надёжной, особенно в условиях постоянного прогресса в сфере высоких технологий обработки информации. Также под влиянием изменений в технологиях меняется и оценка рисков, связанных с перспективными и традиционными угрозами.

Рассмотрим задачу совместной обработки конфиденциальных данных, принадлежащих различным субъектам, с целью получения агрегированных моделей, полезных для субъектов-владельцев данных.

1 Елисеев Владимир Леонидович, кандидат технических наук, АО «ИнфоТеКС», ФГБОУ ВО Национальный исследовательский университет «Московский энергетический институт», Москва, E-mail: vlad-eliseev@mail.ru, ORCID: 0000-0002-9341-7475.

При этом важным условием является сохранение конфиденциальности данных в процессе их обработки, поскольку взаимное доверие субъектов друг к другу является ограниченным. Практически важным примером такой задачи является федеративное обучение глубоких моделей, которые вбирают в себя зависимости, выявленные в данных, и могут использоваться субъектами-владельцами данных в своей деятельности.

Обзор литературы

В обычных центрах обработки данных (ЦОД) реализуются политики организации доступа, обеспечивающие разделение потоков данных, хранилищ и вычислительных средств, арендованных или принадлежащих различным субъектам, которые будем называть *пользователями*. Фактически, для каждого из пользователей в ЦОД организуется изолированная от всех других пользователей среда – *виртуальный ЦОД* [1], состоящий из ресурсов, выделенных пользователю из общего пула физического ЦОД. Меры изоляции обычно определяются на организационно-техническом уровне, что означает наличие рисков, связанных с нарушением регламентов и характеристик системы защиты, к которым относятся ошибки и злонамеренные действия персонала ЦОД, а также сбои в работе оборудования и программного обеспечения системы защиты.

Криптографические методы защиты информации обычно применяются для организации доступа в виртуальный ЦОД и рассчитаны на защиту от внешнего нарушителя в телекоммуникационных каналах. В частности, трафик виртуального ЦОД шифруется при передаче наружу, в отрытую сеть. С точки зрения внешнего нарушителя, такая система представляет собой криптографически и организационно-технически защищенную сущность, которую обычно называют криптоанклавом.

Криптоанклав (англ. security enclave) получает и выдаёт данные исключительно в зашифрованном виде, расшифровывая их только внутри для обработки. Название этой концепции образовано словами «крипто» (от греч. kryptós – тайный, скрытый) и «анклав» (от фр. enclave, от лат. inclavatus – заключенный, запертый). С понятием криптоанклава тесно связаны технологии доверенных вычислений – Trusted Execution Environment (TEE).

Хорошо известным примером криптоанклава являются технологии Intel Software Guard Extensions (SGX) [2]. Она позволяет обрабатывать зашифрованные данные с помощью специального механизма центрального процессора, изолирующего программу от изменений (для предотвращения злонамеренного внедрения кода), а расшифрованные в процессе обработки данные – от инспекции другими программами. Реализация криптоанклава в виде механизма центрального процессора обладает тем недостатком, что существенно ограничивает производительность защищенной обработки данных выделенными страницами оперативной памяти. По этой причине SGX обычно используется только для хранения криптографических ключей и работы с ними, например, в процессе выполнения криптографических протоколов [3]. Для защищенной обработки больших данных SGX и другие подобные технологии не подходят.

Концепция криптоанклава может быть расширена на уровень вычислительной системы, кластера или даже всего ЦОД. В частности, виртуальный ЦОД может использоваться для реализации криптоанклава, однако в этом случае организационно-технических методов изоляции может оказаться недостаточно и для снижения рисков целесообразно использовать шифрование данных при их передаче по каналам внутри физического ЦОД.

Альтернативой криптоанклаву могли бы стать методы гомоморфной криптографии [4], которые обещают непосредственное выполнение вычислений над зашифрованными данными без их расшифрования. В 2009 году была предложена первая схема, обеспечивающая выполнение произвольных операций над зашифрованными данными [5], так называемое полное гомоморфное шифрование. Однако в настоящее время оно реализуется вычислительно чрезвычайно неэффективно, что на несколько порядков замедляет вычисления по сравнению с операциями над незашифрованными данными. Таким образом, гомоморфное шифрование в настоящее время не может использоваться для обработки больших данных.

Анализ показывает, что приемлемым подходом для обработки больших данных с сохранением их конфиденциальности является концепция криптоанклава, реализуемая в масштабе ЦОД при условии использования подходящих средств шифрования. Однако при совместной обработке конфиденциальных данных нескольких субъектов в одном криптоанклаве возникает проблема обеспечения доверия субъектов друг к другу, поскольку каждый из них равноправно обладает доступом в криптоанклав для загрузки своих данных и выгрузки результатов из него. Некоторые примеры совместной обработки конфиденциальных данных перечислены ниже:

- банковские модели оценки кредитоспособности клиентов (банковский скоринг);
- модели оценки риска страхования клиентов (страховой скоринг – страхование жизни, КАСКО и пр.);
- модели машинного обучения на объединенных выборках конфиденциальных данных;
- обработка любых конфиденциальных данных конфиденциальными же алгоритмами (например, экспертные системы диагностики заболеваний).

Федеративное обучение [6] является концепцией машинного обучения общей модели на основе использования данных нескольких субъектов без их прямого объединения. Задача федеративного обучения возникает в случае невозможности открытого соединения нескольких наборов обучающих данных в один. В частности, эта ситуация может возникать из-за ограничений на конфиденциальность отдельных наборов данных.

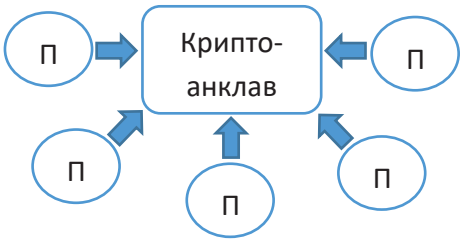
При использовании методов различных методов шифрования следует иметь в виду условия обеспечения конфиденциальности перед лицом тех или иных угроз. Например, одной из угроз для симметричного, асимметричного и постквантового шифрования являются действия внутреннего нарушителя. Если он обладает доступом к секретным ключам шифрования, то это нарушает конфиденциальность данных. В то же время в технологии квантового распределения ключей влияние внутреннего нарушителя минимизировано [7].

Рассмотрим архитектуру криптоанклава с защитой конфиденциальности данных от компрометации внутренним нарушителем на основе технологии квантового распределения ключей (КРК).

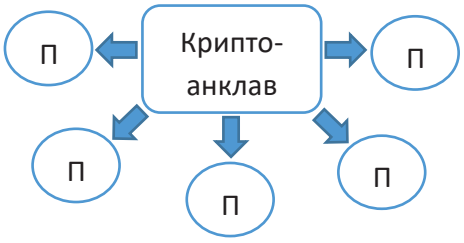
Криптоанклав для федеративного обучения

Целью функционирования криптоанклава обычно является создание каких-то обобщений данных для последующего использования этих обобщений для принятия решений. В рамках концепции федеративного обучения удобно назвать эти обобщения моделями.

Назовём *пользователями* криптоанклава (П) субъекты, загружающие свои данные в криптоанклав и получающие в результате обработки данных модели, которые, с одной стороны, созданы на основе данных, загруженных всеми пользователями, с другой – не содержащие эти данные в явном виде, допускающих их компрометацию. Таким образом, основные сценарии использования криптоанклава можно представить на рис. 1.



а) загрузка данных



б) выгрузка модели

Рис. 1. Сценарии использования криптоанклава

От обычного ЦОД криптоанклав отличается специальной политикой обеспечения безопасности данных, которая обусловлена тем, что, как правило, пользователи загружают свои данные в криптоанклав в расчёте, что эти данные не будут доступны другим пользователям. При этом все пользователи криптоанклава получают выгоду от того, что создаваемые в криптоанклаве модели создаются на основе объединенных данных всех пользователей.

Задачи, решаемые в криптоанклаве сродни задачам безопасных многосторонних вычислений (например, задача о миллионерах) и гомоморфной криптографии (вычисления над зашифрованными данными). В случае криптоанклава прикладные задачи можно решать классическим образом, но при этом сама политика работы с данными в криптоанклаве техническими мерами обеспечивает конфиденциальность этих данных.

На практике пользователи взаимодействуют с криптоанклавом через каналы коммуникаций, используемые как для передачи данных, являющихся конфиденциальными, так и для получения моделей, ценность которых также должна быть защищена от несанкционированного доступа. При этом пользователи криптоанклава не обязаны доверять друг другу, однако необходимо снизить риск компрометации данных вследствие реализации угрозы внутреннего нарушителя пользователя.

Анализ угроз конфиденциальности

Конфиденциальность данных при передаче по каналам коммуникаций может быть обеспечена как организационно-техническими (охрана линий связи), так и криптографическими мерами. При передаче данных через неконтролируемую среду (Интернет) обеспечить конфиденциальность организационно-техническими мерами невозможно, поэтому широко используются криптографические протоколы защиты передаваемых данных.

Все криптографические протоколы используют симметричные криптографические алгоритмы для шифрования данных в канале. Содержательные отличия касаются только способа распределения или выработки общего секретного ключа. Существуют следующие варианты решения этой задачи:

- доверенный курьер;
- протокол Диффи-Хеллмана;
- постквантовые протоколы (PQ-KEM);
- квантовое распределение ключей.

Таблица 1.

Уязвимость технологий распределения ключей

Технологии распределения ключей	Угрозы			
	Рост производительности классических компьютеров	**Квантовая атака Шора**	**Побочные каналы утечки**	**Внутренний нарушитель**
Доверенный курьер	–	–	–	Высокая уязвимость
Протокол Диффи-Хеллмана	Увеличение длины асимметричных ключей согласно закону Мура	Полностью компрометируется	Необходимо защищаться от утечек	Уязвим в любой момент времени
Постквантовые протоколы	– (предположительно неуязвимы)	–	Необходимо защищаться от утечек	Уязвим в любой момент времени
Квантовое распределение ключей	–	–	Необходимо защищаться от утечек	Уязвим только в моменты выработки первого квантового ключа

Каждый из вариантов имеет свои достоинства и недостатки. Перечислим общие угрозы, которые будем рассматривать, как влияющие на конфиденциальность криптографически защищенных данных:

- рост производительности классических компьютеров;
- квантовые атаки Шора и Гровера;
- побочные каналы утечки;
- внутренний нарушитель.

Квантовая атака Гровера одинаково влияет на конфиденциальность данных при любом способе распределения ключей, понижая стойкость симметричных криптографических алгоритмов до квадратного корня от числа возможных секретных ключей. То есть, при квантовой атаке Гровера симметричный ключ длиной 256 бит (число возможных ключей 2^{256}) будет обеспечивать стойкость, как если бы это был ключ длиной 128 бит без атаки Гровера (число возможных ключей $2^{128} = \sqrt{2^{256}}$. Данное снижение стойкости может быть легко компенсировано увеличением длины ключа в 2 раза, поэтому в настоящее время квантовая атака Гровера не считается приводящей к полной компрометации.

Уязвимость технологий распределения ключей к перечисленным выше угрозам сведена в таблицу 1.

Отметим одну важную особенность криптоанклава с точки зрения обеспечения криптографической защиты данных – пользователей, являющихся независимыми субъектами, при работе с криптоанклавами должны быть уверенными, что их данные не будут скомпрометированы вследствие реализации значимых угроз. При этом пользователи не могут влиять на защищенность каналов доступа других пользователей. В частности, внутренний нарушитель одного из субъектов доступа к криптоанклаву может нарушить конфиденциальность всей системы, если от него не будет создана адекватная защита.

Как видно из таблицы 1, единственным теоретически обоснованным способом почти полной защиты от внутреннего нарушителя является квантовое распределение ключей. Защита каналов доступа с помощью квантовых ключей гарантирует некомпрометируемость коммуникаций с криптоанклавом и обеспечивает доверие пользователей ко всей системе. Такую систему можно назвать *квантовым криптоанклавом*. Примером проекта, реализующего концепцию квантового криптоанклава, является Quantumacy [8]. В этом проекте, реализованном в рамках европейской инициативы OpenQKD в 2021-2022 годах, была рассмотрена модель проведения доверенных вычислений в криптоанклаве, доступ к которому обеспечивался с помощью КРК. В качестве модельных прикладных задач рассматривалось машинное обучение для диагностики заболеваний с наборами данных, получаемыми из различных источников. Доступ к источникам данных, согласно предложенной архитектуре, криптографически защищался с помощью технологии КРК.

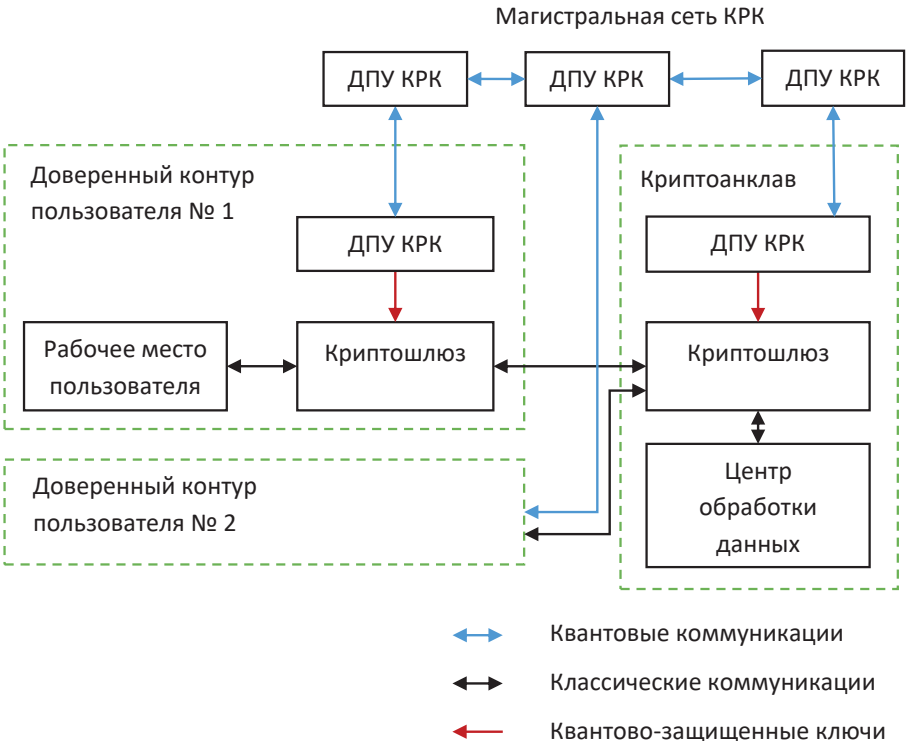


Рис. 2. Архитектура квантового криптоанклава

Архитектура квантового криптоанклава

В состав квантового криптоанклава (рис. 2) входят:

- доверенный промежуточный узел сети квантового распределения ключей (ДПУ КРК);
- криптошлюз, осуществляющий шифрование квантово-защищенными ключами данных между ЦОД и пользователями;
- центр обработки данных, в котором реализуются криптографические и организационно-технические меры защиты и производится совместная обработка данных, полученных от пользователей.

Для подключения к криптоанклаву в состав доверенного контура пользователя должны входить:

- доверенный промежуточный узел сети квантового распределения ключей (ДПУ КРК);
- криптошлюз, осуществляющий шифрование квантово-защищенными ключами данных между ЦОД и пользователями;
- рабочее место пользователя, посредством которого пользователь передаёт свой конфиденциальный набор данных в ЦОД и загружает полученную модель, а также осуществляет необходимые служебные операции при работе с криптоанклавом.

Магистральная сеть КРК [9] состоит из ДПУ КРК, соединённых каналами квантовых коммуникаций, обеспечивающих передачу квантово-защищенных ключей между криптошлюзами. Такой способ распределения криптографических ключей обеспечивает защиту от компрометации внутренним нарушителем.

Выводы

Предложенная архитектура квантового криптоанклава обеспечивает реализацию некомпрометируемого криптографически защищенного доступа в среду доверенных вычислений, реализуемую в ЦОД. По сравнению с концепцией криптоанклава новая архитектура снижает риски компрометации внутренним нарушителем. Технология квантового распределения ключей для обеспечения некомпрометируемости применяется в рамках современной концепции магистральных сетей КРК.

Литература

1. Bari M. F. et al. Data center network virtualization: A survey // IEEE communications surveys & tutorials. – 2012. – Т. 15. – №. 2. – С. 909–928.
2. Costan V., Devadas S. Intel SGX explained //IACR Cryptol, EPrint Arch. – 2016.
3. Park J., Kang B. B. EnclaveVPN: Toward Optimized Utilization of Enclave Page Cache and Practical Performance of Data Plane for Security-Enhanced Cloud VPN // Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. – 2023. – С. 397–411. DOI: 10.1145/3607199.360721.
4. Fontaine C., Galand F. A survey of homomorphic encryption for nonspecialists // EURASIP Journal on Information Security. – 2007. – Т. 2007. – С. 1–10.

5. Gentry C. Fully homomorphic encryption using ideal lattices // Proceedings of the forty-first annual ACM symposium on Theory of computing. – 2009. – С. 169–178.
6. Bharati S. et al. Federated learning: Applications, challenges and future directions //International Journal of Hybrid Intelligent Systems. – 2022. – Т. 18. – №. 1–2. – С. 19-35. DOI: 10.3233/HIS-22000.
7. Прикладные квантовые технологии для защиты информации / Андрущенко А.С., Борисова А.В., Елисеев В.Л., Жиляев А.Е., Иванов О.А., Кармазиков Ю.В., Козлов С.К., Криштоп В.Г., Курнакова А.Д., Моисеевский А.Д., Попов В.Г., Рыбкин А.С. / под редакцией Втюриной А.Г., Елисеева В.Л. – 2-е изд., испр. – М: Медиа Группа «Авангард», 2024. 144 с.
8. «Quantumacy» project – investigating privacy-preserving forms of quantum communication – comes to a close | CERN QTI // URL: https://quantum.cern/news/announcement/quantumacy-project-investigating-privacy-preserving-forms-quantum-communication (дата обращения: 01.02.2025)
9. Елисеев В. Сети квантового распределения ключей – новый уровень сервисов информационной безопасности национальной сети Интернет / В. Елисеев // Интернет изнутри. – 2024. – № 20. – С. 10–15.

QUANTUM CRYPTO ENCLAVE FOR IMPLEMENTING UNCOMPROMISED TRUSTED DATA CENTERS

Eliseev V.L.[2]

Keywords: *crypto enclave, trusted computing, federated learning, quantum key distribution, quantum key distribution network.*

Purpose of the study: *development and justification of the architecture of a quantum-cryptographic system for protecting access to a data center with high requirements for the confidentiality of processed information belonging to various entities, using federated learning problem as the example.*

Methods of research: *systems analysis.*

Result(s): *the problem of ensuring the confidentiality of data belonging to different subjects during their joint processing is considered. The concept of a cryptoenclave is studied as an effective approach to implementing the task. An analysis of modern and prospective threats to cryptographic methods of information protection is carried out. The concept of a quantum cryptoenclave is proposed, combining technologies of cryptographic information protection and quantum key distribution. An example of a possible implementation of a quantum cryptoenclave for solving the problem of federated learning is given.*

Scientific novelty: *an architecture of a quantum cryptoenclave is proposed – a data center with cryptographic access protection using a quantum key distribution network with trusted intermediate nodes.*

References

1. Bari, M.F., Boutaba, R., Esteves, R., Granville, L.Z., Podlesny, M., Rabbani, M.G., ... & Zhani, M.F. (2012). Data center network virtualization: A survey. IEEE communications surveys & tutorials, 15(2), 909–928.
2. Costan, V. (2016). Intel SGX explained. IACR Cryptol, EPrint Arch.
3. Park, J., & Kang, B.B. (2023, October). EnclaveVPN: Toward Optimized Utilization of Enclave Page Cache and Practical Performance of Data Plane for Security-Enhanced Cloud VPN. In Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 397–411).
4. Fontaine, C., & Galand, F. (2007). A survey of homomorphic encryption for nonspecialists. EURASIP Journal on Information Security, 2007, 1–10.
5. Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169–178).
6. Bharati, S., Mondal, M.R.H., Podder, P., & Prasath, V.S. (2022). Federated learning: Applications, challenges and future directions. International Journal of Hybrid Intelligent Systems, 18(1-2), 19–35.
7. Andrushhenko A.S., Borisova A.V., Eliseev V.L., Zhilyaev A.E., Ivanov O.A., Karmazikov Yu.V., Kozlov S.K., Krishtop V.G., Kurnakova A.D., Moiseevskij A.D., Popov V.G., & Rybkin A.S. (2024). Prikladnye kvantovye texnologii dlya zashhity informacii / ed. Vtyurinoj A.G., Eliseeva V.L. – 2nd edition. – M: Media Gruppa «Avangard», 2024. 144 p.
8. «Quantumacy» Project – Investigating Privacy-Preserving Forms of Quantum Communication – Comes to a Close | CERN QTI. (2022). https://quantum.cern/news/announcement/quantumacy-project-investigating-privacy-preserving-forms-quantum-communication.
9. Eliseev V. (2024). Seti kvantovogo raspredeleniya klyuchej – novyj uroven' servisov informacionnoj bezopasnosti nacional'noj seti Internet. Internet iznutri, 20, 10–15.

2 Vladimir L. Eliseev, Ph.D., JSC «InfoTeCS», National research university «Moscow power engineering institute», Moscow. E-mail: vlad-eliseev@mail.ru, ORCID: 0000-0002-9341-7475.