АНАЛИЗ РЕАЛИЗАЦИИ ТЕХНОЛОГИЙ КОНФИДЕНЦИАЛЬНЫХ ВЫЧИСЛЕНИЙ

Загартдинов Б.Н.[1], Поляков М.В.[2]

Цель исследования: *анализ современного состояния технологий конфиденциальных вычислений.*

Метод исследования: *систематизация и анализ существующих решений реализующих аппаратную среду конфиденциальных вычислений.*

Результат исследования: *в статье проведены оценка моделей угроз аппаратных технологий конфиденциальных вычислений, таких как Intel TDX, AMD SEV или ARM CCA, и анализ их реализации. Выявлены общие признаки и рассмотрены особенности каждой из реализаций. Обнаружены основные проблемы, с которыми сталкиваются разработчики подобных систем: сложности с повторным использованием существующих технологий безопасности и необходимость проектирования технологий с учетом жизненного цикла защищаемого программного обеспечения. В каждой реализации применяются различные методы решения данных проблем. Главным преимуществом использования аппаратных технологий конфиденциальных вычислений является обработка данных в защищенных контейнерах, за счет чего обеспечивается конфиденциальность и целостность чувствительной информации. Поэтому решения данного типа могут быть рассмотрены к внедрению в распределенные системы в перспективе позволяя повысить их производительность за счет эффективного использования вычислительных ресурсов без ущерба для конфиденциальности.*

Научная новизна: *состоит в том, что представленная статья является одной из первых отечественных работ, представляющих анализ и систематизацию решений реализующих аппаратную среду конфиденциальных вычислений. Выявлены основные черты характеризующие современные системы конфиденциальных вычислений, а также проблемы, возникающие в процессе разработке таких систем.*

Ключевые слова: *безопасность облачных вычислений, аппаратные доверенные среды выполнения, удаленная аттестация, безопасность данных, информационная безопасность.*

DOI:10.21681/2311-3456-2023-6-122-127

Введение

В современных вычислительных системах и комплексах данные существуют в трех состояниях: в состоянии покоя (например, во время хранения на постоянных носителях информации), в использовании (во временной памяти) и во время передачи по каналам коммуникации. Для защиты данных при передаче по коммуникационным каналам используются хорошо изученные криптографические протоколы для конфиденциального обмена данными. Защита данных в состоянии покоя может рассматриваться как распределенный во времени криптографический протокол с предварительно согласованным общим секретом. В свою очередь вопрос защиты данных в процессе использования остается открытым.

Впервые о защите данных в процессе использования посредством применения криптографической защиты задумались в 1978 Ривест, Адлеман и Дертузос в своей работе[3], а в 1982 году в статье Эндрю Яо[4] впервые была упомянута проблема организации многосторонних безопасных вычислений. Потребовалось несколько десятков лет, чтобы идеи, предложенные Ривестом, Адлеманом, Дертузосом и Яо были восприняты научным сообществом. В настоящий момент, несмотря на большое количество академических работ, описывающих алгоритмы полностью гомоморфного шифрования и протоколы многосторонних безопасных вычислений, идеи не получили широкого

3 Rivest R. L. et al. On data banks and privacy homomorphisms //Foundations of secure computation. – 1978. – Т. 4. – №. 11. – С. 169-180.

4 Yao A. C. Protocols for secure computations //23rd annual symposium on foundations of computer science (sfcs 1982). – IEEE, 1982. – С. 160-164

1 Загартдинов Булат Назимович, магистр НИЯУ МИФИ, специалист НТЦ Вулкан, Москва, Россия. E-mail: me@vaire.lt

2 Поляков Михаил Вадимович, старший преподаватель МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: m.polyakov@bmstu.ru

практического применения и остаются нереализованными в прикладных приложениях по различным причинам. В работах [1] и [2] подробно разобраны существующие проблемы, препятствующие практической реализации гомоморфного шифрования и многосторонних безопасных вычислений.

На практике внедрение механизмов защиты данных во время использования позволяет предотвратить сразу несколько известных классов атак: RowHammer [3], Hyperjacking [4], DMA-атаки [5, 6], ColdBoot [7, 8].

В процессе развития методов построения вычислительных систем было предложено несколько различных решений, частично покрывающих вопросы защиты данных в процессе использования: скремблирование оперативной памяти для защиты от прямого чтения шины данных, Input/Output Memory Management Unit (IOMMU) для защиты от DMA-атак, аппаратные и программные доверенные среды выполнения для защиты от компрометации некоторых приложений, обрабатывающих критичные данные, со стороны непривилегированного ПО, выполняемого на той же системе.

Конфиденциальные вычисления – следующий этап развития прикладных технологий защиты данных во время использования. В то время как каждое решение покрывает лишь часть атак, они обобщают опыт предыдущих технологий и предоставляют приемлемое с практической точки зрения решение проблемы защиты данных во время использования.

Вопросы внедрения концепции конфиденциальных вычислений в индустриальные решения рассматриваются консорциумом конфиденциальных вычислений[5], однако пока термин конфиденциальные вычисления не имеет четкого определения, поскольку предложенные консорциумом формулировки являются достаточно расплывчатыми и нуждаются в доработке [9]. Несмотря на отсутствие строгой формулировки, возможно формализовать ряд требований, которым соответствуют решения, реализующие концепцию конфиденциальных вычислений, в научном сообществе термин используется для обобщения существующих решений, реализующих в первую очередь защиту от атак со стороны гипервизора, а также предоставляющих механизмы аттестации доверенной вычислительной базы.

Далее в работе виртуальная машина будет именоваться гостем, а гипервизор или ОС выполняющая роль гипервизора хостом.

1. Существующие решения

Реализация концепции конфиденциальных вычислений возможна как в рамках центрального процессора, так и за его пределами. Например, в работе [10] представлено решение, реализующее эту концепцию для решения задачи конфиденциального обучения моделей искусственного интеллекта в формате платы расширения с интерфейсом PCIe. Однако поскольку подобные расширения создаются для решения частных задач их применение имеет ограниченный характер. Далее в работе анализируются реализации, расширяющие функционал центрального процессора, поскольку их применение позволяет решать более широкий круг задач.

К индустриальным решениям, реализующим концепцию конфиденциальных вычислений, относятся следующие архитектурные решения:

- Intel Trust Domain Executions (TDX)
- AMD Secure Encrypted Virtualization – Secure Nested Paging (SEV-SNP)
- ARM Confidential Compute Architecture (CCA)
- IBM Protected Execution Facility (PEF)
- IBM Z Secure Execution
- RISC-V Application Processor Trusted Execution Environment (AP-TEE)

Данные решения сформировались вследствие развития отрасли в целом и моделей угроз каждого производителя или исследовательской группы, в частности. Каждое решение имеет уникальные особенности, но можно выделить ряд черт, характерных для каждого из них:

1.1. Аппаратная поддержка изоляции от привилегированного злоумышленника

Каждое решение вводит свой архитектурный примитив изоляции: Trusted Domains, Realm, Confidential/Trusted/Protected Virtual Machine и другие. В зависимости от технологии обеспечивается гарантия сохранения конфиденциальности и целостности против целого класса злоумышленников.

1.2. Малый размер доверенной вычислительной базы

Минимизация доверенной вычислительной базы снижает поверхность атаки позволяя гарантировать другие свойства безопасности вычислительной систем, например конфиденциальность и целостность памяти виртуальной машины.

5 Confidential Computing Consortium Scope [https://confidentialcomputing.io/scope/]

1.3. Аппаратный корень доверия и удаленная аттестация

Большинство технологий предоставляют аппаратный корень доверия (первоначальный этап загрузки в совокупности с платформо-зависимыми секретными параметрами) и протокол удаленной аттестации (верификация программно-аппаратной среды исполнения), с помощью которых удаленный клиент может получить надежные криптографические доказательства, что программное обеспечение было запущено в корректно инициализированной изолированной программно-аппаратной среде на удаленной (или локальной) машине.

2. AMD SEV-SNP

Модель угроз AMD SEV-SNP[6] включает в себя: атаки перехвата гипервизора, DMA атаки, атаки повторного использования на зашифрованных страницах памяти, манипуляции страницами памяти в таблице трансляции виртуальной машины, ColdBoot атаки, откат версии доверенной вычислительной базы.

Не включены в модель угроз атаки по побочным каналам с манипуляцией кэшем и таблицами трансляции, отказ в обслуживании гостевой виртуальной машины.

Основой защиты данных в AMD SEV-SNP является сопроцессор безопасности AMD PSP, встроенный в корпус основного процессора. Сопроцессор безопасности отвечает за шифрование памяти защищаемых виртуальных машин. Шифрование страниц памяти защищаемых виртуальных машин осуществляется с помощью AES на своем ключе, генерируемом при инициализации виртуальной машины, изменяющемся при каждой перезагрузке вычислительной системы. Зашифрованные страницы помечаются специальным битом в таблице трансляции. Технология SEV-SNP предоставляет механизм удаленной аттестации платформы с использованием аппаратного корня аттестации, предоставляемого сопроцессором безопасности. Для защиты целостности страниц защищенных виртуальных машин используется контролируемая сопроцессором безопасности таблица Reverse Mapping Table (RMP). Таблица индексируется физическим адресом страницы хоста, а каждая ее запись содержит физический адрес гостевой страницы, на который отображается соответствующая физическая страница хоста. RMP предотвращает неавторизованную запись в зашифрованные страницы, однако чтение зашифрованного содержимого страниц по-прежнему возможно.

AMD SEV-SNP также вводит разделение привилегий внутри защищенной виртуальной машины на 4 уровня от 0 до 3, где Virtual Machine Privilege Level 0 (VMPL0) наиболее привилегированный, а VMPL3 наименее.

3. Intel TDX

Модель угроз Intel TDX включает в себя атаки с физическим или удаленным доступом к вычислительной машине и контролем над загрузочным ПО, ПО в режиме System Management Mode (SMM), хостовой ОС, гипервизором и периферийными устройствами. Доступность защищаемой виртуальной машины при этом не гарантируется.

В реализации Intel TDX [11] применяются в том числе уже существующие технологии:

- Virtualization Technology (VT) как основа для виртуализации.
- Multi-key Total Memory Encryption (MKTME) в качестве аппаратного компонента используемого для шифрования страниц памяти.
- Guard Extensions (SGX) в качестве источника изученных на практике механизмов аттестации.
- Data Center Attestation Primitives (DCAP) в совокупности с алгоритмами SGX как автономный сервис аттестации.

Расширение Intel TDX вводит новый режим исполнения кода – Secure-Arbitration Mode (SEAM). Модуль TDX – программный компонент, выполняемый в режиме SEAM VMX-root, который предназначен для выполнения функций по управлению защищенными виртуальными машинами. К таким функциям относится запуск и управление защищенными виртуальными машинами – Trust Domains (TDs) в терминологии TDX, а также организация канала коммуникации между гипервизором и защищенными виртуальными машинами. Для управления защищенными страницами памяти используется отдельная таблица Secure-EPT, управление которой также возложено на Модуль TDX.

Каждой защищенной виртуальной машине назначается свой уникальный ключ шифрования памяти. TDX использует MKTME для шифрования страниц памяти защищенных виртуальных машин. Помимо шифрования, защищаемые страницы помещаются в специальную зону, недоступную за пределами Trusted Domain, выделяемую при помощи бита TD Owner. В TDX используются те же механизмы и инфраструктура удаленной и локальной аттестации что и в SGX.

6 AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More [https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf]

4. ARM CCA

Модель угроз ARM CCA [12] включает в себя атаки без физического доступа, направленные на нарушение конфиденциальности или целостности данных защищаемой виртуальной машины, а именно: компрометация гипервизора, DMA атаки, переназначение памяти, программные атаки по побочным каналам.

В архитектуре ARM CCA добавляется новое расширение Realm Management Extension (RME)[7]. RME поддерживает новый тип проверяемой изолированной среды, называемый Realm. Виртуальная машина Realm отличается от доверенной операционной системы или доверенного приложения тем, что она управляется с хоста. В таких областях, как создание и распределение памяти, виртуальная машина Realm действует как любая другая виртуальная машина, управляемая с хоста. Кроме того, в режиме Realm отключены физические прерывания, все прерывания виртуализируются гипервизором, а затем передаются в гостевую операционную систему с помощью команд, обрабатываемых менеджером Realm режима (RMM). Это означает, что скомпрометированный гипервизор может помешать выполнению виртуальной машины Realm, поэтому в данном режиме нет никакой гарантии выполнения гостевой операционной системы, однако обеспечивается целостность и конфиденциальность.

CCA использует расширение Granule Protection Table (GPT) для отслеживания прав доступа к страницам памяти в различных режимах исполнения. Secure Monitor (Root World) управляет GPT, предоставляя интерфейс для изменения состояния таблицы со стороны менее привилегированного ПО (Non-Secure World, Secure World, Realm World).

5. IBM PEF/Z Secure Execution

Технология IBM Z Secure Execution [13] предоставляет поддержку для защищенных виртуальных машин, запускаемых в изолированной среде выполнения начиная с IBM Z15 и LinuxONE III. IBM Z Secure Execution вводит режим ультравизор в архитектуру IBM Z, используемый для подготовки и запуска защищенных виртуальных машин. Пользователь может использовать несколько симметричных ключей шифрования для различных данных, ключи помещаются в специальный заголовок и защищаются ключом шифрования платформы как часть разворачиваемого образа виртуальной машины. Начиная с IBM Z16 и LinuxONE Emperor 4 доступна удаленная аттестация.

Технология IBM PEF реализуемая с POWER9 также добавляет новый режим исполнения кода – ультравизор [14]. Задача ультравизора выступать связующим звеном между защищенным режимом исполнения и нормальным. Гипервизор запускает виртуальную машину, которая, используя инструкцию ESM (Enter Secure Mode) переходит в защищенный режим исполнения. Ультравизор конвертирует виртуальную машину в защищенную путем перемещения ее памяти в защищенную зону, недоступную не доверенному коду. Он использует Доверенный Платформенный Модуль (Trusted Platform Module – TPM) для формирования HMAC ключа, применяемого для проверки целостности, и симметричного ключа, используемого для расшифрования основной ОС. Доступ к TPM предоставляется ультравизору только в корректно загруженной системе, что обеспечивается посредством фиксации значений PCR регистров TPM.

6. RISC-V CoVE

Архитектурным расширением RISC-V CoVE [15] предусматривается защита от широкого класса злоумышленников: от непривилегированного программного обеспечения до системного ПО, аппаратных атак и атак по побочным каналам. Модель угроз RISC-V CoVE включает в себя:

- использование инструкций чтения/записи для доступа к защищаемым регионам памяти;
- программные атаки по стороннему каналу (атаки по кэшам, предсказателю переходов, отказам страниц, статистике выполнения);
- программные изменения памяти по побочному каналу (rowhammer);
- DMA-атаки;
- широкий класс атак внедрения аппаратного сбоя;
- атаки на используемые криптографические алгоритмы и примитивы;
- атаки понижения версии доверенной вычислительной базы.
- защита хоста от атак типа отказа в обслуживании со стороны защищаемой виртуальной машины также включена в модель угроз, в то время как обратная защита, как и в предыдущих решениях, не предусмотрена.

В качестве основы для RISC-V CoVE используется поддержка режима гипервизора, дополняемого конфиденциальным (Confidential) режимом исполнения.

7 Unlocking the power of data with Arm CCA [https://community.arm.com/arm-community-blogs/b/architectures-and-processors-blog/posts/unlocking-the-power-of-data-with-arm-cca]

Отслеживание дополнительного режима исполнения для каждого потока осуществляется посредством бита Confidential Qualifier. Для защиты страниц памяти конфиденциальных виртуальных машин вводится специальная битовая таблица Memory Tracking Table (MTT), содержащая информацию о защищаемых страницах.

Для обеспечения изоляции защищенных виртуальных машин вводится новый программный компонент – Trusted Execution Environment Security Manager (TSM). TSM выполняется в конфиденциальном режиме гипервизора и выступает в роли связующего звена между защищенными виртуальными машинами и гипервизором, выполняющим роль менеджера виртуальных машин. TSM-driver, работающий в режиме Machine, обеспечивает инициализацию системы, переключение между конфиденциальным и стандартным режимами, а также предоставляет интерфейс корня аттестации доверенной вычислительной базы.

Заключение

На текущем этапе развития основными проблемами, препятствующими широкому внедрению концепции конфиденциальных вычислений, являются сложности с повторным использованием существующих технологий безопасности и необходимость проектирования технологий с учетом жизненного цикла защищаемого программного обеспечения. Хотя все решения повторно используют криптографические алгоритмы для реализации механизмов аттестации, текущие реализации основаны на внедрении многих новых аппаратных компонентов безопасности. Новые компоненты требуют большого уровня доверия и изменений в системном программном обеспечении для управления жизненным циклом защищаемых объектов. Еще предстоит сформулировать терминологию для более точного описания набора уже существующих технологий конфиденциальных вычислений, а также связать эти технологии с развивающимися многосторонними вычислениями и гомоморфным шифрованием.

Несмотря на описанные проблемы технологии конфиденциальных вычислений активно развиваются и уже сейчас переходят от нишевого решения к массовому. Об этом свидетельствует повышенный интерес со стороны производителей процессоров, а также рост числа предложений размещения защищенных виртуальных машин у поставщиков облачных услуг, что позволяет повысить эффективность вычислений посредством интеграции технологий в распределенные вычислительные системы уже сейчас.

Литература

1. Аракелов Г. Г. Вопросы применения прикладной гомоморфной криптографии //Вопросы кибербезопасности. – 2019. – №. 5 (33). – С. 70-74.
2. Хлюпин А. А., Саакян А. О., Ниссенбаум О. В. Анализ эффективности алгоритмов шифрования для безопасных многосторонних вычислений //Математическое и информационное моделирование. – 2023. – С. 315-324.
3. Mutlu O., Kim J. S. Rowhammer: A retrospective //IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2019. – Т. 39. – №. 8. – С. 1555-1571.
4. Acosta G. The Role of Vmtheft and Hyperjacking in Virtualization: dissertation – Utica College, 2018.
5. Gross M. et al. Breaking trustzone memory isolation through malicious hardware on a modern fpga-soc //Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop. – 2019. – С. 3-12.
6. Markettos A. T. et al. Thunderclap: Exploring vulnerabilities in operating system IOMMU protection via DMA from untrustworthy peripherals. – 2019.
7. Won Y. S. et al. Practical cold boot attack on iot device-case study on raspberry pi //2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA). – IEEE, 2020. – С. 1-4.
8. Zimerman I., Nachmani E., Wolf L. Recovering AES Keys with a Deep Cold Boot Attack //International Conference on Machine Learning. – PMLR, 2021. – С. 12955-12966.
9. Sardar M. U., Fetzer C. Confidential computing and related technologies: a critical review //Cybersecurity. – 2023. – Т. 6. – №. 1. – С. 1-7.
10. Vaswani K. et al. Confidential machine learning within graphcore ipus //arXiv preprint arXiv:2205.09005. – 2022.
11. Cheng P. C. et al. Intel TDX Demystified: A Top-Down Approach //arXiv preprint arXiv:2303.15540. – 2023.
12. Li X. et al. Design and verification of the arm confidential compute architecture //16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22). – 2022. – С. 465-484.
13. Bornträger C. et al. Secure your cloud workloads with IBM Secure Execution for Linux on IBM z15 and LinuxONE III //IBM Journal of Research and Development. – 2020. – Т. 64. – №. 5/6. – С. 2: 1-2: 11.
14. Hunt G. D. H. et al. Confidential computing for OpenPOWER //Proceedings of the Sixteenth European Conference on Computer Systems. – 2021. – С. 294-310.
15. Sahita R. et al. CoVE: Towards Confidential Computing on RISC-V Platforms //Proceedings of the 20th ACM International Conference on Computing Frontiers. – 2023. – С. 315-321.

IMPLEMENTATION ANALYSIS OF CONFIDENTIAL COMPUTING TECHNOLOGIES

Zagartdinov B.N.[8], Polyakov M.V.[9]

Purpose: *analysis of the current state of confidential computing technologies.*

Methods: *systematization and analysis of existing and developing solutions implementing confidential computing.*

Result: *The article evaluates threat models of confidential computing hardware technologies, such as Intel TDX, AMD SEV or ARM CCA, and analyzes their implementation. Their common features are revealed and the features of each of the implementations are considered. The main problems faced by developers of such systems are revealed: difficulties with the reuse of existing security technologies and the need to design technologies taking into account the life cycle of the protected software. Each implementation uses different methods to solve these problems. The main advantage of using confidential computing technologies is the processing of data in protected containers, thereby ensuring the confidentiality and integrity of sensitive information. Therefore, solutions of this type can be considered for implementation at the design stage of the architecture of computing systems in the future, allowing them to increase their performance by increasing the efficiency of using computing resources without compromising confidentiality.*

Novelty: *lies in analysis and systematization of solutions implementing the hardware environment of confidential computing. The main features characterizing modern systems of confidential computing, as well as problems arising in the process of developing such systems, are revealed. Significant advances in this area will increase the efficiency of computing by sharing computing resources without compromising privacy.*

Keywords: *cloud computing security, hardware trusted execution environment, remote attestation, security of data, information security.*

References

1. Arakelov G.G. Voprosy primeneniya prikladnoj gomomorfnoj kriptografii // Voprosy kiberbezopasnosti [Cybersecurity issues]. – 2019. – № 5(33). – pp. 70-74.
2. Khlyupin A. A., Saakyan A. O., Nissenbaum O. V. Analiz effektivnosti algoritmov shifrovaniya dlya bezopasnyh mnogostoronnih vychislenij // Matematicheskoe i informacionnoe modelirovanie [Mathematical and information modeling]. – 2023. – pp. 315-324.
3. Mutlu O., Kim J. S. Rowhammer: A retrospective // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2019. – T. 39. – №. 8. – C. 1555-1571.
4. Acosta G. The Role of Vmtheft and Hyperjacking in Virtualization: dissertation – Utica College, 2018.
5. Gross M. et al. Breaking trustzone memory isolation through malicious hardware on a modern fpga-soc //Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop. – 2019. – C. 3-12.
6. Markettos A. T. et al. Thunderclap: Exploring vulnerabilities in operating system IOMMU protection via DMA from untrustworthy peripherals. – 2019.
7. Won Y. S. et al. Practical cold boot attack on iot device-case study on raspberry pi //2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA). – IEEE, 2020. – C. 1-4.
8. Zimerman I., Nachmani E., Wolf L. Recovering AES Keys with a Deep Cold Boot Attack //International Conference on Machine Learning. – PMLR, 2021. – C. 12955-12966.
9. Sardar M. U., Fetzer C. Confidential computing and related technologies: a critical review //Cybersecurity. – 2023. – T. 6. – №. 1. – C. 1-7.
10. Vaswani K. et al. Confidential machine learning within graphcore ipus //arXiv preprint arXiv:2205.09005. – 2022.
11. Cheng P. C. et al. Intel TDX Demystified: A Top-Down Approach //arXiv preprint arXiv:2303.15540. – 2023.
12. Li X. et al. Design and verification of the arm confidential compute architecture //16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22). – 2022. – C. 465-484.
13. Bornträger C. et al. Secure your cloud workloads with IBM Secure Execution for Linux on IBM z15 and LinuxONE III //IBM Journal of Research and Development. – 2020. – T. 64. – №. 5/6. – C. 2: 1-2: 11.
14. Hunt G. D. H. et al. Confidential computing for OpenPOWER //Proceedings of the Sixteenth European Conference on Computer Systems. – 2021. – C. 294-310.
15. Sahita R. et al. CoVE: Towards Confidential Computing on RISC-V Platforms //Proceedings of the 20th ACM International Conference on Computing Frontiers. – 2023. – C. 315-321.

8 Bulat N. Zagartdinov, master's student at NRNU MEPhI, specialist of STC Vulkan, Moscow, Russia. E-mail: me@vaire.lt

9 Mikhail V. Polyakov, Senior Lecturer at BMSTU, Moscow, Russia. E-mail: m.polyakov@bmstu.ru