Управление рисками и безопасностью

Подход к обеспечению безопасности промышленных систем управления

Г.П. Акимова, А.Ю. Даниленко, Е.В. Пашкина, М.А. Пашкин, А.А. Подрабинович, И.В. Туманова

Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия

Аннотация. В статье рассмотрены особенности обеспечения информационной безопасности на промышленном предприятии. Предложен способ сегментации вычислительных ресурсов и алгоритмы управления доступом в различных сегментах: корпоративном, инженерно-конструкторском и технологическом.

Ключевые слова: *информационная безопасность, APT-атаки, АСУТП, САПР, управление доступом.*
DOI: 10.14357/20790279210101

Введение

Современная цифровизация всех сфер жизни общества, в том числе большинства отраслей экономики и государственного управления, ведет к серьезному увеличению как количества, так и уровня серьезности компьютерных инцидентов. Хакерские атаки принимают характер не столько попыток вывода из строя информационных систем или отдельных компьютеров, сколько целенаправленного вмешательства в деятельность предприятий и организаций. Если до последнего времени объектами таких атак становились, по большей части, банковские системы с целью хищения денежных средств, сайты СМИ для размещения дезинформации и их компрометации, а также государственные информационные ресурсы, то сейчас наблюдается серьезный рост атак на промышленные предприятия. Основными целями при этом могут быть приостановка или существенное затруднение работы конкурентов, промышленный шпионаж, а также вмешательство в технологические процессы с целью нарушения их хода вплоть до организации техногенных катастроф.

По оценке [1] сложным целенаправленным атакам (атаки типа advanced persistent threat, APT-атаки) подвергаются практически все отрасли народного хозяйства. Так, под прицелом тринадцати рассмотренных авторами [1] APT-группировок оказались в 68% случаев государственные учреждения, в 59% случаев – промышленные предприятия, а также финансовая отрасль и топливно-энергетический комплекс (соответственно 45 и 41% случаев).

В [2] отмечается, что с начала 2020 года количество атак на промышленность держится на высоком уровне. По числу инцидентов эта отрасль занимает второе место. В основном атаки проводились APT-группировками и операторами шифровальщиков (доля атак с использованием шифровальщиков составила 45%). Был зафиксирован очередной всплеск атак на медицинские учреждения. Половину всех инцидентов составляют

атаки шифровальщиков, которые спекулируют данными пациентов, лишают больницы возможности работать, отрезая доступ к информационным системам, листам назначений и осмотров. Атакам подвергаются также исследовательские центры, которые занимаются разработкой вакцины от коронавируса.

В [3] отмечено, что «В России в течение второго полугодия 2018 года хотя бы один раз вредоносные объекты были задетектированы на 45.3% компьютеров АСУ». Далее отмечается, что Россия в рейтинге пострадавших от APT-атак занимает 16 место по этому показателю, наиболее неблагоприятная ситуация складывается во Вьетнаме (70.1%), Алжире (69.9%) и Тунисе (64.6%). Наиболее благополучно дело обстоит в Ирландии (11.7%), Швейцарии (14.9%) и Дании (15.2%).

В [4] проанализировано, какие вызовы уже стоят или вскоре будут стоять перед промышленными предприятиями и чего ожидать от киберпреступников в 2021 году. Отмечены опасности случайных заражений, атак вымогателей, кибершпионажа, APT-атак и ряд других угроз.

В [1] рассмотрены основные цели и последствия атак APT-группировок. В качестве целей выделены нарушение технологического процесса, остановка деловых процессов и вывод из строя инфраструктуры, кража конфиденциальной информации, удар по репутации, кража денег. При этом последствия атак распределены по степени серьезности следующим образом: утечка информации, уничтожение или подмена данных, простои инфраструктуры, нарушение технологического процесса, репутационный ущерб.

Приведенные данные показывают, что задача обеспечения информационной безопасности (ИБ) промышленных предприятий весьма актуальна. Особое значение ей придает сложившаяся ситуация в этой области, описанная в [5], причем авторы отмечают, что основными проблемами, выявляемыми в процессе проведения аудита ИБ на промышленных предприятиях, являются:

1. отсутствие политики информационной безопасности, в которой описаны цели, план аудита и назначен специалист, ответственный за него;
2. отсутствие поддержки и понимания высшего руководства компании в вопросах информационной безопасности и, в частности, аудита;
3. руководители головных предприятий не всегда готовы передавать филиалам документы, относящиеся к защите информации;
4. отсутствие на предприятии специалиста по информационной безопасности. В большинстве организаций его задачи выполняются системными администраторами или специалистами других направлений, не осознающими специфики работы, рисков, и возможного ущерба.

В [1] приведены краткие описания основных каналов, используемых для атак на промышленные объекты. Большинство группировок (до 85%) пытаются доставить вредоносное программное обеспечение (ПО) с помощью фишинга, то есть путем рассылки электронных писем, цель которых — вынудить получателя открыть приложенный файл или перейти по ссылке.

Около 31% APT-групп, атакующих промышленные компании, используют технику drive-by compromise. В ходе такой атаки на компьютер сотрудника во время просмотра зараженного сайта незаметно загружается вредоносное ПО. Чтобы повысить вероятность успеха, злоумышленники стремятся заразить вредоносным ПО именно те сайты, которые часто посещают сотрудники компании-жертвы.

Автоматизация процессов внутри предприятий сопряжена с внедрением специализированного оборудования и программного обеспечения, для которого требуется квалифицированная техническая поддержка. Промышленные компании вынуждены обращаться за ней к подрядчикам, но далеко не все осознают угрозу, которая за этим стоит. Ведь скомпрометировав подрядчика, имеющего удаленный доступ к внутренней сети компании, злоумышленник автоматически получает «пропуск», который позволит ему выполнять действия от имени взломанного поставщика услуг. Такую технику (trusted relationship) используют 15% APT-групп. Другой пример ее возможной реализации – взлом компании-партнера и рассылка фишинговых писем от его имени; это повышает шансы на то, что вредоносное послание откроют. Некоторые группы (15%) доставляют вредоносное ПО в инфраструктуру вместе с поставками оборудования или обновлениями программного обеспечения.

1. Использование механизмов защиты информации

Приведенный анализ показывает важность использования средств защиты информации (СЗИ) в составе применяемого в организации специального и общего программного обеспечения (СПО и ОПО). Только грамотно построенная система обеспечения информационной безопасности может полностью предотвратить или существенно снизить последствия начавшейся атаки злоумышленников. Остано-

вимся кратко на основных категориях СЗИ, применяемых в составе обеих категорий ПО:

- *Идентификация и аутентификация* служат для идентификации пользователя и подтверждения его подлинности, которые требуются для предоставления ему полномочий в системе.
- *Управление доступом* позволяет разграничить действия пользователя в системе в соответствии с предоставленными ему полномочиями. Различают управление доступом по дискреционному и ролевому алгоритмам. В первом случае доступ к действиям предоставляется в соответствии с так называемой матрицей доступа, в которой указаны разрешенные действия со всеми информационными объектами для каждого пользователя системы. Обычно в базе данных хранятся списки разрешенных и запрещенных действий для каждого объекта. В случае ролевого алгоритма список разрешенных действий указывается не для конкретного пользователя, а для роли, на которую могут они назначаться.
- *Протоколирование (аудит)* для ведения протоколов безопасности, в которые входят записи об операциях с базой данных пользователей, операциях с объектами защиты, о начале и завершении сеанса работы с системой.
- *Контроль целостности ПО* в первую очередь требуется для исключения злонамеренного вмешательства в работу СПО, ОПО и СЗИ.
- *Управление установкой ПО* обеспечивает установку исключительно доверенного ПО и исключение установки неразрешенных к использованию программ. Позволяет существенно усложнить или полностью исключить внедрение зловредных приложений.
- *Контроль целостности данных* требуется для исключения случайного или злонамеренного искажения обрабатываемой информации.
- *Шифрование сетевого трафика* внутри предприятия может использоваться для защиты передаваемой по сети информации от внутреннего нарушителя, а в случае внешнего – обмена данными от перехвата и манипулирования злоумышленниками вне организации.
- *Блокировки и оповещения* дают возможность административному персоналу оперативно реагировать на нарушения режима ИБ.
- *Электронная подпись* позволяет обеспечить подтверждение авторства и целостность передаваемых и хранимых данных. В ряде случаев может обеспечивать юридическую значимость электронных документов.
- *Антивирусная защита* требуется для защиты от вредоносного ПО: вирусов, червей, троянских программ.

Необходимо отметить, что большинство перечисленных СЗИ, работают со своими объектами защиты. Например, СЗИ в составе операционной системы (ОС) обеспечивают безопасность файлов, каталогов, ключей реестра и т.д., а средства защиты в составе базы данных – таблиц и записей. Аналогично СЗИ должны присутствовать в составе СПО для обеспечения безопасности специфических информационных объектов, которые могут представляться в базе данных большим числом записей. В частности, для почтовой системы это письма, содержимое почтовых ящиков, адресные книги и.т.д.

2. Вычислительные ресурсы предприятия

Для формализации предложений по организации ИБ предприятия предлагается ввести понятие сегмента локальной вычислительной сети (ЛВС), условно разделив все компьютеры, серверы, коммутаторы и другое оборудование на корпоративный, инженерно-конструкторский и технологический сегменты, которые отличаются как по решаемым задачам, так и по требованиям по обеспечению режима ИБ.

Корпоративный сегмент обслуживает повседневную деятельность предприятия, не связанную с основными производственными процессами. В него входят секретариат, бухгалтерия, отдел кадров, отделы материально-технического снабжения и другие. Этот сегмент также обеспечивает повседневное взаимодействие между подразделениями и сотрудниками в рамках электронного документооборота. Корпоративный сегмент должен иметь выход в Интернет и другие внешние сети, без этого его работа окажется либо сильно затрудненной, либо невозможной.

Для корпоративного сегмента характерно большое количество пользователей (все сотрудники), разнообразие решаемых задач, большое число программ, установленных на компьютерах, широкое использование автоматизированных информационных систем (АИС) различного назначения (кадровых, бухгалтерских и т.д.).

Инженерно-конструкторский сегмент объединяет вычислительные ресурсы, АИС и системы автоматизации проектирования (САПР), применяемые в проектировании и конструкторской проработке продукции, изготавливаемой предприятием. В норме он должен быть полностью отделен от корпоративного сегмента и не иметь выхода во внешние сети, чтобы исключить возможность промышленного шпионажа, а также проникновение зловредных

программ из внешних сетей. Однако это требование практически никогда не выполняется, за исключением ограниченного круга предприятий, работающих в сфере производства военной техники.

Под технологическим сегментом будем понимать автоматизированные системы управления технологическими процессами (АСУТП), работающие на предприятии. Доступ именно в эту часть корпоративных ресурсов позволяет злоумышленникам из APT-группировок вмешиваться в технологические процессы, в том числе организовывать техногенные катастрофы. Этот сегмент обязательно должен быть отделен от всех остальных сегментов, как корпоративного, так и инженерно-конструкторского, и ни в коем случае не иметь соединения с внешними сетями. В этой части должны соблюдаться самые строгие требования по соблюдению режима ИБ, потому что в большинстве случаев АСУТП, работающие в технологическом сегменте, относятся к значимым объектам критической информационной инфраструктуры.

3. Управление доступом

Это средство защиты позволяет обеспечить разграничение доступа пользователей к информационным объектам и действиям в АИС или АСУТП. Все алгоритмы этой категории основаны на информации о пользователях, точнее их учетных записях, содержащейся в отдельной базе данных (БД), в качестве которой может использоваться как общесистемная БД, например, Active Directory в случае домена Windows, так и собственная БД пользователей системы. В БД пользователей должна содержаться информация о системных именах, паролях пользователей, их членстве в группах, а также о привилегиях конкретных учетных записей. В качестве примера привилегий можно привести право на настройку АИС или АСУТП, предоставляемое администраторам и сотрудникам отделов, отвечающих за обеспечение работоспособности оборудования, а также право на чтение и редактирование документов, создаваемых подчиненными сотрудниками, предоставляемое руководителям и делопроизводителям. Именно средства разграничения доступа при их правильной настройке и корректной работе могут свести к минимуму возможность реализации описанных выше атак на инфраструктуру предприятия.

Настройка базы данных пользователей имеет особое значение для подсистем управления доступом. В этой БД, помимо указанной выше информации, содержатся данные о группах пользователей и их ролях. Эта информация используется при работе подсистемы управления доступом по дискреционному и ролевому алгоритмам. Именно правильное формирование списка ролей и набора групп пользователей обеспечивают точный учет деловой логики организации и, в конечном итоге, точное соответствие действий пользователей их реальным полномочиям.

При этом БД пользователей в корпоративном сегменте обычно представляет собой копию структуры предприятия со всеми подразделениями, их руководителями и сотрудниками. В этом случае не возникает особых сложностей с объединением сотрудников в группы и назначением прав на информационные объекты, поскольку каждое подразделение решает свои специфические задачи, а обмен данными между ними (внутренний документооборот) достаточно хорошо регламентирован и понятен всем сотрудникам, задействованным в нем.

Совершенно иная ситуация складывается в инженерно-конструкторском и технологическом сегментах. Для инженерно-конструкторского сегмента авторам наиболее логичным представляется формирование пользовательских групп не по формальным подразделениям, а по общности решаемых задач. В этом случае наиболее естественным будет объединить в группу сотрудников, работающих над одним проектом, разрабатывающих одно изделие, вне зависимости от их формальной подчиненности. При этом доступ к разрабатываемой документации должен определяться в точном соответствии с должностными обязанностями и характером выполняемой работы. Так, к конструкторской документации должны иметь доступ как конструкторы, так и технологи, при этом конструкторы имеют доступ, позволяющий модифицировать данные, а технологи только их читать. Аналогичное распределение прав может быть реализовано для случая технологической документации, модифицировать которую могут сотрудники технологических отделов, а читать также и конструкторы изделия.

Характерной особенностью технологического сегмента можно считать малое количество допущенных в него пользователей, поскольку этот круг ограничен следующими категориями сотрудников: операторы, непосредственно управляющие технологическим процессом и отслеживающие его параметры; руководители, контролирующие работу операторов; наладчики оборудования, которые получают доступ к системе только при проведении регламентных или ремонтных работ; системные администраторы, выполняющие настройку АСУТП и ее обслуживание, в том числе ведение баз данных, резервное копирование, установку об-

новлений ОПО, СПО, антивирусных средств. Также желательно сегментировать технологический сегмент, не допуская возможности вмешаться в работу установки сотрудников, работающих с другим оборудованием. Это может быть реализовано на уровне подсистемы управления доступом, но наиболее логичное и радикальное решение – физическое разделение участков сети.

Для технологического сегмента предлагаются следующие правила разграничения доступа в зависимости от состояния обслуживаемого оборудования:

– операторы считывают показания приборов, включают и отключают оборудование, дают команды на изменение параметров технологических процессов;
– руководители имеют право только на чтение всех данных, доступных операторам, а также протоколов работы систем;
– наладчики могут работать только тогда, когда оборудование выключено или переведено в сервисный режим;
– системные администраторы, одновременно исполняющие обязанности администраторов безопасности, получают доступ к АСУТП только при выключенном оборудовании. В случае непрерывных производственных процессов необходимо задействовать на время обновления ПО резервные компьютеры.

4. Управление информационными потоками

В промышленных системах управления можно выделить несколько информационных потоков, которые могут быть использованы для APT-атак на предприятие. В первую очередь необходимо рассмотреть потоки информации, поступающей в корпоративный сегмент вычислительной сети. Это входящая корреспонденция, электронные письма, данные, проступающие из сети Интернет. Относительно этого потока можно констатировать, что правила обращения с данными не отличаются от правил, применяемых во всех организациях и их АИС. Эти правила работы широко описаны в литературе, например, в [6]. Основными принципами в этой части являются: персонификация всех данных в АИС, в том числе отправляемой и получаемой информации, получение деловой корреспонденции выделенными сотрудниками или подразделениями (секретариатами), предоставление доступа к этим данным в соответствии с должностными обязанностями сотрудников по распоряжению руководителей организации и подразделений.

В случае инженерно-конструкторского и технологического сегментов такие потоки информации практически отсутствуют, единственным исключением может быть получение фрагментов конструкторской или технологической документации от смежных предприятий. В этом случае перед вводом полученных данных в АИС или САПР необходимо удостовериться, что они получены из надежного источника, а также выполнить проверку с помощью антивирусных средств.

Основным внешним информационным потоком для инженерно-конструкторского и технологического сегментов сети следует признать обновления ОПО и СПО, а также ввод настроек технологического оборудования. Для контроля обновлений может применяться цифровая подпись, которой разработчики подписывают формируемые пакеты данных. Этот механизм обеспечивает как персонификацию получаемых пакетов обновлений, так и их неизменность. Что касается изменения настроек, то это действие должно выполняться исключительно специалистами, квалификация которых позволяет проверить корректность вводимых данных. Как отмечалось выше, получение информации от внешних подрядчиков, занятых поддержкой оборудования и СПО, в том числе ввод обновлений может рассматриваться как один из перспективных каналов APT-атак, противодействие которым является важнейшей задачей. Заметим, что предоставление сотрудникам внешних организаций непосредственного доступа в инженерно-конструкторский и технологический сегменты (например, с помощью удаленного рабочего стола) должно рассматриваться как грубейшее нарушение режима ИБ.

Заключение

Широкое внедрение цифровых технологий во все отрасли народного хозяйства, образование, государственное управление, которое часто называют их цифровизацией, невозможно без надежного обеспечения безопасности обрабатываемой информации, причем системы безопасности должны быть максимально гибкими для учета особенностей деловой логики автоматизируемых предприятий и организаций. В связи с этим алгоритмы работы таких систем постоянно совершенствуются, это относится и к подсистемам управления доступом пользователей к информационным объектам. Вместе с тем наблюдается устойчивый рост попыток вмешательства хакерских группировок в работу различных организаций, в том числе промышленных предприятий.

Предлагаемые в настоящей работе алгоритмы управления доступом пользователей к информа-

ционным объектам, потокам информации и действиям в АИС, АСУТП и САПР на промышленных предприятиях позволят существенно снизить ущерб от компьютерных атак, направленных на дезорганизацию работы и злонамеренное вмешательство в технологические процессы.

Литература

1. *APT-атаки на промышленные компании* в России. Обзор тактик и техник 2019. ptsecurity.com. https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-industry-2019.
2. *Актуальные киберугрозы:* III квартал 2020 года. ptsecurity.com. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3.
3. *Ландшафт угроз* для систем промышленной автоматизации. Второе полугодие 2018. https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/.
4. *Киберугрозы* для промышленных предприятий в 2021 году. https://ics-cert.kaspersky.ru/reports/2020/12/02/ics-threat-predictions-for-2021/.
5. *Баранкова И.И., Михайлова У.В., Быкова Т.В.* Сложности, возникающие при проведении аудита информационной безопасности на предприятии**.** Вестник УрФО. 2019. № 1(31). С. 53–56.
6. *Даниленко А.Ю.* Безопасность систем электронного документооборота: Технология защиты электронных документов. 2020. №13. 240 с.

Акимова Галина Павловна. Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия. Ведущий научный сотрудник. Кандидат технических наук. Количество печатных работ: более 70. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Даниленко Андрей Юрьевич. Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия. Ведущий научный сотрудник. Кандидат физико-математических наук. Количество печатных работ: более 40 (в т.ч. 1 монография). Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных. E-mail: danilenko@isa.ru. (Ответственный за переписку, адрес на время самоизоляции andrey955@mail.ru)

Пашкина Елена Владимировна. Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия. Ведущий программист. Количество печатных работ: более 15. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: pashkina@isa.ru

Пашкин Матвей Александрович. Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия. Научный сотрудник. Количество печатных работ: более 20. Область научных интересов: системное программирование, информационные технологии, информационно-аналитические системы, электронный архив. E-mail: pashkin@isa.ru

Подрабинович Андрей Александрович. Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия. Ведущий программист. Количество печатных работ: более 10. Область научных интересов: системное программирование, проектирование и создание методов и программных средств управления электронными документами, защита информации в документооборотных системах. E-mail: podrabinovich@isa.ru

Туманова Ирина Владимировна. Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия. Ведущий программист. Количество печатных работ: более 10. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: tumanova-irin@mail.ru

An approach to securing industrial control systems

G.P. Akimova, A.Yu. Danilenko, E.V. Pashkina, M.A. Pashkin A.A. Podrabinovich, I.V. Tumanova
Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia

Abstract. The article discusses the features of ensuring information security at an industrial enterprise. A method for segmentation of computing resources and algorithms for access control in various segments: corporate, engineering and technological, are proposed.

Keywords: *information security, APT attacks, APCS, CAD, access control.*
DOI: 10.14357/20790279210101

References

1. *APT-ataki na promyshlennyye* kompanii v Rossii. Obzor taktik i tekhnik 2019. [APT attacks on industrial companies in Russia. Review of tactics and techniques 2019]. ptsecurity.com. https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-industry-2019/.
2. *Aktual'nyye kiberugrozy:* III kvartal 2020 goda [Current Cyber Threats: Q3 2020]. ptsecurity.com. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3.
3. *Landshaft ugroz* dlya sistem promyshlennoy avtomatizatsii. Vtoroye polugodiye 2018. [Threat landscape for industrial automation systems. Second half of 2018]. https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/.
4. *Kiberugrozy* dlya promyshlennykh predpriyatiy v 2021 godu. [Cyber Threats to Industrial Enterprises in 2021]. https://ics-cert.kaspersky.ru/reports/2020/12/02/ics-threat-predictions-for-2021/.
5. *Barankova I.I., Mikhaylova U.V., Bykova T.V.* 2019. Slozhnosti, voznikayushchiye pri provedenii audita informatsionnoy bezopasnosti na predpriyatii. [Difficulties arising during the audit of information security at the enterprise. Ural Federal District Bulletin]. Vestnik UrFO. [Ural Federal District Bulletin]. 1: 53-56. DOI: 10.14529/secur190108.
6. *Danilenko A.Yu.* 2020. Bezopasnost' sistem elektronnogo dokumentooborota: Tekhnologiya zashchity elektronnykh dokumentov. Izd. 2-ye, dopolnennoye. [Security of electronic document management systems: Technology for the protection of electronic documents. Ed. 2nd, supplemented]. Moscow: LENAND. 240 p. ISBN 978-5-9710-6788-7.

Akimova G.P. PhD, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: akimova@isa.ru

Danilenko A.Yu. PhD, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: danilenko@isa.ru

Pashkina E.V. Lead programmer. Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: pashkina@isa.ru

Pashkin M.A. Researcher. Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: pashkin@isa.ru

Podrabinovich A.A. Lead programmer. Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: podrabinovich@isa.ru

Tumanova I.V. Lead programmer. Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: tumanova-irin@mail.ru